

SIEMENS

SIMATIC NET

TeleControl Configuration - IEC 60870-5

Configuration Manual

Preface

Functions and requirements **1**

Communication mechanisms **2**

Configuration **3**

Commissioning **4**

Diagnostics and maintenance **5**

OUC program blocks (CP) **A**

SINEMA Remote Connect (CP) **B**

WBM of the TIM 1531 IRC **C**

Security **D**

Bibliography **E**

Configuration and diagnostics


02/2023


C79000-G8976-C509-04


Legal information

Warning notice system

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

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

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

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

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


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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Preface

Validity of this manual

This configuration manual is valid for the following SIMATIC NET communications modules that support the IEC 60870-5 protocol:

- CP 1243-1
- CP 1243-7 LTE
- CP 1243-8 IRC
- CP 1542SP-1 IRC
- TIM 1531 IRC

You will find the device versions and the required configuration software products in the section Communications modules (Page 11).

Abbreviations/device names

The following abbreviations/acronyms are frequently used in this manual:

- **Module / device / CP / TIM**

Names for the respective communications module

- **Mobile wireless CP**

CP 1243-7 LTE

- **STEP 7**

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

- **WBM**

"WBM" is the acronym for the "Web Based Management", the pages of the TIM Web server for configuration and diagnostics data.

New in this edition

- TIM 1531 IRC V2.3 and CP 1542SP-1 IRC V2.2

New firmware versions with the following new functions:

- TLS extension for the protocol DNP3
- TLS extension for the protocol IEC 60870-5-104
- Secure authentication for the protocol IEC 60870-5-101/104

- New configuration software

STEP 7 Professional V18 with the following functions relevant for the products:

- Configurability of the functions specified above
- Changed handling of certificates

Replaced manual edition

Edition 05/2021

Structure of the documentation

The documentation for the SIMATIC NET telecontrol communications modules consists of the following manuals in each case:

- Operating instructions or product manual
- Configuration manuals (1 configuration manual for each telecontrol protocol)

You can find the Internet links for the manuals in the Bibliography (Page 219).

For modules that support the IEC 60870-5 protocol, the documentation consists of the following documents:

CP modules

- **Operating instructions**

Valid for the respective CP

- Application, functions, requirements (CPUs, software etc.)
- Hardware description
- Installation, wiring, commissioning, operation
- Configuration (only telecontrol-independent functions)

If you use telecontrol functions, read the respective configuration manual.

- Diagnostics, maintenance
- Technical specifications, approvals, accessories

- **Configuration Manual IEC 60870-5**

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

TIM 1531 IRC

- **Manual**

- Application and functions
- Requirements (CPUs, configuration software, etc.)
- Hardware description
- Installation, wiring, commissioning, operation
- Diagnostics, maintenance
- Technical specifications, approvals, accessories

- **Configuration Manual IEC 60870-5**

Configuration and diagnostics in STEP 7 Professional (TIA Portal)

Current manual edition on the Internet

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

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

Required experience

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

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

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>.

License conditions

Note

Open source software

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

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

Security information

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

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

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

For additional information on industrial security measures that may be implemented, please visit

Link: (<http://www.siemens.com/industrialsecurity>)

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under

Link: (<https://www.siemens.com/cert>)

Before configuring and commissioning the modules, learn about their security functions: Functions, performance data and configuration limits (Page 16)

Observe the security recommendations in the "Security" appendix: Security (Page 209)

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

Table of contents

	Preface	3
1	Functions and requirements.....	11
1.1	Communications modules.....	11
1.2	Configuration examples	12
1.3	Usable CPUs.....	15
1.4	Software requirements	15
1.5	Functions, performance data and configuration limits	16
1.5.1	CP 1243-1	16
1.5.2	CP 1243-7 LTE.....	18
1.5.3	CP 1243-8 IRC.....	20
1.5.4	CP 1542SP-1 IRC	21
1.5.5	TIM 1531 IRC	24
2	Communication mechanisms	29
2.1	Communications options	29
2.2	Addressing.....	29
2.3	Connection establishment.....	31
2.4	Acknowledgment.....	31
3	Configuration.....	33
3.1	Communication types.....	33
3.2	Basic settings.....	34
3.3	Time-of-day synchronization	37
3.4	Configuration of interfaces, networks and network nodes	44
3.4.1	WAN settings of the interfaces	44
3.4.2	Networking of the interfaces.....	45
3.5	Ethernet interface	48
3.5.1	Ethernet addresses.....	48
3.5.2	Advanced options	49
3.5.2.1	TCP connection monitoring.....	49
3.5.2.2	Transmission settings.....	50
3.5.3	Web server access	50
3.5.3.1	CP.....	50
3.5.3.2	TIM 1531 IRC	50
3.6	Serial interface.....	51
3.6.1	WAN parameters.....	51
3.6.2	Advanced options	51
3.6.2.1	Dedicated line.....	51
3.6.2.2	Dialup network	53

3.6.2.3	Transmission settings.....	55
3.7	IEC parameters of interfaces.....	55
3.7.1	Transmission settings - IEC 60870-5	55
3.7.2	Settings IEC master	57
3.7.3	Settings IEC station	58
3.8	Configuring WAN networks.....	60
3.9	Web server (TIM 1531 IRC).....	62
3.10	Web diagnostics of the TIM 1531 IRC.....	64
3.11	DNS configuration	64
3.12	Communication with the CPU	65
3.13	E-mail configuration	70
3.14	Subscriber numbers.....	71
3.15	Secure communication between CPU and module.....	73
3.16	Log settings.....	74
3.17	SNMP	75
3.18	Global certificate manager	76
3.19	CP: Security and certificates	77
3.19.1	Security user.....	77
3.19.2	Log settings - Filtering of the system events	77
3.19.3	SYSLOG	77
3.19.4	VPN	78
3.19.4.1	VPN (Virtual Private Network).....	78
3.19.4.2	Creating a VPN tunnel for S7 communication between stations	79
3.19.4.3	VPN communication with SOFTNET Security Client (engineering station)	81
3.19.4.4	Establishment of VPN tunnel communication between the CP and SCALANCE M	81
3.19.4.5	CP as passive subscriber of VPN connections.....	82
3.19.5	Certificate manager	82
3.19.6	Handling certificates	83
3.19.7	Secure communication between CPU and communications module.....	85
3.19.8	CP 1542SP-1 IRC: Certificates for telecontrol connections with TLS.....	86
3.20	TIM 1531 IRC: Protection and certificates.....	86
3.20.1	Protection.....	86
3.20.2	Configuring access protection	88
3.20.3	TIM 1531 IRC: Handling certificates for TLS.....	89
3.21	Telecontrol connections.....	94
3.21.1	Telecontrol connections.....	94
3.21.2	"Network data" editor.....	95
3.21.3	Specifying connection paths	97
3.21.4	Connection table	101
3.21.5	Parameters of IEC connections	104
3.21.5.1	General	104
3.21.5.2	TCP connection monitoring.....	105
3.21.5.3	IEC 60870-5 security options.....	106
3.21.5.4	Security statistics options (IEC 60870-5-104).....	109
3.21.5.5	Query options.....	110

3.21.5.6	Third-party device parameters.....	111
3.22	Data points.....	112
3.22.1	Data point configuration.....	112
3.22.2	Datapoint types.....	119
3.22.3	Status IDs of the data points.....	121
3.22.4	"General" tab.....	122
3.22.5	Master function of the data points.....	123
3.22.6	Data point index.....	124
3.22.7	Process image, type of transmission, event classes.....	126
3.22.8	Read cycle.....	128
3.22.9	"Trigger" tab.....	129
3.22.10	Threshold value trigger.....	131
3.22.11	Analog value preprocessing.....	133
3.22.12	Command options.....	140
3.22.13	Partner stations.....	144
3.23	Messages.....	144
3.24	Character set for user names, passwords and messages.....	150
4	Commissioning.....	151
4.1	Commissioning the CP.....	151
4.2	Set time for operation with Security / SINEMA RC.....	151
5	Diagnostics and maintenance.....	153
5.1	Diagnostics options.....	153
5.2	Web server S7-1200: Connection establishment.....	155
5.3	Online security diagnostics via port 8448.....	156
5.4	Telegram protocol diagnostics.....	157
5.4.1	Message protocol: Structure and functions.....	157
5.4.2	Details.....	158
5.5	SNMP.....	159
5.6	Processing status of the messages (SMS / e-mail).....	160
5.7	Maintenance.....	162
A	OUC program blocks (CP).....	163
A.1	Validity and requirements.....	163
A.2	Program blocks for OUC.....	163
A.3	Changing the IP address during runtime.....	167
A.4	SMS messages via OUC.....	168
A.5	TC_CONFIG for changing configuration data of the CP.....	171
A.6	IF_CONF_*: SDTs for the configuration data of the CP.....	174
B	SINEMA Remote Connect (CP).....	181
B.1	Validity and requirements.....	181
B.2	Connection to SINEMA RC.....	181

B.3	Telecontrol via SINEMA RC	183
B.4	Security > VPN > SINEMA Remote Connect	183
C	WBM of the TIM 1531 IRC	187
C.1	Supported Web browsers	187
C.2	Establishing a connection to the WBM of the TIM	187
C.3	General functions of the WBM.....	188
C.4	Start page.....	189
C.5	System	191
C.5.1	Device info	191
C.5.2	SD card.....	192
C.5.3	System time.....	192
C.5.4	NTP	192
C.5.5	Web server	193
C.5.6	DNS configuration	193
C.6	Maintenance	194
C.6.1	Firmware.....	194
C.6.2	Operating status	195
C.7	Diagnostics.....	196
C.7.1	Events	196
C.7.2	Notifications.....	198
C.8	LAN	198
C.8.1	Ethernet interface [Xn]	198
C.9	Telecontrol	200
C.9.1	Partner information	200
C.9.1.1	Connection overview	200
C.9.1.2	Send buffer.....	204
C.9.2	Data points.....	206
C.10	Logging.....	206
D	Security.....	209
D.1	Security recommendations.....	209
D.2	Syslog messages of the TIM 1531 IRC.....	212
D.2.1	Structure of the Syslog messages	212
D.2.2	Tags in Syslog messages	213
D.2.3	Explanation of the messages.....	215
D.2.4	Messages for TIM 1531 IRC	215
E	Bibliography	219
	Index.....	223

Functions and requirements

1.1 Communications modules

Communications modules for the telecontrol protocol IEC 60870-5

The following SIMATIC NET communications modules can be used for the telecontrol protocol IEC 60870-5.

Meaning of symbols in the table:

- X = Supported
- - = Not supported

Table 1- 1 Communications modules for IEC 60870-5

Module Article number	Number of interfaces *			Station type			STEP 7 product	Required firmware
	IE IEC 60870- 5- 104	RS IEC 60870- 5- 101	M	Master	Node station	Station		
TIM 1531 IRC 6GK7 543-1MX00-0XE0	3	1 **	- ***	X	X	X	STEP 7 Professiona I	V2.3
CP 1542SP-1 IRC 6GK7 542-6VX00-0XE0	1	-	- ***	-	-	X	STEP 7 Professiona I	V2.2
CP 1243-8 IRC 6GK7 243-8RX30-0XE0	1	-	-	-	-	X	STEP 7 Basic **** / Professiona I	V3.3
CP 1243-1 6GK7 243-1BX30-0XE0 6AG1 243-1BX30-2AX0	1	-	-	-	-	X	STEP 7 Basic **** / Professiona I	V3.3
CP 1243-7 LTE 6GK7 243-7KX30-0XE0 6GK7 243-7SX30-0XE0	-	-	1	-	-	X	STEP 7 Basic **** / Professiona I	V3.3

* IE = Ethernet interfaces, RS = serial interfaces, M = integrated mobile wireless interface

** No GSM modules are supported for connection to the serial interface.

*** TIM modules can be connected to mobile wireless networks via modems.

**** STEP 7 Basic with connection of the CP to a third-party master. See note below.

Notes on the table

Notes on the columns:

- **Station type "Node station"**

A node station is located in the plant hierarchy between the master station and other lower-level stations. The module requires at least two interfaces.

In the configuration, the "network node type" of the interface connected to the master station is configured as "Node station". See section Networking of the interfaces (Page 45) for more on this.

- **STEP 7 product with S7-1200 CPs**

S7-1200 CPs can be configured under STEP 7 Basic for connection to a third-party master.

You need STEP 7 Professional project to connect the CPs to SIMATIC NET master or node stations configured in STEP 7.

- **Firmware**

The required firmware versions of the modules relate to the complete configuration described in this manual. You can find the required STEP 7 version for this in the section Software requirements (Page 15).

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

1.2 Configuration examples

Below, you will find several configuration examples with the communications modules that can be used.

Communication via Ethernet / Internet, sending e-mails

In the sample configuration shown, S7 stations communicate with the master station via the Ethernet interfaces of the different modules.

With their Ethernet interfaces, TIM modules enable connection to a redundant master station.

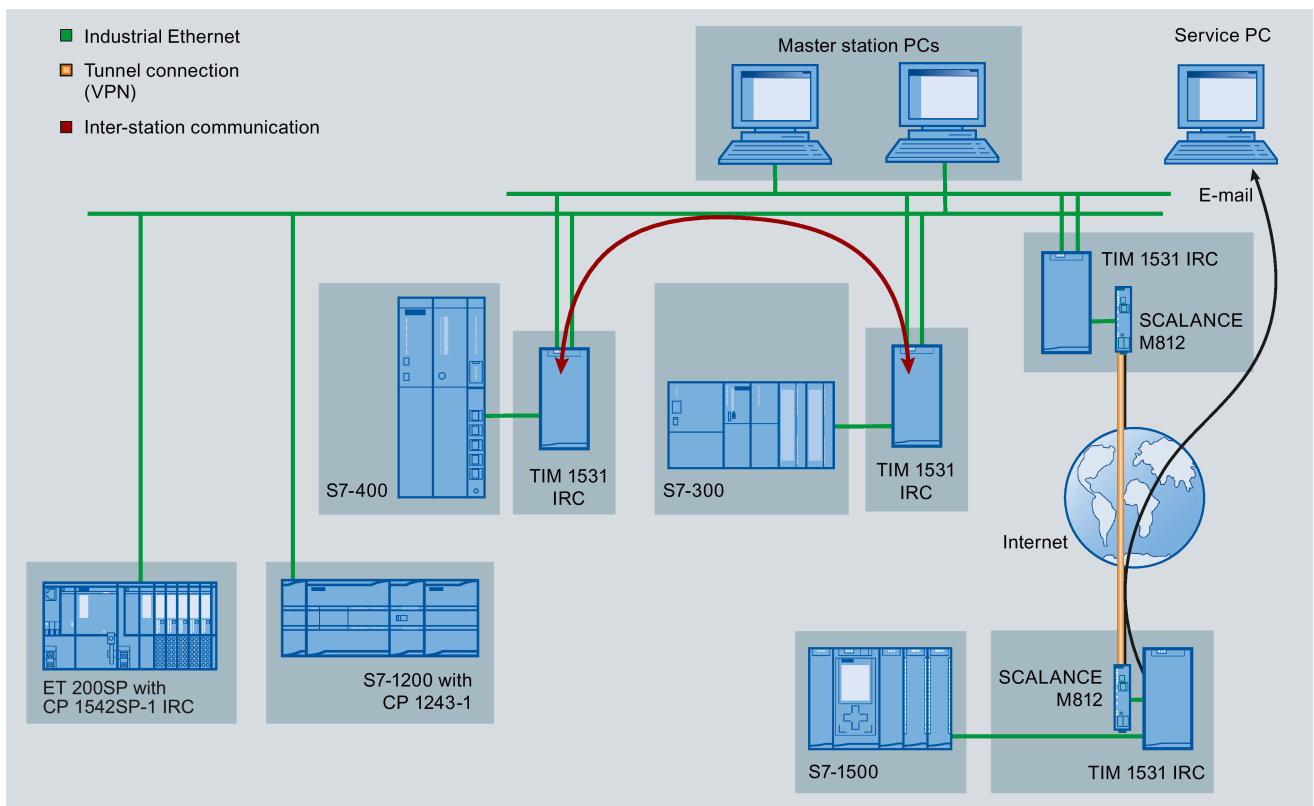


Figure 1-1 Communication via Ethernet / Internet

E-mails

The modules can send e-mails. The following recipients are possible:

- For configured event-driven e-mails:
 - PCs with an Internet connection
 - Cell phones
- For e-mails via OUC blocks:
 - SIMATIC stations with the appropriate program blocks

Direct communication

Direct communication between S7 stations with communications module is possible over IP-based networks. The frames do not run via the master station.

Direct communication can be enabled by the following mechanisms:

- Configured telecontrol connections
For the requirements, see Communications options (Page 29).
- Program blocks of Open User Communication
See OUC program blocks (CP) (Page 163)

Path redundancy using the serial interface

In the following example, the Ethernet interface and the serial interface are used with the TIM 1531 IRC to set up redundant transmission paths.

- Ethernet interface for communication via Ethernet / Internet
- Serial interface for communication via a WAN network (dedicated line or dialup network)

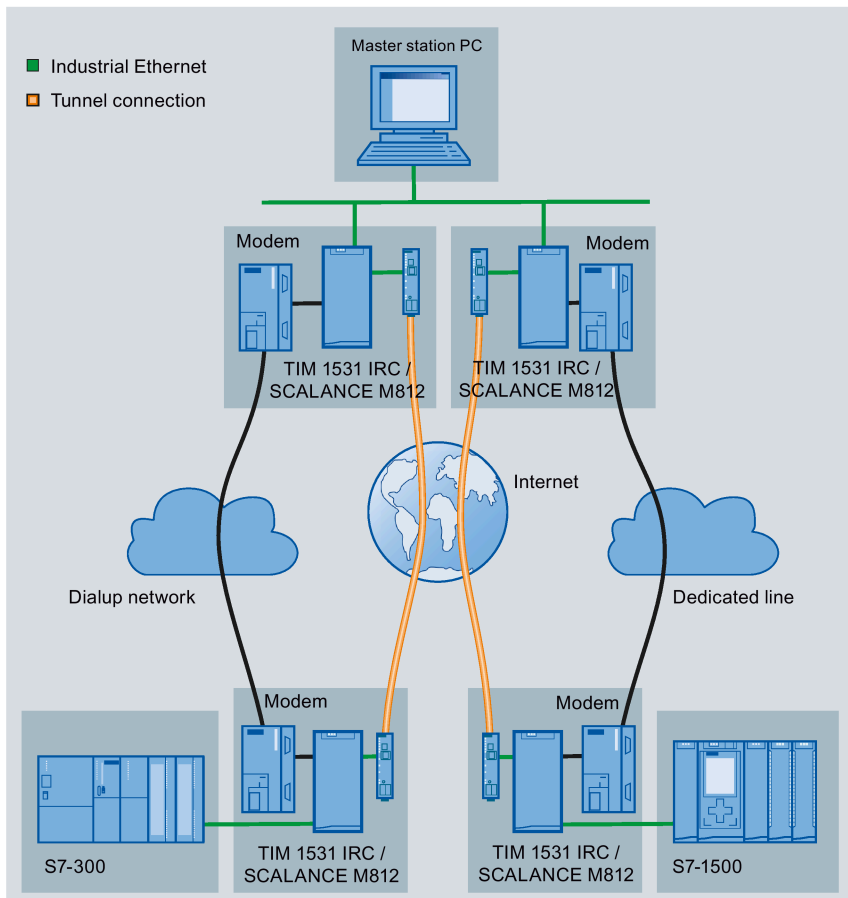


Figure 1-2 Communication via redundant paths

Path redundancy is also possible over two Ethernet networks.

1.3 Usable CPUs

Compatible CPUs

The following can be configured as assigned CPUs of the communications modules:

- **TIM 1531 IRC as of V2.1**

- S7-1500

All standard CPUs as of firmware version V2.1

All redundant CPUs (H-CPU, R-CPU) as of firmware version V2.6

- ET 200SP

As of firmware version V2.1, the TIM 1531 IRC supports connection to:

All CPUs that can be configured in STEP 7 as of firmware version V2.5

- S7-300

All CPUs with PROFINET interface

- S7-400

All CPUs that can be configured in STEP 7

- **CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC**

CPU as of firmware version V4.2

The full functionality of the CP is only available with a CPU as of V4.4.

- **CP 1542SP-1 IRC**

CPUs as of firmware version V2.0:

- CPU 1510SP-1 PN
- CPU 1510SP F-1 PN
- CPU 1512SP-1 PN
- CPU 1512SP F-1 PN

You will find more detailed information on the CPUs and the BusAdapters in the manual *I6I* (Page 220).

1.4 Software requirements

Software for configuration and online functions

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

- STEP 7 Basic / Professional V18

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

1.5 Functions, performance data and configuration limits

1.5.1 CP 1243-1

Number of CMs/CPs per station

In each S7-1200 station, up to three CMs/CPs can be plugged in and configured.

To use telecontrol communication, three CP 1243-1 modules can be plugged in per station.

Connection resources

- **Telecontrol connections inclusive Inter-station communication / Direct communication**

The CP can establish connections to up to 4 communication partners.

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

For information on configuration of direct communication between stations, see section Communications options (Page 29).

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

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

- S7 connections (PUT/GET)
 - Including connections for S7 routing
- Connections via program blocks (OUC) to S7 stations

- **Online functions**

1 connection resource is reserved for online functions.

- **PG/OP connections**

- 1 connection resource for PG connections
- 3 connection resources for OP connections

Number of data points for the data point configuration

Maximum number of configurable data points per CP

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

Frame memory (send buffer)

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

The send buffer is divided equally among all configured communications partners. The size of the frame memory can be set in STEP 7, refer to the section Process image, type of transmission, event classes (Page 126).

The maximum size of the send buffer is:

- TeleControl Basic: 64000 frames
- DNP3: 100000 events
- IEC: 100000 events

Messages (e-mail)

- Sending of up to 10 messages (e-mails) with configuration in the message editor

IPsec tunnel (VPN)

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

Firewall rules

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

The firewall rules are divided up as follows:

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

1.5.2 CP 1243-7 LTE

Connection resources

- **Telecontrol connections**

- DNP3 / IEC

The CP can establish connections to up to 4 communication partners.

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

- TeleControl Basic

1 reserved connection for user data exchange with the telecontrol server

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

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

- Send to partner: Max. 3 ("Send buffer" parameter enabled)
- Receiving from partners: Max. 15 ("Send buffer" parameter disabled)

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

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

- S7 connections (PUT/GET)

Including connections for S7 routing

- Connections via program blocks (OUC) to S7 stations

- **PG/OP connections**

- 1 connection resource for PG connections
- 3 connection resources for OP connections

- **Online functions**

1 connection resource is reserved for online functions.

- **TeleService connections**

- Max. 1 TeleService connection

- **Connections to NTP servers**

Max. 1 connection to an NTP server

User data

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

User data per frame with the various connection types:

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

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

Number of data points for the data point configuration

The maximum number of configurable data points under the telecontrol protocols is:

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

Frame memory (send buffer)

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

The send buffer has the following maximum size:

- TeleControl Basic: 64000 frames
- DNP3: 100000 events
- IEC: 100000 events

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

Messages: E-mail / SMS

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

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

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

IPsec tunnel (VPN)

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

Firewall rules

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

The firewall rules are divided up as follows:

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

1.5.3 CP 1243-8 IRC

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

Number of data points for the data point configuration

Maximum number of configurable data points per CP: 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 events. The size of the frame memory is divided equally among all configured communications partners. It can be set in STEP 7, refer to the section Communication with the CPU (Page 65).

You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Process image, type of transmission, event classes (Page 126).

Messages: E-mail

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

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

IPsec tunnel (VPN)

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

Firewall rules

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

The firewall rules are divided up as follows:

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

1.5.4 CP 1542SP-1 IRC

Number of CPs per station

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

For details of the permitted special modules and the slot rules, refer to the manual.

Connection resources

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

See CP operating instructions /6/ (Page 220)

Also:

- **Telecontrol connections**

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

TeleControl Basic

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

1.5 Functions, performance data and configuration limits

- Additional Inter-station communication

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

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

- Send to partner: Max. 3 ("Send buffer" parameter enabled)
- Receive from partners: Max. 15 ("Send buffer" parameter disabled)

DNP3 / IEC 60870-5

- The CP can establish connections to up to 4 communications partners.
A partner is a single or redundant master or a station (Direct communication).
Communication between stations is configured via the telecontrol connections.

SINAUT ST7

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

- 8 individual connections with partners
- 4 redundant connections with partners
- 8 connections for inter-station communication between ST7 stations
- A combination of the three options

- **Online connections**

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

- **HTTP**

TCP connections for HTTP access: Max. 12

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

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

In total maximum of 16, of which:

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

Messages (e-mail)

- Sending of up to 10 messages (e-mails) can be configured with the message editor.
Maximum number of characters that can be transferred per e-mail: 256 ASCII characters including any value sent at the same time
- Sending e-mails via the TMAIL_C program block

Frame memory (send buffer)

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

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

The maximum size of the send buffer is:

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

Number of data points for the data point configuration

Maximum number of configurable data points per CP:

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

Security functions

The CP supports the following security functions:

- **Encrypted e-mails**

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

- SSL/TLS
- STARTTLS

- **Certificates**

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

- **Secure telecontrol communication**

The telecontrol protocols provide the following Security functions:

- **TeleControl Basic**

As an integrated security function, the telecontrol protocol encrypts the data for transfer between the CP and telecontrol server. The interval for the key exchange between the CP and telecontrol server can be set.

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

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

1.5 Functions, performance data and configuration limits

- **ST7**

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

- MSC

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

- MSCsec

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

- **DNP3**

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

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

- **IEC 60870-5-104**

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

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

For information on communication via SINEMA Remote Connect, see appendix.

1.5.5 TIM 1531 IRC

Connection resources

- **Telecontrol connections**

The number of connections or communications partners is limited for the two interface types and every individual interface.

Note that redundant connection paths of a connection between two partners require two connection resources on each partner.

- Max. number of connections: 128

Distribution over 4 interfaces can take place in any way (max. 128 per interface).

- **E-mail**

A connection to send e-mails can be established during runtime.

- **S7 connections**

- Max. 4 connection resources for PG/OP connections (see below)

- **PG/OP connections**
4 connection resources for connections to the engineering station or HMI devices
(included in the configuration limits of the S7 connections, see above)
- **PG routing**
Max. 4 connections at the same time
- **Online functions**
See PG/OP connections
- **HTTP/HTTPS**
Max. 2 connections per Ethernet interface

Number of data points for the data point configuration

The maximum number of configurable data points is 3000.

Message memory: Send buffer / SD card

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

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

The maximum size of the send buffer is:

- ST7: 250 000 frames
- DNP3/IEC: 100 000 events

You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Process image, type of transmission, event classes (Page 126).

For information on saving events on an optional SD card, see section Basic settings (Page 34).

Messages: E-mail

Up to 10 messages which the TIM can send as e-mails can be configured in STEP 7.

- Number of characters per e-mail

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

Security functions of the transmission protocols

The transmission protocols that can be used for telecontrol communication support the following security functions:

ST7

- **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 a configurable Key exchange interval.

DNP3

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

IEC 60870-5-101 / 104

- The TIM supports the use of the following functions:
 - IEC 60870-5-101 / 104
Secure authentication according to IEC 60870-5-7
 - IEC 60870-5-104
TLS connections

Further security functions of the TIM

The TIM also supports the following security functions:

- **NTP (secure)**

For secure transfer during time-of-day synchronization

- **STARTTLS / SSL/TLS**

For the secure transfer of e-mails

- **HTTPS**

For secure access to the Web server of the TIM

- **SNMPv3**

For secure transmission of network analysis information safe from eavesdropping

Note**Plants with security requirements - recommendation**

Use the following options:

- If you have systems with high security requirements, use the secure protocols, for example HTTPS or SNMPv3.
- If you connect to public networks, you should use security modules with a firewall.

With security modules, individual devices, automation cells or network segments of an Ethernet network can be protected. The following security modules, for example, are suitable for this: SCALANCE S, SCALANCE M800

Formatting the SD card

The SD card of the TIM 1531 IRC must have the following formatting to be able to save configuration data.

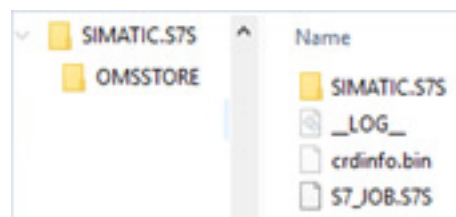


Figure 1-3 Formatting the SD card

You can find information on formatting the SD card in the STEP 7 information system under the search term "Formatting the S7-1500 memory card".

Communication mechanisms

2.1 Communications options

Communication paths

With telecontrol communication, the following paths or connections are possible:

- **Master ⇔ Station connections**
- **Redundant connections**

If two subscribers can be reached via different networks, you can create a maximum of two connections between the subscribers to establish path redundancy.

- **Direct communication (Station ⇔ Station)**

With direct communication, stations communicate directly with each other without the frames being transmitted from a master station. Two stations can thus communicate directly with each other via individual data points.

For information on the configuration, refer to section Master function of the data points (Page 123).

2.2 Addressing

To configure and commission the communications module, the following information is required:

Address information of the communications module

For the addressing, the following parameters must be configured for the module:

- **ASDU address**
Address of the information object (station) on the data link layer
You need the ASDU address to identify the master and the stations in the IEC network.
- **Indexes of the data points (Data point index = Information object address)**
For information on the configuration, see Data point index (Page 124).
- **Address, depending on network type and module type:**
 - IP address and subnet mask; as an alternative: IP address of a DHCP server
If you use DNS, there must be a DNS server (see below) and this must be reachable for the module.
 - Telephone number (for dial-up network)
 - WAN address (for dedicated line)

- Listener port
 - Listener port of the station. The master needs the port number to establish the connection.
 - Listener port of a third-party device with the function "Master"
- DNS server address(es)
 - You need a DNS server if the station sends requests to devices via their FQDN, for example the NTP server.
 - You need a DNS server if the master establishes connections to the stations via their FQDN.

Uniqueness of the addresses

Addressing must be unique within a subnet and within the STEP 7 project.

If you want to use subscriber numbers/station addresses twice in different subnets, you must create two STEP 7 projects.

Uniqueness of the ASDU address

For modules with telecontrol connections that are configured via the "Network data" editor, a consistency check determines the uniqueness of the address.

For CPs with a firmware version $\leq V3.0$ whose telecontrol connections are configured via the "Partner stations" parameter group, the address cannot be checked for uniqueness with a consistency check. You must ensure uniqueness of the address in this case.

Address information of the master

The following information of the master is required for the configuration of the module:

- ASDU address (address of the information object of the master on the data link layer)
- Address of the master, depending on network type:
 - IP address / subnet mask + port number of the listener port of the master
 - or
 - Name resolvable by DNS
(You need the DNS server address, the DNS server must be accessible by the module.)
 - Telephone number (for dial-up network)
 - WAN address (for dedicated line)

Redundant IEC master

The two devices of a redundant master have an identical ASDU address.

They only require different IP addresses or host names.

Configurations with connections over the Internet: VPN connections

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

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

Remember the following points when configuring:

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

2.3 Connection establishment

Connection establishment

The master establishes the connection (call operation / polling). This also applies to stations with data points for which the "Master function" option is enabled.

If an established connection is interrupted, a master module tries to re-establish the connection.

Note**Connection interrupted by the mobile wireless network provider**

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

Connection establishment in Open User Communication and PG/OP communication

In Open User Communication in an S7 station, the CPU is the connection partner.

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

This also applies to the situation when a different S7 station sends data. In this case, the receiver station calls the corresponding receiver modules.

2.4 Acknowledgment

Acknowledgment mechanisms for the protocol IEC 60870-5-104

Configuration: Interface of the module > "Advanced options" > Transmission settings - IEC 60870-5"

2.4 Acknowledgment

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

Upon reception, the master sends the send sequence number from this or (if several data frames are received) the last data frame back to the module as an acknowledgment. The module stores the send sequence number returned by the master as the reception sequence number and uses it as an acknowledgment.

Data frames whose send sequence number is equal to or less than the current receive sequence number are evaluated as successful and deleted from the send buffer of the module.

Parameters:

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

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

If k is reached and t_1 has not yet expired, the module does not send any data frames until all sent data frames have been acknowledged by the master.

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

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

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

For information on the configuration, refer to the section Transmission settings - IEC 60870-5 (Page 55).

Recommendations of the specification:

- w should not be greater than $\frac{2}{3} k$.
- Recommended value for k: 12
- Recommended value for w: 8

Configuration

3.1 Communication types

"Communication types"

In this parameter group, you enable the communication capability of the module.

Depending on the module type, you can define the telecontrol protocol and other communication types.

- **Enable telecontrol communication**

Enables telecontrol communication with the communication partners.

- **Protocol type**

- ST7
- DNP3
- IEC 60870-5

- **Enable 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 remains possible, however.

S7 routing is supported by the following modules:

- CP 1243-1, CP 124x-7, CP 1243-8
As of CP firmware V2.1 with CPU \geq V4.2
- CP 1542SP-1 IRC
As of CP firmware V1.0 with CPU \geq V2.0
- TIM 1531 IRC

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.

- **Enable S7 communication**

Enables the functions of S7 communication with the station CPU and S7 routing in the module.

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

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.

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

Configurable with:

- CP 1243-1
- CP 1243-7 LTE
- CP 1243-8 IRC
- CP 1542SP-1 IRC

For additional details, see appendix SINEMA Remote Connect (CP) (Page 181).

3.2 Basic settings

IEC basic settings

Not all parameters are displayed with every module type.

- **Listener port**

Own listener port of the module. The master needs the port number to establish the connection.

The port number applies to all interfaces of the communications module.

Range of values: 1024...65535

Default: 2404

- **Frame memory size**

Only with TIM 1531 IRC

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

The size of the frame memory is divided equally among all configured communications partners. For information on the size of the frame memory, see "Performance data and configuration limits".

You will find details of how the send buffer works (storing and sending events) as well as the options for transferring data in the section Process image, type of transmission, event classes (Page 126).

- **Max. command lifetime**

Only with TIM 1531 IRC

Maximum age of received commands of type Single/Double command with time tag (<58>/<59>)

If the time stamp is older than the value configured here at the time of receipt, the command is canceled without feedback. The parameter is evaluated by stations and node stations.

Range of values: 1...65

Default: 20

Private ASDUs

Only with TIM 1531 IRC

You specify the TYPE IDENTIFICATION of the respective ASDU type using the configurable value. The 'private range' of 136...254 for type identification is reserved for user-specific applications.

For received private ASDUs, the TIM checks the type identification and evaluates the configured value in each case.

With a configuration of 0 (zero), the TIM does not evaluate type identification.

- **ASDU type for PG routing**

Type identification for ASDUs for transferring S7 frames (PG routing)

Range of values: 136...254

Default: 0

- **ASDU type for status distribution**

Type identification for ASDUs for transferring the path status of the connection

Range of values: 136...254

Default: 0

- **ASDU type for connection termination**

Type identification for ASDUs to announce connection termination with temporary connections

Temporary connections are terminated by the RTU3000C.

Range of values: 136...254

Default: 0

Secure communication options

Validity: TIM 1531 IRC, CP 1542SP-1 IRC

- **Secure listener port**

Own listener port for TLS communication.

The port number applies to all interfaces of the communications module.

Range of values: 1024...65535

Default: 19998

Retentive saving of events

Only with TIM 1531 IRC

If you use an optional SD card in the TIM, in this parameter group you set the conditions for saving the values of frames whose data points are configured as an event.

You set the behavior via the following parameters:

- **Enable retentive saving**

Activates the retentive saving of events on the SD card in the event of connection disruptions.

- **Number of events before saving**

Saving events on the SD card starts when the number of events in the send buffer configured here is reached.

- **Interruption time before saving**

Saving events on the SD card starts when the time of the connection interruption configured here is reached.

- **Max. number of events in the archive file**

Maximum number of events in the stored archive file

When the number is exceeded, the oldest events are overwritten.

For the maximum number of savable events, see section Functions, performance data and configuration limits (Page 16).

IP routing

Only with TIM 1531 IRC

Note

The function is not intended for large data volumes.

Restrict routing via the TIM to approx. 1 Mbit/s so that productive operation of the TIM is not impaired.

IP routing

- **Allow IP routing**

Enables IP routing via the interfaces of the module.

- **Routing method**

Defines the paths for IP routing:

- Local: IP routing only between the Ethernet interfaces of the module
- Via subnets: IP routing via a maximum of 10 configurable routers that can be accessed via the module's interfaces.

Router addresses

- **Ethernet interface**

Ethernet interface of the module via which IP routing is to be configured. The IP addresses of the interfaces used for IP routing need to be permanently configured.

An interface can be selected several times for different routes.

Note**Consistency of the address parameters**

STEP 7 does not check the consistency between manually configured addresses and the parameters of the module's Ethernet interfaces.

Ensure consistency with the address parameters of the respective interface.

- **Address type**

Selection of the IP version of the address parameters configured below (IPv4 / IPv6)

When using IPv6 addresses, you must enable IPv6 for the respective interface.

- **Network address**

Network address of the routing destination (IP address * subnet mask)

- **Subnet mask / Prefix**

Subnet mask (IPv4) or prefix (IPv6) of the routing destination

- **Router address**

3.3 Time-of-day synchronization

Time-of-day synchronization and security

If you enable the security functions in modules with security, you will find the parameter group under "Security".

When security functions are enabled, you need to regularly synchronize the time of day of the communications module.

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 communications module 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.

The communications module can obtain the time of day from an external source (for the methods see below) and forward the time of day to the station or the connected WAN networks.

When an external time source is used, the connected S7 station can obtain the current time of day both via the CPU and via a communications module (TIM, CP).

Note

Recommendations

- **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.

If the CPU takes the time from a communications module, disable time-of-day synchronization of the CPU.

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

- **Longer synchronization cycles with unstable networks**

If a network often has connection problems, you can increase its synchronization cycle.

In this way, you avoid the frames being marked as "invalid" and discarded after the synchronization time expected by the slave has elapsed.

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 methods of the communications modules

The modules support the following methods and functions (receiving/forwarding) of time-of-day synchronization:

- **TIM 1531 IRC**

- NTP
- From WAN
- To local station
- To WAN

- **CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC**

The CP can only be a time slave for the connected subnet.

- Time from partner
- NTP
- Time from CPU
- Forwarding the time to the CPU

- **CP 1542SP-1 IRC**
 - NTP
 - From WAN

CPs do not support forwarding the time to connected subnets.

Methods for receiving the time of day

- **NTP / NTP (secure)**

Network Time Protocol

Time-of-day synchronization only via Ethernet

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

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

Recommendation with NTP:

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 UTC time.

Note on the TIM 1531 IRC:

When an FQDN is used as address of the NTP server, up to 240 characters can be entered.

- **From WAN**

The TIM adopts the time of day from one or more subscribers in the connected network.

The following can be time masters:

- A synchronized CPU
- Subscriber with time receiver
- A master station PC connected to the Ethernet network

- **Time from partner (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC / CP 1542SP-1 IRC)**

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

- **Time from CPU (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC)**

As of V4.2, the CPU 1200 synchronizes all CMs/CPs of the station with 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.

- **Setting the time of day manually using the WBM (TIM 1531 IRC)**

If you have configured a time source for the TIM, you can also set the time via the WBM, see section System time (Page 192).

Receive time > Time zone support

You will find the following parameters in this parameter group:

- Enable time difference

This option is intended for communications modules of the type "Station" which receive the time from the master and forward their local time to the station (CPU with UTC time).

When the option is enabled, the communications module adapts its local time, which it forwards to the CPU, to the time of the CPU (UTC).

The communications module keeps its local time, even if it is synchronized by the CPU in turn.

- Time difference:

Select the time span (minutes) to compensate for the difference between the local time of the communications module and the CPU time (UTC).

Example: If the communications module has a local time of "UTC" and the CPU has a time of "UTC - 1", select "- 60" in the drop-down list.

Time of day forwarding by a CP 1200

- Forwarding the time to the CPU (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC)

Requirement: CP firmware \geq V3.0 and CPU firmware \geq V4.2

If both modules in the station have the specified firmware versions, the time of day of the CP is automatically forwarded to the CPU. Since the CPU automatically adopts the CP time, you no longer require the forwarding option using the PLC tag, like with CP firmware < V3.

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

Time of day forwarding by the CP 1542SP-1 IRC

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

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

CPs: Time of day forwarding by the PLC tag

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

For more on this, see parameter group "Communication with the CPU".

Forwarding time of day by the TIM

The TIM can forward its time of day as follows:

- **To connected networks**

Configuration with "Time of day synchronization" > "Send time" or "Receive time"

The procedure for configuration differs in Ethernet and classic WAN networks, see below.

- **On the assigned CPU**

- Configuration with "Time of day synchronization" > "Send time"

- Configuration with "Communication with the CPU" > "Time to CPU"

With this method the time-of-day is made available to the CPU via a PLC tag.

Decide on one of the two methods for forwarding to the CPU and disable the other.

Time configuration with the TIM 1531 IRC

Parameter groups for time-of-day synchronization

For the Ethernet-based time-of-day synchronization, make the settings in the parameter groups "Receive time" and "Send time".

With time-of-day synchronization via classic WAN networks, these two parameter groups of the serial interfaces of the TIM take on the values that you configured directly in the connected classic WAN network (see below).

- **Receive time**

Here you specify via which of the connected networks the TIM will receive the time of day. You configure this parameter group for the TIM modules with the network type "Node station" and "Station".

Here is where you also configure the NTP servers if the TIM is to be synchronized directly via NTP. This is usually only one TIM that functions as time master in the network.

You can also determine the interface of the TIM via which the time is received over WAN and make settings relating to the synchronization cycle.

- Enable daylight-saving time switchover

Enables automatic switchover to standard and daylight-saving time (daylight-saving time switchover).

The module accepts time frames received from the master with daylight-saving time without correcting the time.

Node stations forward time frames with daylight-saving time from the master to the stations without correction.

- **Send time**

Here you specify the networks on which the TIM will forward the time of day.

You configure this parameter group for TIM modules with the network type "Master station" in other word on the TIM that functions as time master in the network.

Configuration on the Ethernet interface of the TIM 1531 IRC

Time master

1. In the parameter group "Receive time" of the TIM to be time master configure the time source with one of the following options:
 - From NTP server
 - From local station
(take the time from the assigned CPU)
 - From WAN
(Take the time from a network via a specific connection partner)
2. Configure the interface of the TIM via which time frames will be forwarded in the parameter group "WAN settings" as network node type "Master station".
3. In the parameter group "Send time" for the interface from step 2, enable the option "Send time to WAN via... (interface)".

Via the interface, the time frames are forwarded to the connected network.

For an Ethernet interface with the setting "Net work type" = "Neutral", enabling the function has no effect because the S7 protocol does not work with time masters and slaves.
4. If necessary, enable the "To local station" option in the "Send time" parameter group if the assigned CPU should also be synchronized.

Time slaves

1. Configure the interfaces of the other TIM modules that will be time slaves in the parameter group "WAN settings" as network node type "Node station" or "Station".

The function is supported for the Ethernet interface with the MSC protocol and for the serial interface, not for an Ethernet interface with the setting "Network type" = "Neutral".
2. Network the interfaces of the TIM modules involved with each other and with the interface of the time master.
3. For the stations set the parameters of time-of-day synchronization in the parameter group "Receive time".
4. If necessary, enable the "To local station" option in the "Send time" parameter group if the assigned CPU should also be synchronized.
5. If the time is to be forwarded from a specific interface of the TIM to the WAN network, enable this in the parameter group "Send time" > "To WAN". You can make settings relating to the synchronization cycle for each enabled interface.

Configuring the synchronization via classic WAN networks

For classic networks, you configure the "Time-of-day synchronization" in the parameter group of the same name.

The settings for synchronization are then adopted by all serial interfaces of the connected TIM modules.

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

TIM modules (time master and slaves)

1. Classic WAN network

For classic networks the "Time-of-day synchronization" is enabled in the parameter group of the same name. You also specify the synchronization cycle.

The settings for synchronization are then adopted by all connected TIM modules.

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

2. In the parameter group "Receive time" of the TIM to be time master configure the time source with one of the following options:
 - From NTP server
 - From local station
(take the time from the assigned CPU)
 - From WAN
(take the time from a network)
3. Configure the interface of the master TIM as network node type "Master station".
4. Configure the interfaces of the other TIM modules (time slaves) as network node type "Node station" or "Station".
5. If necessary, enable the "Send time to local station" option in the "Send time" parameter group of the stations if the assigned CPU should also be synchronized.
6. If the time is to be forwarded from a specific interface of the TIM to the WAN network, enable this in the parameter group "Send time" > "To WAN". You can make settings relating to the synchronization cycle for each enabled interface.

WAN network

1. In the parameter group "Time-of-day synchronization" of the network enable the option "Enable time-of-day synchronization for WAN".
2. Configure the required synchronization cycle.
3. Network the interfaces of all TIM modules involved with the WAN network.

The settings configured for the WAN network are adopted in the following parameter groups of the connected TIM modules:

- For the time master (Master station): "Send time" parameter group
- For the time slaves (node stations / station): "Receive time" parameter group

Optional: Specify time partner (TIM 1531 IRC)

If multiple time masters are connected in the network, you can define a specific subscriber as time master with the TIM 1531 IRT.

1. Configure the telecontrol connections via the serial interfaces of the two devices.
2. After the telecontrol connections have been created, you can select the partner configured via the connection at the time slave.

Selection at parameter "Receive time > Obtain time from partner" of the serial interface

In the "No connection partner" setting, the TIM accepts the time from all connected time masters.

3.4 Configuration of interfaces, networks and network nodes

3.4.1 WAN settings of the interfaces

WAN settings

The following parameters determine the properties of the interfaces and the connected WAN networks.

First, configure the respective module interface. The subsequently connected WAN network adopts the most important settings.

- **WAN type**

Selection of the WAN type of the interface:

- IP-based
Default setting of the Ethernet interface
- Classic WAN
Default setting of a serial interface

- **Network type**

For IP-based WAN:

- IEC 60870-5
- Neutral

For classic WAN:

- Dedicated line
- Dialup network

Note that conventional WAN networks are only supported for TIM modules.

- **Network node type**

Decides the Network node type of the interface:

- Master station
- Node station

For modules that act as node station, the interfaces are configured as follows:

- Interface in the direction of the master station: "Node station"
- Interface in the direction of the lower-level network: "Master station"

- Station

You will find an illustration in the section Networking of the interfaces (Page 45).

- **Modem type**

The modem type for connection to the serial interface must be configured for the network type "Dialup network" and, in the case of the classic TIM modules, also for the network type "Dedicated line".

The entries have the following meanings:

- MD2
Dedicated line modem (network type "Dedicated line")
- MD3
Modem for analog dialup networks (network type "Dialup network")
- MD4
ISDN modem (network type "Dialup network")
- MD720
The GSM modem MD720 is not supported because it uses frame format FT2.
- Third-party modem
Any compatible modem for the network types "Dedicated line" or "Dialup network" (analog / ISDN / GSM)

3.4.2 Networking of the interfaces

Module interfaces

The arrangement of the module interfaces in the STEP 7 device symbol (network view) corresponds largely to the structure of the respective device.

For example, the interfaces of a TIM 1531 IRC are arranged as follows:

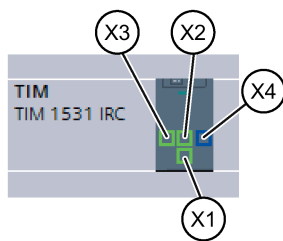


Figure 3-1 Device symbol of the TIM with interface numbers

Networking interfaces

To network an interface depending on the initial situation you have different options:

- Creating a subnet
- Connecting two target devices via a new subnet
- Connecting devices to existing subnet
- Selecting an existing subnet from the "Subnet" list

You will find the description of the individual methods in the STEP 7 information system.

Networking WAN interfaces

Recommendation networking:

To network the interfaces with a WAN network, the following procedure is recommended:

1. Network the WAN networks in the network view of STEP 7.

In the graphic network view, you have an overview of the subnets of the entire system in the project.

2. First configure the interface parameters described in the section WAN settings of the interfaces (Page 44):

- WAN type
- Network type
- Network node type
- Modem type

3. Select the relevant interface to create a new WAN network. Alternatively:

In the parameter group "Network interface with" of the interface:

- Using the "Add new subnet" button

On the interface in the device symbol of the module:

- Using the shortcut menu "Create subnet"
- Graphically by dragging (holding the mouse pointer pressed) to the interface symbol of the communications partner

A new WAN network is created that adopts the network type from the connected interface.

Network representation of a classic WAN

A classic WAN network is displayed in blue.

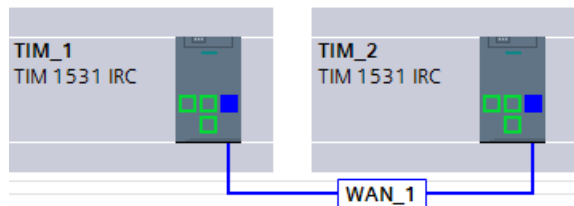


Figure 3-2 TIM modules, serial interfaces networked via classic WAN.

Network with node stations

In the following figure, the center TIM is a node station. The "Network node type" parameter of the interfaces is configured as follows:

- Interface in the direction of the master station: "Node station"
- Interface in the direction of the lower-level network: "Master station"

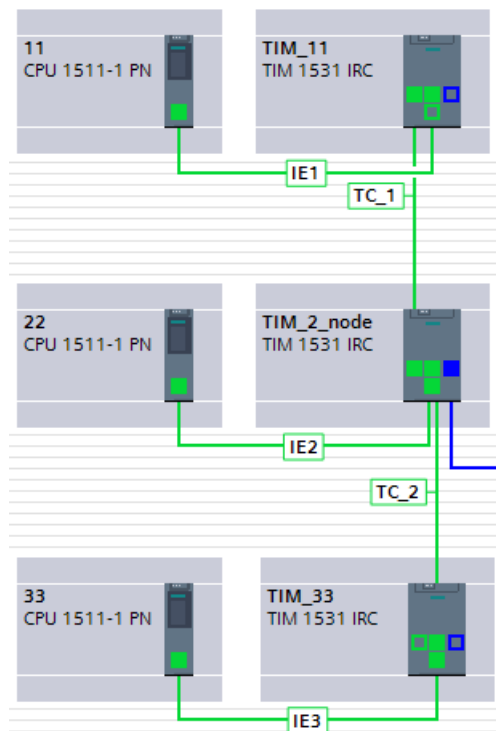


Figure 3-3 Network with master station (top), node station (center) and station (bottom)

3.5 Ethernet interface

3.5.1 Ethernet addresses

The Ethernet interface

- **Ethernet CPs**

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

- **Mobile wireless CPs**

Mobile wireless CPs do not have a physical Ethernet interface.

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

When using security functions, you must network the interface.

Ethernet addresses

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

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

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

Use IPv6 protocol

In addition to IPv4, you can optionally enable IPv6 for the CP.

Options for mobile wireless CPs:

- **Dynamic IP address**

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

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

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

Ethernet interface > Port [Xn P1]

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

For information on configuring the WAN settings, refer to the section WAN settings of the interfaces (Page 44).

3.5.2 Advanced options

3.5.2.1 TCP connection monitoring

Ethernet interface > Advanced options > TCP connection monitoring

The settings of the two parameters at the Ethernet interface govern TCP connections via this interface.

You can adapt the parameters in the properties of the telecontrol connections for each connection segment.

- **TCP connection monitoring time**

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

With the setting 0 (zero), the function is disabled.

Default setting: 180 s

Permitted range

- TIM 1531 IRC

1...65535 s

- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC

0...65535 s

- CP 1542SP-1 IRC

0...32767 s

- **TCP keepalive timeout**

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

With the setting 0 (zero), the function is disabled.

Default setting: 10 s

Permitted range

- TIM 1531 IRC
1...65535 s
- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
- CP 1542SP-1 IRC
0...32767 s

3.5.2.2 Transmission settings

You will find the specific parameters of the telecontrol protocol in the section IEC parameters of interfaces (Page 55).

3.5.3 Web server access

3.5.3.1 CP

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 /7/ (Page 221).

You will find information on the Web server of the ET 200SP in the manual /8/ (Page 221).

3.5.3.2 TIM 1531 IRC

Access to the Web server

You can activate access to the Web server of the TIM via HTTP/HTTPS for each individual Ethernet interface.

As default access is disabled. Refer to the explanations in section Security recommendations (Page 209).

You enable the Web server and make further settings in the parameter group "Web server", see section Web server (TIM 1531 IRC) (Page 62). There you can also enable or disable access.

For access to the Web server you need to enable access on the Ethernet interface ("Access to the Web server") and enable the Web server itself "Web server".

3.6 Serial interface

3.6.1 WAN parameters

You network the interface using the "Subnet" drop-down list.

WAN address

Here, you define the length of the optional address field (LADDR) for the link layer address.

- **Address format (2-byte address)**

Please note: The address format must be the same for all stations of the IEC network (60870-5-101).

- When the option is disabled, the ASDU address is saved in 1 byte (least significant byte of the word).

The range of values for the link layer address is 1...255.

- If the option is enabled, the address range of the link layer address (see below) is increased to 1...65535.

- **WAN address**

Optional link layer address of the interface

Standard range of values: 1...255

Increased range of values with enabled "2-byte address" parameter: 1...65535

3.6.2 Advanced options

3.6.2.1 Dedicated line

Settings dedicated line

Settings serial interface

- **Interface standard**

Standard of the serial interface: RS232 / RS485

Select the following value:

- RS232

When a modem with an RS-232 interface is connected to the interface of the TIM

- RS485

When a modem with an RS-485 interface is connected

With parallel connection of several modems to the interface of the TIM (star-shaped network)

- **RS-485 termination**

Enable this option when connecting a terminating resistor for the RS-485 bus when a star-shaped network is connected.

Time options

- **Send delay time (after RTS)**

The Send delay time (after RTS) (ms) is started after RTS is set.

- Value = 0

The module waits to send data until it receives the CTS signal (ready to send) from the modem.

- Value > 0

The module does not wait for the CTS signal of the modem, but sends as soon as the configured time has elapsed.

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

- **Send delay time (after CTS)**

The delay time (ms) is used when readiness to send (CTS signal) is received from the modem and when 0 (zero) has been configured for the "Send delay time (after RTS)".

- Value = 0

Transmission is not delayed until the CTS signal of the modem.

- Value > 0

As soon as the CTS signal is received from the modem, the send delay time is started. Sending starts after the time has elapsed.

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

- **RTS off delay**

Only configurable with: TIM 1531 IRC

The RTS OFF delay (ms) defines when the module takes back the RTS signal after sending.

- Value = 0

The module takes the RTS signal back immediately after sending the last character.

- Value > 0

Once the last character has been sent, the RTS OFF delay elapses before the module takes back the RTS signal.

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

3.6.2.2 Dialup network

Settings dialup network

Settings serial interface

- **Interface standard**

Standard of the serial interface: RS232 / RS485 - can be switched over

Select one of the following values:

- RS232

When a modem is connected to the interface of the TIM

- RS485

Connection of the internal terminating resistor of the TIM

With parallel connection of several modems to the interface of the TIM (star-shaped network)

- **RS-485 termination**

Enable the option when connecting a terminating resistor for the RS-485 bus when a star-shaped network is connected.

Call parameters

- **Dialing command**

Dialing command for the local modem

Possible values:

- D (AT command)
- DP (AT command, pulse dialing)
- DT (AT command, tone dialing)

When possible use the dialing command "D".

- **Dialing prefix**

Access number (outside line) for a private branch exchange (typical entry 0 or 9) or for an alternative telephone provider.

Permitted range: Max. 12 digits

With direct connection to the dial-up network and without an alternative telephone provider, this parameter can remain empty.

- **Own phone number**

Entry of your own telephone number for the network node including the area code.

Permitted values:

- Digits 0 ... 9
- Plus character (+) as placeholder for the trunk prefix (usually 00 or 09) before the international area code

Example: +1230123456789

AT initialization

- **User-defined**

If the option is enabled the AT initialization string for the basic settings of the modem can be assigned manually.

If the option is disabled, the AT initialization string is preset for the specific modem:

- MD3 : AT\$45=3\N0F0&W
- MD4 : AT\$45=83\$P1\N0&W

- **Initialization string**

Input box for the AT initialization string

Time options

- **Dial test interval**

The test interval (min) is started when no connection could be established by the communications module after 3 attempts. When the test interval elapses, the communications module attempts to establish a connection again.

If it fails to establish the connection again, the test interval is restarted.

If a new frame is pending for transfer during the test interval in a master station TIM, the TIM attempts to establish a connection immediately.

Default setting: 5. Permitted range: 0...255

- **Max. connection duration**

Only for interfaces with the Network node type "Master station".

Maximum connection duration (s) for a dial-up connection. When the time elapses, the connection is terminated. Frames that are still pending for transmission in the station are transferred the next time a connection is established.

With 0 (null), the dial-up connection is retained until all pending data has been transferred.

Default setting: 5. Permitted range: 0...65535

- **Repetition factor**

The repetition factor determines how often a data frame that has not been acknowledged positively is repeated.

Mobile wireless settings

Communication using mobile wireless networks is not supported.

3.6.2.3 Transmission settings

You will find the specific parameters of the telecontrol protocol in the section IEC parameters of interfaces (Page 55).

3.7 IEC parameters of interfaces

3.7.1 Transmission settings - IEC 60870-5

Transmission settings - IEC 60870-5

- **ACTTERM**

Enables the sending of acknowledgments with the cause of transmission ACTTERM (cause of transmission <10>).

With this, the end of command processing is signaled to the partner.

With direct communication between two stations, ACTTERM must be configured identically for both partners.

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

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

Permitted range: 1..65535

Default setting: 1

You define the mode of command processing for each individual command data point, see Command options (Page 140).

- **Monitoring time for connection establishment (t₀)**

Monitoring time for the connection establishment (t₀) in seconds. If the communication partner does not confirm connection establishment within the monitoring time, the module attempts to establish the connection again.

Permitted range: 1..255

Default setting: 30

- **Frame monitoring time (t_1)**

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

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

Permitted range: 1..255

Default setting: 15

Note

Settings on the master

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

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

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

After receiving data from the master, the module acknowledges the received data either:

- If the module sends data to the master itself within t_2 , it acknowledges the data frames received from the master during t_2 at the same time along with the sent data frame (I format).
- The module sends an acknowledgment frame (S format) to the master at the latest when t_2 elapses.

Permitted range: 1 ... 255

Default setting: 10

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

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

Monitoring time in seconds during which the module does not receive any frames from the master.

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

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

Permitted range: 1 ... 255

Default setting: 30

- **Difference (k) between $N(S)$ and $N(R)$**

The difference between the send sequence number $N(s)$ and receive sequence number $N(r)$ of a frame.

The master returns the send sequence number of a frame from the module as acknowledgment, which the sending module then saves as the receive sequence number. Frames whose send sequence number is lower than the receive sequence number after

the difference configured here is added are evaluated as having been successfully transferred and are deleted from the send buffer of the module.

Permitted range: 1 ... 64

Default setting: 12

- **Max. no. of unacknowledged data frames (w)**

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

Permitted range: 1..8

Default setting: 8

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

Acknowledgment mechanism for the IEC protocol

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

Upon reception, the master sends the send sequence number from this or (if several data frames are received) the last data frame back to the module as an acknowledgment. The module stores the send sequence number returned by the master as the reception sequence number and uses it as acknowledgment.

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

Recommendations of the specification:

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

3.7.2 Settings IEC master

IEC master

You can find the following parameters in the "Settings IEC master" parameter group of the interfaces of the communications module configured at the IEC network type and the "Master station" network node type.

- **Polling basic interval**

This is where you define the basic interval for station calls by the master station.

Value range: 0 ... 65535 seconds

Default: 30

With the setting 0 (zero), the function is disabled. No cyclic polling takes place, not even for the parameters listed below, the calculation of which is based on the polling basic interval.

The basic interval is used for the calculation of the following parameters in the connection configuration:

- Interval for general request
- Interval for counter general request
- Interval for group request
- Interval for counter group request

For information on the configuration, refer to the section Query options (Page 110).

- **Max. number of events per call**

Maximum number of events that can be sent in the response frame of the station after being called by the master station.

Range of values: 0 ... 65535

Default: 0

With the setting 0 (zero), the function is disabled (no limitation).

With respect to the "Partner monitoring time" parameter, see also the section Settings IEC station (Page 58).

3.7.3 Settings IEC station

Event settings

Requirements

- The network node type of the interface is "Station" or "Node station".
- The data points are of the same type.
- The indexes of the data points are in sequence without gaps.

Refer to section Data point index (Page 124).

Function

You can set the form of transfer for the data point types listed below. The settings apply to data points configured as event (triggered).

The function corresponds to the "SQ" bit of the "VARIABLE STRUCTURE QUALIFIER field" according to IEC 60870-5-101.

- **Transfer behavior**

- Single transfer:

The object address is transferred individually.

SQ = 0

- Sequential transfer

The object addresses are created contiguously to save data volume during transfer.

SQ = 1

Settings of supported data point types

When Transfer behavior = "Sequential transfer" is configured, the following parameters apply to the listed data point types.

Transfer of the buffered events is triggered as soon as one of the two following conditions is met.

- **Number of events**

Transfer when the configured number of buffered events has been reached.

- **Delay time**

Transfer when the configured delay time (seconds) has been reached.

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

Other station-relevant parameters

The following station-relevant parameters are defined during configuration of the connections:

- Spontaneous
- Polling mode

For information on the configuration, refer to section Connection table (Page 101).

You can find other parameters in the following parameter groups:

- Response to general request / Assignment to group request

(cause of transmission 20 - 41)

- You configure the assignment of individual data points to a general request or group request in the data point configuration, see section "General" tab (Page 122).
- You configure the intervals of the requests in the telecontrol connections, see section Query options (Page 110).

3.8 Configuring WAN networks

Parameters of classic WAN networks

First configure the parameter group "WAN settings" of the communications module interfaces, see section WAN settings of the interfaces (Page 44).

The most important settings of the interface are taken from the connected WAN network when a new network is generated.

The classic WAN networks, shown in blue in STEP 7, have the following parameter groups.

General

Like for any other network, this is where you configure the name and the S7 subnet ID.

Network settings

Network configuration

- **Protocol type**

The following telecontrol protocols may be available, depending on the module type:

- ST7
- DNP3
- IEC 60870-5

- **Network type**

The network type is taken from the connected interface:

- Dedicated line
- Dialup network

Access method

Only with dedicated line

- **Access method**

The access method is preset and cannot be changed:

- Polling

Frame parameters

The parameters are preset and cannot be changed.

- **Frame format**

- FT1.2

- **Acknowledgment type**

- Short acknowledgment (1 byte)

- **Repetition factor**

The repetition factor determines how often a data frame that has not been acknowledged positively is repeated:

- 3

- **Max. frame length**

Maximum size of a data frame within the network:

- 240

Network settings

- **Dependence on direction**

Direction dependency of the network

- Duplex
- Half duplex

- **Transmission speed**

Speed at which the communications module and modem communicate.

From the drop-down list, select a value that is supported by all connected modems.

Time-of-day synchronization

- Enable time-of-day synchronization for WAN

When the parameter is enabled, you specify whether the time for the time-of-day synchronization of the connected stations should be transmitted via the WAN network.

You specify the synchronization cycle if the parameter is enabled.

Note

Transfer of the setting by stations

The connected TIM modules adopt the settings made here on the network.

For information on the time-of-day concept, see section Time-of-day synchronization (Page 37).

Station list

This is where you can find an overview table of the stations connected to the network with their most important parameters.

The WAN address is the station address.

3.9 Web server (TIM 1531 IRC)

The Web server of the TIM

The TIM provides you with the functionality of a Web server for access using a Web browser. The following functions are available via the Web server:

- Read access
 - A selection of diagnostics data
 - A selection of configuration data
- Write access
 - Setting the time
 - Firmware update
 - Module restart
 - Reset to factory settings
 - Recording of statistics values of the Ethernet interfaces

For a description of the content, refer to the section WBM of the TIM 1531 IRC (Page 187).

Access rights via "Global security settings"

The rights for access to the Web server are configured in STEP 7 in the Global security settings. Only users created there can log on with the Web server using HTTP/HTTPS.

The following preset roles are relevant for Web server access:

- NET Standard
- NET Diagnose

The required rights for diagnostics, access to the Web server and reading and writing data are thus enabled.

You will find further help on the roles and rights of users in the STEP 7 information system.

Access to the Web server and starting Web diagnostics

To be able to connect to the Web server of the TIM, access to the Web server must be enabled for every Ethernet interface, see also section Web server access (Page 50). As default access is disabled.

For information on starting Web diagnostics, see section Web diagnostics of the TIM 1531 IRC (Page 64).

"Web server" parameter group

General

- **Enable Web server on this module**
Enables data processing in the Web server of the TIM and allows access to this data.
- **Allow access only using HTTPS**
Allows access to the Web server only with the secure protocol HTTPS.

Note

"Allow access only using HTTPS" (security function enabled)

Note the following when the "Allow access only using HTTPS" option is enabled in the "Web server" parameter group:

- The data is transferred encrypted.

Requirements

- The roles specified above with the corresponding rights must be assigned to the user.
 - If the firewall is activated, the HTTP/HTTPS protocols must be allowed.
-

Automatic update

- **Enable automatic update**
Enables automatic updating of the displayed values.
If the option is disabled, only the values at the time of connecting to the Web server are displayed.
- **Update interval**
Select the interval at which you require an update of the displayed values.
Default setting: 30. Permitted range: 5...999

Overview of the interfaces

Here you can see the releasing access to the Web server via the Ethernet interfaces of the TIM.

You can activate access to the Web server of the TIM via HTTP/HTTPS for each individual Ethernet interface.

The settings for activation in the parameter groups "Web server access" and "Web server" are adopted reciprocally in the other parameter group.

3.10 Web diagnostics of the TIM 1531 IRC

Requirements

- The Web server of the module is enabled in the configuration, "Web server" parameter group, and the interface is selected.
- The interface is enabled for access to the Web server in the configuration, "Ethernet interface > Access to Web server" parameter group.

Starting Web diagnostics

1. Establish a physical connection between the engineering station and the SIMATIC station.
2. Set the PC interface in such a way that the module can be reached.
Further help is available in the "Set PG/PC Interface" dialog box.
3. In the STEP 7 project, click the "Web diagnostics" button under the "Web diagnostics" parameter group to establish the connection to the Web browser of the module.

The content is supplied by the integrated Web server of the module. For information on operation and on the contents, see section WBM of the TIM 1531 IRC (Page 187).

3.11 DNS configuration

DNS server

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

DNS server for e-mail server address

During e-mail configuration, the address of the mail server via which the e-mails are sent must be specified. The address of the mail server can be specified as an IP address or as an FQDN.

If you specify the server address as an FQDN you need to configure a DNS server. In this case the IP address of the mail server is determined via the configured DNS server.

3.12 Communication with the CPU

Communication with the CPU

Using the first three parameters, you specify the CPU access by the TIM in the CPU sampling cycle. You will find the structure of the CPU sampling cycle in the section Read cycle (Page 128).

- **Cycle idle time**
Wait time between two sampling cycles of the CPU memory area
- **Max. number of write jobs**
Maximum number of write jobs to the CPU memory area within a CPU sampling cycle
- **Max. number of read jobs**
Maximum number of low-priority read jobs from the CPU memory area within a CPU sampling cycle

Watchdog bit

- **TIM monitoring / CP monitoring**
Via the watchdog bit, the CPU can be informed of the status of the telecontrol communication of the communications module.

CP time

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

CP diagnostics

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

- **Enable advanced CP diagnostics**

Enable the option to 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, depending on the functions supported by the CP.

- **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 warning**

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

- **Frame memory occupation**

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

- **Current IP address**

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

- **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

PLC tags for partner status / path status

Via the PLC tag that can be configured here, you can monitor the following information about the reachability of the communications partners:

- **Partner status**

Reachability of the remote communications partner

- **Path status**

Status of the connection path or the redundant connection paths to the remote communications partner

For information on communication and the possible connection paths, see section Communications options (Page 29).

For every configured communications partner to which a single or redundant telecontrol connection is created, you can create a PLC tag of the type Word.

Assignment of the PLC tags for partner status / path status

In the two bytes of the PLC tag of the data type Word (DB, memory bit, output) the following information is output:

- **Byte 0: Partner status**
- **Byte 1: Path status**

Byte 0 "Partner status"

Byte 0 codes information on the reachability of the communications partner, on the existing connections and connection paths and on the status of the send buffer of the TIM.

Table 3-1 Assignment of byte 0: Meaning of the bit statuses

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Path redundancy	Connection mode	Temporary connection *	<i>(Reserved)</i>	Frame memory **		Path status	Partner status
0: No redundancy 1: Redundancy exists	0: Permanent 1: Temporary	0: Partner not reachable 1: Partner reachable *	-	0: Send buffer OK 1: Memory occupation > 80 % 3: Overflow (memory allocation 100 %)		0: Not all paths reachable 1: All paths reachable	0: Partner not reachable 1: Partner reachable

** Partners that support temporary connections are set to "accessible" if the partner itself terminates the connection and there is no connection established.

** Status of the send buffer:

If Bit 2 or Bit 2+3 is set on a send buffer overflow or prewarning, the two bits are only reset when the memory occupation falls below 50%.

For information on the send buffer, see section Process image, type of transmission, event classes (Page 126).

Byte 1 "Path status"

Byte 1 shows the status of the connection path (configured connection) to the partner from the point of view of the local TIM.

A maximum of 2 paths (main and substitute path) to a partner can be configured, see section Communications options (Page 29).

Both connection paths must start or end on a local TIM.

The byte shows the following:

- The paths via which the partner can be reached.
- The path currently being used
- The TIM interface via which the main path was configured.
- The TIM interface via which the substitute path was configured.

The path of a connection is specified as a combination of the used interfaces of the TIM and the status of the path.

Byte assignment

Byte 1 is assigned as follows:

- Two bits for the interface of the main path
- Two bits for the interface of the substitute path
- Two bits for the status of the main path
- Two bits for the status of the substitute path

Table 3-2 Assignment of byte 1

Bits 6 + 7	Bits 4 + 5	Bits 2 + 3	Bits 0 + 1
Configured interface		Path status	
Coding for substitute path	Coding for main path	Substitute path (2nd path)	Main path (1st path)

• **Configured interface**

The TIM interfaces "Ethernet 1" (IE1), "Ethernet 2" (IE2), "Ethernet 3" (IE3) and WAN1 are numbered through from 0 . 3 (decimal):

- 0 = Ethernet interface IE1 (X1)
- 1 = Ethernet interface IE2 (X2)
- 2 = Ethernet interface IE3 (X3)
- 3 = Serial interface WAN1 (X4)

Status of bit 5 (7)	Status of bit 4 (6)	Meaning
0	0	Coding for Ethernet interface X1 (decimal: No. 0)
0	1	Coding for Ethernet interface X2 (decimal: no. 1)
1	0	Coding for Ethernet interface X3 (decimal: no. 2)
1	1	Coding for serial interface X4 (decimal: no. 3)

- **Path status**

- Main path = 1. Path (bits 0 + 1)
- Substitute path = 2nd path (bits 2 + 3)

Status of bit 1 (3)	Status of bit 0 (2)	Meaning bit 1	Meaning bit 0
0	0	Bit 1: Path not current	Bit 0: Subscriber not reachable
0	1	Bit 1: Path not current	Bit 0: Subscriber reachable
1	0	Bit 1: Path current	Bit 0: Subscriber not reachable
1	1	Bit 1: Path current	Bit 0: Subscriber reachable

Coding options of byte 1

Same coding of the configured interface for the main and the substitute path means that there is no path redundancy (only one interface configured). The path status is output via the bits of the main path (1st path).

Table 3-3 Coding options for the path status

Configured interface		Path status	
Coding for substitute path	Coding for main path	Substitute path (2nd path)	Main path (1st path)
0 0	0 0 (Coding for IE1)	Irrelevant (not redundant)	Status IE1
0 0	0 1 (Coding for IE2)	Status IE1	Status IE2
0 0	1 0 (Coding for IE3)	Status IE1	Status IE3
0 0	1 1 (Coding for WAN1)	Status IE1	Status WAN1
0 1	0 0	Status IE2	Status IE1
0 1	0 1	Irrelevant (not redundant)	Status IE2
0 1	1 0	Status IE2	Status IE3
0 1	1 1	Status IE2	Status WAN1
1 0	0 0	Status IE3	Status IE1
1 0	0 1	Status IE3	Status IE2
1 0	1 0	Irrelevant (not redundant)	Status IE3
1 0	1 1	Status IE3	Status WAN1
1 1	0 0	Status WAN1	Status IE1
1 1	0 1	Status WAN1	Status IE2
1 1	1 0	Status WAN1	Status IE3
1 1	1 1	Irrelevant (not redundant)	Status WAN1

3.13 E-mail configuration

Configuring e-mails

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

In the message editor ("Messages" entry), you configure the individual e-mails, see section Messages (Page 144).

Requirements for e-mail

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

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

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

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

E-mail configuration

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

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

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

- Port no. 587

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

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

- Port no. 465

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

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

On configuration of the passwords, see Character set for user names, passwords and messages (Page 150).

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 82).

3.14 Subscriber numbers

Subscriber numbers

In this folder, you configure the station address and the assignment of the CPU depending on the communications module:

- **CP**
 - ASDU address
ASDU address of the station
The communication module and the station (CPU) have the same ASDU address.
 - Structured ASDU address
Structured ASDU address of the station
The CPU is assigned automatically to the communications module via the rack.
- **TIM**
 - Assigned CPU
The drop-down list only shows the CPUs that are networked with the TIM.
 - Password of the assigned CPU
If the assigned CPU is protected with "No access (complete protection)", enter the password that is configured for the CPU under "Protection & Security > Access level".
 - ASDU address
ASDU address of the station
The communication module and the station (CPU) have the same ASDU address.
 - ASDU address
Structured ASDU address of the station

Observe the basic addressing policies in the section Addressing (Page 29).

Assignment of the CPU and configuration of the subscriber addresses

For modules that communicate via telecontrol connections ("Network data" editor), you assign the CPU and configure the module addresses in the "Subscriber numbers" parameter group.

- **Assigned CPU**

With the following communications modules, which are located in the same rack as the CPU, the local CPU is automatically assigned to the module:

- CPs (S7-1200, ET 200SP)

For communication modules that are not in the same rack as a CPU, you must assign the module to a CPU with which it is networked via the drop-down list. This affects:

- TIM 1531 IRC

The TIM 1531 IRC can be assigned a CPU of the following SIMATIC families: S7-300, S7-400, S7-1500, ET 200SP

When you assign the TIM 1531 IRC to an S7-1500R/H CPU, the system IP address of the S7-1500R/H CPU is used for communication of the TIM with the CPU.

Structured addressing of the IEC protocol

The ASDU address can be configured in two input fields with different formats:

- ASDU address

The address is configured unstructured here as an integer.

Range of values: 0..65534

- Structured ASDU address

You can configure the address structured according to IEC 60870-5-3 here. Plant-based structuring of the ASDU address is enabled by structured addressing.

Two address levels (octets) can be configured.

Range of values: 0.0..255.254

The configured values of the two fields are linked. A configured value is converted and displayed in the other input field.

Conversion of the values:

The values are designated as follows for the conversion:

- ASDU address

Designation of the integer value: X

- Structured ASDU address

Designation of the values of the 2nd octet: A.B

The configured value is applied to the other field according to the following formula:

$$X = A * 256 + B$$

3.15 Secure communication between CPU and module

Secure communication with certificates

You need to assign the certificate of the CPU to a communications module in the following cases.

Required for:

- Communications module in separate rack (TIM 1531 IRC)
and
- CPU 1500 / CPU 1500 SP as of V2.9

Requirements:

- The CPU is assigned to the module under "Subscriber numbers".
- You are logged in with the role "NET Administrator".
- The password for protection of confidential PLC configuration data has been created in the CPU. The communication certificate with ID "1" and common name of subject "PLC name//Communication-1" is thus created in the certificate manager of the CPU.

The communication certificate must be assigned to the module that is assigned to the CPU. There are the following procedures for this.

Procedures

Use one of the following two methods.

Using the global certificate manager for the CPU

The local communication certificate of the CPU is recreated in this case.

1. Select the CPU: "Protection & Security > Certificate manager".
2. Select the "Use global security settings for certificate manager" check box.
3. After the following dialog is confirmed, the communication certificate is removed from the certificate manager of the CPU.
4. To create a new communication certificate, select the "Protection & Security > Connection mechanisms" menu in the general settings.
5. Create a new communication certificate under "PLC communication certificate". To do so, click on "..." on the right.
6. Click "Add" in the subsequent window.
7. Confirm the settings in the "Create certificate" window with "OK".

Result: The certificate is available in the certificate manager of the CPU and in the global certificate manager.

Assigning the certificate to the module:

1. In the project navigation, open "Security settings" > "Security features" > "Certificate manager".
2. Select the "Device certificates" tab.
3. Right-click on the communication certificate and select "Assign to".
4. Click the "Assigned" option for the module to which the certificate should be assigned.
5. For "Usage", switch from "Device certificate" to "Trusted certificate".

You can also assign the certificate via the local certificate manager of the module.

Using the local certificate manager of the CPU

The local communication certificate of the CPU is used directly in this case, but needs to be assigned to the communications module via export and import.

1. Select the CPU and choose the "Protection & Security > Certificate manager" menu in the general settings.
2. Right-click on the communication certificate and select "Export".
3. Save the certificate.

Assigning the certificate to the module:

1. In the project navigation, open "Security settings" > "Security features" > "Certificate manager".
2. Select the "Device certificates" tab.
3. Import the communication certificate.
4. Right-click on the communication certificate and select "Assign to".
5. Click the "Assigned" option for the module to which the certificate should be assigned.
6. For "Usage", switch from "Device certificate" to "Trusted certificate".

You can also assign the certificate via the local certificate manager of the module.

3.16 Log settings

Log settings

Validity: TIM 1531 IRC

Events can be recorded in log files for monitoring. You can set how the events are recorded:

- Local logging

Messages on internal events and errors are saved in the diagnostics buffer of the TIM.

The following events can be recorded:

- Audit log: Audit events
- System log: System events

- Network Syslog

The messages on the events are sent to a Syslog server in UDP format according to RFC 5424 or RFC 5426. Details about the structure of the Syslog frames and the supported event buffer entries can be found in the section Security (Page 209).

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

3.17 SNMP

SNMP

The scope of performance of the modules is given in the relevant manual.

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

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.

3.18 Global certificate manager

Certificates 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".

You can find all local certificates of SIMATIC NET communications modules in the global certificate manager.

3.19 CP: Security and certificates

3.19.1 Security user

Creating a security user

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

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

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

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

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

3.19.2 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.

3.19.3 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.

3.19.4 VPN

3.19.4.1 VPN (Virtual Private Network)

VPN - IPsec

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

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

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

Properties

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

Areas of application

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

Cell protection concept

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

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

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

- Data espionage
- Data manipulation
- Unwanted access

3.19.4.2 Creating a VPN tunnel for S7 communication between stations

Requirements

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

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

Note

Communication also possible via an IP router

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

Procedure

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

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

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

Select "Activate security features"

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

You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

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

Note

Current date and current time on the CP for VPN connections

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

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

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

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

Configure the properties of the VPN group

1. Double-click on the newly created VPN group.
Result: The properties of the VPN group are displayed under "Authentication".
2. Enter a name for the VPN group. Configure the settings of the VPN group in the properties.
These properties define the default settings of the VPN group that you can change at any time.

Note

Specifying the VPN properties of the CPs

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

Result

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

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

3.19.4.3 VPN communication with SOFTNET Security Client (engineering station)

Set up VPN tunnel communication between the SOFTNET Security Client and the CP as described in section Creating a VPN tunnel for S7 communication between stations (Page 79).

VPN tunnel communication works only if the internal node is disabled

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

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

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

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

Disable the node in the SOFTNET Security Client tunnel overview:

1. Remove the checkmark in the "Enable active learning" check box.
The lower-level node initially disappears from the tunnel list.
2. In the tunnel list, select the required connection to the CP.
3. With the right mouse button, select "Enable all members" in the shortcut menu.
The lower-level node appears again temporarily in the tunnel list.
4. Select the lower-level node in the tunnel list.
5. With the right mouse button, select "Delete entry" in the shortcut menu.

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

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

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

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

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

3.19.4.5 CP as passive subscriber of VPN connections

Setting permission for VPN connection establishment with passive subscribers

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

This is the case in the following typical configuration:

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

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

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

3.19.5 Certificate manager

Assignment of certificates

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

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

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

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

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

3.19.6 Handling certificates

Certificate for authentication

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

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

For the secure transfer of e-mails via SSL/TLS and SSL certificate is created for the module. 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.

If the module communicates with non-Siemens partners when the security functions are enabled, the relevant certificates of the communications partners must be exchanged. To do this, follow the steps below:

1. Importing third-party certificates from communications partners
⇒ Global security settings of the project (certificate manager)
2. Assigning certificates locally
⇒ Local security settings of the module ("Certificate manager" table)

These two steps are described in the next two sections.

Importing third-party certificates from communications partners

Import the certificates of the communications partners of third-party vendors using the certificate manager in the global security settings of the STEP 7 project. Follow the steps outlined below:

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

Assigning certificates locally

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

1. In the STEP 7 project select the module.
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.

Exporting certificates for applications of third-party vendors

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

1. In the STEP 7 project open the global certificate manager:
Global security settings > Certificate manager
2. Open the "Device certificates" tab.
3. In the table select the row with the required certificate and select the shortcut menu "Export".
4. Save the certificate in the file system of the PC of the connected engineering station.

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

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 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.

3.19.7 Secure communication between CPU and communications module

Procedure

Requirements:

- The CPU is assigned to the module under "Subscriber numbers".
- You are logged in with the "NET Administrator" role.
- Special feature with ST7:
 - When using TD7onCPU, the procedure described below is not necessary.

The communication certificate must be assigned to the module that is assigned to the CPU. There are various procedures for this:

Using the global certificate manager for the CPU

The local communication certificate of the CPU is hereby recreated.

1. Select the CPU: "Protection & Security > Certificate manager".
2. Select the "Use global security settings for certificate manager" check box.
3. After the following dialog is confirmed, the communication certificate is removed from the certificate manager of the CPU.
4. To create a new communication certificate, select the "Protection & Security > Connection mechanisms" menu in the general settings.
5. Create a new communication certificate under "PLC communication certificate". To do so, right-click on "...".
6. Click "Add" in the subsequent window.
7. Confirm the settings in the "Create certificate" window with "OK".

Result: The certificate is available in the certificate manager of the CPU and in the global certificate manager.

To assign the certificate to the module:

1. In the project navigation, open "Security settings" > "Security features" > "Certificate manager".
2. Select the "Device certificates" tab.
3. Right-click on the communication certificate and select "Assign to".
4. Click the "Assigned" check box for the module to which the certificate should be assigned.
5. For "Usage", switch from "Device certificate" to "Trusted certificate".

Assignment can also take place via the local certificate manager of the module.

Using the local certificate manager of the CPU

The local communication certificate of the CPU is used directly, but needs to be assigned to the communications module via export and import.

1. Select the CPU and choose the "Protection & Security > Certificate manager" menu in the general settings.
2. Right-click on the communication certificate and select "Export".
3. Save the certificate.

To assign the certificate to the module:

1. In the project navigation, open "Security settings" > "Security features" > "Certificate manager".
2. Select the "Device certificates" tab.
3. Import the communication certificate.
4. Right-click on the communication certificate and select "Assign to".
5. Click the "Assigned" check box for the module to which the certificate should be assigned.
6. For "Usage", switch from "Device certificate" to "Trusted certificate".

Assignment can also take place via the local certificate manager of the module.

3.19.8 CP 1542SP-1 IRC: Certificates for telecontrol connections with TLS

For information on handling certificates for use of TLS for the telecontrol connections, see section TIM 1531 IRC: Handling certificates for TLS (Page 89).

3.20 TIM 1531 IRC: Protection and certificates

3.20.1 Protection

Protection functions

The module provides various access levels to restrict access to certain functions.

NOTICE

Configuring an access level does not replace the know-how protection

Configuring access levels prevents unauthorized changes to the module by restricting the download rights.

This does not, however, provide write or read protection for blocks on a memory card. Use the know-how protection to protect the code of blocks on the memory card.

The table of access levels

You configure the access levels in the table. The green check mark in the columns on the right of the particular access level indicate the maximum possible operations without knowing the password for this access level.

The default access level is "Full access (no protection)". Every user can read and modify the configuration. No password has been configured and no password is required for online access.

You can configure the following access levels:

- **Full access (no protection)**

The configuration and the blocks can be read and modified by anybody.

- **Read access**

With this access level, without entering the password, only read access to the hardware configuration and the blocks is possible; in other words, you cannot download the blocks or hardware configuration to the TIM without entering the password. Without the password, writing test functions and firmware updates are also not possible.

- **No access (complete protection)**

If the module is completely protected, neither read nor write access to the hardware configuration and blocks is possible.

If you want to use the functions of the unmarked access levels, you will need to enter a password.

With the legitimization provided by using the password, you once again have full access to the module.

Behavior of a password-protected module during operation

Protection of the module is effective after the settings have been loaded on the module.

Before an online function is executed, a check is made to establish whether or not it is permitted. If there is password protection, you will be prompted to enter the password.

Example:

The module was configured for read access and you want to use the "Modify tags" function. Since this is write access, the configured password must be entered before the function can be executed.

The functions protected by the password can only be executed by one PG/PC at any one time. Another PG/PC cannot log on.

The access rights to the protected data apply for the duration of the online connection or until the access rights are canceled again with "Online > Delete access rights".

Each access level allows unrestricted access to certain functions even without entering a password, for example identification using the "Accessible devices" function.

3.20.2 Configuring access protection

Configuration

You can enter several passwords setting up different access rights for different user groups.

The passwords are entered in the table so that precisely one access level is assigned to each password.

The "Access level" column shows how the password takes effect.

Example:

You select the access level "No access (complete protection)" for the module and enter your own password for each of the access levels higher up the table.

For users that do not know any of the passwords, the module is completely protected.

For users who know one of the set passwords the effect depends on the table row in which the password is located:

- The effect of the password in row 1 "Full access (no protection)" is as if the CP was unprotected. Users that know this password have unrestricted access to the module.
- The effect of the password in row 2 "Read access" is as if the module was write-protected. Despite knowing the password, users that know this password only have read access to the module.
- The effect of the password in row 3 "No access (complete protection)" is as if the CP was write and read protected. Users that know this password only have read access to the module.

Procedure

Follow the steps below to set the parameters for the access levels of the module:

1. Open the module properties in the Inspector window.
2. Open the "Protection" entry in the navigation panel.
A table with the possible access levels is displayed in the Inspector window.
3. Select the required access level in the first column of the table. The green check mark in the columns on the right of the particular access level indicate which operations are still possible without entering the password.
4. If you have selected an access level other than "Full access":
 - Assign a password for full access in the "Password" column in the first row (full access).
 - Repeat the selected password in the "Confirm password" column to protect against incorrect entries.
 - Make sure that the password is adequately secure; in other words, that it does not include a pattern that can be machine read!
 - The entry of the password in the first row "Full access (no protection)" is obligatory and allows a user who knows the password unrestricted access to the module, regardless of the selected access level.

5. As necessary, assign other passwords to the required access levels if the selected access level permits this.
6. Download the hardware configuration so that the access level takes effect.

Result

The hardware configuration and the blocks are protected from unauthorized online access according to the set access level. If an operation cannot be executed without a password due to the set access level, a dialog appears prompting entry of a password.

3.20.3 TIM 1531 IRC: Handling certificates for TLS

Secure communication with telecontrol modules

The communication via TLS described below is supported by the following modules:

- TIM 1531 IRC V2.3 as of firmware version V2.3
Together with CPU 1500 as of firmware version V2.9
Supported telecontrol protocols: DNP3 and IEC 60870-5-104
- CP 1542SP-1 IRC as of firmware version V2.2
Together with ET 200SP CPU as of firmware version V2.9
Supported telecontrol protocols: DNP3 and IEC 60870-5

The communications modules use TLS 1.2; communication complies with IEC/TS 62351-3.

Communication between CPU and telecontrol module

CP: Communication via backplane bus

If the CPU and telecontrol CP are in the same rack, communication between them runs via the backplane bus. The CPU is automatically assigned to the telecontrol CP.

TIM 1531 IRC: TLS communication with the CPU via Ethernet

The TIM 1531 IRC is not inserted in the rack of the CPU but in a separate rack. The connection to the CPU runs over Ethernet and uses secure communication via TLS for all usable telecontrol protocols.

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. When you create a certificate for the CPU and assign the TIM to the CPU, the certificate is entered automatically.

Creating the CPU certificate and assigning the CPU (TIM 1531 IRC)

Requirements

The following requirements must be met in order to create and assign certificates:

- As STEP 7 project user, you have at least the rights of the "NET Administrator" role.
For more on this, see "Security settings > Users and roles > Assigned roles".
- The devices have the required minimum firmware version, see above.
- The configuration data of the CPU is protected.

For more on this, see "Protection & Security > Protection of confidential PLC configuration data"

To be able to assign your local CPU to the TIM 1531 IRC, the following requirement must be met:

- CPU and TIM 1531 IRC are networked.
- The desired telecontrol protocol is enabled for the TIM under "Communication types".

Creating the certificate of the CPU

First, you need to create a certificate generated by the system (global certificate manager of the STEP 7 project) for the CPU. The locally created certificate of the CPU cannot be used for communication.

When the CPU is assigned to the TIM (see below), the ID of the newly created CPU certificate is automatically entered at the following locations:

- In the "Subscriber numbers" dialog of the TIM
- In the certificate manager of the TIM as partner certificate

Proceed as follows to create the CPU certificate:

1. For the CPU, select the parameter group "Protection & Security > Certificate manager > Global security settings".
2. Enable the "Use global security settings for certificate manager" option.

Note:

When the option is enabled, existing local certificates of the CPU are deleted.

3. Go to "Protection & Security > Connection mechanisms > Communication to TIA Portal and HMI".
4. In the "PLC communication certificate" row, right-click on the icon for the drop-down list.

5. Click "Add" under the open drop-down list.

The "Create certificate" dialog opens with the following options, among others:

- Usage: TLS Client / Server
- Certificate authority (CA): Signed by certification authority
- Common name of subject: Name of the selected CPU
- Encryption method: EC
- Hash algorithm: sha256

If necessary, you can add another address type for the CPU under "Subject Alternative Name (SAN)".

6. Retain the settings and click "OK".

The newly created TLS certificate is shown in the device certificate table with the "TlsServer" service for the CPU.

7. Open the global certificate manager in the project navigation:

"Security settings > Security features > Certificate manager > Device certificates"

8. Select the newly created certificate of the CPU (see above for ID) and open the "Assign" shortcut menu.
9. In the list, select the TIM to which the CPU should be assigned.
10. In the "Used as" row in the ("Not assigned") cell, select the "Trusted certificate" option and click on the green checkmark.
11. Close the dialog with OK.

Assign CPU to TIM 1531 IRC

1. For the TIM that is to communicate with the CPU, open the "Subscriber numbers" parameter group.
2. Right-click on the icon for the drop-down list in the "Assigned CPU" row.
The list of networked CPUs opens.
3. Select the CPU to be assigned to the TIM and click on the green checkmark below it.
The name of the CPU is displayed in the "Assigned CPU" row.
At the same time, the ID of the certificate created previously for the CPU is automatically displayed in the "Communication certificate" row.

Further configuration

Then configure the other stations as communication partners and the corresponding telecontrol connections.

TLS for telecontrol connections

TLS for project-internal telecontrol connections

You can configure secure communication via TLS for telecontrol connections of communications modules that use one of the following protocols:

- IEC 60870-5-104
- DNP3

You configure secure communication for the telecontrol connections ("TeleControl" task card).

1. First create the telecontrol connections.
2. Select the main connection and the "Secure Communication (TLS)" parameter group there.
3. Activate the "Enable secure communication" option.

When all certificates of the connection partners are present, the own certificate ID and the partner certificate ID are automatically applied to the entire connection, including sub-connections, for Siemens devices.

TLS for telecontrol connections with third-party devices

If you want to use secure communication via TLS for telecontrol connections with third-party devices, you need to perform some additional steps.

You need to create a certificate for the third-party device, apply the ID to the connection parameters, export the certificate and the associated CA certificate, and import it into the third-party device.

First create the connection as described above and then activate the "Enable secure communication" option. Proceed as follows.

Importing a third-party certificate or creating and assigning it

Alternatively, you can make the third-party certificate available to the STEP 7 project:

- Import

If required, you can save and import the certificate of the third-party device in the file system of the engineering station.

To import, open the "Trusted certificates and root certification authorities" tab in the global certificate manager, click in a free row and open the "Import" shortcut menu.

You then need to assign the imported certificate to the TIM (see below).

- Create

Alternatively, you can create a certificate for the third-party device in STEP 7 and import it into the third-party device.

Follow these steps:

1. Open the global certificate manager in the project navigation:
"Security settings > Security features > Certificate manager > Device certificates"
2. Click on the "Create" shortcut menu in a free row.
The "Create certificate" dialog opens.

3. Select the following options for the certificate of the third-party device:

- Usage: TLS Client / Server
- Certificate authority (CA): Self signed
- Common name of subject: Enter the name of the third-party device.

Adapt the other parameters to the functionality of the third-party device.

The following are possible, for example:

- Encryption method: RSA
- Key length: 2048
- Hash algorithm: sha256

4. Click "OK" to close the dialog.

The certificate appears in the table.

You will need the certificate ID for the assignment and the telecontrol connection.

5. Select the newly created certificate and open the "Assign" shortcut menu.

6. In the list, select the TIM with which the third-party device should communicate via the telecontrol connection.

7. In the "Used as" row in the ("Not assigned") cell, select the "Trusted certificate" option and click on the green checkmark.

8. Close the dialog with OK.

You will need the certificate ID for the telecontrol connection.

Exporting a certificate for a third-party device and importing it

When you have imported the device certificate of the third-party device, you only need to export the device certificate of the TIM and the associated CA certificate.

If you have created the device certificate of the third-party device in STEP 7, you also have to export this.

Follow these steps:

1. Device certificate for the third-party device created in STEP 7

- In the global certificate manager, open the "Trusted certificates and root certificate authorities" tab.
- Select the device certificate for the third-party device and click the "Export certificate" shortcut menu.
- Save the certificate in the file system of the engineering station.

You can change the default file format "*.der".

You can find a description of the functions of the certificate file formats in the "Exporting certificates" section in the help system.

2. Device certificate of the TIM
 - In the global certificate manager, switch to the "Device certificates" tab.
 - Select the device certificate of the TIM as partner certificate for the third-party device.
 - Make the "Issuer" column fully visible.
You need the name of the issuer to export the issuing CA certificate.
 - Export the selected device certificate of the TIM via the "Export certificate" shortcut menu.
3. Issuing CA certificate
 - Change to the "Certificate authority (CA)" tab.
 - Select the CA certificate that is issuer for the device certificate of the TIM.
When you expand the CA certificate, all derived device certificates are displayed below it, including that of the TIM.
 - Export the selected CA certificate via the "Export certificate" shortcut menu.
4. For communication during runtime, export all saved certificates into the third-party device or its configuration tool.

Entering the certificate ID in the telecontrol connection

1. Switch back to the created telecontrol connection, parameter group "Secure Communication (TLS)".
2. Enter the following values manually for connection with a third-party device:
 - Partner certificate ID: ID of the imported or manually created certificate for the third-party device
 - Own certificate ID: ID of the TIM certificate

Continue with the configuration of the other parameters.

3.21 Telecontrol connections

3.21.1 Telecontrol connections

Telecontrol connections

Telecontrol relationships between the communications modules involved are required for telecontrol communication. Depending on the module type and the firmware version, you perform the configuration in the following parameter groups:

- "Partner stations" parameter group
- or
- "Network data" editor

Configuration in the "Partner stations" parameter group

For the following CPs, which only function as stations, the relationships to the master station or to the master are configured in the "Partner stations" parameter group:

- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC up to firmware V3.0
- CP 1542SP-1 IRC up to firmware V1.0

All other settings required for communication with the master station are taken from the other configuration data of the CPs and do not have to be specially configured for the connections.

Configuration in the "Network data" editor

For the following modules, configure telecontrol connections in the "Network data" editor:

- CP 1243-1 / CP 1243-8 IRC as of firmware V3.1
- CP 1243-7 LTE as of firmware V3.3
- CP 1542SP-1 IRC as of firmware V2.0
- TIM 1531 IRC as of firmware V2.0

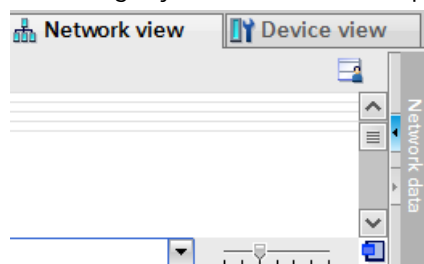
3.21.2 "Network data" editor

Opening the editor "Network data" > "TeleControl" tab

To open the editor, follow the steps below:

1. Open the network view of the project.

On the right you will find the collapsed "Network data" editor.



2. Open the "Network data" editor using the arrow symbol.

The editor is displayed with several tabs, on the left the "Network overview" tab.

3. Expand the editor until the "TeleControl" tab appears.

This tab is further divided into the following tabs:

- ST7
- DNP3
- IEC 60870

Depending on the protocol used, select the corresponding tab to configure the telecontrol connections.

Display and show/hide columns

	Connection	Starting po...	Start subs...	Start interface	Endpoint	End ...	Partner list	End interface/address
	*	*	*		*	*		
	Section_1	1	1	TIM_1 - Ethernet i...	2	2	2,3	TIM_2 - TIM_2 - Ethernet i.
	Section_2	2	2	TIM_2 - Ethernet i...	1	1	2,3	TIM_1 - TIM_1 - Ethernet i.
	Section_3	TIM_2	2	TIM_2 - Serial Inter.	3	3	1	TIM_3 - TIM_3 - Serial Inte
	Section_4	3	3	TIM_3 - Serial Inter.	1	1	1	TIM_2 - TIM_2 - Serial Inte
	Section_5	TIM_2	2	TIM_2 - Ethernet i...	1	1	3, 12	TIM_1 - TIM_1 - Ethernet i.
	Section_6	2	2	TIM_2 - Serial Inter.	3	3	3	TIM_3 - TIM_3 - Serial Inte
	Section_7	3	3	TIM_3 - Serial Inter.	2	2	2	TIM_2 - TIM_2 - Serial Inte
	Section_99	1	1	TIM_1 - Ethernet i...	Third-party device	99	99	192.168.2.99
	Section_8	1	1	TIM_1 - Ethernet i...	1200	12	12	TIM_2 - TIM_2 - Ethernet i.
	Section_9	TIM_2	2	TIM_2 - Ethernet i...	1200	12	1	S7-1200-Station_1 - CP 1..
	Section_10	1200	12	CP 1243-8 IRC - Et...	1	1	1	TIM_2 - TIM_2 - Ethernet i.

Figure 3-4 "Network data" editor, "Telecontrol > ..." tab

In the "Telecontrol connections" table, you can display or hide the columns, arrange them and optimize the column width. Right-click on a column header to access the shortcut menu.

- Arrange columns

If you click on a column header and hold down the left mouse button, you can move the column within the table.

- Show/Hide

You can show or hide individual columns using this function in the shortcut menu.

This increases the legibility of the table.

- Show all columns

Shows all columns of the table.

- Optimize width / Optimize width of all columns

You use these shortcut menus to optimize the width of the selected column or all columns in the table.

The column width adapts to the widest entry in this column.

Some fields of the table can be edited, in others you configure the parameter via a drop-down list.

Boxes with a missing or bad configuration are shown with a red background.

Names of the connections

You can adapt the default names of the connections.

A maximum of 129 characters from the following ASCII character sets (numbers decimal) are permitted:

- **No. 32..126**

Space , ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { | } ~

- **No. 128, 130..140, 142, 145..156, 158..159, 161..172**

€ , f „ ... † ‡ ^ % ¢ Š ‹ Œ Ž ‘ ’ ’ ’ ’ • — ~ ™ š › œ ž Ÿ j † £ ¤ ¥ ¦ § ¨ © ª « ¬

- **No. 174..255**

® ¯ ° ± ² ³ ´ μ , ¹ º » ¼ ½ ¾ ¿ 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

Error displays

Faulty connection points, networks or parameters are highlighted in red in the tables.

Causes of faulty connections include, for example:

- Starting point and endpoint are identical.
- The connection runs through an impermissible network.
- The connection runs through an invalid subscriber.

Delete invalid or redundant connections

If there are unauthorized or unwanted redundant connections, you must delete a connection path:

1. In the "Configured connection paths" table, select the unwanted connection path.
2. Click "Delete" in the shortcut menu.

3.21.3 Specifying connection paths

Rules for connection configuration

Note the following rules for connection configuration:

- Connections can be configured for the following networks:
 - Connections in Ethernet networks between TIM modules and CPs
 - Connections in classic WAN networks (dedicated line/dialup network) - only between TIM modules
- You can create connections between endpoints (subscribers) that are configured in the STEP 7 project.

Fields are available in the connection table for the address data and interface parameters of both endpoints.
- You can create connections between an endpoint of the STEP 7 project and a "third-party device" that is not configured in STEP 7. The third-party device is located in another IP subnet and can be reached via a network gateway.

In this case, configure the network gateway as an endpoint of the connection.

- The endpoint of a connection is always the CPU or a PC application, not the communications module.
Exception: Third-party device
- A connection segment must be created for the way there and the way back for each connection.
Example of a connection between Partner 1 and 2:
 - Connection segment 1 ⇒ 2
 - Connection segment 2 ⇒ 1
- You can configure single and redundant connections between two subscribers.
- Two connections to a partner via the same interface of a module are not allowed.
- A connection via an inconsistent network is invalid.

Example of inconsistent networks:

- A subscriber of a connection segment is connected to another telecontrol protocol.
Connections via nodes that are not configured as node stations.
Subscriber with incompatible modems
Incompatible settings of two modems in a connection
Incompatible settings between modem and network parameters

Interface-specific configuration of the connection segments

Connections between two endpoints can run over multiple subscribers.

A connection segment between two subscribers can be used for multiple connections.

Individual settings can be configured for specific connection segments and the associated interfaces of the modules. For this reason, the individual connection segments between the interfaces of two devices are displayed in separate lines in the connection table.

Connection	Starting po...	Start subs...	Start interface	Endpoint	End ...	Partner list	End interface/address
Section_1	1	1	TIM_1 - Ethernet i...	2	2	2,3	TIM_2 - TIM_2 - Ethernet i.
Section_2	2	2	TIM_2 - Ethernet i...	1	1	2,3	TIM_1 - TIM_1 - Ethernet i.
Section_3	TIM_2	2	TIM_2 - Serial Inter.	3	3	1	TIM_3 - TIM_3 - Serial Inte
Section_4	3	3	TIM_3 - Serial Inter.	1	1	1	TIM_2 - TIM_2 - Serial Inte
Section_5	TIM_2	2	TIM_2 - Ethernet i...	1	1	3, 12	TIM_1 - TIM_1 - Ethernet i.
Section_6	2	2	TIM_2 - Serial Inter.	3	3	3	TIM_3 - TIM_3 - Serial Inte
Section_7	3	3	TIM_3 - Serial Inter.	2	2	2	TIM_2 - TIM_2 - Serial Inte
Section_99	1	1	TIM_1 - Ethernet i...	Third-party device	99	99	192.168.2.99
Section_8	1	1	TIM_1 - Ethernet i...	1200	12	12	TIM_2 - TIM_2 - Ethernet i.
Section_9	TIM_2	2	TIM_2 - Ethernet i...	1200	12	1	S7-1200-Station_1 - CP 1..
Section_10	1200	12	CP 1243-8 IRC - Et...	1	1	1	TIM_2 - TIM_2 - Ethernet i.

Figure 3-5 "Network data" editor, "Telecontrol > ..." tab

Creating connections and searching for connection paths

Follow these steps to create connections:

1. Click the "Starting point" field in the next free row.

A drop-down list with the available endpoints is displayed.

The first row below the table header is reserved for entering filters; see section Connection table (Page 101).

2. Select the starting point (CPU) from the table with a double-click.

3. Click the "Endpoint" field in the same row.

Select the endpoint (CPU or PC application) from the table with a double-click.

- Special case: "Third-party device":

If you want to create a third-party device as endpoint instead of an endpoint from a STEP 7 project, leave the default entry "Third-party device" in the cell.

Configure the interface of the starting point as well as the address data and other parameters of the third-party device by means of entries in the corresponding fields.

With a third-party device as endpoint, the connection search via the dialog described below is disabled.

After an endpoint is selected from the STEP 7 project, the starting point and endpoint are displayed in the table row. The other fields are usually empty and have a red background.

Once a connection has been created, the actual course of the connection is not always defined yet. Especially with larger networks, several connection paths are often possible.

To facilitate searching the connection path, the search function is available via the "Add new connection path" icon:



4. Leave the table row with the selected starting point and endpoint highlighted and click on the "Add new connection path" icon.

The dialog for defining connection paths opens:

Dialog "Add connection paths"

The possible connection paths are searched for automatically, which is indicated by the progress bar at the bottom of the dialog.

- The status and result of the search are displayed in the "Information" field below.
- The connection paths found are displayed in the "Select a connection path ..." upper table.
- Details for a selected connection path are shown in the "Connection path" table.
- When selecting a connection path, the "Preview" table shows which connection points of the selected connection path are transferred to the connection editor when you click "Add".

5. Select the desired connection path(s).

- If one or more connection paths are displayed in the upper table, select the desired connection path and click on "Add".

"Information" shows whether the connection path has been added or whether it has already been configured.

- If you want to use a redundant connection, select a second path and click on "Add".

Close the dialog using the "Close" button if the added connection paths correspond to the project defaults.







- If no connection is displayed in the table, there is a configuration error in the corresponding stations or networks.

In this case, close the dialog with the "Close" button and complete the configuration.

The "Connection path" table supports you in checking the connection paths. For every configured connection, the detailed connection path is shown here.

A station symbol with an identifier for the connection point is displayed in the "Position" column. The color of the identifier indicates the validity of the connection point:

- Blue: Valid connection point
- Red: Invalid connection point

Icon	Meaning
	Starting point
	Node-input
	Node-output
	Endpoint
 	Examples of invalid connection points

Parameters of the connection table

Here, you configure the parameters of the connection table for each connection segment. You can find the description of the parameters in the section Connection table (Page 101).

The "Properties" tab, which shows additional parameters for each connection segment, is displayed below the connection table.

"Properties" tab of the connections

In the parameter groups, you can check the connection segment, correct it if necessary and configure additional properties.

You can find a description of the parameter groups in the section Parameters of IEC connections (Page 104).

3.21.4 Connection table

Filter

The first row below the table header contains a filter function with which you can restrict the selection of configurable subscribers and connection options. Using filters reduces the number of combination possibilities and increases the clarity.

Once you have created some connection segments, enable the filter by entering a recurring name or partial name in the filter cell. The cell is given a colored background, see figure.

	Connection	Starting po...	Start subs...	Start interface	Endpoint	End ...	Partner list
	*	1	*		*	*	
	Section_1	1	1	TIM_1 - Ethernet interfac..	2	2,3	
	Section_99	1	1	TIM_1 - Ethernet interfac..	Third-party device	99	99
	Section_8	1	1	TIM_1 - Ethernet interfac..	1200	12	12
	Section_10	1200	12	CP 1243-8 IRC - Ether..	1	1	1

Figure 3-6 Connection table

The filter "1" is set in the "Starting point" column.

Example:

You have created connections with the starting points "1200", "1" and "2".

When "1" is entered in the filter cell, only the segments whose starting points start with this partial string are shown: "1" and "1200"

Filters set in multiple columns multiply.

The selection "*" shows all existing connection segments.

The filter icon on the left in the first row () shows or hides an existing filter.

The filter can be applied to all columns with an asterisk (*) in the first cell.

Note:

If you have created connections and set a filter, you cannot create any new connections. You need to reset the filter first in order to create new connections.

Parameters

If parameters are already used by the configuration, the values are transferred to the respective columns.

- **Name**

You can change the default name of the connection segment between two subscribers.

See section "Network data" editor (Page 95) for information on this.

- **Starting point**

Select the desired starting point of the connection from the drop-down list.

– The starting point of a connection is a CPU.

- **Start subscriber**

Station address of the starting point

- **Start interface**

Interface of the starting point module through which the connection runs.

- **Endpoint**

Select the endpoint of the connection.

Endpoints of a connection can be:

- A CPU
- A third-party device

The network node type of third-party devices is configured in the properties dialog of the connection, see section Third-party device parameters (Page 111).

Note

Changing the endpoint

If you retroactively change the endpoint of a connection, the new connection segments are added when searching for the connection path.

Note that the segments of the previous connection are retained. You need to delete these yourself.

- **End subscriber**

Station address of the endpoint

- **Partner list**

When a partner (endpoint) is selected that is located in the STEP 7 project, its station address is automatically found during the connection search and entered in the partner list.

In connection segments used for multiple connections, the station address of all destination subscribers is entered.

Note

Manual entry for third-party device

For a third-party device that is not configured in the STEP 7 project, you must enter the station address manually.

The station addresses are entered separated by commas.

- **End interface/address**

Interface of the endpoint module through which the connection runs.

For a third-party device that is not configured in the STEP 7 project, you must enter the IP address (Ethernet) or the telephone number (dial-up network) of the partner manually.

- **End port**

Relevant for third-party device (master / station)

Number of the listener port of the partner

For modules of the STEP 7 project, the value is taken from the configuration. It can be changed.

You need to enter the port number for a third-party device.

Range of values: 0 ... 65535

Default: 2404

- **Partner monitoring time**

Relevant for all subscriber types

If the station module does not receive a sign of life from the master on the application layer within the configured time, it classifies the connection as disrupted and terminates it.

After sending data, the master module expects a response from the station within the configured time.

Note

Redundant connection paths

If you configure redundant connection paths between two partners, configure the same time for both paths.

Range of values: 0 ... 65535

With the setting 0 (zero), the function is disabled.

- **Spontaneous**

The parameter for the transmission mode determines whether ASDUs (events) of the station may be sent spontaneously over this connection segment.

Range of values:

- Yes

The module can send spontaneous ASDUs (cause of transmission <3>).

- No

The module does not send spontaneous ASDUs.

Default: Yes

Note

Collisions on full duplex dedicated lines

If you connect a serial interface to a dedicated line with the "half-duplex" connection type, you must disable Unsolicited transfer.

To avoid collisions, you should also disable Unsolicited transfer when connecting to full duplex multidrop dedicated lines.

- **Polling mode**

Relevant for master, third-party device (master)

This is where you define the mode in which the master station calls the station.

The value configured for the station is transferred to the master station and stored there.

Ranges of values:

- Cyclic

The station is called cyclically. The duration of the polling cycle is calculated from the "Class 0 polling interval" parameter, see above.

- After startup

The station is only called after the initial startup and after a restart.

If no unsolicited transmission is enabled for a station, no data is transmitted during operation when this option is selected.

- **Temporary**

Partners with enabled "Temporary" option are classified as "accessible" if they terminate the connection themselves (e.g. RTU3000C).

Parameters for redundant connection paths

If redundant connection paths are configured, these are configured in the same way as the main paths.

The parameters of the redundant connection paths are distinguished by the following suffix:

- *** (red)**

The parameters of the redundant connection paths have the same functions as those for the main path. See above for the meaning.

Examples:

- **Start interface (red.)**

Interface of the starting point module through which the redundant connection runs.

- **End interface (red.)**

Interface of the endpoint module through which the redundant connection runs.

3.21.5 Parameters of IEC connections

3.21.5.1 General

If you select a connection in the "Telecontrol connections" table in the "Network data" editor, additional parameter groups for this connection are displayed in the "Properties" tab of the Inspector window.

In the parameter groups, you can check the connection, correct it if necessary and configure additional properties.

General

- **Connection**
Shows the name of the connection and the protocol.
You can also change the connection name here.
- **Connection points**
Shows the most important parameters of the connection.
You can also change the station address of a third-party device here.

3.21.5.2 TCP connection monitoring

Ethernet interface > Advanced options > TCP connection monitoring

The settings of the two parameters at the Ethernet interface govern TCP connections via this interface.

You can adapt the parameters in the properties of the telecontrol connections for each connection segment.

- **TCP connection monitoring time**
Function: If no data traffic takes place within the TCP connection monitoring time, the module sends a keepalive frame to the communication partner.
With the setting 0 (zero), the function is disabled.
Default setting: 180 s
Permitted range
 - TIM 1531 IRC
1...65535 s
 - CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
 - CP 1542SP-1 IRC
0...32767 s

- **TCP keepalive timeout**

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

With the setting 0 (zero), the function is disabled.

Default setting: 10 s

Permitted range

- TIM 1531 IRC
1...65535 s
- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC
0...65535 s
- CP 1542SP-1 IRC
0...32767 s

If you have configured a redundant connection to a partner, the parameters can be set separately for both connection paths.

3.21.5.3 IEC 60870-5 security options

Secure Authentication

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

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

- Key exchange interval
- Authentication requests before key exchange

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

Parameters

- **Enable IEC security options**

Select the option if you want to use Secure Authentication.

Note:

Make sure that you enable the option for all connections of the module that are to use this function.

- **Security statistics**

Specifies whether the statistics of security events are sent to the master. Security events are authentication requests of the master to the station module. If this option is activated, all authentication requests are stored in the station module with date, time and result and sent to the master for further evaluation.

Security statistics events are only output if a SCADA system is connected to the master.

Range of values:

- Do not send security statistics
- Send security statistics

When this option is enabled, the statistics parameters that can be selected are released for configuration under the table.

Default setting: Do not send security statistics

- **Secure hash algorithm (SHA)**

Selection of the Secure Hash Algorithm (SHA)

Range of values:

- SHA-256

- **Key length**

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

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

- 32 bytes

- **Max. number of key status queries**

If the number of key status queries of a master configured here is exceeded within the key exchange interval, the module notifies all other connected master stations. The master station from which the queries were sent is not notified.

The module enters a message in the diagnostic buffer of the CPU.

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

- **Authentication requests before key exchange**

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

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

Recommendation: Set the number for the station module twice as high as for the master.

- **Key exchange interval**

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

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

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

- **Authentication timeouts**

Maximum wait time of the module after an authentication request to the master. If the waiting time for the response from the master is exceeded, the module generates a security event and sends this to the master.

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

- **Authentication and data length for key status challenge**

Data length (CLN) of an authentication Challenge or session key status Challenge

Range of values: 1... 65535 s. Default setting: 4

- **Max. number of authentication failures**

Maximum number of authentication failures before the Challenger sends an error message and the session key is changed.

Range of values: 1... 65535 s. Default setting: 25

- **Max. number of sent error messages**

Maximum number of sent error messages. When the configured number is reached, the station stops the sending of error messages.

Range of values: 1... 65535 s. Default setting: 100

- **Max. number of key changes**

Maximum number of session key changes due to authentication failures. When the configured number is reached, session key changes due to authentication failures are stopped until the session key is generated for another reason.

Range of values: 1... 65535 s. Default setting: 50

- **Max. number of response timeouts**

For the master: Maximum number of response timeouts

When the configured value is reached, the master aborts the current action.

Range of values: 1... 65535 s. Default setting: 20

- **Max. number of key changes due to restart**

For the master: Maximum number of key exchanges due to station restart

When the configured value is reached, the master sends no more session keys to the station until the next key change timeout.

Range of values: 1... 65535 s. Default setting: 20

- **Pre-shared key**

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

- Manual configuration

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

- Import as file

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

The pre-shared key of a station module must be identical to the pre-shared key of the master.

See also

Security statistics options (IEC 60870-5-104) (Page 109)

3.21.5.4 Security statistics options (IEC 60870-5-104)

Security statistics (IEC 60870-5-104)

The statistics parameters are released for configuration when the "Send security statistics" option in the "Security basic options" is enabled.

The following table contains those security statistics options according to IEC/TS 60870-5-7 and IEC/TS 62351-5 that you can configure for the individual telecontrol connection segments.

When the options are enabled, the communications module as station sends security statistics events to the master, where they are available for further evaluation. Based on the frequency of these events, you can reach conclusions on possible attacks or vulnerabilities of your system.

Security statistics events are only output if a SCADA system is connected to the master.

Security statistics options

When Secure Authentication is used, a station keeps statistics for different values.

The events are transferred via the ASDU type "Information 41" (integrated total for the statistic).

The following table lists the statistics parameters supported by the module according to IEC/TS 62351-5.

- Threshold

A threshold value can be configured for each statistics value. When this threshold is exceeded, transfer as event to the partner is triggered.

The range of values is 0...65535.

With the setting 0 (zero), the function is disabled. No statistics data is transferred for the value in question.

- IOA

You need to assign an IOA (IOA - Information object address) to each value in the statistics via the configuration.

The range of values is 0...16777215.

For the critical frames, you can configure under the table which ASDU types should be classified as critical.

Parameter	Default
Unexpected messages threshold	3
Unexpected messages (IOA)	0
Authorization failures threshold	5
Authorization failures (IOA)	0
Authorization failures (IOA)	5
Authentication failures (IOA)	0
Response timeout threshold	3
Response timeouts (IOA)	0
Key changes due to authentication failure threshold	3
Key changes due to authentication failure (IOA)	0
Sent messages threshold (total)	100
Total number of sent messages (IOA)	0
Received messages threshold (total)	100
Total number of received messages (IOA)	0
Sent critical messages threshold	100
Sent critical messages (IOA)	0
Received critical messages threshold	100
Received critical messages (IOA)	0
Discarded messages threshold	10
Discarded messages (IOA)	0
Sent error messages threshold	10
Sent error messages (IOA)	0
Received error messages threshold	10
Received error messages (IOA)	0
Successful authentications threshold	100
Successful authentications threshold	0
Session key changes threshold	10
Session key changes (IOA)	0
Failed session key changes threshold	5
Failed session key changes (IOA)	0

3.21.5.5 Query options

The following parameters can be found in the parameter groups "Options 1st Path" / "Options 2nd Path" of the IEC connections.

Call intervals

The following parameters define the intervals of special calls of the master for the station (cause of transmission 20 - 41).

All parameters are configured as multiples of the "Polling basic interval", see section Settings IEC master (Page 57).

- **Interval for general request**
Defines the interval with which general requests of the master are answered.
- **Interval for group request**
Defines the interval with which the respective group request of the master is answered.
- **Interval for counter general request**
Defines the interval with which counter general requests of the master are answered.
- **Interval for counter group request**
Defines the interval with which the respective counter group request of the master is answered.

You define the setting as to whether a general request is answered and the assignment to a group request for each individual data point in the data point configuration.

3.21.5.6 Third-party device parameters

Third-party device parameters

Only valid for partners that are not configured in the STEP 7 project.

- **Partner station address / Station address (red.)**
Station address (ASDU address) of the third-party device, that is accessible via a connection or a redundant connection path.
- **Network node type third-party device / Network node type third-party device (red.)**
Define the network node type of the third-party device that is accessible via a connection or a redundant connection path:
 - Master station
(Master)
 - Node station
For modules that act as a node station, the following applies:
The interface in the direction of the master station is configured as a "node station".
The interface in the direction of the lower-level network is configured as a "Master station".
 - Station

3.22 Data points

3.22.1 Data point configuration

Data point-related communication with the CPU

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

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

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

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



WARNING

Writing values to outputs

- PLC tags
When referencing to PLC tags, note that the values are written immediately to the outputs of the CPU without first being processed by the user program with write access. Writing values has a direct influence on the process.
- DB variables
When referencing to DB variables, written values are only used when processed by the user program.

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

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

Note

Number of PLC tags

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

The formats and S7 data types of the PLC tags that are compatible with the data point types of the modules can be found in the section Datapoint types (Page 119).

Access to the memory areas of the CPU

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

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

Configuring the data points and messages in STEP 7

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

- Selecting the communications module
Shortcut menu "Open the data point and messages editor"
- Via the project navigation:
Project > directory of the relevant station > Local modules > required communications module

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

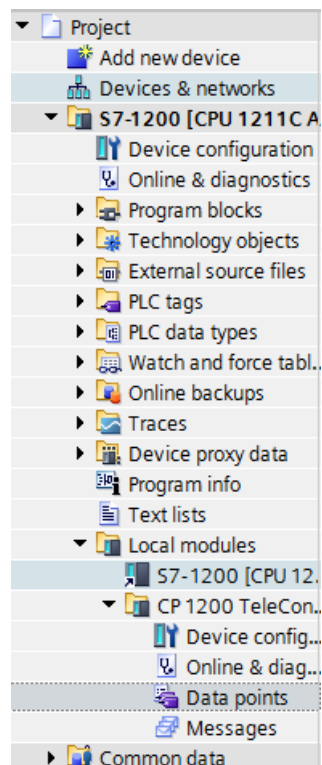


Figure 3-7 Configuring data points and messages

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



Figure 3-8 Switching over between the two editors

Creating objects

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

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

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



Figure 3-9 Data point table

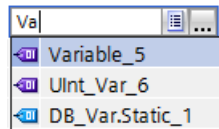
You configure the remaining properties of every object using the drop-down lists of the other table columns and using the parameter boxes shown at the bottom of the screen.

Assigning data points to their data source

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

For the assignment you have the following options:

- Click on the table symbol  in the cell of the "PLC tag" column.
All configured PLC tags and the tags of the created data blocks are displayed. Select the required data source with the mouse or keyboard.
- Click the symbol .
A selection list of the configured PLC Tags and the blocks is displayed. From the relevant table, select the required data source.
- In the name box of the PLC tag, enter part of the name of the required data source.
All configured PLC tags and tags of the data blocks whose names contain the letters you have entered are displayed.



Select the required data source.

Note

Assignment of parameter values to PLC tags

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

Arranging columns and rows, showing/hiding columns

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

- Arrange columns

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

- Sorting objects

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

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

- Adapting the column width

You can reach this function with the following actions:

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

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

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



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

- Showing / hiding columns

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

Copying data points and messages

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

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

- Cut
- Copy
- Paste

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

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

- Delete

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

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

Exporting and importing data points

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

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

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

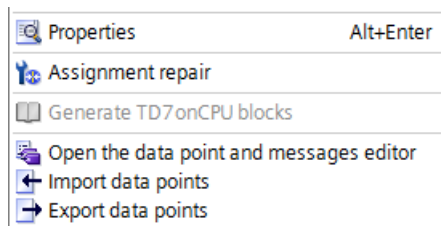


Figure 3-10 Shortcut menu of the module

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

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

Export

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

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

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

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

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

Editing the export files

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

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

The lines of the CSV file have the following content:

- Line 1: ,Name,Type,
This line must not be changed.
- Line 2: PLC,<CPU name>, <CPU type>,
Meaning: PLC (designation of the station class), CPU name, CPU type
Only the elements <CPU name> and <CPU type> may be changed.
The CPU type must correspond exactly to the name of the CPU in the catalog.
- Line 3: Module,<module name>,<module type>,
Meaning: Module (Designation of the module class), module type, module name
Only the elements <module name> and <module type> may be changed.
Be careful when changing the module names if you want to import data points into several modules (see below).
The module type must correspond exactly to the name of the module in the catalog.
- Line 4: Parameter names (English) of the data points
This line must not be changed.
- Lines 5..n: Values of the parameters according to line 4 of the individual data points
You can change the parameter values for the particular station.

Importing into a module

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

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

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

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

When you import data points into a module, but some required PLC tags have not yet been created in the CPU, the corresponding data point information cannot be assigned. In this

case, you can subsequently create missing PLC tags and then assign them the imported data point information. The "Assignment repair" function is available for this (see below).

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

Importing into several modules

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

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

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

Restrictions for the import of data points

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


- An attribute required by the module is missing in the CSV file to be imported.
Example: If a data point to be imported uses a time trigger, the import will be aborted if no time-of-day synchronization was configured for the module.
- The telecontrol protocol used by the module differs from that of the original module.
Modules with the same telecontrol protocol are compatible with each other:

Only when importing into several modules:

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

Assignment repair

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

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

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

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

3.22.2 Datapoint types

During the configuration of the user data to be transferred, each data point is assigned to a data point type.

Afterwards the protocol-specific data point types along with the compatible S7 data types are listed.

The "Direction" column shows the transmission direction:

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

With the ST7 protocol the transmission direction can be read from the object name.

Note

Effect of the change of arrays for data points

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

Data point types of the "IEC 60870-5" protocol

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

Format (memory requirements)	Data point type	IEC type	Direction	S7 data types	Operand area
Bit	Single-point information	<1>	in	Bool	I, Q, M, DB
	Single-point information with time tag CP56Time2a ¹⁾	<30>	in	Bool	I, Q, M, DB
	Single command	<45> ⁴⁾	out	Bool	Q, M, DB
	Single command with time tag CP56Time2a ¹⁾	<58> ^{5) 6)}	out	Bool	Q, M, DB
	Double command with time tag CP56Time2a ¹⁾	<59>	out	Bool	DB ²⁾
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag CP56Time2a ¹⁾	<32>	in	Byte, USInt	I, Q, M, DB
	Regulating step command with time tag CP56Time2a ¹⁾	<60>	out	Byte, USInt	DB ²⁾
Integer (16 bits)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag CP56Time2a ¹⁾	<34>	in	Int	I, Q, M, DB
	Measured value, scaled value	<11>	in	Int	I, Q, M, DB
	Measured value, scaled value with time tag CP56Time2a ¹⁾	<35>	in	Int	I, Q, M, DB
	Set point command, normalized value	<48> ⁴⁾	out	Int	Q, M, DB
	Set point command, scaled value	<49> ⁴⁾	out	Int	Q, M, DB
	Set point command, normalized value with time tag CP56Time2a ¹⁾	<61> ⁵⁾	out	Int	Q, M, DB
	Set point command, scaled value with time tag CP56Time2a ¹⁾	<62> ⁵⁾	out	Int	Q, M, DB

Format (memory requirements)	Data point type	IEC type	Direction	S7 data types	Operand area
Integer (32 bits)	Bitstring of 32 bits	<7>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a ¹⁾	<33>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals	<15>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals with time tag CP56Time2a ¹⁾	<37>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits	<51> ⁴⁾	out	UDInt, DWord	Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a - control direction ¹⁾	<64> ⁵⁾	out	UDInt, DWord	Q, M, DB
Floating-point number (32 bits)	Measured value, short floating point number	<13>	in	Real	Q, M, DB
	Measured value, short floating point number with time tag CP56Time2a ¹⁾	<36>	in	Real	Q, M, DB
	Set point command, short floating point number	<50> ⁴⁾	out	Real	Q, M, DB
	Set point command, short floating point with time tag CP56Time2a ¹⁾	<63> ⁵⁾	out	Real	Q, M, DB
Data block (1...2 Bit) ²⁾	Double-point information	<3>	in	ARRAY [0...1] of Bool	DB
	Double-point information with time tag CP56Time2a ¹⁾	<31>	in	ARRAY [0...1] of Bool	DB
	Double command	<46> ⁴⁾	out	ARRAY [0...1] of Bool	DB
	Regulating step command	<47> ⁴⁾	out	ARRAY [0...1] of Bool	DB
	Double command with time tag CP56Time2a ¹⁾	<59> ^{5) 6)}	out	ARRAY [0...1] of Bool	DB
	Regulating step command with time tag CP56Time2a ¹⁾	<60> ^{5) 6)}	out	ARRAY [0...1] of Bool	DB
Data block (1...32 Bit) ³⁾	Bitstring of 32 bits ³⁾	<7>	in	³⁾	DB
	Bitstring of 32 bits with time tag CP56Time2a ^{1) 3)}	<33>	in	³⁾	DB
	Bitstring of 32 bits ³⁾	<51> ⁴⁾	out	³⁾	DB
	Bitstring of 32 bits with time tag CP56Time2a - control direction ^{1) 3)}	<64> ⁵⁾	out	³⁾	DB

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

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

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

⁴⁾ For IEC 60870-5-104, these IEC types can be configured as an alternative to those with footnote ⁵⁾, but it is not possible to mix the two IEC types.

⁵⁾ These IEC types are only supported by IEC 60870-5-104.

⁶⁾ You configure the "Max. command lifetime" of the commands in the "Basic settings" parameter group of the modules.

Mirroring with Single Command

For the following commands, you can activate mirroring of the current value in the station to the master:

- Single Command <45>

The local value of this data point can be monitored for changes and transferred to the master when changed. A change to a local value can be caused by manual operator input on site, for example.

To allow the value resulting from local events or interventions to be transferred to the master, the data point in question requires a channel for mirroring back. For this, a second data point "Single-point information <1>" is required. Follow the steps below to configure the mirroring function.

Create the data points:

- In the master module
 - Single Command <45>
 - Single-point information <1>

On the master, you need to write the mirrored value into a variable. Therefore, assign the two data points to different variables in the master module.

Assign the same index for both data points.

- In the station module
 - Single Command <45>
 - Single-point information <1>

In the station module, assign the two data points to the same variable.

Assign the same index for both data points.

The value mirrored by the station is written to the "Single-point information <1>" data point type on the master.

Time stamp of the data with the IEC protocol

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

3.22.3 Status IDs of the data points

Status identifiers

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

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

Quality descriptor - IEC 60870-5

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

Quality descriptor - IEC 60870 Part 5-101

Table 3- 5 Bit assignment of the status byte

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

3.22.4 "General" tab

Data point table

You will find the most important parameters in the first tab of the data point editor in the default setting of the data point table.

If you hover over the title bar of the data point table with the mouse, you can display all parameters of the data point configuration via the shortcut menu.

General

Parameters:

- **Name**
Unique name of the data point
- **PLC tag**
For the assignment, see section Data point configuration (Page 112).
- **Data point type**
See section Datapoint types (Page 119)
- **Data point index**
See section Data point index (Page 124)
- **Master function**
Enables the master function of the data point.
For the meaning, refer to section Master function of the data points (Page 123).

- **Type of transmission**
For the type of transmission, see section Process image, type of transmission, event classes (Page 126).
- **Read cycle**
Only for inputs
For the read cycle, see section Read cycle (Page 128).
- **Response to general request**
Enables the data point for the response to a general request. If the function is disabled, the value of the data point is not sent to the communications partner following a general request.
- **Assignment to group request**
Assigns the data point to a group request.
For group queries of the master to the respective group, the value of the data point is sent to the master.

3.22.5 Master function of the data points

The master function for direct communication

Direct communication between two telecontrol stations, in which the frames are not transmitted by a master station, is enabled by activating the master function of the data points.

Requirements

Requirements for configuring direct communication between two data points of two partners are:

- A telecontrol connection must be created between the two partners.
- The "Unsolicited" option is selected in the telecontrol connection.
- The data point must be assigned to a partner.

Configuration in the "Partner of data point" column of the data point table.

Meaning of the master function

- **"Master function" enabled**

The values of the data point are handled in the same way as with a master:

- **Input data points (direction "in")**

Input data points are received by the partner according to the parameters set at the partner.

The "Transfer after call" type of transfer is set permanently.

The options for "Analog value preprocessing" are disabled.

- **Output data points (direction "out")**

Output data points are sent to the partner according to the trigger configuration.

The "Every value triggered" type of transfer is set permanently.

To activate the option, refer to section "General" tab (Page 122).

- **"Master function" disabled**

- **Input data points (direction "in")**

Input data points are handled according to the configuration.

The type of transfer and the options for "Analog value preprocessing" can be freely configured.

- **Output data points (direction "out")**

Output data points are handled according to the configuration.

The "Transfer after call" type of transfer is selected automatically and cannot be changed.

3.22.6 Data point index

The index of a data point is the Information object address.

On the program side, the indexes are in ascending order by default when the data points are created. You can configure the indexes according to your requirements and the following rules.

Configuration of the data point index

Structured addressing

The index can be configured in two input fields with different formats:

- Data point index

The index is configured unstructured here as an integer.

Range of values: 1..16777215

- Structured index

You can configure the index structured according to IEC 60870-5-3 here. Plant-based structuring of the data points is enabled by structured addressing.

Three address levels (octets) can be configured.

Range of values: 0.0.1..255.255.255

The configured values of the two fields are linked. A configured value is converted and displayed in the other input field.

Conversion of configured values

The values are designated as follows for the conversion:

- Data point index

Designation of the integer value: X

- Structured index

Designation of the values of the 3rd octet: A.B.C

The configured value is applied to the other field according to the following formula:

$$X = A * 256 * 256 + B * 256 + C$$

Configuration rules

The following rules apply to configuring the data point index.

- The indexes per communications partner must be unique in a module.

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

- The indexes of two data points can be identical if the two data points are configured for different partners.

Example:

- Data point 1, index 1, partner 1
- Data point 2, index 1, partner 2
- Data point 3, index 2, partner 1
- Data point 4, index 2, partner 7

- The corresponding partner indexes must be identical at the send and receive ends.

Index and "sequential transfer"

Validity:

- Modules
 - CP 1243-7 LTE
 - TIM 1531 IRC
- Network node type of the interface for telecontrol communication: Station or node station
- Parameter group: Interface > Advanced options > Settings IEC station > Event settings > Transfer behavior

The joint transfer of event frames in one sequence can be configured for data points without time stamp.

The following requirements must be met for the sequential transfer:

- The data points are of the same type.
- The indexes of the data points are in sequence without gaps.

3.22.7 Process image, type of transmission, event classes

Storage of values

As a rule the values of all data points are stored in the image memory of the module. Values in the image memory are transferred only after being called by master station TIM.

Events are also stored in the send buffer and can be transferred unsolicited.

The image memory, the process image of the module

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

The values are sent only after a query by the communications partner - see below "Transfer after call" in the "Types of transmission" section - or along with a message from the send buffer that needs to be transferred immediately.

The send buffer

The send buffer of the TIM is the memory for the individual values of data points that are configured as an event. You will find the size of the send buffer in the manual of the relevant module.

The capacity of the send buffer is divided up equally for all enabled partners.

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

If a frame was transferred to the communications partner, the transferred value is deleted from the send buffer.

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

- If the send buffer reaches a fill level of 80%, a warning message is output.
- If the fill level of the send buffer reaches 100%, no more values are saved until the fill level falls below 100% again.

Saving the data point values

As a rule, the values of data points are stored in the image memory of the module and transferred only when queried by the communications partner.

Events are also stored in the send buffer and can be transferred unsolicited.

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

- **Static value (no event)**

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

Static values correspond to the following type of transmission "Transfer after call (class 0)".

- **Event**

The values of data points configured as an event (triggered type of transmission) are also entered in the image memory of the module. The values are also entered in the send buffer.

Types of transmission and event classes

The following types of transmission are possible:

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

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

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

For output data points, this option is the default setting and cannot be changed.

- **Triggered**

Data points are configured as an event using a triggered type of transmission. The values of these data points are entered in the image memory and also in the send buffer.

The values of an event are saved as soon as the configured trigger conditions are met.

The following event classes are available:

- **Every value triggered**

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

- **Current value triggered**

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

For information on the different trigger types, see section "Trigger" tab (Page 129).

3.22.8 Read cycle

Input data points are assigned to the read cycle of the CPU in the data point configuration in the "General > Read cycle" tab.

Structure of the CPU scan cycle

The cycle with which the transferring module (TIM) scans the memory area of the CPU is made up of the following phases:

- **High-priority read jobs**

- (Fast cycle)**

- For all data points with the assignment "Fast cycle" the PLC tags are read in every scan cycle.

- As a rule, it is sufficient to assign only data to be acquired quickly, such as alarms and contact changeover messages as well as command, setpoint and parameter objects for the 1oon check, to the fast cycle.

- For information on the 1oon check, see the Glossary.

- **Write jobs**

- In every cycle, the values of a certain number of unsolicited write jobs are written to the CPU.

- The number of tags written per cycle is specified for the transferring module in the "Communication with the CPU" parameter group with the "Max. number of write jobs" parameter. The tags whose number exceeds this value are then written in the next or one of the following cycles.

- **Low-priority read jobs - proportion**

- (Normal cycle)**

- For data points with the assignment "Normal cycle", a proportion of the values of their PLC tags is read in every scan cycle.

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

- **Cycle idle time**

This waiting time between two scan cycles is used to reserve adequate time for other processes that access the CPU.

3.22.9 "Trigger" tab

Trigger

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

Saving the value of a data point configured as an event

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

- **Threshold value trigger**

The value of the data point is saved when this reaches a certain threshold. The threshold is calculated as the difference compared with the last stored value, refer to the section Threshold value trigger (Page 131).

- **Time trigger**

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

- **Event trigger (Trigger tag)**

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

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

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

Note

Fast setting of triggers

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

Note

Hardware trigger

You need to reset hardware triggers via the user program

Transmission time

Whether the value of an event is transmitted to the communication partner immediately after activating the trigger or with a delay depends on whether spontaneous sending or asymmetric communication is possible in the network.

You set the spontaneous transfer of events in the "Network data" editor of the telecontrol connections for each connection segment using the "Spontaneous" parameter.

Enable archiving

Only configurable with: TIM 1531 IRC

The option enables the values of events to be saved retentively on an SD card in addition to in the send buffer in the event of connection problems.

The function is supported for data points in the observation direction of the following information object classes:

- Single-point information
- Double-point information
- Step position information
- Measured value
- Integrated totals
- Bitstring

For information on activation and on the options for retentive saving, see section Basic settings (Page 34).

Archiving is possible for the following data point types:

- ST7
 - Bin04B_S / Bin08X_S
 - Ana04W_S / Ana04R_S
 - Mean04W_S
 - Cnt01D_S / Cnt04D_S
 - Dat12D_S / Dat12x1D_S
 - Cmd01B_S / Cmd08X_S
 - Set01W_S
 - Par12D_S / Par12x1D_S
- DNP3
 - Binary Input Event (2)
 - Counter Input Event (22)
 - Analog Input Event (32)
 - Octet String Event (111)

- IEC 60870-5
 - Information objects <1/5/30/32>
 - Measured value <9/11/13/34/35/36>
 - Integrated totals <15/37>
 - Bitstring <7/33>

Station state events

Only configurable with TIM 1531 IRC and data point type "Single-point information" (1 / 45)

- **Station state event type**

Select the event at which the station sends frames to the defined partner. The frame is transferred together with the object number.

- No station state event
- Status of local CPU changed
- Connection status to local CPU changed
- Connection status to substation changed
- SD card error

- **Substation address**

When selecting the option "Connection status to substation changed", enter the station address of the substation whose connection status has changed.

3.22.10 Threshold value trigger

Note

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

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

Smoothing factors and any configured integration interval are taken into account in the calculation.

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

Note

Threshold value trigger with configured mean value generation

With enabled mean value generation, the absolute method for the calculation of the threshold value deviation is used for analog values with the threshold value trigger.

For the time sequence of the analog value preprocessing refer to the section Analog value preprocessing (Page 133).

Threshold value trigger

Function

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

Two methods are used to calculate the threshold value deviation:

- **Absolute method**

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

- **Integrative method**

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

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

The application of the integrative method to analog values can be switched off via the "Integration interval" (Analog value preprocessing).

Absolute method

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

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

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

Integrative method

The integration threshold value calculation works with a cyclic comparison of the integrated current value with the last stored value. The calculation cycle in which the two values are compared is configurable; see "Integration interval" in section Analog value preprocessing (Page 133).

(Note: The calculation cycle must not be confused with the scan cycle of the CPU memory areas).

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

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

Table 3- 6 Example of the integration calculation of a threshold value configured with 2.0

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

With the change in the process value shown in the example, the threshold value trigger configured with 2.0 is initiated twice:

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

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

3.22.11 Analog value preprocessing

The TIM supports analog value preprocessing. For analog value data points, some or all of the functions described below can be configured.

Requirements and restrictions

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

Note

Restrictions due to configured triggers

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

Sequence of the analog value preprocessing options

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

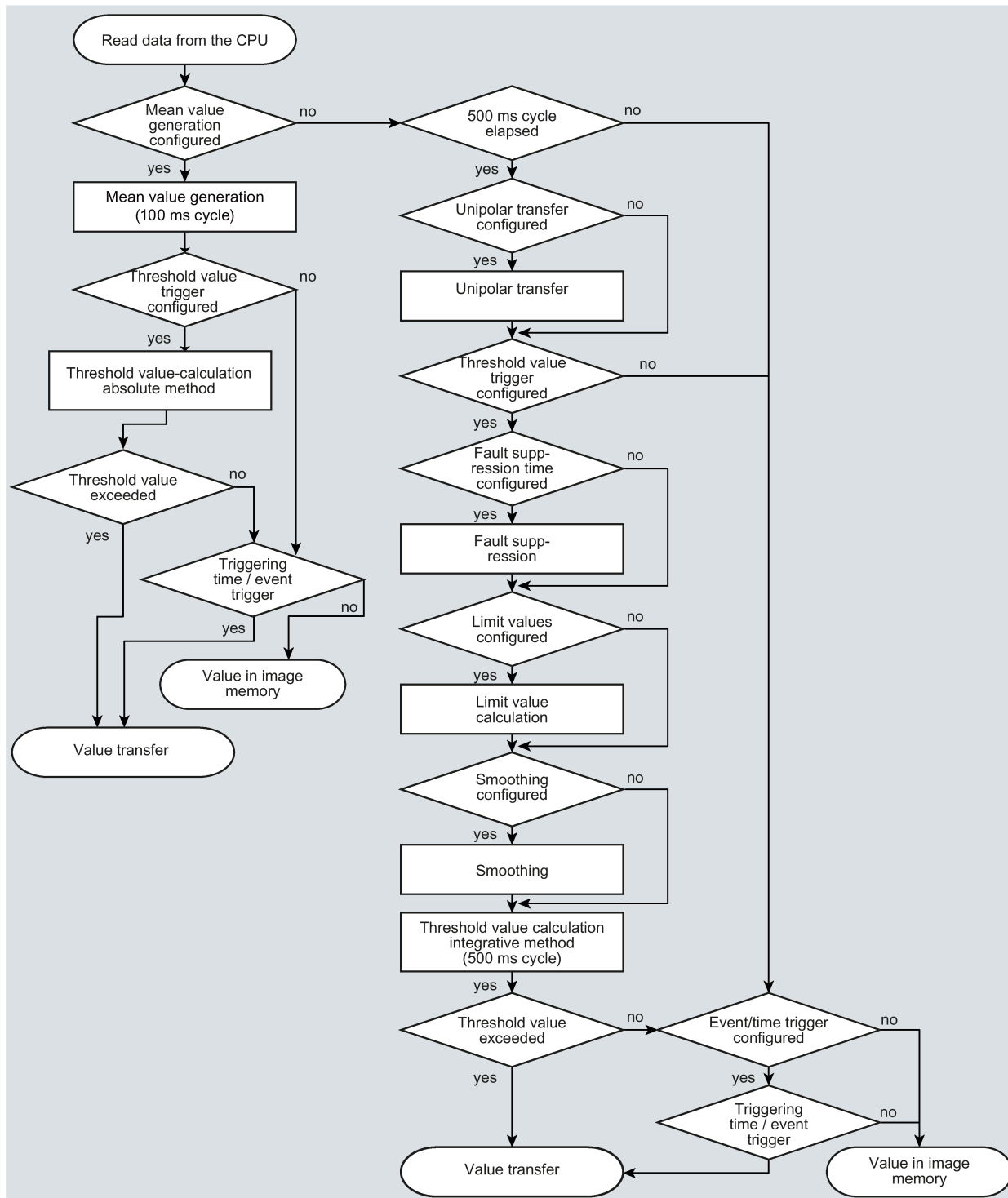


Figure 3-11 Sequence of the analog value preprocessing

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

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

Mean value generation

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

For the following protocols, mean value generation is only supported for integers of type "Int":

- TeleControl Basic
- DNP3
- IEC 60870-5

Note

Restricted preprocessing options if mean value generation is configured

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

- Unipolar transfer
 - Fault suppression time
 - Smoothing
 - Threshold value calculation only with the absolute method
-

Function

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

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

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

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

Input modules: Overflow range / underflow range

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

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

Note

Fault suppression time > 0 configured

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

Unipolar transfer

Restrictions

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

Function

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

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

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

Fault suppression time

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

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

Function

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

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

If the value returns to the measuring range before the fault suppression time elapses, the current value is transferred.

Input modules

The suppression is adjusted to analog values that are acquired directly by the S7 analog input modules as raw values. These modules return the specified values for the overflow or underflow range for all input ranges (also for live zero inputs).

An analog value in the overflow range (32767 / 7FFF_h) or underflow range (-32768 / 8000_h) is not transferred for the duration of the fault suppression time. This also applies to live zero inputs. The value in the overflow/underflow range is only sent after the fault suppression time has elapsed, if it is still pending.

Recommendation for finished values that were preprocessed by the CPU:

If the CPU makes preprocessed finished values available in bit memory or in a data block, suppression is only possible or useful if these finished values also adopt the values listed above 32767 / 7FFF_h or -32768 / 8000_h in the overflow or underflow range. If this is not the case, the parameter should not be configured for preprocessed values.

For finished values preprocess in the CPU, the limits for the overflow and underflow can be freely assigned.

Integration interval

The integration interval is used for threshold value processing of analog values according to the integration principle. The threshold value is used for the threshold value trigger; see also section Threshold value trigger (Page 131).

The entered value determines the time interval in which analog values are integrated.

With the setting 0 (zero), the threshold value is calculated without integration. This means lower data volume. In this case, the absolute method is used.

Smoothing factor

Requirements for the function

Configuration of the threshold trigger for this data point

Restrictions

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

Function

Analog values that fluctuate quickly can be evened out using the smoothing function.

The smoothing factors are calculated according to the following formula as with S7 analog input modules.

$$y_n = \frac{x_n + (k - 1) y_{n-1}}{k}$$

where

y_n = smoothed value in the current cycle n

y_{n-1} = smoothed value in the previous cycle $n-1$

x_n = value acquired in the current cycle n

k = smoothing factor

The following values can be configured for the module as the smoothing factor.

- 1 = No smoothing
- 4 = Weak smoothing
- 32 = Medium smoothing
- 64 = Strong smoothing

Set limit value 'low' / Set limit value 'high'

Requirements for the function

- Configuration of the threshold trigger for this data point
- Supported variable types of the CPU

The analog value data point must alternatively be linked to one of the following variables:

- PLC tag in the bit memory address area
- DB variable (variable in data block)

Limit value configuration is not possible for PLC tags that access hardware modules (input/output operand area).

The configuration of limit values is pointless for measured values that have already been preprocessed on the CPU.

Function

In these two input boxes, you can set a limit value in the direction of the start of the measuring range or in the direction of the end of the measuring range.

You can also evaluate the limit values, for example as the start or end of the measuring range.

Recommendation for quickly fluctuating analog values:

If the analog value fluctuates quickly, it may be useful to smooth the analog value first if limit values are configured.

Status identifier "OVER_RANGE" / "overflow"

With protocols that support status identifiers, if the limit value is overshoot or undershot, the status identifier of the data point is set for measured range violation, indicated below as the identifier "OV". This status identifiers are described in the section Status IDs of the data points (Page 121).

The "OV" bit of the status identifier of the data point is set as follows when the relevant analog value is transferred:

- Limit value 'high':
 - If the limit value is exceeded: OV = 1
 - If the value then falls below the limit value: OV = 0
- Limit value 'low':
 - If the value falls below the limit value: OV = 1
 - If the value then exceeds the limit value: OV = 0

Configuration of the limit value

Depending on the data type, a limit value is configured as an integer decimal number or as a floating-point number.

Table 3-7 Value ranges of the limit values

Data type	Range of values
Int	-32768 ... 32767
DInt	-2147483648 ... 2147483647
Real	1.175495E-38 ... 3.402823E+38
LReal	2.225073E-308 ... 1.797693E+308

Note

Limit value 0 (zero)

- The entry of the value 0 is interpreted as a deactivated limit value for most modules.
Exceptions:
- For the following modules, 0 is also possible as limit value:
 - CP 1243-7 LTE V3.3
 - TIM 1531 IRC V2.2

The following table specifies the ranges of a 32-bit number with regard to the ranges of the raw value of an analog input or output module.

Range	Value of the 16-bit PLC variable *		Module output [mA]			Measuring range [%]
	Decimal	Hexadecimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
Overflow	32767	7FFF	> 23.515	> 23.515	> 22.810	> 117.593
Overrange	32511	7EFF	23.515	23.515	22.810	117.593
	... 27649	... 6C01	... 20.001	... 20.001	... 20.001	... 100.004
Nominal range (unipolar / life zero)	27648	6C00	20		20	100
	... 0	... 0000	... 0		... 4	... 0

Range	Value of the 16-bit PLC variable *		Module output [mA]			Measuring
Nominal range (bipolar)	27648 ... 0 ... -27648	6C00 ... 0000 ... 9400		20 ... 0 ... -20		100 ... 0 ... -100
Underrange (unipolar / life zero)	-1 ... -4864	FFFF ... ED00	-0.001 ... -3.518		3.999 ... 1.185	-0.004 ... -17.59
Underrange (bipolar)	-27649 ... -32512	93FF ... 8100		-20.001 ... -23.516		-100.004 ... -117.593
Undershoot / wire break	-32768	8000	< -3.518		< 1.185	< -17.593

* The value ranges (underflow / overflow) in PLC variables with different data types are as follows:

- Int
 - -32768
 - 32767
- DInt
 - -2147483648
 - 2147483647
- Real
 - -3.4000E+038
 - 3.4000E+038
- LReal
 - -1.7000E+308
 - 1.7000E+308

Note

Evaluation of the value even when the option is disabled

If you enable one or both options and configure a value and then disable the option later, the grayed out value is nevertheless evaluated.

To disable the two options, delete the previously configured values limit values from the input boxes and then disable the relevant option.

3.22.12 Command options

Output options

The output options correspond to the specification IEC 60870-5-101 - Qualifier of command.

Parameters

The two output options under "Control Code" can be activated alternatively:

- **LATCH_ON/OFF**

- Qualifier of command - QU (Type 1.1) <1> persistent output

The function permanently latches a command output to the value 0 or 1.

Note:

The latched value is only canceled by a new command. Alternatively, the command can be reset by the user program.

- **PULSE_ON**

Qualifier of command - QU (Type 1.1)

The function evaluates the number and length of the signals (pulses) of command outputs from a master station.

Coding:

- <1> short pulse duration

Corresponding parameter for the module: "Short pulse duration"

- <2> long pulse duration

Corresponding parameter for the module: "Long pulse duration"

The output option "Command execution mode" can be activated independently:

- **Command execution mode**

Qualifier of command / Qualifier of set-point command - S/E (Type 6)

Coding:

- <0> execute

- <1> select

The function defines whether a command is transferred directly to the CPU (direct command transmission) or whether the system waits for a confirmation of execution (execute) after the selection (select) before the command is forwarded.

The station module acknowledges receipt of the selection ASDU with the Qualifier <1> select.

After receiving the acknowledgment, the master sends the execution ASDU with the Qualifier <0> execute.

Processing

- LATCH_ON/OFF
The function latches the value of a command as described above.
- PULSE_ON/OFF
The function is coded by the master via a "Qualifier of command". The following codes are evaluated by the communication module in the station:
 - QU (Type 1.1) <0> no additional definition
Corresponding parameter for the module: "Pulse control"
 - QU (Type 1.1) <1> short pulse duration
Corresponding parameter for the module: "Short pulse duration"
 - QU (Type 1.1) <2> long pulse duration
Corresponding parameter for the module: "Long pulse duration"
 - S/E (Type 6) <0> execute
Corresponding parameter for the module: "Command execution mode"
 - S/E (Type 6) <1> select
Corresponding parameter for the module: "Command execution mode"

Data point types

The output options can be configured for the following data point types:

- Control Code (LATCH_ON/OFF / PULSE_ON)
 - Single command ... <45>, <58>
 - Double command ... <46>, <59>
 - Regulating step command ... <47>, <60>
- Command execution mode
 - Single command ... <45>, <58>
 - Double command ... <46>, <59>
 - Regulating step command ... <47>, <60>
 - Set-point command ... <48>, <49>, <61>, <62>

Parameter

Name:	Control Code
Range of values:	<ul style="list-style-type: none"> • PULSE_ON • LATCH_ON/OFF
Explanation:	Output option of the command output. See above for the meaning.

Name: **Number of pulses / Max. Number of pulses**
Default: 1
Explanation: Number of pulses that the data point of the master sends to the corresponding data point of the station.
In the station, the parameter monitors the number of pulses sent by the master. If the number of pulses received from the master exceeds the specified value, the command is rejected.

Name: **Pulse control**
(only "Double command")
Range of values:

- Short pulse duration
- Long pulse duration

Explanation:

- Short pulse duration
Short pulses are intended for time-critical processes, e.g. for controlling circuit breakers.
- Long pulse duration
Long pulses are intended for process that are not time-critical.

Name: **Short pulse duration (s)**
Range of values: 0 ... 65535
Default: 0
Explanation: Commands from the master with the Qualifier of command = <1> (short pulse duration) are output by the communications module for the duration configured here.
If "Short pulse duration" is configured with the value 0 (zero), commands are discarded by the module with the Qualifier of command of <1>.

Name: **Long pulse duration (s)**
Range of values: 0 ... 65535
Default: 0
Explanation: Commands from the master with the Qualifier of command = <2> (long pulse duration) are output by the communications module for the duration configured here.
If "Long pulse duration" is configured with the value 0 (zero), commands are discarded by the module with the Qualifier of command of <2>.

Name: **Command execution mode**
Range of values:

- Execute directly
- Select and operate

Default: Execute directly

Explanation:

- Execute directly

"direct command transmission"

The command is immediately transmitted to the CPU of the station for execution.

- Select and operate

"select / execute"

Procedure:

– The command is triggered in the master module

The "Select" frame is sent from the master station to the communications module of the station.

– The station acknowledges receipt.

– The master data point sends the execution frame after receiving the acknowledgment from the station.

– The station only forwards the command to the CPU when it receives the "Operate" frame from the master within the configured "Max. time between Select and Operate".

The station must not receive any other data frame between Select and Operate.

Note: "Max. time between Select and Operate" is configured in the transmission settings of the respective interface.

3.22.13 Partner stations

Activating the partners of the data point

All partners with which a telecontrol connection has been configured are shown in the table.

Enable the partner or partners with which the selected data point is to exchange data using the check box:

3.23 Messages

Configuration of the messages

If important events occur, the communications module can send configured messages. No program blocks need to be used for the configuration.

To transfer messages, telecontrol communication (parameter group "Communication types") no longer needs to be enabled.

The following are configurable:

- E-mails

The recipient can be a PC with an Internet connection or an S7 station.

- SMS (only mobile wireless CPs or TIM modules)

The recipient can be a mobile phone or an S7 station.

Up to 10 messages (e-mail or SMS) can be configured per module.

You configure the messages in the message editor of the module. Alternatively, you will find it:

- In the shortcut menu of the module
- Via the project navigation: Directory of the station > Local modules > Communications module

For the view in STEP 7, refer to the section Data point configuration (Page 112).

Triggering sending of messages

The sending of the message is triggered by an event that is configured in the "Trigger" tab (see below).

Prerequisites, required information and procedure

E-mails

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

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

Required information:

- Access data of the SMTP server: Address, port number, user name, password
- When using STARTTLS or SSL/TLS: Certificate of the e-mail service provider
- E-mail addresses of the recipients
- APN (mobile wireless CPs)

You obtain the access data for the mobile wireless network and for an APN for transferring e-mails from your network provider. You configure this in the parameter group "Mobile wireless communication settings".

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"
- 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 module:
Parameter group "Security" > "Certificate manager"

SMS (mobile wireless CPs or TIM)

Required information:

- Number of the SMSC

You perform the configuration in the following parameter groups:

- Enabling the SMS function:
"Communication types" > "Enable SMS"
- Configuration of the SMSC
"Mobile wireless communication settings"
- Configuring the SMS
Message editor

"Message parameter"

Here you configure the phone number or the recipient, the subject (e-mail) and the text of the message.

Text: Number of characters

Maximum number of characters that can be transferred in the message text:

- SMS: Max. 160 ASCII characters including any value sent at the same time
- E-mail: 256 ASCII characters including any value sent at the same time

For the value, see below, "Include value" parameter.

Character set for message texts

Entry of the following permitted characters as ASCII character sets (hexadecimal value and character name):

- 0x20
Space
- 0x21 ... 0x5F
! " # \$ % & ' () * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S
T U V W X Y Z [\] ^ _
- 0x61 ... 0x7E
a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
- 0x7C, 0x7E
| ~
- Manual line break (↵)
In message texts, you can insert a line break using <Shift>+<Enter>.

"Trigger"

In the "Trigger" parameter group you configure triggering for sending the message and other parameters.

- **E-mail trigger / SMS trigger**

Specifies the event for which the sending of the message is triggered:

- **Use PLC tag**

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

Resetting the trigger bit:

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

In all other cases, you need to reset the trigger bit with the user program.

Note

Fast setting of the diagnostics trigger tag

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

Frequent sending of SMS

Depending on the system environment, sending an SMS can take up to 2 minutes. To guarantee secure transmission of SMS in mobile wireless modules, a minimum interval of 10 seconds is recommended for triggering SMS.

- 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.

To specify the partner, see below, "Partner for trigger" parameter.
- **Connection to a partner established**

Triggers the sending of the message when the connection returns.

To specify the partner, see below, "Partner for trigger" parameter.
- **Connection establishment to partner failed**

Triggers the sending of the message when the telecontrol connection to a partner could not be established.
- **TeleService session started**

(Mobile wireless CPs)

Triggers the sending of the message when telecontrol communication is enabled and a TeleService connection is established.
- **TeleService session ended**

(Mobile wireless CPs)

Triggers the sending of the message when telecontrol communication is enabled and a TeleService connection has been terminated.
- **Weak mobile wireless network**

(SMS only)

If the mobile wireless connection for telecontrol communication is too weak, an SMS message is triggered and sent to the configured recipient.
- **VPN connection established**

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

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

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

Triggers the sending of the message when the VPN connection is interrupted.
- **SINEMA RC connection established**

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

Triggers the sending of the message when the VPN or OpenVPN connection is established or returns.
- **SINEMA RC connection terminated**

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

Triggers the sending of the message when the VPN or OpenVPN connection is interrupted.
- **Partner for trigger**

Here you select from the configured partners of the device the partner whose connection is affected in the trigger options "Connection to a partner established" or "Connection to a partner 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 the messages (SMS / e-mail) (Page 160).

- **PLC tag for processing status**

PLC tag of the type DWORD for the processing status

- **Include value**

When the option is enabled, the module 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 value of a PLC tag supports the following data types:

- Bool, Byte, Char, USInt, Int, UInt, Word, DWord, UInt, DInt, Real, String
- Arrays of these data types

- **PLC tag for value**

PLC tag in which the value to be sent is written.

Error messages

If an error message for the trigger type is displayed when compiling the station, check the configuration.

If you have configured one of the following options as trigger type for the message:

- VPN / IPSec / SINEMA RC
- Check the following:
 - Are the security functions enabled?
 - Is VPN activated?
 - Are additional options set correctly?

3.24 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 OPQRS
TUVWXYZ[\]^_
- 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>.

Commissioning

4.1 Commissioning the CP

Requirement: Configuration prior to commissioning

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

Commissioning the module

Further commissioning involves the following steps:

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

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

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

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

4.2 Set time for operation with Security / SINEMA RC

Manual setting the time of day during commissioning

Note

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

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

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

Recommendation:

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

Diagnostics and maintenance

5.1 Diagnostics options

The following diagnostic options are available with most modules. Some functions are limited to specific data types or protocols.

LEDs of the module

You can find information on the LED displays in the manual for the respective module.

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

If your engineering station is connected to a module via Ethernet, you will receive the following information about the selected module here:

- Connection status of the engineering station with the module

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

Using the online functions, you can read various diagnostic information from the relevant module from an engineering station on which the STEP 7 project is stored and perform maintenance functions.

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

Online access

This is where you establish the online connection to the module.

For the procedure, refer to the STEP 7 information system.

Diagnostics

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

- **General**

General information on the module

- **Diagnostic status > Device-specific events**

Here you will find the diagnostics buffer entries of the module and an overview of the sent messages (SMS messages / e-mails).

- **Diagnostics buffer**

This is where you can find entries in the diagnostics buffer of the TIM.

- **Ethernet interface[X1/2/3]**

Address and statistical information

- **Industrial Remote Communication**

Here, you obtain WAN-specific information on the TIM module:

- **Partner**

Here you will find address and configuration data of the partners, connection statistics and additional diagnostics information. Click on a subscriber to display additional information.

You will also find information on the partners in the WBM, see below.

- **Data point list**

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

- **Telegram protocol diagnostics**

With this function, you can enable, evaluate and display the logging of frames of the module.

For a description, refer to section Telegram protocol diagnostics (Page 157).

- **Ethernet diagnostics**

With the Logging function, you can log the data traffic of the TIM using PCAP functionality for diagnostics purposes.

If an error occurs or if the TIM behaves in an unwanted manner, the communication behavior of the TIM can be recorded. The frame traffic of the TIM is recorded for a defined time or for a configurable number of frames.

The log files are stored as PCAP files on the connected PC and can be evaluated with the Wireshark program, for example.

- **Time**

Specification of the current time in the module and the time source. Possibility to set the time in the module.

Functions

You can run the following functions here:

- **Firmware update**
- **Assign IP address**
- **Assign PROFINET device name**
- **Reset to factory settings**

For information on the functions, refer to the section Maintenance (Page 162).

Web server (WBM) of the TIM 1531 IRC

From a PC you can use HTTP/HTTPS to access the Web pages (WBM) of the TIM. The WBM returns a variety of information.

For access to the content, refer to the section WBM of the TIM 1531 IRC (Page 187).

Partner status and connection status in the WBM

You will see the configured partners and the status of the connections to the local and remote communications partners of the TIM on the page "Telecontrol" > "Partner information" of the WBM. For details, see section Partner information (Page 200).

Partner and connection information to the CPU

The TIM can signal the status of the connection and the connection paths to the communications partner to its local CPU via a PLC tag. For information on the configuration, refer to section Communication with the CPU (Page 65).

SNMP

For information on the functions, refer to the section SNMP (Page 159).

5.2 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.

5.3 Online security diagnostics via port 8448

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.

5.4 Telegram protocol diagnostics

The SINAUT special diagnostics is available for the following modules:

- S7-1200 telecontrol CPs
- TIM 1531 IRC

5.4.1 Message protocol: Structure and functions

The "Message protocol" function is used to record transferred message frames.

See the "Operation" paragraph below for information on activating the function.

Structure of the "Message protocol" dialog

After activation, the columns show the following data:

- No.
 - Symbol for incoming or outgoing message frames
 - Message frame number, consecutive
- Block
Length of the message frame block in which the message frame was transferred.
- Header fields
Hexadecimal display of some header data
For the meaning, refer to section Details (Page 158).
- Subscriber (source / destination)
Subscriber numbers of the sending (source) and receiving (destination) subscriber
- Object (source / destination)
Object number of the data object in the message frame for source and destination subscriber
- Index
Address parameters for net data in data messages (channel number)

- Date, time and status
Time stamp of message frame and time status from time of transfer
For information on the display, see section Details (Page 158).
- Net Data
Hexadecimal display of the net data of the message frame
For the meaning, refer to section Details (Page 158).

Operation

You operate the function using the three buttons underneath the dialog described above.

- Activate telegram protocol diagnostics
Clicking the button starts logging of the transferred message frames.
400 message frames are recorded per recording cycle. A maximum of 10000 message frames can be stored in a circular buffer.
- Refresh
Updates the recording; a new recording cycle is started.
- Save
Saves the recorded message frames in a binary file. You define the storage location using the button.
- Show saved
Shows the recorded and saved frames.

5.4.2 Details

Detailed information

Header fields

The 5 fields output in hexadecimal format have the following meaning:

- 1st field: Message counter
0...7
- 2nd field: Control code
- 3rd field: Function selection
 - 0: Processing in TIM
 - 1: Processing in CPU

- 4th field: Address extension
 - 0: ST1 message without address extension
 - 1: ST1 message with address extension
 - 2: ST7 message
- 5th field: Direction bit
 - 0: Monitoring direction
 - 1: Control direction

Net Data

The column shows the net data of the message frame.

The values are displayed in hexadecimal format.

Date, time and status

The column shows the time stamp of the message frame in the following format:

Year/Month/Day_Hour:Minute:Second_Time status

Assignment of the time status:

- 2^0
 - 0: Time is invalid
 - 1: Time is valid
- 2^1
 - 0: Standard time
 - 1: Daylight saving time
- 2^2
 - Not used
- 2^3
 - 0: No meaning
 - 1: Notification time for daylight saving/standard time changeover

Only in time synchronization message frame

5.5 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).

Scope of performance of the module as SNMP agent

Not all functions described below are available with every module. Refer to the manual of the respective module for information on the functional scope.

The communications modules support data queries in the following SNMP versions:

- SNMPv1 (standard)
- SNMPv3 (Security)

They return the contents of MIB objects of the standard MIB II according to RFC1213.

- **MIB II**

The MIB supports the following groups of MIB objects:

- System
- Interfaces

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

- IP
- ICMP
- TCP
- UDP
- SNMP

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

- Address Translation (AT)
- EGP
- Transmission

The modules do not support traps.

For more detailed information about the MIB files and SNMP, refer to the manual /9/ (Page 221).

Configuration

For information on the configuration, see section SNMP (Page 75).

5.6 Processing status of the messages (SMS / e-mail)

Processing status of messages

If the option "Enable identifier for processing status" option is set in the "Trigger" tab of the STEP 7 message configuration, the module outputs a status.

The processing status provides information about the processing state 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 meaning of the statuses is as follows:

Processing status of the telecontrol messages

Table 5- 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: <ul style="list-style-type: none"> • SIM card invalid • No network • Wrong destination phone number (number not reachable)

Table 5- 2 E-mail: Meaning of the status ID output in hexadecimal format

Status	Meaning
0000	Transfer completed free of errors
82xx	Other error message from the e-mail server Apart from the leading "8", the message corresponds to the three-digit error number of the SMTP protocol.
8401	No channel available. Possible cause: There is already an e-mail connection via the module. A second connection cannot be set up at the same time.
8403	No TCP/IP connection could be established to the SMTP server.
8405	The SMTP server has denied the login request.
8406	An internal SSL error or a problem with the structure of the certificate was detected by the SMTP client.
8407	Request to use SSL was denied.
8408	The client could not obtain a socket for creating a TCP/IP connection to the mail server.
8409	It is not possible to write via the connection. Possible cause: The communications partner reset the connection or the connection aborted.
8410	It is not possible to read via the connection. Possible cause: The communications partner terminated the connection or the connection was aborted.
8411	Sending the e-mail failed. Cause: There was not enough memory space for sending.
8412	The configured DNS server could not resolve specified domain name.
8413	Due to an internal error in the DNS subsystem, the domain name could not be resolved.
8414	An empty character string was specified as the domain name.
8415	An internal error occurred in the cURL module. Execution was aborted.
8416	An internal error occurred in the SMTP module. Execution was aborted.
8417	Requests to SMTP on a channel already being used or invalid channel ID. Execution was aborted.
8418	Sending the e-mail was aborted. Possible cause: Execution time exceeded.
8419	The channel was interrupted and cannot be used before the connection is terminated.

Status	Meaning
8420	Certificate chain from the server could not be verified with the root certificate of the module.
8421	Internal error occurred. Execution was stopped.
8450	Action not executed: Mailbox not available / unreachable. Try again later.
84xx	Other error message from the e-mail server Apart from the leading "8", the message corresponds to the three-digit error number of the SMTP protocol.
8500	Syntax error: Command unknown. This also includes the error of having a command chain that is too long. The cause may be that the e-mail server does not support the LOGIN authentication method. Try sending e-mails without authentication (no user name).
8501	Syntax error. Check the following configuration data: Alarm configuration > E-mail data (Content): <ul style="list-style-type: none"> • Recipient address ("To" or "Cc").
8502	Syntax error. Check the following configuration data: Alarm configuration > E-mail data (Content): <ul style="list-style-type: none"> • Email address (sender)
8535	SMTP authentication incomplete. Check the "User name" and "Password" parameters in the configuration.
8550	SMTP server cannot be reached. You have no access rights. Check the following configuration data: <ul style="list-style-type: none"> • Module configuration > E-mail configuration: <ul style="list-style-type: none"> – User name – Password – Email address (sender) • Alarm configuration > E-mail data (Content): <ul style="list-style-type: none"> – Recipient address ("To" or "Cc").
8554	Transfer failed
85xx	Other error message from the e-mail server Apart from the leading "8", the message corresponds to the three-digit error number of the SMTP protocol.

5.7 Maintenance

Maintenance functions

You can find a description of the following maintenance functions in the manual or operating instructions of the respective module, see Bibliography (Page 219).

- Firmware update
- Reset
- Module replacement

OUC program blocks (CP)

A.1 Validity and requirements

Validity

The functions described below are supported by the following modules:

- CP 1243-1
 - As of firmware \geq V3.1
- CP 1243-7 LTE
 - As of firmware \geq V3.1
- CP 1243-8 IRC
 - As of firmware \geq V3.1
- CP 1542SP-1 IRC
 - As of firmware \geq V2.0

Observe the deviations between the firmware versions for secure communication (Secure OUC); see below.

A.2 Program blocks for OUC

Using the program blocks for Open User Communication (OUC)

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

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

Note

No different program block versions

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

Requirements for Secure OUC

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

- STEP 7: As of V16
- CPU firmware
 - CPU-1200: As of V4.4
 - CPU 151xSP: As of V2.0
- CP firmware
 - CP 1200: As of V3.2
 - CP 1542SP-1 IRC: As of V2.1

Supported program blocks for OUC

The following instructions in the specified minimum version are available for parameter assignment of the 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 module. Configure the time-of-day synchronization.

To change the configuration data of the module during runtime:

- **T_CONFIG V1.0**

Program-controlled configuration of the 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 167).

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.

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

- **TC_CONFIG**

Program-controlled change of configuration data of mobile wireless CPs

You can find the program blocks in STEP 7 in the "Instructions > Communication > Open User Communication" task card.

Connection descriptions in system data types (SDTs)

The blocks listed above use the CONNECT parameter for the relevant connection description. TMAIL_C uses the parameter MAIL_ADDR_PARAM.

The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

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

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

The corresponding SDT is then created with its parameters.

Usable SDTs

- **TCON_IP_V4**

For transferring frames via TCP or UDP

- **TCON_QDN**

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

- **TCON_IP_RFC**

For transferring frames via ISO-on-TCP (direct communication between two S7 stations)

- **TADDR_Param**

For transferring frames via UDP

- **TMail_V4**
For transferring e-mails addressing the e-mail server using an IPv4 address
Recommendation for mobile wireless applications:
Set the parameter "WatchdogTime" from "MAIL_ADDR_PARAM" to a value higher than 3 minutes.
- **TMail_V6**
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)
- **IF_CONF**
For changing configuration data of mobile wireless CPs using the TC_CONFIG
- **TCON_IP_V4_SEC**
Only CP 1200
For the secure transfer of data via TCP
- **TCON_QDN_SEC**
Only CP 1200
For the secure transfer of data via the host name
- **TMail_V4_SEC**
For secure transfer of e-mails addressing the e-mail server using an IPv4 address
- **TMail_V6_SEC**
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 parameter assignment.

A.3 Changing the IP address during runtime

Changing the IP address during runtime

You can change the following address parameters of the CP at runtime controlled by the program:

- IP address
- Subnet mask
- Router address

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

Note**Changing the IP parameters with a dynamic IP address**

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

Requirements - Configuration

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

Requirements - STEP 7 version

- STEP 7 ≥ V14

Requirements - Firmware versions

- **CP 1243-1 / CP 1243-8 IRC**
 - CP firmware ≥ V2.1.7x
 - CPU firmware ≥ V4.2
- **CP 1542SP-1 IRC**
 - CP firmware ≥ V1
 - CPU firmware ≥ V2.0 (CPU 151xSP)

Program blocks

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

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

- **T_CONFIG**

Along with:

- IF_CONF_V4
- IF_CONF_NTP
- IF_CONF_V6
- IF_CONF_DNS

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

Note

No feedback from the CP

"T_CONFIG" does not support feedback from the CP to the CPU. Errors in the block call or in setting the address parameter are not reported. The block outputs "BUSY" or "DONE" regardless of whether the address parameter was set.

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

A.4 SMS messages via OUC

Sending e-mails / SMS messages via OUC

With mobile wireless CPs, you only require the program blocks and system data types (SDTs) described below to transfer SMS messages using Open User Communication (OUC).

In contrast, the event-driven sending of e-mails or SMS messages is independent of program blocks and is configured in STEP 7 in the message editor of the respective module.

Note

Frequent sending of SMS

Depending on the system environment, sending an SMS can take up to 2 minutes.

To guarantee secure transmission of SMS, a minimum interval of 10 seconds is recommended for triggering SMS.

You can control this, for example, by setting the "REC" parameter in the TCON and TSEND_C blocks.

SMS messages via program blocks

Sending SMS messages to one partner

To do this, create the following blocks or system data types (alternatives):

- TCON + TDISCON + TSEND + TCON_Phone
- TSEND_C + TCON_Phone

Receiving SMS messages from one partner

To do this, create the following blocks or system data types (alternatives):

- TCON + TDISCON + TRCV + TCON_Phone
- TRCV_C + TCON_Phone

If you do not enter a phone number in the "PhoneNumber" parameter of the TCON_Phone system data type, the CP cannot receive any SMS messages.

Receiving SMS messages from several partners

As an alternative, you can create a separate block set for each partner as described above for 1 partner or a single block set with the following special feature in the TCON_PHONE block:

If you enter an asterisk (*) after the phone number body in the "PhoneNumber" parameter of the TCON_Phone block, the asterisk acts as a placeholder for all authorized phone numbers with this phone number body.

You configure the phone numbers authorized for access to the CP in STEP 7 in the "Security" parameter group of the CP.

Message text to be sent in the "DATA" parameter

You enter the message text as a string in the "DATA" parameter of TSEND or TSEND_C.

A message can contain up to 160 characters. If the message text contains more than 160 characters, the text is distributed over two or more SMS messages.

Reading out the message text from the "DATA" parameter

To receive an SMS message, parameterize the message text to be read out in the TRCV / TRCV_C blocks in the "DATA" parameter via a data block (DB).

Create a DB of the data type "Struct". Open the properties dialog of the DB (shortcut menu of the DB) and disable optimized block access in the "Attributes" parameter group.

In the structure of the DB, create the following data types for the SMS messages:

- DTL
12 bytes for the time stamp of the received SMS message (time stamp from the network)
- String[22]
String of 22 bytes for the phone number of the sender (+ 2 byte string header)
- String[160]
String of 160 bytes for the message text (+ 2 byte string header)
The SMS message text can contain max. 160 characters.

Per SMS message the structure requires memory space of 198 bytes.

Storing the last 10 received SMS messages

You can output up to 10 received SMS messages from the receive block by making the entry "SMSSTORE" for the "PhoneNumber" parameter of TCON_PHONE.

To store the received data from 10 SMS messages, you need to create an adequately large structure (2000 bytes) for the "DATA" parameter of the receiving block. As described above, the structure has the following organization:

- Received data SMS 1 (DTL, String[22], String[160], Byte)
- Received data SMS 2 (DTL, String[22], String[160], Byte)
- ... to
- Received data SMS 10 (DTL, String[22], String[160], Byte)

The received data of every SMS message has the following structure:

- DTL
12 bytes for the time stamp of the received SMS message (time stamp from the network)
- String[22]
String of 22 bytes for the phone number of the sender (+ 2 byte string header)
- String[160]
String of 160 bytes for the message text (+ 2 byte string header)
- Byte
Status of the SMS message
If more than one SMS message is received the status of every SMS is stored in this status byte:
 - 0 = Invalid
 - 1 = Unread
 - 2 = Read

When receiving multiple SMS messages, per SMS message the structure requires memory space of 200 bytes.

Length information at "LEN" and "DATA" for the blocks "TRCV" / "TRCV_C"

When receiving SMS messages via the blocks TRCV or "TRCV_C" if you enter length information in the "LEN" parameter, this can lead to incorrect information in the data storage of the received information.

Recommendation: Set LEN = 0 and enter the length information in the "DATA" parameter.

Character set for the SMS text

The CP supports the following ASCII character set (hexadecimal value and character name) for SMS message texts sent via program blocks:

- 0x0A
LF (line feed)
- 0x0D
CR (carriage return)
- 0x20
Space
- 0x21 ... 0x5A
! " # \$ % & ' () * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S
T U V W X Y Z
- 0x61 ... 0x7A
a b c d e f g h i j k l m n o p q r s t u v w x y z

A.5 TC_CONFIG for changing configuration data of the CP

Meaning

With the program block TC_CONFIG, you can modify parameters of a mobile wireless CP configured in STEP 7. The configured values are not overwritten retentively. The overwritten values remain valid until TC_CONFIG is called again or until the station starts up again (cold restart after cycling power).

If the STEP 7 configuration data of the CP needs to be changed permanently, the block needs to be called again each time the station restarts (cold restart) or a modified project must be downloaded to the station.

The CONFIG parameter points to the memory area with the configuration data. The configuration data is stored in a data block (DB). The DB cannot be created with optimized block access. The structure of the DB is specified by the system data type (SDT) IF_CONF_v4.

The configuration data to be modified on the CP is put together as necessary in blocks in the SDT "IF_CONF_..." for the individual parameters.

Parameters that are not intended to change as a result of the block are not entered in the SDT. They retain the value configured in STEP 7.

For detailed information on assigning the parameters of the SDT IF_CONF_v4, refer to the section IF_CONF_*: SDTs for the configuration data of the CP (Page 174).

The INTERFACE parameter references the name of the interface of the mobile wireless CP. You will find the name of the interface in the STEP 7 project in the standard tag table of the station in the "System constants" tab under the entry with the value of the "Hardware identifier" of the CP.

Requirements

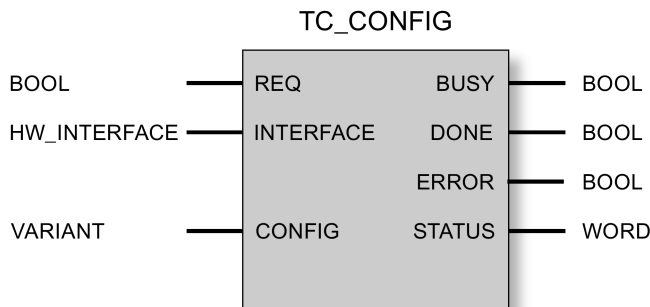
- To be able to use the function, there must already be values present in the STEP 7 basic configuration of the CP.
- For using the "IF_CONF_PrefProvider" parameter field (preferred mobile wireless networks) of the SDT "IF_CONF_v4":

The mobile wireless network to be used must be set as follows in the configuration of the CP:

"Mobile wireless communication settings > List of preferred networks":

"Preferred mobile wireless networks" = "Contract network and alternative networks"

Call interface in FBD representation



Explanation of the formal parameters

The following table explains all the formal parameters for the TC_CONFIG instruction

Parameter	Declaration	Data type	Range of values	Description
REQ	INPUT	BOOL	0, 1	The processing of the block is started and the status codes initialized on a rising edge. Updating of the DONE, ERROR and STATUS status codes when there is no positive edge.
INTERFACE	INPUT	HW_Interface (WORD)		Reference to the interface of the local CP
CONFIG	INOUT	VARIANT	See also "IF_CONF: SDT for telecontrol configuration data"	Reference to the memory area with the collected configuration data to be modified
ENO	OUTPUT	BOOL	0: Error 1: Error-free	Enable output If there is a runtime error with the instruction, ENO = 0 is set.
BUSY	OUTPUT	BOOL	0: Execution of the instruction not yet started, completed or aborted 1: The instruction is executing	Condition code of the execution status of the block

Parameter	Declaration	Data type	Range of values	Description
DONE	OUTPUT	BOOL	0: - 1: The instruction executed successfully	This parameter indicates whether or not the job was completed without errors. For the meaning in conjunction with the parameters ERROR and STATUS, refer to Codes of the block.
ERROR	OUTPUT	BOOL	0: - 1: Error	Error code For the meaning in conjunction with the parameters DONE and STATUS, refer to Codes of the block.
STATUS	OUTPUT	WORD		Status code For the meaning in conjunction with the parameters DONE and ERROR, refer to Codes of the block.

The codes BUSY, DONE and ERROR

The codes of DONE and ERROR are relevant only when BUSY = 0.

BUSY	DONE	ERROR	Meaning
0	0	0	No job being executed

You will find all other code combinations of DONE and ERROR in the following table.

The codes DONE, ERROR and STATUS

The following table shows the condition codes formed based on DONE, ERROR and STATUS that must be evaluated by the user program.

DONE	ERROR	STATUS	Meaning
1	0	0000H	Job executed without errors
0	0	7000H	No job processing active (first block call)
0	0	7001H	Job processing started (first block call)
0	0	7002H	Job processing already active (renewed block call when BUSY = 1)
0	1	80E0H	Internal error
0	1	80E6H	No query in progress (block call not started)
0	1	80EBH	Query temporarily rejected (the CP is currently being configured by STEP 7)
0	1	80F6H	Format error of a parameter in the called data block (wrong length, wrong format or invalid value) Check the "IF_CONF" SDT.
0	1	80F7H	Wrong ID in the parameter fields of the configuration data: Check the "IF_CONF" SDT.

A.6 IF_CONF_*: SDTs for the configuration data of the CP

Structure of the IF_CONF DB for the TC_CONFIG program block

The CONFIG parameter of the TC_CONFIG program block references the memory area containing the configuration data of the mobile wireless CP to be modified. The configuration data stored in a data block is described as a structure of the IF_CONF_* system data type (SDT).

To be able to use the function, there must already be values present in the STEP 7 basic configuration of the CP.

The IF_CONF DB is made up of a header followed by blocks that correspond to the parameters in the configuration of the CP.

The CP configuration data to be modified is collected together as IF_CONF fields. Parameters that will not be modified are ignored in the IF_CONF structure and remain as they were configured in the STEP 7 project.

Creating the DB and the IF_CONF structures

You can create the parameters of the CP within the IF_CONF DB in one or more structures each with one or more fields.

You will need to type in the data types of the fields using the keyboard. They are not displayed in the selection list. The data types are not case-sensitive.

Follow the steps below to create the IF_CONF.DB:

1. Create a data block of the type "Global DB" with block access "Standard".
2. Create a structure (data type "Struct") in the table of the parameter configuration of the DB.
You can specify any name.
3. Under this structure add a header by assigning the name of the header and typing it in in the cell of the data type "IF_CONF_Header".
The header of the structure and its three parameters (see below) is created.
4. Create another structure for the first parameter to be changed by typing in the required data type (for example "IF_CONF_APN") in the cell of the data type.
5. Repeat the last step for all parameters you want to change in the CP using TC_CONFIG.
6. Finally, update the number of fields in the header in the "subfieldCnt" parameter.

Header of IF_CONF

Table A-1 IF_CONF_Header

Byte	Parameter	Data type	Initial value	Description
0 ... 1	fieldType	UINT		Field type: Must always be 0.
2 ... 3	fieldId	UINT		Field ID: Must always be 0.
4 ... 5	subfieldCnt	UINT		Total number of blocks contained in the DB (structures) for the parameters to be changed

General parameters of the parameter fields

Each field has the following general parameters:

- Id
This parameter identifies the field and must not be modified.
- Length
This parameter indicates the length of the field. The value serves as information.
Fields with strings and / or arrays have a variable length. Due to hidden bytes, the actual length of fields can be greater than the sum of the displayed parameters.
- Mode
The following values are permitted to these parameters:

Table A- 2 Values of "Mode"

Value	Meaning
1	Permanent validity of the configuration data Not relevant for the CP
2	Temporary validity of the configuration data, including deleting of existing permanent configuration data The permanent configuration data is replaced by the structures configured in the block.

"APN settings"

Corresponding parameter group in the configuration:
"Mobile wireless communication settings > APN settings"

Table A- 3 IF_CONF_APN

Parameter	Data type	Initial value	Description
Id	UINT	4	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 174
Mode	UINT		Validity (1, 2) - see above (general parameters)
AccesspointGPRS	STRING [98]		APN: Name of the access point from the mobile wireless network to the Internet
AccesspointUser	STRING [42]		APN user name
AccesspointPassword	STRING [22]		APN password

"CP identification"

Corresponding parameter group in the configuration:
 "Security > CP identification"

Table A- 4 IF_CONF_Login

Parameter	Data type	Initial value	Description
Id	UINT	5	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 54
Mode	UINT		Validity (1, 2) - see above (general parameters)
ModemName	STRING [22]		Access ID The value cannot be set.
ModemPassword	STRING [22]		Telecontrol password The password with the CP 1242-7 (6GK7 242-7KX30-0XE0) cannot be changed via the SDT.

"Telecontrol server" (DNS)

Corresponding parameter group in the configuration:
 "Partner stations > Telecontrol server"

This field is only used when the telecontrol server is addressed with a name that can be resolved by DNS. If the telecontrol server is addressed with its IP address, the "IF_CONF_TCS_IP_V4" field is used.

If there is more than one telecontrol server, use the field once per server.

Table A- 5 IF_CONF_TCS_Name

Parameter	Data type	Initial value	Description
Id	UINT	6	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 266
Mode	UINT		Validity (1, 2) - see above (general parameters)
TcsName	-	-	- reserved -
	STRING [254]		Name of the telecontrol server that can be resolved by DNS or IP address as string
RemotePort	UINT		Port of the telecontrol server
Rank	UINT		Priority of the server [1, 2] 1 = first telecontrol server, 2 = second telecontrol server (second server not relevant)

"SMSC"

Corresponding parameter group in the configuration:
 "Mobile wireless communication settings > Mobile wireless settings"

Table A-6 IF_CONF_SMS_Provider

Parameter	Data type	Initial value	Description
Id	UINT	10	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 28
Mode	UINT		Validity (1, 2) - see above (general parameters)
SMSProvider	STRING [20]		Subscriber number of the SMS center (SMSC) of the mobile wireless network provider with which the mobile wireless contract was signed for this station.

"PIN"

Corresponding parameter group in the configuration:
 "Mobile wireless communication settings > Mobile wireless settings"

Table A-7 IF_CONF_PIN

Parameter	Data type	Initial value	Description
Id	UINT	11	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 16
Mode	UINT		Validity (1, 2) - see above (general parameters)
Pin	STRING [8]		PIN of the SIM card inserted in the CP The parameter is not relevant if the PIN was correctly configured. If the PIN was incorrectly configured, the correct PIN can be entered.

"Authorized phone number"

Corresponding parameter group in the configuration:
 "Security > Authorized phone numbers"

Table A-8 IF_CONF_WakeupList

Parameter	Data type	Initial value	Description
Id	UINT	13	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 246
Mode	UINT		Validity (1, 2) - see above (general parameters)
WakeupPhone [1...10]	ARRAY [1...10] of STRING [22]		Phone number subscriber authorized to wake up The asterisk (*) at the end of a call number is used a placeholder for direct dialing numbers.

"Preferred mobile wireless networks"

Corresponding parameter group in the configuration:
 "Mobile wireless communication settings > List of preferred networks"

Requirement:

The mobile wireless network to be used must be set as follows in the configuration of the CP:

"Mobile wireless communication settings > List of preferred networks":
 "Preferred mobile wireless networks" = "Contract network and alternative networks"

Table A- 9 IF_CONF_PrefProvider

Parameter	Data type	Initial value	Description
Id	UINT	14	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 46
Mode	UINT		Validity (1, 2) - see above (general parameters)
Provider [1...5]	ARRAY [1...5] of STRING [6]		Parameter "Contract network and preferred networks" 1st to 5th preferred mobile wireless network to which the CP dials in other than the contract network. No. 1 with highest priority, no. 5 with lowest priority. Entry of the Public Land Mobile Network (PLMN) of the network provider consisting of Mobile Country Code (MCC) and Mobile Network Code (MNC). Example (test network of Siemens AG): 26276

TeleService access (DNS name / IP address of the server)

Corresponding parameter group in the configuration:
 "Mobile wireless communication settings > TeleService settings"

Access data of the TeleService server (switching station). If there is more than one TeleService server, use the field once per server.

With IF_CONF_TS_Name only a TeleService server configured in STEP 7 can be changed but no new one created. If you attempt to create the configuration of a TeleService server with the block. the internal error 80E0 is output at TC_CONFIG.

Table A- 10 IF_CONF_TS_Name

Parameter	Data type	Initial value	Description
Id	UINT	20	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 266
Mode	UINT		Validity (1, 2) - see above (general parameters)
ts_name	String [254]		Name of the TeleService server that can be resolved by DNS or IP address as string
RemotePort	UINT		Port of the engineering station
Rank	UINT		Priority of the server [1] or [2]: <ul style="list-style-type: none"> • 1 = server 1 • 2 = server 2 (not relevant)

TeleService access (IP address of the server)

IP address of the TeleService server. No longer usable as of firmware version V2.1 of the CP.

If there is more than one TeleService server, use the field once per server.

Table A- 11 IF_CONF_TS_IF_V4

Parameter	Data type	Initial value	Description
Id	UINT	21	ID of the parameter field
Length	UINT		Length of the parameter field in bytes: 14
Mode	UINT		Validity (1: permanent, 2: temporary)
RemoteAddress	IP_V4		IP address of the TeleService server
RemotePort	UINT		Port of the TeleService server
Rank	UINT		Priority of the server [1] or [2] 1 = server 1, 2 = server 2

SINEMA Remote Connect (CP)

B.1 Validity and requirements

Validity

Communication via SINEMA Remote Connect is supported by the following modules:

- CP 1243-1
 - As of firmware V3.1
- CP 1243-7 LTE
 - As of firmware V3.1
- CP 1243-8 IRC
 - As of firmware V3.1
 - Under ST7 as MSC station as of firmware V3.2
- CP 1542SP-1 IRC
 - As of firmware V2.0
 - Under ST7 as MSC station as of firmware V2.1

The functions are supported by the following software versions:

- SINEMA Remote Connect
 - As of software version V1.3

B.2 Connection to SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

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

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

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

The CP can also handle telecontrol communication via the SINEMA RC server.

Parameter groups

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

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

For information on the supported protocols and configuration, see section Telecontrol via SINEMA RC (Page 183).

Applications

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

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

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

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

Table B- 1 Use cases and parameters to be activated

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

* Explanation of the parameter abbreviations:

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

TC - Communication types > Telecontrol communication enabled

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

B.3 Telecontrol via SINEMA RC

For information on possible applications of communication via SINEMA Remote Connect, see section Connection to SINEMA RC (Page 181).

Requirements

Perform the necessary configuration of SINEMA Remote Connect - Server (not in STEP 7) before configuring the CP in STEP 7. The CP and the communications partner of the CP must be configured in the SINEMA RC Server.

Configuration of the telecontrol communication via SINEMA Remote Connect

Follow the steps below when configuring the module for use of telecontrol communication via SINEMA RC:

1. In the "Communication types" parameter group activate telecontrol communication and select the protocol.
The option for communication via SINEMA RC is not yet visible.
2. Change to the "Security" parameter group and enable the security functions.
(In the "Communication types" parameter group the SINEMA RC option appears disabled and grayed out)
3. Open the "Security > VPN" parameter group and enable VPN.
4. For the parameter "VPN connection type" select the option "Automatic OpenVPN configuration via SINEMA Remote Connect Server" if this is not preset.
(In the "Communication types" parameter group the SINEMA RC option becomes usable.)
5. Change to the "Communication types" parameter group and enable the option "Telecontrol communication via SINEMA Remote Connect".
6. Create the remaining configuration of the SINEMA RC connection of the CP under "Security > VPN".

For information on the configuration, see section Security > VPN > SINEMA Remote Connect (Page 183).

B.4 Security > VPN > SINEMA Remote Connect

Remote maintenance with SINEMA Remote Connect (SINEMA RC)

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

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

Preparatory steps

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

- Configuration of SINEMA Remote Connect Server
Configure SINEMA RC Server as necessary (not in STEP 7). The communications module and its communications partners must be configured in the SINEMA RC Server.
- Exporting the CA certificate (optional)

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

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

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

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

Configuration of SINEMA Remote Connect

Importing your own certificate

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

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

VPN > General

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

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.

WBM of the TIM 1531 IRC

C.1 Supported Web browsers

Web browser

For secure access to the Web server of the TIM the following Web browsers are suitable:

- Internet Explorer (version 11)
- Google Chrome (version 68)
- Firefox (version 62)

You will find the specified Web browsers, information and any necessary addons on the Internet.

C.2 Establishing a connection to the WBM of the TIM

Possible connections

You can establish a connection between a PC and the TIM using the HTTP/HTTPS protocol:

- LAN connection

With a local connection from the PC to the TIM you can connect directly.

- Connection via WAN (Internet/mobile wireless)

The TIM must be reachable via a fixed IP address.

With connections via the Internet / mobile wireless network you need to use the security protocol "HTTPS".

Requirements

Requirements for access to the TIM:

- The TIM must be reachable via an IPv4 address.
- The PC must be in the same subnet as the TIM.
- The TIM must be reachable.

Connection to the Web server of the TIM

Follow the steps below to connect the PC to the Web server of the TIM:

1. Open the Web browser.
2. Enter the address (IP address / host name) of the TIM (or the router) in the address line of the Web browser either via the HTTP or HTTPS protocol:
 - http://<Address>
 - https://<Address>

When selecting the protocol, make sure that it is released in the configuration of the TIM ("Web server" tab).

With HTTPS connections via the Internet when you log in the first time, a warning can appear that the Web page is not secure or that the certificate is not trustworthy. If you are sure that you have entered the correct address, ignore the message. If necessary add the connection to the exceptions (depending on the Web browser).

The logon window of the TIM opens.

3. In the "User name" input box, enter the name of a user or administrator configured in STEP 7.
The rights assigned in "Global security settings" of the STEP 7 project apply.
4. Enter the corresponding password in the "Password" input box.
5. Click the "Log in" button.

The Web server opens with the start page:

C.3 General functions of the WBM

You set the WBM language with the setting of the browser being used.




The following languages are supported:

- German
- English

Displays and symbols in the title bar

The displays and symbols in the WBM title bar have the following meaning:

Symbol	Function
User: 1	Name of the currently logged in user
Log out	User logout
Number of active sessions: 1	Number of connections to a PC
2015-01-28 14:30:37	Date and time of the last page update of the WBM in local time of the TIM (yyyy-mm-dd hh:mm:ss)

Symbol	Function
	The automatic update of the WBM display is enabled. The data is fetched at the interval configured under "System > Web server".
	The automatic update of the WBM display is disabled.
Turn on	Switches on the automatic update of the WBM display.
Turn off	Switches off the automatic update of the WBM display.
	Prints out the current WBM page

C.4 Start page

After logging in to the WBM, the start page appears.

On the left you will find the navigation area with the main levels of the WBM.

Navigation in the WBM

By clicking on an entry in the navigation area on the left open the WBM page you want for further information or on which you want to configure or program.

The WBM opens the first tab of the entry.

On other pages with several tabs change to the relevant tab by clicking on the tab name.

Start page

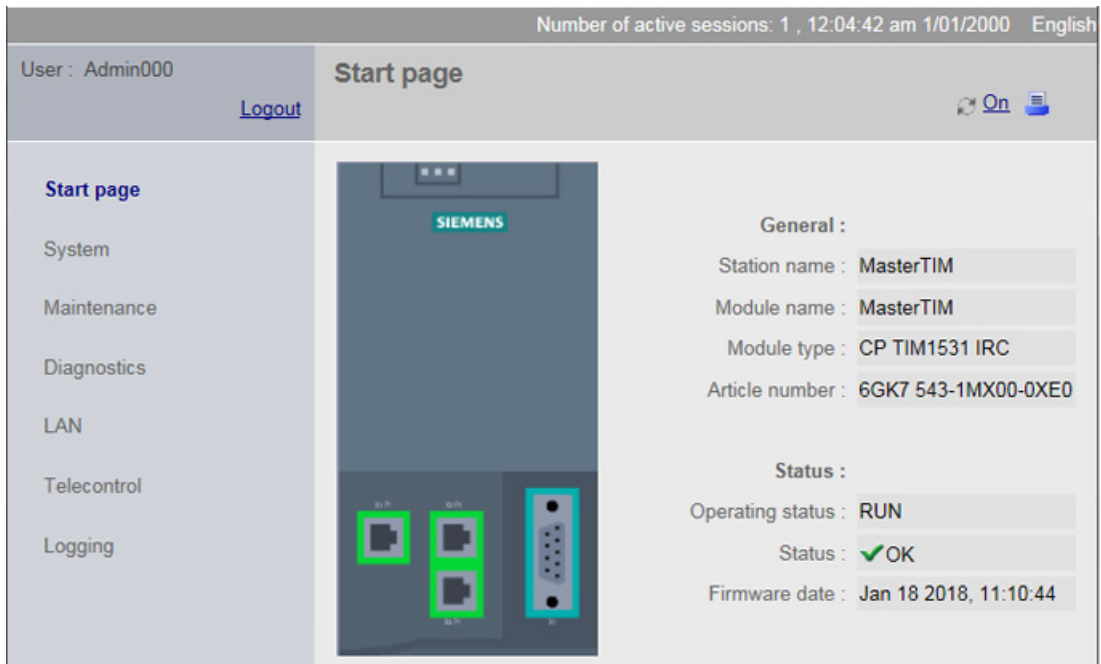


Figure C-1 Start page of the WBM

The page shows general data of the module.

General

- **Station name**
Parameter configured in STEP 7
- **Module name**
Parameter configured in STEP 7
- **Module type**
- **Article number**

Status

- **Operating status**

Current operating status of the TIM

- **Status**

Status of the firmware startup of the TIM:

- TIM started up free of errors
- Startup aborted with error

- **Firmware date**

Date the firmware currently being used was generated

Format: MMM DD YYYY, hh:mm:ss

C.5 System

C.5.1 Device info

Module

- Short designation
Parameter configured in STEP 7
- Article number
- Hardware product version
- Firmware version
- Rack
- Slot

Module information

- Module name
Parameter configured in STEP 7

Vendor information

- Vendor
- Serial number
Serial number of the device

C.5.2 SD card

SD card

SD card

- **SD card inserted**

yes / no

- **Free memory space / total**

Display of the free memory space still available and the total usable memory capacity

- **Content**

Display of the messages and files saved on the SD card

C.5.3 System time

System time

The current system time of the TIM is displayed in the title bar of the WBM.

- **Input box for time**

Format: YYYY-MM-DD hh:mm:ss

In the input box, you can manually enter the time and transfer it to the TIM.

When making your entry, keep to the specified format.

Month, day, and hour can also be entered as single digits. Example: March is accepted as "03" or as "3".

- **Apply time of day**

When you click this button, you transfer the time entered above to the TIM.

- **Adopt PC time**

When you click this button, the TIM adopts the time of day from the connected PC.

C.5.4 NTP

NTP

- **NTP server list**

Shows the addresses of the configured NTP servers.

C.5.5 Web server

Web server

- **Disable Web server**

Disables the Web server of the TIM. The setting is adopted in the configuration data of the TIM.

Note**No HTTP/HTTPS connection to the TIM**

If you disable the Web server of the TIM, you lose the possibility to access the TIM via HTTP/HTTPS.

Access is only possible again after loading the configuration data (with enabled Web server access).

- **Automatic update**

Enable the option if the contents of the Web pages are to be updated automatically.

If the option is disabled, the pages are updated at the interval you configured in STEP 7.

- **Update interval (s)**

Here, the update interval configured in STEP 7 is displayed

in seconds.

If the option is enabled (above) you can enter the desired update interval manually.

- **Save**

Applies the update interval entered manually.

C.5.6 DNS configuration

DNS server list

- **List of configured DNS servers**

Servers configured in STEP 7

C.6 Maintenance

C.6.1 Firmware

Firmware

This page displays the most important version data of the firmware currently being used.

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

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

If a new firmware version is available, you can download the firmware file from the PC to the TIM via this WBM page.

Note

Digitally signed and encrypted firmware prevents manipulation by third parties

To be able to check the authenticity of the firmware, the firmware is digitally signed by Siemens. This allows manipulation by third parties to be detected and prevented.

Note

Do not operate during the update

During the update of the firmware until the TIM restarts, the WBM is not blocked.

Do not perform any operations during this time (e.g. no restart).

Note

Do not switch off the power supply

During activation of the firmware do not switch off the power supply. This avoids the occurrence of inconsistent statuses.

Firmware

The following information is shown:

- **Firmware version**
Version of the firmware currently being used by the TIM.
- **Date**
Date the firmware was generated

Firmware update

Download the firmware file to the file system of your connected PC.

- **File**

After selecting a firmware file stored on the PC using the "Browse" button, the file name is displayed here.

- **Browse**

Searches the file system of the PC for a firmware file saved there that is intended to be loaded on the TIM.

- **Load on device**

By clicking the button, download the selected firmware file to the TIM.

Note that updating the firmware can take a while. You can recognize the current status of the firmware download based on the LED pattern.

After updating the firmware the TIM starts up again automatically.

C.6.2 Operating status

Operating statuses

Apart from using this WBM page, you can also execute the functions described below using the switch of the TIM.

The buttons have the following functions:

- **Run a restart**

When restarting, existing telecontrol connections are interrupted and cyclic processing stops. The TIM restarts.

- **Reset to factory settings**

Note

Data loss: Note the effects of a reset

Before you reset, note the effects.

Resets the TIM to the factory settings. During this all parameters are reset to the initial statuses as shipped and the TIM restarts.

If you use an SD card and you want to reset the TIM to the factory settings, you must pull the SD card (while disconnected from the power) before resetting. If the SD card remains inserted, the TIM starts up again with the configuration data on the SD card.

Resetting to factory settings: Effect

Note

Configuration data is deleted

Resetting to factory settings deletes all configuration data in the TIM.

- **Deleted data**

The following data is deleted by resetting to factory settings:

- Configured IP addresses of the LAN interfaces X1, X2 and X3
- All other configuration data in the work memory of the TIM

- **Data not deleted**

The following data is not deleted by resetting to factory settings:

- MAC addresses of the LAN interfaces

C.7 Diagnostics

C.7.1 Events

Diagnostics messages

Table

The table lists the last diagnostics events to occur on the TIM with the following information:

- **Number**

Consecutive number

- **Time**

Time of the diagnostics event

- **Date**

Date of the diagnostics event

- **Event type**

The diagnostics messages are classified as follows:

- INFO
Information about a special event
- WARNING
Warning of a possibly unwanted event
- ERROR
Internal error. The TIM starts up.
- FATAL
Serious error that impairs or interrupts the operation of the TIM.

- **Event**

Plain text of the diagnostics event

Copy of the diagnostics buffer

Using the button, you save the content of the diagnostics buffer on the PC.

The diagnostics buffer

The diagnostics buffer receives diagnostics messages for internal events and errors. It can hold a maximum of 200 entries. When the maximum number is exceeded, the oldest entries are overwritten.

The entries in the diagnostics buffer contain a consecutive number, a classification, a time stamp and the message text.

Below you will find several examples of events that are entered in the diagnostics buffer:

- TIM startup
- Change to the configuration
- Establishment/abort of the communications connection
- Time-of-day synchronization
- Power failure

C.7.2 Notifications

Messages

Table

The table lists the last messages of the TIM with the following information:

- **Number**
Consecutive number
- **Time**
Time of sending
- **Trigger**
Trigger that fired generation of the message.
- **Recipient**
Configured recipient of the message
- **Message**
Message text
- **Processing status**
Status of the sending of the message

You will find an overview of the possible statuses in the section Processing status of the messages (SMS / e-mail) (Page 160).
- **Type**
Type of the message

C.8 LAN

C.8.1 Ethernet interface [Xn]

- The three Ethernet interfaces of the TIM are selected via the upper tabs.
 - X1 ... X3
- The parameters of the selected interface are shown in the lower series of tabs:
 - IPv4 parameters
 - IPv6 parameters
 - Statistics

IPv4 parameters

Network attachment

- **MAC address**

IP parameters

- **IP address**

Current IP address

- **Subnet mask**

Default or last configured subnet mask.

- **Default router**

Configured default router

- **Address assignment**

Shows how obtaining the IP address is configured in STEP 7:

- Set IP address in the project
- IP address from DHCP server
- Set IP address on the device

The IP address obtained using other services outside the configuration

Ports

- **Port number**

Port of the interface

- **Connection status**

- OK: Existing connection to the network
- Not OK: No connection

- **Settings**

Behavior of the network setting:

- Automatic
- Manual setting for transmission speed and direction dependency

- **Mode**

Used transmission speed and direction dependency (duplex/half duplex)

- **Connection medium**

Connected medium (copper / optical)

IPv6 parameters

- **IPv6 address**
Currently used IPv6 address
- **Gateway**
Display of IPv6 addresses of up to two gateways

Statistics

Statistics

The following statistical data of the interface since the TIM last started up is displayed.

- **Bytes received**
- **Received frames discarded**
Number of messages that were discarded on receipt due to address, protocol or data errors.
- **Error on receipt**
Number of internal errors on receipt
- **Frames with unknown protocol**
Number of messages with the wrong protocol
- **Bytes sent**
- **Sent unicast frames**
- **Dropped frames**
Number of frames that were discarded due to errors when sending.
- **Error sending**
Number of internal errors when sending
- **Frames in the send mailbox**
Number of unsent frames waiting for transfer.

C.9 Telecontrol

C.9.1 Partner information

C.9.1.1 Connection overview

The tab shows you information on the communications partners and the connection status of the TIM.

Table

The column headers have the following meaning:

- **Connection status**

The status of the connections to the assigned CPU and to the remote partners is shown as follows:

- **Green: Connected**

All connections are established.

- **Yellow: Connected**

Some of the possible connections are established.

- **Red: Disconnected**

None of the possible connections is established

- **Partner**

Possible partner types:

- Local CPU

The CPU assigned to the TIM in the configuration.

- Application

(e.g. WinCC)

- TIM

TIM of the remote station

- Partner CPU

CPU of the remote station

- CP ...

CP of the remote station (CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC / CP 1542SP-1 IRC)

- **Subscriber number**

Subscriber number of the partner

When you click on the '±' icon in a table row, the relevant parameters are displayed.

The following information is available on each subscriber:

- Information on the subscriber
- Information on the transmission path

Information on the subscriber

Local CPU

- **Status**
Operating status of the local CPU
- **Number of connections**
Number of connections between the TIM and local CPU

Remote partner

- **Partner type**
 - Application (e.g. WinCC)
 - CPU
CPU of the remote station
 - TIM
 - CP ...
- **Subscriber number**
Subscriber number of the partner
- **Time master**
Display of the option configured on the partner:
Yes / No
- **Security options**
Display of the active access level (protection):
ON / OFF
- **Connection status**
 - Connected
 - Not connectedFor the meaning of the colors, see above (Connection overview).
- **Frame memory status**
State of the send buffer, only relevant for a communications module:
 - **Normal operation**
The send buffer is working normally. The memory space allocation is between 10 and 80 %.
 - **80% limit reached**
When the ST7 protocol is used, the TIM switches to the forced image mode at 80 % occupation of the send buffer.
 - **Overflow**
100% occupation of the send buffer

Transmission path

Information on the transmission path

Local CPU

- **Interface ID**
Ethernet interface of the TIM for connection with the local CPU
X1 (ETH1) / X2 (ETH2) / X3 (ETH3)
- **CPU type**
Type of the local CPU
- **Connection status**
 - Connected
 - Not connected
- **CFB reference**
Local ID (decimal) of the S7 connection
- **Local TSAP**
Local TSAP of the S7 connection
- **Remote TSAP**
Remote TSAP of the S7 connection
- **IP address**
IP address of the CPU

Remote partner

- **Address**
IP address or WAN address of the interface of the TIM
- **Interface**
Ethernet interface of the TIM for connection with the remote partner
X1 (ETH1) / X2 (ETH2) / X3 (ETH3)
- **CFB reference**
Local ID (decimal) of the S7 connection
- **Connection type**
Display of several of the following connection properties:
 - PBK connection
Configured S7 connection
 - ST7
ST7 connection via classic WAN

- DNP3
DNP3 connection via classic WAN network
- IEC
IEC 60870-5-101 connection via a classic WAN network
- MSC connection
Only ST7: Connection of the MSC protocol for which no S7 connection is required.
- CR connection
Read/write connection to the local CPU that does not require an S7 connection.
- X connection
Unconfigured S7 connection that uses the SFCs "X_SEND" and "X_RCV".
- Permanent / temporary
Permanent or temporary telecontrol connection
- GPRS / no GPRS
GPRS connection or no GPRS connection
- local / remote
Connection to a local or remote partner
- **Connection status**
 - Connected
 - Disconnected

C.9.1.2 Send buffer

The tab provides information on the send buffer (frame memory) of the local or remote TIM.

Information on the send buffer

Information on the send buffer of the TIM:

- **Size (memory spaces)**
Configured size of the send buffer as number of memory spaces
One memory space is reserved per frame.
- **Free (memory spaces)**
Memory currently free as number of memory spaces
- **Free (%)**
Currently free memory space in percent
In brackets: Number of configured events / Max. number of events

Table

The column headers have the following meaning:

- **Source subscriber**
Subscriber number of source subscriber from which the connection is established.
- **Destination subscriber**
Subscriber number of destination subscriber to which the connection is established.
- **Number of events**
Number of configured events of the source subscriber

Parameters

When you click on the '±' icon in a table row, the relevant parameters are displayed.

- **Unconditional spontaneous**
Number of stored frames to be sent unconditionally and spontaneously (only relevant in dial-up networks).
- **Prioritized**
Number of stored frames to be sent with high priority.
- **Identification**
Hexadecimal value that codes the information below.
 - Unconditional spontaneous (9)
Number of frames with the transmission mode "Spontaneous (unsolicited - direct transfer)"
 - XGA (10)
Only ST7: Pending general request
 - Overflow (11)
Send buffer overflow prewarning
 - Transmission stop (12)
Sending data to the remote partner is temporarily blocked because the partner cannot be reached or a memory bottleneck has occurred at the partner.
 - Forced image mode (14)
Only ST7: When the send buffer is 80% full, the TIM switches to the forced image mode.
To prevent a send buffer overflow, all data frames are treated as image frames. Send buffer frames are also treated as image frames; the data is overwritten by newer data.
 - Locked (15)
The send buffer is locked.

C.9.2 Data points

The tab shows you information on the configured data points of the TIM.

Data points

- **Data point number**
Consecutive number
- **Name & type**
Name and type of the data point
When you hold the cursor over the column entries, additional properties of the data points are displayed in tooltips.
- **Type identifier**
Type of the data point
- **Object number**
Object number of the ST7 data point
- **Object group**
Object group (DNP3 / IEC 60870-5; the static variants are displayed with DNP3)
- **Data point index**
Index of the DNP3/IEC data point
- **Status**
Occasion of transfer/status of TIM
- **Current value**
Currently saved value
- **Historical value**
Last sent value
- **Time stamp**
Time stamp of last value change

C.10 Logging

Functions of logging

On this page, you can log the data traffic of the TIM using PCAP functionality for diagnostics purposes.

If an error occurs or if the TIM behaves in an unwanted manner, the communication behavior of the TIM can be recorded. The frame traffic of the TIM is recorded for a defined time or for a configurable number of frames.

The log files are stored as PCAP files on the connected PC and can be evaluated with the Wireshark program, for example.

Options:

- **Ethernet Interface X1 / X2 / X3**
Enable the interfaces for which you want to record data.
- **Data volume (kB)**
Via the input box, you specify the overall size of the logging file.
Maximum file size: 10000 kB
- **Recording acc. to time**
If the option is enabled, the recording is made for a configurable time.
Via the input box, you specify the recording time in seconds.
Max. recording duration: 600 s
- **Recording acc. to frames**
If the option is enabled, the recording is made for a configurable number of frames.
Via the input box, you specify the number of frames.
Max. number of frames: 500 s
- **Start**
With this button you start the logging.
- **Stop**
With this button you stop the logging.

Security

D.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/21764/dl>)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the module directly to the Internet. If a connection of the module to the Internet is required, use the security variants of the telecontrol protocols or use protection mechanisms in front of the module. 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 and security functions of the CPU
Configure access to the CPU under "Protection and Security".
Use the other security functions of the CPU to prevent unauthorized access to the station.
You will find information on this in the information system of STEP 7.
- Security function of the communication
 - Using the security functions of the telecontrol protocols.
 - Use the secure protocol variants, for example NTP (secure) or SNMPv3.
 - 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.
- Deactivate DHCP at interfaces to public networks such as the Internet, for example, to prevent IP spoofing.

Table: Meaning of the column titles and entries

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

- **Protocol / function**
Protocols that the device supports.
- **Port number (protocol)**
Port number assigned to the protocol.
- **Default of the port**
 - Open
The port is open at the start of the configuration.
 - Closed
The port is closed at the start of the configuration.
- **Port status**
 - Open
The port is always open and cannot be closed.
 - Open after configuration
The port is open if it has been configured.
 - Open (login, when configured)
As default the port is open. After this port is configured, the communications partner needs to log in.
 - Closed after configuration
The port is closed because the module is always client for this service.
- **Authentication**
Specifies whether or not the protocol authenticates the communications partner during access.

The following ports are relevant. Not all protocols are supported by every device type.

Table D- 1 Server ports

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
IEC 60870-5-104	2404 (TCP) Can be set	Closed	Open after configuration	No
IEC 60870-5-104 with TLS	19998 (TCP) Can be set	Closed	Open after configuration	Yes, when Secure Communication is enabled.
S7 and online connections	102 (TCP)	Open	Open after configuration	No
Online security diagnostics (security devices)	102 (TCP)	Open	Open after configuration *	Yes

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
Communication via SINEMA RC	443 (TCP), 5243 (UDP)	Closed	Open after configuration	Yes
HTTP	80 (TCP)	Closed	Open after configuration	No
HTTPS	443 (TCP)	Closed	Open after configuration	Yes
SNMP	161 (UDP)	Closed	Open after configuration	No (SNMPv1) Yes (SNMPv3)
IPsec (Security devices)	500 (UDP)	Closed	Open after configuration	Yes

* Some service providers consider the opening of port 102 a security vulnerability. To avoid opening port 102 during online diagnostics, see section Online security diagnostics via port 8448 (Page 156).

Ports of communication partners and routers

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

These can be:

- NTP / NTP (secure) / 123 (UDP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- SINEMA RC Autoconfiguration / 443 (TCP) - can be set
- SINEMA RC and OpenVPN / 1194 (UDP) - can be set in SINEMA RC
- IPsec / 500 (TCP) / 4500 (UDP)
- OpenVPN / 1194 (UDP)
- Syslog / 514 (UDP)

D.2 Syslog messages of the TIM 1531 IRC

D.2.1 Structure of the Syslog messages

The Syslog server collects log information of the devices about specific events. The Syslog messages are received by the Syslog server via the set UDP port (standard: 514) and output according to RFC 5424 or RFC 5426. The Syslog protocol prescribes a fixed sequence and structure of the possible parameters.

Syslog messages are structured as follows according to RFC 5424:

Part / Parameter	Explanation
HEADER	
PRI	PRI contains the coded priority of the Syslog message, broken down into Severity (severity of the message) and Facility (origin of the message).
VERSION	Version number of the Syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2010-01-01T02:03:15.0003+02:00" as the local time including the time zone and correction for daylight saving / standard time if needed.
HOSTNAME	References the source computer with its name or the IP address. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX IPv6 address according to RFC4291 Section 2.2 "-" is output if information is missing. Example in the product: The station name configured in the "System" tab for the RTU.
APP-NAME	Device or application from which the message originates. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.
STRUCTURED-DATA	
timeQuality	The structured data element "timeQuality" provides information on system time. Example: [timeQuality tzKnown="0" isSynced="0"] The "tzKnown" parameter indicates whether the sender knows its time zone (value "1" = known; value "0" = unknown). The "isSynced" parameter indicates whether the sender is synchronized with a reliable external time source, e.g. via NTP (value "1" = synchronized; value "0" = not synchronized).
sysUpTime	The "sysUpTime" parameter is meta-information about the message. It specifies the time (in hundredths of seconds) since the last re-initialization of the network management part of the system.
MSG	
MESSAGE	Message as ASCII string (English)

Note

Additional information

You can read more detailed information on the structure of the Syslog messages and on the meaning of the parameters in the RFCs:

<https://tools.ietf.org/html/rfc5424>

<https://tools.ietf.org/html/rfc5426>

D.2.2 Tags in Syslog messages

The tags are displayed in the section "Syslog messages" in the field "Message text" within curly brackets {variable}.

The output messages can contain the following tags:

Tag	Description	Format	Possible values or example
{Ip address}	IPv4 address according to RFC1035 IPv6 address according to RFC4291 Section 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{FQHN}	Fully Qualified Host Name: Completely specified host name; specification as domain (FQDN) or as IP address.	FQDN: host1.com IPv4: %d.%d.%d.%d	server1 192.168.1.105
{Src port} {Dest port}	Port number (decimal)	%d	0 ... 65535
{Client mac} {Dest mac} {Src mac}	MAC address	%02x:%02x:%02x:%02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	Layer 4 protocol or service used that generated the event.	%s	UDP TCP WBM Telnet SSH Console TFTP SFTP
{Group}	Name for identification of the group (string)	%s	it-service
{User name}	String (without spaces) that identifies the authenticated user by his or her name.	%s	<name>
{Local interface}	Symbolic name of the local interface	%s	Console
{Action user name} or {Destination user name}	Identifies the user based on his/her name This is not the authenticated user.	%s	<First name>.<Surname>
{Role}	Symbolic name of the group role	%s	Administrator
{Time minute} {Timeout}	Number of minutes	%d	44
{Time second}	Number of seconds	%d	44
{Failed login count}	Number of failed login attempts	%d	10
{Max sessions}	Maximum number of sessions	%d	10
{Vap}	Symbolic name of the virtual access point interface	(%s) or (%s %s)	VAP1.1
{Status} {Reason}	Additional status information (number or text)	must start with "(" and end with ")"	(Invalid group cipher) (Unknown peer)
{Wlan interface}	Symbolic name of the WLAN interface	%s	WLAN1
{Ssid}	SSID in ASCII representation; any number of spaces.	%s	MyWLAN
{ssid_Hex}	SSID in Hex representation	%02x%02x%02x%02x%02x%02x	050E081234
{Channel}	Name of the channel	%s	12
{Signal strength}	Signal strength	%d	12
{Version}	Name of the version (without spaces)	%s	V1.0.3SP1
{Resource}	Resource name protected by the protection level concept (without spaces)	%s	FullReadAccess

Tag	Description	Format	Possible values or example
{Trigger condition}	Character string (without spaces) for a trigger condition that activates the relevant function.	%s	E/A-Pin FB-88
{Trigger pin}	String (without spaces) for an IO pin that triggered the event.	%s	DI1
{Firewall rule}	String (with space) for the firewall rule set	%s	Rule1
{Subject}	String (with space) for the subject in the certificate. Used as part of the certificate-based authentication and must include Unicode characters.	%s With UTF8 code: %S	(Peter Maier)
{Config detail}	String (with space) for the configuration	%s	OpenVPN
{Connection name}	Name of the VPN connection		to_Baugruppe1
{Firewall accept}	Firewall action executed (accepted package)		ACCEPT
{Firewall action reject}	Firewall action executed (rejected package)		REJECT DROP
{Length}	Length of the network packet (in bytes)	%d	52
{Network interface}	Symbolic name of a network interface	%s	vlan 1

D.2.3 Explanation of the messages

This section describes the Syslog messages. The structure of the messages is based on IEC 62443-3-3.

D.2.4 Messages for TIM 1531 IRC

User identification and authentication

Message text	{Protocol}: User {User name} logged in from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.0.1.
Explanation	Valid login information that was specified during login.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{Protocol}: User {User name} failed to log in from {IP address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.
Explanation	Incorrect user name or password specified during login.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Message text	{protocol}: User {user name} logged out from {ip address}.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
Explanation	User session ended - logged out.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 1.1

Session lock

Message text	{Protocol}: The session of user {User name} was closed after {Time second} seconds of inactivity.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The session of user admin was closed after 60 seconds of inactivity.
Explanation	The current session was ended due to inactivity.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.5

Limiting the number of simultaneous sessions

Message text	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
Example	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The maximum number of 10 concurrent login sessions exceeded.
Explanation	The maximum number of parallel sessions has been exceeded.
Severity	Warning
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.7

Non-repudiation

{Protocol}: User {User name} has changed {Config detail} configuration.

Example	SSH: User admin has changed VLAN configuration.
Explanation	A user has changed specific configuration values. In the example, the "admin" user has changed the VLAN configuration.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

Example	SSH: User admin has initiated a reset to factory defaults.
Explanation	A user has initiated a reset to default settings. In the example, the user "admin" has initiated a reset to default settings.
Severity	Info
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 2.12

Software and information integrity

Message text	Integrity violations in configuration data detected
Example	Integrity violations in configuration data detected
Explanation	An integrity fault was detected while the configuration integrity was being checked.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 3.4

Restoration of the automation system**{Protocol}: Firmware {Version} was activated.**

Example	WBM: Firmware v2.0 was activated.
Explanation	A firmware version was successfully activated. In the example, the firmware version "v2.0" was successfully activated.
Severity	Notice
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: Firmware activation failed.

Example	WBM: Firmware activation failed.
Explanation	The firmware activation has failed.
Severity	Error
Facility	local0
Standard	IEC 62443-3-3 Reference: SR 7.4

Bibliography

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.

You can find additional references in the bibliographies of the individual manuals.

/1/

SIMATIC NET - TeleControl

Siemens AG

Configuration manuals of the protocols:

- TeleControl Basic

- SINAUT ST7

- DNP3

- IEC 60870-5

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

12/

12/

SIMATIC NET
TIM 1531 IRC
Operating instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/24710/man>)

13/

SIMATIC NET
CP 1243-1
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/103948898>)

14/

SIMATIC NET
CP 1243-8 IRC
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/21162/man>)

15/

SIMATIC NET
CP 1243-7 LTE
Operating Instructions
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15924/man>)

16/

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

/7/

SIMATIC
S7-1200 Automation System
system manual
Siemens AG
Link: (<http://support.automation.siemens.com/WW/view/en/34612486>)

/8/

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

/9/

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

/10/

SIMATIC NET
Industrial Ethernet
System manual
Siemens AG

- Volume 1: Industrial Ethernet
Link: (<https://support.industry.siemens.com/cs/ww/en/view/27069465>)
- Volume 2: Passive network components
Link: (<https://support.industry.siemens.com/cs/ww/en/view/84922825>)

Index

A

Abbreviations, 3
Authentication, 25

C

Classic WAN, 47
Connection interrupted, 31
Connection resources, 24
Connection status - diagnostics, 155
Consistent data area, 18
Cross-references (PDF), 5

D

Data buffering, 19, 25
Data points - Configuration, 112
Diagnostics messages, 196
Direct communication, 13
 Configuration, 123
Documentation - Structure, 4

E

E-mail
 Number of messages, 19, 25
Encryption, 25

F

Forced image mode, 126
Frame memory, 19, 25

G

Gateway (VPN), 82
Glossary, 6

I

Image memory, 126
Importing a certificate - e-mail, 70
Internet connections, 31

IP address - fixed, 48
IPsec, 78

M

MIB, 160
Mirroring, 121
MSC, 26
MSCsec, 26

N

Node station, 12
NTP (secure), 39
IPsec tunnel

O

Online diagnostics, 33
Online functions, 154
OUC (Open User Communication), 163

P

Partner status - diagnostics, 155
Passive VPN connection establishment, 82
Port 8448, 156

R

RS-485
 Configuration, 52, 53

S

S7 connections
 Enable, 33
SD card, 25, 35
Security
 Protocols, 25
Security diagnostics, 156
Security functions, 23
Send buffer, 19, 25, 126
SIMATIC NET glossary, 6

SMS

- Number of messages, 19
- SMTPS, 70
- SNMP, 159
- SNMPv3, 26, 75
- Spontaneous, 130
- SSL/TLS, 70
- STARTTLS, 70
- STEP 7 - version, 15
- SYSLOG, 77

T

- Time stamp, 18
- Trigger tag - resetting, 129, 145

U

- User data, 18

V

- VPN, 19, 31, 78

W

- WAN - creating a network, 46
- Web server, 50