

# SIEMENS

## SIMATIC NET

### S7-1500 - TeleControl TIM 1531 IRC

#### Operating Instructions

#### Preface

---

#### Application and functions

---

1

#### LEDs, connectors, switches, card slot

---

2

#### Installation, connecting up, commissioning

---

3

#### Configuration

---

4

#### The Web server (WBM)

---

5

#### Diagnostics and upkeep

---

6

#### Technical specifications

---

7

#### Approvals

---

8

#### Dimension drawings

---

A

#### Accessories

---

B

#### Documentation references




---

C

## 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.

 <b>DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.
 <b>WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.
 <b>CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.
<b>NOTICE</b>
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:

 <b>WARNING</b>
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

## CAUTION

To prevent injury, read the manual before use.

## Validity of this manual

This manual is valid for the following product:

TIM 1531 IRC

Article number: 6GK7 543-1MX00-0XE0

Hardware product version 1

Firmware version 1.0

Communications module for SIMATIC S7-1500 / S7-400 / S7-300, SINAUT ST7 protocol, with three RJ-45 interfaces for communication via IP-based networks (WAN / LAN) and an RS-232/RS-485 interface for communication via classic WAN networks



Figure 1 TIM 1531 IRC

You will find the the article number of the device on the top right of the housing.

You will find the hardware product version of the device printed as a placeholder "X" on the right of the device (for example X 2 3 4). In this case, "X" would be the placeholder for hardware product version 1.

You will find the MAC addresses of the three Ethernet interfaces at the front in the middle of the housing.

## Purpose of the manual

This manual describes the properties of this device and shows application examples.

The manual supports you when installing, connecting up and commissioning the device.

The required configuration steps for the device are described.

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

## Required experience

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

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

## Abbreviations/acronyms

This manual often uses the following abbreviations/acronyms:

- **TIM / submodule / module**

The names are used instead of the full product name "TIM 1531 IRC" of the device.

- **ST7**

Short form for the telecontrol protocol "SINAUT ST7"

- **WBM**

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

## Cross references

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

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

## Current manual release on the Internet

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

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/24710/man>)

## Sources of information and other documentation

You will find an overview of further reading and references in the Appendix of this manual.

---

## License conditions

---

### Note

#### Open source software

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

---

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

- OSS\_TIM1531IRC\_86.pdf
- OSS\_TIM1531IRC-TI\_76.pdf

## Security information

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

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

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit

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

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

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

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

## Firmware

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

## Training, Service & Support

You will find information on training, service and support in the multilanguage document "DC\_support\_99.pdf" on the Internet pages of Siemens Industry Online Support:

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

## SIMATIC NET glossary

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

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

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

## Recycling and disposal



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

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

Keep to the local regulations.

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

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

# Table of contents

	<b>Preface .....</b>	<b>3</b>
<b>1</b>	<b>Application and functions .....</b>	<b>11</b>
1.1	Properties of the TIM .....	11
1.2	Communications services .....	12
1.3	Security functions.....	15
1.4	Other services and properties.....	17
1.5	Configuration examples .....	19
1.6	Performance data and configuration limits .....	23
1.7	Requirements and compatibility.....	25
1.7.1	Software requirements.....	25
1.7.2	Usable CPUs .....	25
<b>2</b>	<b>LEDs, connectors, switches, card slot .....</b>	<b>27</b>
2.1	Overview: LEDs, connectors, switches, card slot.....	27
2.2	LEDs .....	28
2.3	Electrical connectors.....	30
2.3.1	Ethernet interfaces (X1, X2, X3).....	30
2.3.2	Serial interface X4.....	30
2.3.3	X80: External power supply .....	31
2.4	Switch.....	31
2.5	SD card slot .....	33
<b>3</b>	<b>Installation, connecting up, commissioning.....</b>	<b>35</b>
3.1	Important notes on using the device.....	35
3.2	Installation.....	35
3.3	Connecting up.....	37
3.4	Inserting the SD card .....	38
3.5	Commissioning .....	39
3.6	Startup - LED pattern .....	40
<b>4</b>	<b>Configuration .....</b>	<b>41</b>
4.1	Security recommendations .....	41
4.2	Configuration in STEP 7 .....	43
4.3	Communication types .....	45
4.3.1	Communication types .....	45
4.3.2	Communication via the SINAUT ST7 protocol .....	46

4.4	Settings .....	48
4.5	Overview: Connection to LAN / WAN .....	48
4.6	WAN settings .....	50
4.7	Networking a TIM (Ethernet addresses / WAN settings) .....	52
4.8	Ethernet-specific parameters .....	54
4.8.1	Ethernet interface > address parameters .....	54
4.8.2	TCP connection monitoring.....	54
4.9	Advanced options .....	54
4.9.1	MSC protocol settings.....	54
4.9.2	Dedicated line .....	57
4.9.3	Dialup network .....	61
4.10	Ethernet interface > Access to the Web server .....	65
4.11	Creating telecontrol connections.....	66
4.12	Time stamp .....	71
4.13	Web server.....	72
4.14	Communication with the CPU .....	73
4.15	Time-of-day synchronization.....	77
4.16	MSC authentication.....	81
4.17	SMSC.....	82
4.18	E-mail configuration .....	82
4.19	SNMP.....	83
4.20	Security and protection .....	85
4.20.1	Certificate manager.....	85
4.20.2	Handling certificates.....	85
4.20.3	Protection .....	87
4.20.4	Configuring access protection.....	88
4.21	Data points.....	90
4.21.1	Data point configuration .....	90
4.21.2	"General" tab.....	96
4.21.3	Datapoint types .....	97
4.21.4	Process image, type of transmission, event classes, triggers .....	99
4.21.5	Read cycle .....	102
4.21.6	"Trigger" tab .....	103
4.21.7	Threshold value trigger .....	104
4.21.8	Analog value preprocessing.....	106
4.21.9	Command outputs.....	112
4.21.10	Partner stations .....	113
4.22	Messages.....	114
4.22.1	Message configuration.....	114
<b>5</b>	<b>The Web server (WBM) .....</b>	<b>117</b>
5.1	Supported Web browsers .....	117
5.2	Establishing a connection to the WBM of the TIM.....	117



5.3	General functions of the WBM.....	118
5.4	Start page .....	119
5.5	System .....	120
5.5.1	Device info .....	120
5.5.2	SD card .....	121
5.5.3	NTP .....	121
5.5.4	DNS configuration.....	121
5.6	Diagnostics .....	122
5.6.1	Diagnostics messages .....	122
5.6.2	Notifications .....	123
5.7	LAN .....	124
5.7.1	Ethernet interface [Xn] .....	124
5.8	Telecontrol .....	126
5.8.1	Partner information .....	126
5.8.2	Data points.....	130
<b>6</b>	<b>Diagnostics and upkeep.....</b>	<b>131</b>
6.1	Diagnostics options.....	131
6.2	Online functions .....	132
6.3	SNMP.....	133
6.4	Processing status of the messages (SMS / e-mail).....	135
6.5	Update firmware.....	137
6.6	Resetting to factory settings .....	139
6.7	Module replacement .....	141
<b>7</b>	<b>Technical specifications .....</b>	<b>143</b>
7.1	Technical specifications .....	143
7.2	Pinout of the Ethernet interfaces .....	145
7.3	Pin assignment of the serial interface.....	145
<b>8</b>	<b>Approvals.....</b>	<b>147</b>
<b>A</b>	<b>Dimension drawings.....</b>	<b>151</b>
<b>B</b>	<b>Accessories .....</b>	<b>153</b>
B.1	Power supply .....	153
B.2	SD cards .....	153
B.3	Routers, modems, antennas.....	155
B.3.1	Dedicated line and dialup network modems .....	155
B.3.2	MODEM MD720.....	156
B.3.3	Router SCALANCE M.....	157
B.3.4	Mobile wireless antennas .....	158
B.4	Cables, connecting cables.....	160
B.4.1	Connecting cables for connecting modems.....	160
B.4.2	Cable for RS-485 connection.....	162

<b>C</b>	<b>Documentation references .....</b>	<b>163</b>
	<b>Index .....</b>	<b>167</b>

# Application and functions

## 1.1 Properties of the TIM

### Application

The TIM 1531 IRC is a telecontrol communications module for the following SIMATIC automation systems:

- S7-300
- S7-400
- S7-1500

The TIM serves as the connection of the SIMATIC stations via public or private infrastructures to a telecontrol master station. Precisely one local CPU is assigned to the TIM.

As a standalone device it is not dependent on the S7 device family or rack type of the assigned CPU.

For the telecontrol communication the TIM uses the "SINAUT ST7" protocol.

Due to the capability of the TIM to establish redundant transmission paths between stations and to the master station and the option of storing process values the communication has a high degree of reliability.

### Master station types

As the connection partner of the TIM in a telecontrol master station, the following computer assisted applications are supported:

- SINAUT ST7cc
- SINAUT ST7sc
- SIMATIC PCS 7 / WinCC TC
- SIMATIC WinCC OA

If no master station PC is used, the TIM can be used as a master station. For visualization, for example, an HMI panel can be used via the CPU.

## Interfaces of the TIM

The TIM is equipped with the following interfaces:

- **3 x Ethernet interface RJ-45**

Connection to three different subnets

Telecontrol communication via IP-based WAN/LAN networks

- **1 x serial interface**

Default can be switched over by configuration: RS-232 ⇔ RS-485

Telecontrol communication via the following WAN networks:

- Classic WAN networks: Dedicated line, dialup network
- IP-based networks (can be switched over by the configuration)

You will find the supported transmission protocols and network types in the section Communications services (Page 12).

## Network node types

With its four interfaces, the TIM can be used at the following positions of a WAN network:

- Master station
- Node station
- Station

## Expansion of existing SINAUT systems

In existing SINAUT systems with SIMATIC S7-300/400 stations and TIM modules for the telecontrol functions, the TIM 1531 IRC can be used universally for expansions.

# 1.2 Communications services

The following communications services are supported:

## Telecontrol communication

### Network types

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

- Industrial Ethernet
- Dedicated line / wireless network
- Analog dial-up network, ISDN network

- Mobile wireless networks (with the aid of a SCALANCE M router)
  - GSM / GPRS (2G)
  - UMTS (3G) / HSPA+
  - LTE (4G)
- IP-based wireless networks

You will find an overview of the transmission paths and network types in the section Overview: Connection to LAN / WAN (Page 48).

### **The "SINAUT ST7" protocol**

For telecontrol communication via telecontrol networks the TIM uses the ST7 protocol on the application layer (OSI layer 7).

The protocol supports the following functions and services

- **Communication with the control center**

The TIM communicates via LAN or WAN with an application in the master station.

You will find the supported master station types in the section Properties of the TIM (Page 11).

- **Direct communication**

In dial-up networks, mobile wireless networks and Ethernet networks, there is direct communication between the subscribers.

- **Inter-station communication**

In dedicated line networks and with communication via the Internet with a mobile wireless network (GSM/MSC), the TIM supports inter-station communication between S7 stations via the master station.

With inter-station communication, the TIM establishes a connection to the master station. The master station forwards the messages to the destination station.

- **Messages: SMS / e-mail**

When configurable events occur, the TIM can send SMS messages to mobile telephones and e-mails to PCs with an Internet connection.

- SMS messages can be sent if the TIM is connected to a mobile wireless network via the serial interface and a GSM or GPRS module (MODEM MD720).
- If the TIM is connected, e-mails can be sent via the Ethernet interface.

You configure the e-mail protocol to be used and the server access in STEP 7 in the parameter group "E-mail configuration".

You configure the messages in the message editor, see section Message configuration (Page 114). The use of program blocks is not necessary for this.

You will find information about addressing in ST7 and configuring in the section Communication types (Page 45).

### Protocols with security functions

- **MSC**

For secure telecontrol communication the transmission protocol "MSC" (OSI layer 3) is available. MSC can be used for communication between two TIM modules (not between the TIM and a master station application).

MSC is IP-based and can be used in the following networks:

- Ethernet
- Internet (DSL)
- Mobile wireless network (GSM) and Internet

The following variants of the protocol are available:

- MSC
  - Simple Internet communication via the Internet (DSL)
- MSCsec
  - Secure Internet communication when security requirements are higher.

- **IPsec / VPN (via router SCALANCE M)**

VPN stands for highly secure communication via mobile wireless and the Internet (DSL) using a SCALANCE M mobile wireless router.

For a description of the protocols, refer to the section Security functions (Page 15).

### S7 communication

For reading / writing data from and to the local CPU via S7 connections, the following services are supported.

- **PG communication**

Communication with an engineering station

- **PUT/GET**

To exchange data with a local S7-300/400 CPU the TIM supports communication using the the program blocks PUT/GET as client and server.

- **READ/WRITE**

To exchange data with a local S7-1500 CPU the TIM supports communication using the the program blocks READ/WRITE as client and server.

The Ethernet interfaces of the TIM must be configured with the network type "Neutral" for the S7 communications services.

You will find information on the communications functions and the program blocks in the STEP 7 information system.

## Web server connections (WBM)

- **HTTP/HTTPS**

The TIM has an integrated Web server with which you can connect from a PC via HTTP/HTTPS. Connections are possible via LAN or WAN

The Web pages display diagnostics information and configuration data.

You will find information on the content and operation in the section The Web server (WBM) (Page 117).

## 1.3 Security functions

### Security functions of the transmission protocols

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

- **MSC**

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

- **MSCsec**

MSCsec supports authentication of the communications partners and data encryption with a user name and password.

In addition to this, the shared automatically generated key is renewed between the communications partners at a configurable Key exchange interval.

### Further security functions of the TIM

The TIM also supports the following security functions:

- **NTP (secure)**

For secure transfer during time-of-day synchronization (with telecontrol communication disabled)

- **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, see below.

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

---

**Additional protection be using security modules**

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. The following security modules are suitable for connecting the TIM to public networks:

- SCALANCE M800

Mobile wireless routers for IP-based data transfer in mobile wireless networks of the standards GPRS, EGPRS, UMTS, LTE

- SCALANCE S

Security modules for connection to Ethernet networks

The data transfer of the TIM along with a security module can be protected from the following attacks by a combination of different security measures:

- Data espionage
- Data manipulation
- Unwanted access

Secure underlying networks can be operated via additional Ethernet interfaces of the TIM or CPU.

Using the security modules mentioned above SCALANCE M / SCALANCE S the following additional security functions can be used:

- **Firewall**

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

- **Protection for devices and network segments**

The protection provided by the firewall can cover individual devices, several devices or even entire network segments.



- **Communication made secure by IPsec tunnels (VPN)**

VPN tunnel communication allows the establishment of secure IPsec tunnels for communication with one or more security modules.

VPN can be used for communication via mobile wireless and the Internet (DSL) along with a SCALANCE M router. The SCALANCE M800 product line includes various VPN routers with encryption software and a firewall.

The router can be put together with other modules to form VPN groups during configuration. IPsec tunnels (VPN) are created between all security modules of a VPN group. All internal nodes of these security modules can communicate securely with each other through these tunnels.

- **Logging**

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

You will find further information on the functionality and configuration of the security functions in the information system of STEP 7 and in the manual /9/ (Page 165).

## 1.4 Other services and properties

### Other services and properties

- **Data point configuration**

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

- **Saving messages**

Data messages that cannot be transferred to the communications partner due to connection disruptions are saved.

- In the message memory up to 100000 messages can be buffered.
- If an SD card is used, messages can also be saved on the SD card.

- **IP configuration**

The TIM supports IP addresses according to IPv4.

Address assignment:

- The IP address, the subnet mask and the address of a gateway can be set manually in the configuration.
- As an alternative, the IP address can be obtained from a DHCP server or by other means outside the configuration.

- **Time-of-day synchronization**

On every interface the TIM provides the option of receiving and forwarding the time of day.

Synchronization method NTP (Network Time Protocol) via Industrial Ethernet:

- NTP
- NTP (secure)

You will find information in the section Time-of-day synchronization (Page 77).

For information on the format of the time stamp of the messages, refer to the section Time stamp (Page 71).

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

With the aid of the Web server, you can display module and diagnostics data.

- **Storage and event-driven transfer of process data**

The TIM can store events of different classes and transfer the corresponding process values individually or bundled together to the communications partner. The transfer can be triggered by various triggers.

- **Analog value processing**

Analog values can be preprocessed on the TIM according to various methods, see section Analog value preprocessing (Page 106).

- **Online functions**

From an engineering station (ES) on which STEP 7 is installed, you can use the online functions of STEP 7 via an Ethernet interface of the TIM to access the S7 CPU if the station is located in the same IP subnet.

The following online functions are available:

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

For a remote station located in a different IP subnet or that can be reached via the Internet, these functions can only be used if the ES (with CP 1628 or via SCALANCE S) is connected to the station via a VPN tunnel.

- **SNMP**

As an SNMP agent, the TIM supports data queries using SNMPv1 and SNMPv3 (Simple Network Management Protocol).

For more detailed information, refer to section SNMP (Page 133).

## 1.5 Configuration examples

Below, you will find configuration examples for the TIM.

### Sending SMS messages

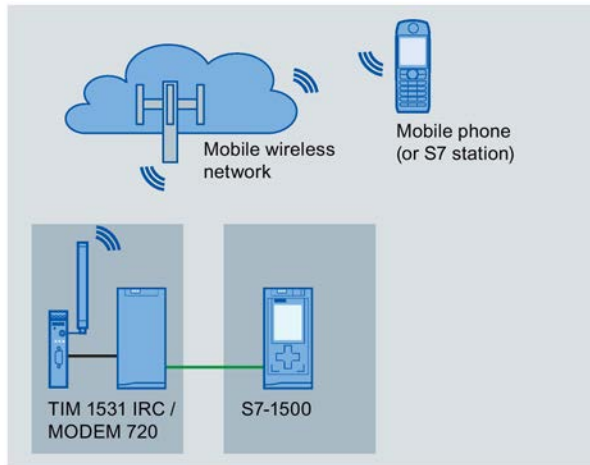


Figure 1-1 Sending messages by SMS

The TIM can send SMS messages to a mobile phone. SMS messages are generated and sent due to events.

## Communication via Ethernet / Internet, sending e-mails

In the sample configuration shown, S7 stations communicate with a redundant master station via the Ethernet interfaces of the TIM.

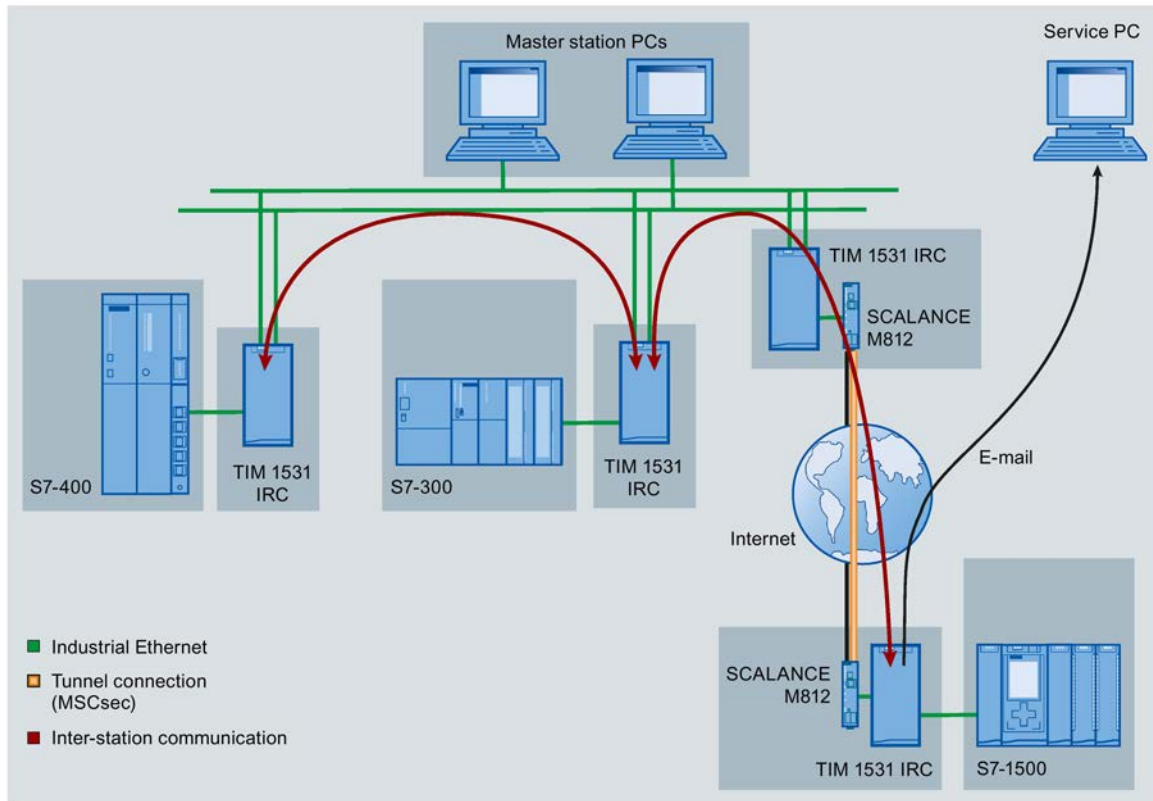


Figure 1-2 Communication via Ethernet / Internet

### E-mails

The TIM can generate and send e-mails due to events. Possible recipients include:

- PCs with an Internet connection
- Mobile phones
- SIMATIC stations with the appropriate program blocks

### Inter-station communication

Inter-station communication between S7 stations with a TIM is possible via IP-based and WAN networks.

Inter-station communication via mobile wireless runs via a master station that forwards the messages to a target subscriber.

## Path redundancy using the serial interface

In the following example in addition to the Ethernet interface, the serial interface of the TIM is also used. This allows redundant transmission paths to be set up.

The figure shows two examples in which the following interfaces are used:

- Ethernet interface for communication via Ethernet / Internet  
The TIM modules use the transmission protocol MSC or MSCsec.
- Serial interface for communication via a WAN network (dedicated line or dialup network)

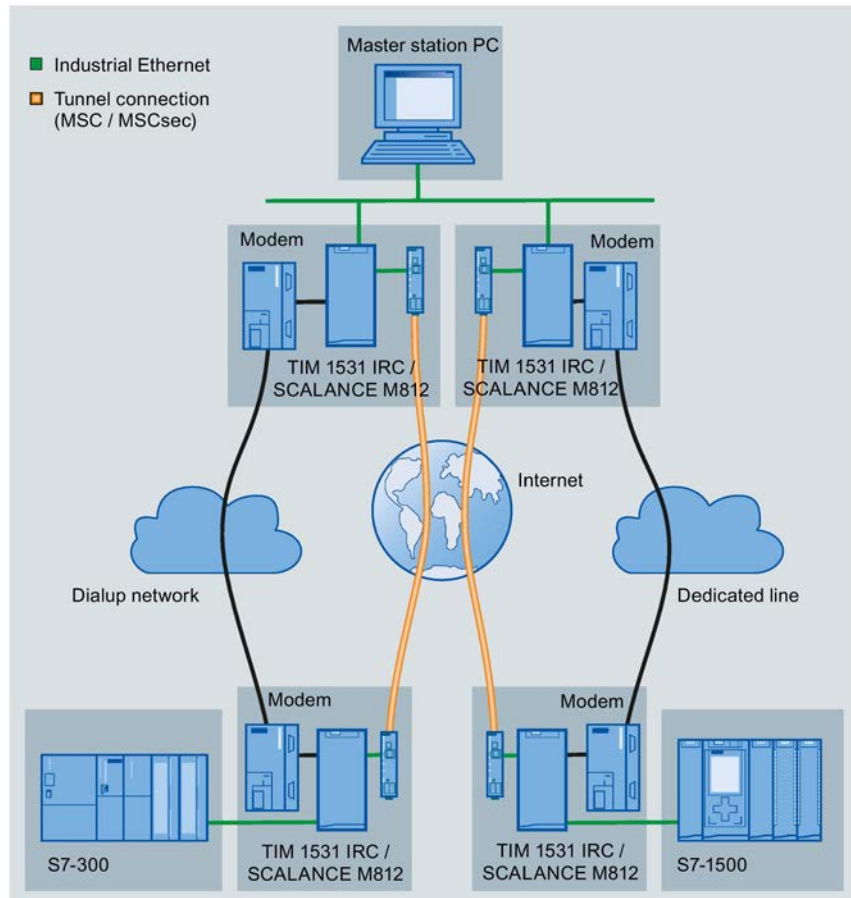


Figure 1-3 Communication via redundant paths

## Telecontrol communication via mobile wireless and wireless networks

### Mobile wireless

In these examples the TIM modules of the master communicate with the station or node station TIMs via mobile wireless:

- Left: Use of the Ethernet interface with VPN
- Right: Use of the serial interface and the transmission protocol MSCsec

### Private wireless networks

The left station TIM is configured as a node station. Underlying this an analog wireless network with several stations is connected via the serial interface. An IP-based wireless network could also be connected via the Ethernet interface.

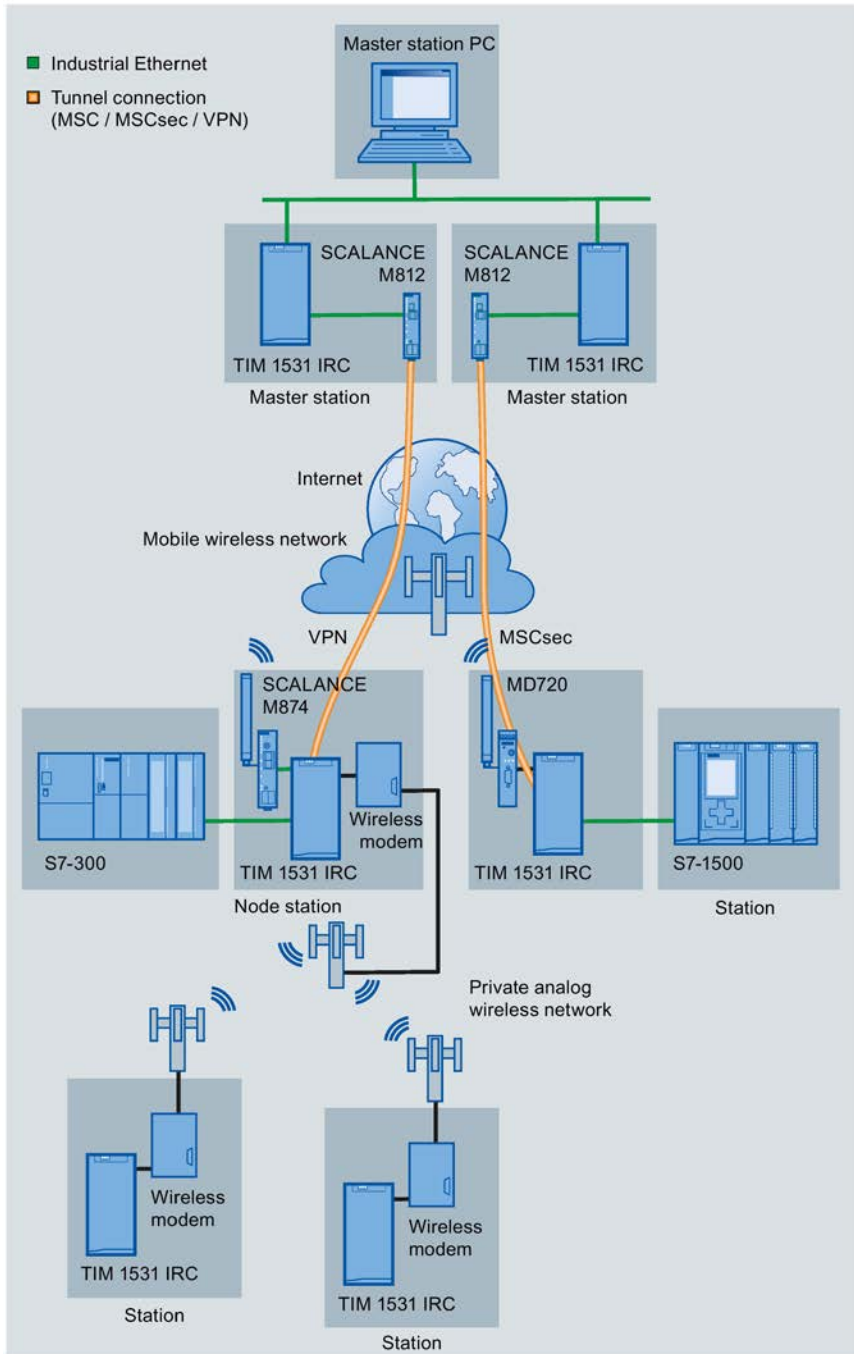


Figure 1-4 Communication using mobile wireless (at the top) and wireless (at the bottom)

## 1.6 Performance data and configuration limits

### Connection resources

- **Telecontrol connections**

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

The maximum number of connections or communications partners depends on the network node type with which the interface is set.

Network node type	Interface	Max. number per interface type	Network type	Max. number of connections / partners per interface
Master station	Ethernet X1	128	TCP	<ul style="list-style-type: none"> <li>• 62 S7 connections</li> <li>or</li> <li>• 127 MSC connections</li> </ul>
	Ethernet X2			62 S7 connections
	Ethernet X3			62 S7 connections
	Serial X4	32	Dedicated line	32 partners
			Dialup network	32 partners
Node / station	Ethernet X1	32	TCP	<ul style="list-style-type: none"> <li>• 16 S7 connections</li> <li>or</li> <li>• 1 MSC connection</li> </ul>
	Ethernet X2			16 S7 connections
	Ethernet X3			16 S7 connections
	Serial X4	16	Dedicated line	16 partners
			Dialup network	16 partners

- **E-mail / SMS**

At runtime, a connection can be established to send an e-mail or SMS message.

- **S7 connections**

- When using ST7 communication:

66 connection resources in total incl. telecontrol connections (see above) and max. 4 PG/OP connections (see below)

- Without using ST7 communication:

4 connection resources only for PG/OP connections (see below)

- **Online functions**

See PG/OP connections

- **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)
- **HTTP/HTTPS**  
Max. 2 connections per Ethernet interface
- **Connectable control center applications**  
Number of SINAUT control centers connectable via Ethernet ST7cc / ST7sc Max. 4

### Number of data points for the data point configuration

The maximum number of configurable data points is 1000.

### Message memory: Send buffer / SD card

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

The send buffer has a maximum size of 100000 messages. The size of the message memory is divided equally among all configured communications partners.

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, triggers (Page 99).

You can set saving of messages on an optional SD card in the configuration, see section Settings (Page 48).

### Messages: E-mail / SMS

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

- Number of characters per SMS message

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

- 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



## **1.7 Requirements and compatibility**

### **1.7.1 Software requirements**

#### **Software for configuration and online functions**

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

- STEP 7 Professional V14.0 + SP1 + Update 1

### **1.7.2 Usable CPUs**

#### **Compatible CPUs**

The following can be used as the local CPU of the TIM:

- S7-1500  
All CPUs that can be configured in STEP 7 as of firmware version V2.1
- S7-300  
All CPUs that can be configured in STEP 7 with a PROFINET interface
- S7-400  
All CPUs that can be configured in STEP 7



## LEDs, connectors, switches, card slot

### 2.1 Overview: LEDs, connectors, switches, card slot

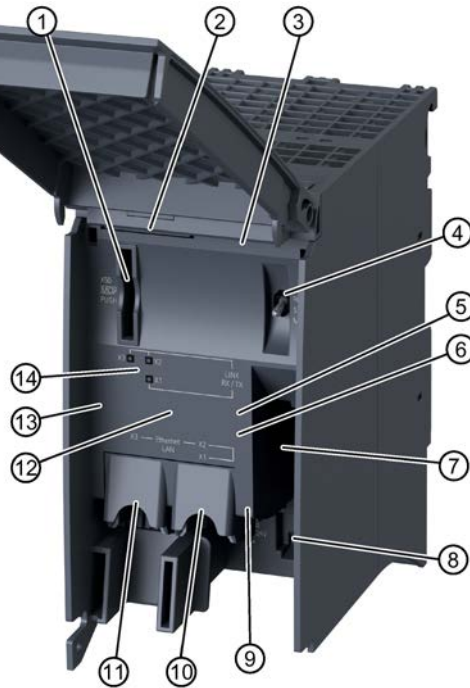


Figure 2-1 Location of the elements LEDs, connectors, switches, SD card slot

Table 2- 1 Meaning of the number symbols

①	X50: Receptacle for SD card	⑧	X80: Power supply (socket)
②	Status and diagnostics LEDs (covered): RUN, ERROR, CONNECT	⑨	X1: Ethernet interface (Gigabit Ethernet)
③	Article number (covered)	⑩	X2: Ethernet interface (Fast Ethernet)
④	Switch	⑪	X3: Ethernet interface (Fast Ethernet)
⑤	MAC address Ethernet interface X2	⑫	Serial number (2D matrix code, alphanumeric)
⑥	MAC address Ethernet interface X1	⑬	MAC address Ethernet interface X3
⑦	X4: Serial interface, plug (RS-232/RS-485)	⑭	LEDs for Ethernet communication status: X1, X2, X3

## 2.2 LEDs

At the top on the front of the TIM there are the status and diagnostics LEDs that can also be seen when the front cover is closed.




Position	LED name	Meaning
Left	<b>RUN</b>	Operating mode
Middle	<b>ERROR</b>	Error
Right	<b>CONNECT</b>	Connection status (to the CPU / to the communications partner)

Below the front cover there are LEDs for the communication status of the Ethernet interfaces:

LED name	Meaning
X1 / X2 / X3	Communication status of Ethernet interface, X1, X2 and X3












The LED symbols have the following meaning:

Table 2- 2 Legend for the tables

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

## Status and diagnostics LEDs

Table 2- 3 Meaning of the LED patterns in productive operation \*

RUN (yel- low/green)	ERROR (red)	CONNECT (green)	Meaning
			No supply voltage or supply voltage too low
	-	-	TIM in RUN mode
	-	-	TIM in STOP mode
	-	-	TIM in maintenance status
-	-		All configured connections established **
-	-		No configured connections established **
-	-		At least one configured connection aborted **
-		-	Missing or incorrect configuration
-		-	Duplicate IP address detected

\* During startup and during the firmware update the TIM shows deviant LED patterns.

\*\* Relates to connections both to the CPU and to the communications partner.

- **Startup**

For the LED pattern see section Startup - LED pattern (Page 40).




- **Firmware update**

For the LED pattern see section Update firmware (Page 137).

## LEDs of the Ethernet interfaces

Every interface has an LED that informs about the connection status with Ethernet and the message traffic of the port.

Table 2- 4 Meaning of the LED statuses

X1 / X2 / X3 (yellow/green)	Meaning
	No connection to the Ethernet network
	Ethernet connection without data transfer
	Ethernet connection with data transfer

## 2.3 Electrical connectors

### 2.3.1 Ethernet interfaces (X1, X2, X3)

#### Ethernet ports

The Ethernet connectors are located behind the cover of the housing. The interfaces are RJ-45 jacks according to IEEE 802.3.

---

#### Note

##### Connection to subnets

The three Ethernet interfaces are not designed as a switch, but are intended for connection to different networks. Operation in the same physical network is not permitted.

---

The pin assignment of the Ethernet interfaces and other data can be found in the section Technical specifications (Page 143).

### 2.3.2 Serial interface X4

#### Serial interface X4

The serial interfaces are designed as 9-pin D-sub miniature male connectors.

The interface can be operated in the two following standards:

- RS-232
- or
- RS-485

You specify the standard to be used with the configuration in STEP 7, see section Advanced options (Page 54).

You will find the pinout of the interface in the section Pin assignment of the serial interface (Page 145).

### 2.3.3 X80: External power supply

#### External power supply

The connector X80 (socket) for the external 24 VDC power supply is located on the front of the TIM.

The power supply is connected to the TIM with the supplied plug-in terminal block. The plug-in terminal block is designed so that it can only be plugged in in one position in the X80 socket of the TIM.

The connector X80 has electronic reverse polarity protection.

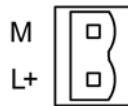


Figure 2-2 Connector X80 for the power supply

Table 2- 5 Pin assignment of the socket for the external power supply

Labeling	Function
M	Reference ground
L+	24 VDC

For information on the connector, refer to the section "Connecting up (Page 37)".

You will find further data on the power supply in section Technical specifications (Page 143).

## 2.4 Switch

#### Operating status switch

<p><b>⚠ WARNING</b></p> <p><b>EXPLOSION HAZARD</b></p> <p>Do not press the button if there is a potentially explosive atmosphere.</p>
---

The switch is a combined element with switch and button functions. It has three settings:

- **RUN**

RUN mode

This is the basic setting for productive operation.

## 2.4 Switch

- **STOP**

### STOP mode

Set the TIM to STOP before disconnecting the power supply. Setting to STO may also be necessary if an error/fault occurs to be able to restart the TIM afterwards.

In STO mode, the following functions are disabled:

- Telecontrol operation of the TIM
- Time-of-day synchronization via Telecontrol connections
- S7 connections are terminated.

The following functions remain enabled:

- Access to the WBM of the TIM
- Time-of-day synchronization with NTP
- Diagnostic functions of the TIM

- **MRES**

### Maintenance status

The setting "MRES" is adopted by pressing and holding down the switch in this position (button function).

By pressing the switch for at least 5 seconds, the functions described below are triggered. If you release the switch before the 5 seconds have elapsed, the TIM shows no reaction.

Functions:

- Restart

When the switch is pressed in STOP mode

The TIM restarts.

- Resetting to factory settings

Only when the switch is pressed during a restart

The TIM is reset to the factory settings. Note the effects of the reset, particularly the deletion of the configuration data.

For information on the effects of resetting, refer to the section Resetting to factory settings (Page 139).



## Functions in the setting "MRES"

Functions when holding the switch in the "MRES" setting for more than 5 seconds:

Table 2- 6 Button functions

Function	Previous setting or action	Effect
<b>Restart</b>	Pressing the switch from the "STOP" setting	The TIM restarts. Release the switch at the beginning of the restart.
<b>Reset</b>	Pressing the switch after triggering a restart	The TIM is reset to the factory settings. All the configuration data is deleted.

For the relevant LED patterns see the following section:

- Startup - LED pattern (Page 40)
- Resetting to factory settings (Page 139)

## 2.5 SD card slot

### "X50": Slot for an optional SD card

You have the option of using an SD card as an exchangeable storage medium for storing important data.

- Configuration data
- Process data

Values of data points configured as an event.

An SD card does not ship with the TIM.

#### Compatible cards

You will find a list of compatible SD cards in the appendix SD cards (Page 153).

Use one of the SD cards listed there.

The minimum size is 24 MB. If you use an SD card with less storage space, it is possible that not all process data (see below) can be saved retentively.

#### Card errors / diagnostics

Card errors are indicated by entries in the diagnostics buffer.

#### Inserting the card

Inserting the SD is described in the section Inserting the SD card (Page 38).

## Retentive storage of important data on the SD card

The SD card is an exchangeable storage medium for storing the following data safe from power failure.

- **Configuration data**

The configuration data is backed up on the SD card following every change in a configuration file. Storing configuration data on the SD card serves the following purpose:

- Device replacement without engineering station

If the TIM needs to be replaced for maintenance purposes or another location, by transferring the SD card from the previous to the new TIM, the configuration data can be made available to the new TIM. In this case, you do not need an engineering station with a STEP 7 project.

The configuration data is saved on the SD card when the TIM starts up.

For information on device replacement refer to section Module replacement (Page 141).

- **Process data**

You have the option of storing values of data points configured as an event. This serves the following purposes:

- Storage when there are connection disruptions

If the TIM cannot send the data to its communications partner due to connection disruptions, this remains stored until the connection is restored.

- Storage if there is a power failure

You can specify whether values of events are stored globally in the configuration of the TIM. There are also options for storing on the SD card for every data point created as an event.

## Installation, connecting up, commissioning

### 3.1 Important notes on using the device

#### Safety notices on the use of the device

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

#### Overvoltage protection



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

### 3.2 Installation

<b>NOTICE</b>
<p><b>Install and remove the TIM only when the power is off</b></p> <p>Switch off the power supply of the TIM before you install or remove the TIM. Installing and removing modules with the power supply on can lead to damage to the modules and to loss of data.</p>

3.2 Installation

<p><b>NOTICE</b></p> <p><b>Installation location - Dependency of the temperature range</b></p> <p>Note the dependency of the permitted temperature range of the installation location.</p> <ul style="list-style-type: none"> <li>• Horizontal installation of the rack (DIN rail) means a vertical position of the modules.</li> <li>• Vertical installation of the rack (DIN rail) means a horizontal position of the modules.</li> </ul> <p>You will find the permitted temperature ranges in the section Technical specifications (Page 143).</p> <p><b>Minimum clearances</b></p> <p>Mount the TIM so that its upper and lower ventilation slits are not covered, allowing adequate ventilation as protection from overheating.</p> <p>Keep to the following minimum clearances for the circulation of air when the rack is installed horizontally:</p> <ul style="list-style-type: none"> <li>• Above the TIM: At least 33 mm</li> <li>• Below the TIM: At least 25 mm</li> </ul>
---

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

Installation on a DIN rail

<p><b>Note</b></p> <p><b>Protecting the modules from slipping on the DIN rail</b></p> <p>If you install the modules in an area with mechanical load, use suitable clamping devices at both ends of the device group to secure the modules on the DIN rail, e.g. Siemens and retainer 8WA1808.</p> <p>The end retainers prevent the modules separating under mechanical load.</p>
--

The TIM is suitable for mounting on a standard rail of the S7-1500 (article number 6ES7590-1Axx0-0AB0).

1. Hang the TIM on the mounting rail.
2. Tilt the TIM towards the back.
3. Screw the TIM at the bottom using the securing screws (tightening torque 1.5 Nm).
4. Ground the mounting rail, see next section.

## Grounding

For reasons of electrical safety, the DIN rail must be connected to the protective conductor system (PE) of the electrical system.

You will find details on grounding and installation in the SIMATIC S7-1500/ET 200MP Manual Collection, see /2/ (Page 164).

## Removal from the DIN rail

Follow the steps below to remove the TIM from the DIN rail:

1. Switch the TIM to STOP.
2. Turn off the power supply to the TIM.
3. Pull off the Ethernet cables and the serial bus.
4. Release the securing screws of the TIM.
5. Tilt the TIM out of the standard rail.

## 3.3 Connecting up

### Order of the work

<b>NOTICE</b>
<b>Connection only with power off</b>
Only connect the TIM with the power switched off.

Requirement: The TIM is mounted.

1. Connect the external power supply to the terminal block of connector X80.
2. Connect the cables of the Ethernet networks in the required ports of the TIM.

Note the permitted combinations of the Ethernet connectors in the section Ethernet interfaces (X1, X2, X3) (Page 30).

3. Plug the cable to the modem in the serial connector of the TIM.

When connecting a star shaped network, remember to connect the terminating resistor for RS-485 operation of the interface. See also the section below.

<b>NOTICE</b>
<b>Contacting the shield of the cable on the plug</b>
The shield of the cable must be contacted. To do this, strip the insulation from the end of the cable and connect the shield to functional earth.

For the network connection products from the Siemens accessories program are recommended, see Appendix Cables, connecting cables (Page 160)

Turn the power supply on only after the TIM has been completely wired and connected.

The further procedure is described in the section Commissioning (Page 39).

### Power supply at connector X80

Recommendation: Use the same power supply as the CPU if this is in the vicinity of the TIM.

The 2-terminal plug-in terminal block with polarity reversal protection has the following pin assignment for the X80 socket:

Terminal	Assignment
L+	24 VDC
M	Ground

You will find information about the connectable cable cross sections, power consumption and further technical details in section Technical specifications (Page 143).

### RS-485: Connection of the terminating resistor

If you connect a star-shaped network with several dedicated line or dialup network modems to the serial interface of the TIM then operate the serial interface with the RS-485 standard.

You set the RS-485 standard in the configuration of the TIM. With a network operating according to RS-485 you also need to activate the cable terminating resistor of the bus cable in the configuration.

## 3.4 Inserting the SD card



Figure 3-1 Slot for the SD card (yellow frame)

You will find the SD cards supported by the TIM in the appendix SD cards (Page 153).

<b>NOTICE</b>
<b>Only remove / insert the SD card when the power is off</b>
You can only remove or insert the SD card when the TIM is not supplied with power.
If you remove or insert the SD card during operation, data on the card can be damaged.

Inserting the SD card

1. Insert the SD card into the compartment until you can feel the card lock in place.

Removing the SD card

1. By pressing, unlock the card.
2. After unlocking it takes the card out of the slot.

## 3.5 Commissioning

### Requirement

Requirements for commissioning the TIM are as follows:

- The TIM is mounted and connected up.
- The TIM is fully configured in STEP 7, refer to the section Configuration (Page 41).
- The STEP 7 project with the TIM is open on the engineering station.
- For loading, the engineering station is connected to an Ethernet interface of the TIM.

### Downloading the configuration data

To start productive operation the TIM requires the STEP 7 configuration data.

To download the configuration data, follow the steps outlined below:

1. Change the switch of the TIM to the RUN setting.
2. Turn on the power supply to the TIM.

The TIM starts up with the factory defaults and remains standing with a yellow flashing RUN LED.

You will find information on the LED displays during startup in the section Startup - LED pattern (Page 40).

3. Start by downloading the configuration data.

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

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

On completion of the download close the front cover of the TIM.








### 3.6 Startup - LED pattern

During startup the TIM shows different LED patterns than at runtime. You will find the LED patterns at runtime in the section LEDs (Page 28).

#### LED patterns at startup / restart
















The LED symbols have the following meaning:

Table 3-1 Legend for the tables

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

The table below describes the LED patterns in the individual startup phases of the TIM.

Table 3-2 Meaning of the LED patterns at startup

Startup phase	RUN (yellow/green)	ERROR (red)	CONNECT (green)	Meaning
1				Hardware initialization and downloading the operating system
2				Downloading the firmware
3				Downloading the configuration data
4				Startup successful / start of productive operation
<b>Startup aborted</b>				
4				The startup was incorrect and was aborted. *

\* If the startup is incorrect, note which phase (1, 2, 3) is reached and when it is aborted. You may be able to localize the error.



# Configuration

## 4.1 Security recommendations

Keep to 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.
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
- Check regularly for new features on the Siemens Internet pages.
  - Here you will find information on network security:  
Link: (<http://www.siemens.com/industrialsecurity>)
  - Here you will find information on Industrial Ethernet security:  
Link: (<http://w3.siemens.com/mcms/industrial-communication/en/ie/industrial-ethernet-security/Seiten/industrial-security.aspx>)
  - You will find an introduction to the topic of industrial security in the following publication:  
Link:  
([http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP02-0BA4\\_BR\\_Network\\_Security\\_en\\_112015.pdf](http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP02-0BA4_BR_Network_Security_en_112015.pdf))

### Physical access

Restrict physical access to the device to qualified personnel.

### Network attachment

Do not connect the TIM directly to the Internet. If a connection of the TIM to the Internet is required, use the security variants of the telecontrol protocols or use protection mechanisms in front of the TIM. Protection mechanisms are for example a SCALANCE M router or a SCALANCE S security module with firewall.

### Security functions of the product

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

- Protection levels  
Configure a protection level of the CPU.  
You will find information on this in the information system of STEP 7.
- Security function of the communication
  - Using the security functions of the telecontrol protocols.
  - Use the secure protocol variants for example NTP (secure) or SNMPv3.
  - Leave access to the Web server deactivated.

### Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel.  
See also the preceding section for information on this.
- Do not use one password for different users and systems.

### Protocols

#### Secure and non-secure protocols

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

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

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

#### Table: Meaning of the column titles and entries

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

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

- **Default of the port**
  - Open  
The port is open at the start of the configuration.
  - Closed  
The port is closed at the start of the configuration.
- **Port status**
  - Open  
The port is always open and cannot be closed.
  - Open after configuration  
The port is open if it has been configured.
  - Open (login, when configured)  
As default the port is open. After configuring the port, the communications partner needs to log in.
  - Closed after configuration  
The port is closed because the TIM is always client for this service.
- **Authentication**  
Specifies whether or not the protocol authenticates the communications partner during access.

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
<b>S7 and online connections</b>	102 (TCP)	Open	Open after configuration	No
<b>HTTP</b>	80 (TCP)	Closed	Open after configuration	No
<b>HTTPS</b>	443 (TCP)	Closed	Open after configuration	Yes
<b>SNMP</b>	161 (UDP)	Open	Open after configuration	Yes (with SNMPv3)

## 4.2 Configuration in STEP 7

### Configuration in STEP 7

You configure the modules and networks in STEP 7 Professional. You will find the required version in the section Software requirements (Page 25).

The following sections describe the STEP 7 configuration. If individual parameters are not described here, you will find help help in the STEP 7 information system.

### Components of a rack

The TIM is configured as a standalone device. In the station of the TIM, no further devices need to be configured.

The assigned CPU with which the TIM exchanges data is configured in a separate rack. You will find the compatible CPUs in the section Usable CPUs (Page 25).

### Configuration - overview

Configuration involves the following steps:

1. Create a STEP 7 project with security functions activated.

---

#### Note

##### Activated security functions

If you have not yet activated any security functions or have logged on in "Global security settings", you first need to log on as a security user.

The configuration of the TIM is only possible with activated security functions.

Also for access to the Web server of the TIM, the users must be created in "Global security settings".

---

2. Insert the required TIM modules and SIMATIC stations with CPU, input/output modules and the other required modules and configure the modules.
3. Create PLC tags for the data to be transferred in the CPU.  

The input and output data of the station is not addressed directly by the TIM but via PLC tags. You require these for the data points of the TIM (see below).
4. Create the necessary networks for networking the interfaces.  

Refer to the information in the section Networking a TIM (Ethernet addresses / WAN settings) (Page 52).
5. Complete the configuration of the modules and networks.
6. Create telecontrol connections for the telecontrol communication using ST7.  

For telecontrol connections that use the S7 protocol (Network type "Neutral") you do not need to create any separate S7 connections.  
You will find the description in the section Creating telecontrol connections (Page 66).
7. Create the required data points and messages.
8. Save the project.

For complete commissioning of the TIM, you need to download the configuration data to the relevant TIM. The project data is stored in the work memory of the TIM.

When using an optional SD card, the data is stored on the SD card of the TIM, see section Commissioning (Page 39).

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

## Copying functions for larger projects

The copying functions of STEP 7 reduce configuration effort. Use the copying functions in particular with large projects with several identical or similar stations.

- Copying devices and stations

If you use several similar TIM modules or CPUs in a project, it is advisable to configure the first device first and then to copy the entire configuration data. This can include the following objects:

- The user program of CPUs
- PLC tags of CPUs
- Data points of TIM modules

After copying the address parameters and other various parameters need to be adapted.

Recommendation:

Network the interfaces only after copying the devices.

- Copying PLC tags

If you use several similar items of input and output data, you can copy PLC tags in the tag table.

After copying you only need to adapt the address parameters.

- Copying data points

In much the same way as with PLC tags, you can also copy data points.

For a detailed description of the functions, refer to the section Data point configuration (Page 90).

## 4.3 Communication types

### 4.3.1 Communication types

#### "Communication types"

In this parameter group you specify the protocol for the telecontrol communication.

- **Enable telecontrol communication**

The communication with the communications partners via telecontrol protocols is activated generally.

- **Protocol type**

- **ST7**

The protocol is preallocated.

## 4.3.2 Communication via the SINAUT ST7 protocol

### The ST7 protocol

#### Network types

ST7 is a protocol for telecontrol communication via WANs (Wide Area Network).

With ST7 it is possible to communicate via the following network types:

- Classic WAN networks
- IP-based WAN networks

#### Subscriber types

The following subscriber types that support the ST7 protocol are possible communications partners:

- SIMATIC stations with TIM modules or a CP capable of ST7
- Control center applications capable of ST7

#### Connections

Communication with the ST7 protocol runs via configurable connections. You make the required settings in the STEP 7 configuration.

### Communication via single or redundant telecontrol connections

The ST7 communication between two subscribers runs via configurable paths. To do this, telecontrol connections are created in the "Network data" editor in the "Telecontrol" tab, see section Creating telecontrol connections (Page 66).

When different networks between two subscribers have been created in the network configuration, you can create redundant telecontrol connections. In the configuration these are displayed in the "Network data" editor. There the main and the substitute path are specified.

To check the reachability of a communications partner of the TIM, you can write the connection status to "PLC tags for partner status / path status", see section Communication with the CPU (Page 73).

For redundant telecontrol connections, the behavior is as follows.

- **Main path**

If the connection between the two subscribers is undisturbed, the main path is always used.

The status of the main path is rechecked each time there is communication and saved in the PLC tag.

- **Substitute path**

If the connection via the main path is disturbed, communication is switched to the substitute path.

The status of the substitute path, on the other hand, is only registered when communication is established.

If you configure a dialup network connection as the substitute path via which generally a connection is seldom established, you can test the reachability via this path for example by synchronizing the time of day once daily via this path. To do this a connection must be established once daily via the dialup network. The reachability is then updated once daily in the PLC tag.

## Addressing communications partners and network nodes

Since the communication between two ST7 subscribers can run via different paths and subnets, precise addressing of the individual subscribers in the ST7 network is necessary. The following two parameters serve this purpose:

- **Subscriber number**

The subscriber number is unique for every subscriber in an ST7 network. The following subscribers require a subscriber number:

- **TIM**

Communications module for the ST7 protocol

- **CP 1243-8 IRC**

Communications module for the ST7 protocol

- **CPU**

The local CPU that is assigned to the communications module as the end point of a telecontrol connection receives a subscriber number via the ST7 protocol.

With a CP1243-8 IRC and a TIM 300, the local CPU is assigned automatically via the rack. With the TIM 1531, you assign the local CPU in the "Station address" parameter group.

- **Application of the master station PC**

The application that you configure in the PC station of the master station.

For the TIM and the assigned CPU, the subscriber number is configured in the parameter group "Station address" of the TIM.

For the application of the master station PC, the subscriber number is configured in the telecontrol connection: Editor "Network data" > "Telecontrol" tab

- **WAN address**

For every networked serial interface in a classic ST7 network a WAN address is assigned. This is unique throughout the network.

Since telecontrol connections can run via several network nodes and node stations, unique addressing of the interfaces involved is necessary.

The WAN address is configured in the parameter group "WAN parameters" of the serial interface.

## 4.4 Settings

### Retentive saving of events

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

For the general reaction, the following parameters are available:

- Activate retentive saving

When there are connection disruptions activates the retentive saving of events on the SD card.

- 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 after a connection failure.

- Interruption time before saving

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

Whether or not the values of the individual data points are saved is specified in the configuration of the individual data point in the "Trigger" tab, see section Data points (Page 90).

For the maximum number of savable messages see section Performance data and configuration limits (Page 23).

## 4.5 Overview: Connection to LAN / WAN

### Transfer options

The interfaces of the TIM support the following network types and protocols:

#### Ethernet interfaces

- IP-based

Communication via LAN (copper / FO cable), Internet and IP-based wireless networks

- Neutral (via S7 connection)
- MSC / MSCsec

For information on the protocol variants, refer to the section Communications services (Page 12).

- Mobile wireless with VPN

IP-based mobile wireless communication (with gateway to the Internet) only with SCALANCE M router



**Serial interface**

- **Classic WAN**

- Dedicated line (incl. analog wireless network)
- Dial-up network (analog, ISDN mobile wireless)

- **IP-based**

- MSC / MSCsec via GPRS

**Connection combinations: TIM - master station**

The following table provides an overview of the various connection options and the devices required for them (modems, routers, switches).

The table contains the information for the interfaces of the TIM and for the master station. The protocols or services used are listed.

Network type / transmission path	Connection TIM		Standard, protocol, service	Master station connection	Master station type
	Serial interface	Ethernet interface			
Ethernet	-	SCALANCE M / SCALANCE S	VPN	SCALANCE M / SCALANCE S	<ul style="list-style-type: none"> <li>• Control center PC</li> <li>• Master station TIM</li> </ul>
	-	SCALANCE X / W		SCALANCE X / W	<ul style="list-style-type: none"> <li>• Control center PC</li> <li>• Master station TIM</li> </ul>
Mobile wireless + Internet	-	DSL router	MSC / MSCsec	DSL router	Master station TIM
	-	SCALANCE M	MSCsec	SCALANCE M	Master station TIM
	-	SCALANCE M	VPN	SCALANCE M	Master station TIM
IP wireless network	-	IP wireless modem	IP	IP wireless modem	Master station TIM
Dedicated line	Dedicated line modem	-	RS-232 / RS-485	Dedicated line modem	Master station TIM
	Analog wireless modem			Analog wireless modem	
Analog dial-up network	Dial-up network modem	-	V.32bis/V.34bis	Dial-up network modem	Master station TIM
ISDN dial-up network	ISDN modem	-	<ul style="list-style-type: none"> <li>• ISDN</li> <li>• ISDN + GSM/CSD</li> </ul>	<ul style="list-style-type: none"> <li>• ISDN modem</li> <li>• MODEM MD720</li> </ul>	Master station TIM
	ISDN modem	-	<ul style="list-style-type: none"> <li>• ISDN</li> <li>• ISDN + GSM/CSD</li> </ul>	<ul style="list-style-type: none"> <li>• ISDN modem</li> <li>• MODEM MD720</li> </ul>	Master station TIM

Network type / transmission path	Connection TIM		Standard, protocol, service	Master station connection	Master station type
	Serial interface	Ethernet interface			
Mobile wireless network	MODEM MD720	-	GSM/CSD	<ul style="list-style-type: none"> <li>• DSL router</li> <li>• MODEM MD720</li> </ul>	Master station TIM
			GSM + MSC/MSCsec	<ul style="list-style-type: none"> <li>• DSL router</li> </ul>	

You will find information on the accessories in the following sections or literature sections:

- Modems:
  - Dedicated line and dialup network modems (Page 155)
  - MODEM MD720 (Page 156)

To connect a modem to the TIM a cable must be ordered.
- SCALANCE M: Router SCALANCE M (Page 157)
- For the various requirements, different SCALANCE M routers are available.
- SCALANCE S: /10/ (Page 165)
- Connecting cables between TIM and modem: Cables, connecting cables (Page 160)

## 4.6 WAN settings

### WAN parameters of interfaces

In this parameter group of the interfaces of the TIM you will find parameters that decide the properties of the connected WAN network:

- **WAN type**

Selection of the WAN type of the interface:

  - IP-based
 

Default setting of the Ethernet interface
  - Classic WAN
 

Default setting of the serial interface

To use MSC via GPRS, the serial interface can be changed to "IP-based".

- **Network type**

For classic WAN:

- Dedicated line
- Dialup network

For IP-based WAN:

- Neutral
- Mobile wireless with VPN
- MSC

- **Connection mode**

Decides the Network node type of the interface:

- Master station
- Node station

With TIM modules operating as a node station, both interfaces - in the direction of the master station and in the direction of the underlying subnet - must be configured as "Node station".

- Station

With the classic network types dedicated line and dialup network, a modem needs to be connected to the serial interface of the TIM. You select the suitable modem type using the following parameters (serial interface only):

- **Modem type**

- 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

Siemens-GSM modem MD720 (network type "Dialup network")

- Third party modem

Any compatible modem for the network types "Dedicated line" or "Dialup network" (analo / ISDN)

If you configure "Dialup network" and want to transmit via mobile wireless, you need to select "MD720" as the modem type.

## 4.7 Networking a TIM (Ethernet addresses / WAN settings)

### Interfaces of the TIM

The arrangement of the interface in the STEP 7 device symbol (network view) corresponds to the structure of the device. The interfaces are arranged as follows:

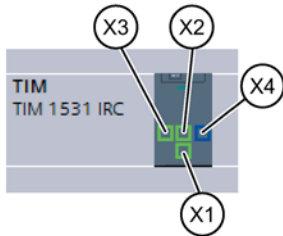


Figure 4-1 Device symbol of the TIM with interface numbers

### 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.

### Interface networking with the TIM

You will find the transmission options of the TIM depending on the interface in the section Overview: Connection to LAN / WAN (Page 48).

#### 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 (Page 50):
  - WAN type
  - Network type
  - Connection mode (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 TIM

- 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.

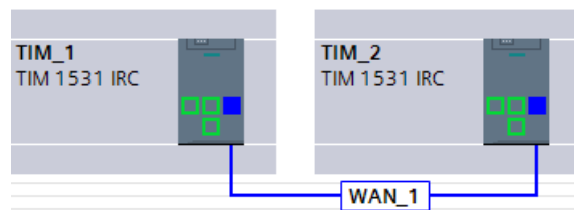


Figure 4-2 TIM modules, serial interfaces networked via classic WAN.

### MSC connections

Note the options of using the "MSC" protocol via the interfaces of the TIM:

#### Note

#### MSC via TIM interfaces:

- **Ethernet interface X1**  
Of the three Ethernet interfaces, MSC is supported only by interface X1.
- **Serial interface**  
For the serial interface you need to set the WAN type "IP-based" and the Network type "MSC".

MSC connections are represented as follows:

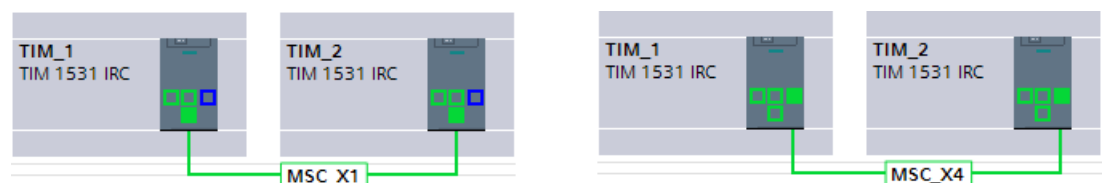


Figure 4-3 MSC connection via Ethernet interface X1 (left) and via serial interface (right)

The color of the serial changes from blue to green if the WAN type is changed from "Classic WAN" to "IP-based".

## 4.8 Ethernet-specific parameters

### 4.8.1 Ethernet interface > address parameters

#### Ethernet interface > Ethernet addresses > IP protocol ...

In the following parameter groups configure the IP address parameters of the Ethernet interface.

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

#### Ethernet interface > Port [Xn P1]

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

### 4.8.2 TCP connection monitoring

#### Ethernet interface > Advanced options > TCP connection monitoring

- **TCP connection monitoring time**

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

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

- **TCP keepalive monitoring time**

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

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

## 4.9 Advanced options

### 4.9.1 MSC protocol settings

The following descriptions apply to the MSC-specific parameter groups of the two interface types of the TIM.

For information on each of the following parameter groups "TCP connection monitoring" and "Port" see section Ethernet-specific parameters (Page 54).

## MSC protocol settings - Ethernet: MSC master station

The description applies to the parameter group of the Ethernet interface with the Connection mode "Master station".

### Access to MSC master station

First set whether the MSC master station or the router should be reachable with DNS via a fixed or a dynamic IP address.

The MSC master station is connected to the Internet via a router.

If the router can be reached via a dynamic IP address, there must be at least a reachable DNS server in the network.

- **MSC port of the router**

The port number is preset. If necessary, you can change the port number. Note that the port number of both partners must be identical. The port number cannot be configured for the station.

Default setting: 26382. Permitted range: 1024...65535

- **Host name**

If the router should be reachable using the host name enter it here.

- **IP address DNS server**

Here, enter the addresses of the DNS servers in the subnet.

### MSC monitoring settings

- **MSC monitoring time**

Monitoring time (minutes) for the MSC connection

– Behavior of the master station:

If there is no data traffic between the MSC master and station within the monitoring time, the MSC master sends a sign of life message to the station.

– Behavior of the master station:

if no sign of life message comes from the MSC master within the monitoring time, the station sets all subscribers reachable via MSC as disrupted.

Default setting: 10. Permitted range: 0...65535

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

- **Collect data volume**

If the option is enabled, the MSC master passes the monthly transferred data volume of the stations to online diagnostics.

## MSC protocol settings - Ethernet: MSC station/node station

The description applies to the parameter group of the Ethernet interface with the Connection mode "Station" / "Node station".

### MSCsec protocol

The use of the secure protocol variant is configured only in the stations. You can also enable use of MSCsec for individual stations of an MSC network.

- **Activate security protocol MSCsec**

If the option is enabled, the secure version of the MSC protocol "MSCsec" is used.

- **Key exchange interval**

Time (h) after which the secret key is renewed between the MSC station and master station.

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

### MSC protocol settings - serial interface: MSC station

The description applies to the parameter group of the serial interface regardless of the setting of the "Connection mode" parameter.

#### GPRS access

Here you configure the data of the access to the mobile wireless network.

- **Activate PIN**

Activates the PIN of the installed SIM card. If the contract with your network provider does not include a PIN, then disable this function.

- **PIN / Repeat PIN**

Entry of the PIN of the SIM card inserted in the modem. Not required for mobile wireless contracts without a PIN.

- **Extra transmission time**

Time offset (s) with slow networks to prevent premature stopping of connection establishment.

Default setting: 10. Permitted range: 0...65535. If you enter 0 (zero), the function is disabled.

The following values are usual:

- Mobile wireless networks: 10
- Wireless or satellite transmission: 0 .. 1

- **Max. allowed disruption time**

Tolerance time (s) for a detected connection disruption.

If there is still a disruption on the connection when the set time has elapsed, the disruption is signaled to all connection partners of the disrupted station.

Default setting: 0. Permitted range: 0...255. If you enter 0 (zero), the function is disabled.



### MSCsec protocol

- **Activate security protocol MSCsec**

If the option is enabled, the secure version of the MSC protocol "MSCsec" is used.

Can only be configured if the setting of the Connection mode of the interface is "Station" or "Node station".

- **Key exchange interval**

Time (h) after which the secret key is renewed between the MSC station and master station.

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

### APN settings

Here you configure the access point (APN) from the mobile wireless network to the Internet.

- **APN - country**

Country of the network provider that provides the APN.

Select the country and one of the preset network providers or select the entry "User-defined" and configure the APN manually.

- **APN - provider**

name of the network provider that provides the APN. Select the name from the drop-down list.

- **APN**

Access Point Name

Name of the access point. You obtain this information from your network provider.

- **APN user name**

Entry of the user name for Internet access via the mobile wireless network. You obtain this information from your network provider.

- **APN password**

Entry of the password for Internet access via the mobile wireless network. You obtain this information from your network provider.

## 4.9.2 Dedicated line

### Settings dedicated line

Only the configurable parameters are explained.

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

- **Operating mode**

The operating mode of the serial interface specifies the mode of the data transfer.

A maximum of one serial interface of a TIM module may be operated in DMA mode.

Range of values:

- Interrupt (block)

This operating mode applies to the transmit and receive mode. The default mode Interrupt (block) is suitable for all connections. 4 characters are transferred per block. Following this, there is an interrupt. The received characters are checked only after a complete message has arrived.

- DMA

This operating mode applies to the transmit and receive mode. The DMA mode should be used for connections with a high baud rate or a lot of message traffic, however not for GSM networks.

- Interrupt (individual characters)

This operating mode is used only in the receive direction. In the transmit direction, the block mode continues to be used. The interrupt mode is suitable for extremely bad lines. An interrupt is triggered per transmitted character and each character is analyzed immediately after it is received allowing extremely good diagnostics of transmission errors. This mode is more reliable than the block mode but is slower.

### Number of spontaneous frames

- **Number of spontaneous frames**

Only for interfaces with the Connection mode "Station" / "Node station".

The parameter decides after how many messages the master station has the opportunity of transferring its pending messages to the station. As maximum, the configured number of spontaneous frames that are pending at the time of the first call frame are transferred.

Default setting: 200. Permitted range: 0...255

If 0 (zero) is set, all spontaneous frames are sent at the call.

### Connection

- **Extra transmission time**

Time offset (s) with slow networks to prevent premature stopping of connection establishment.

Default setting: 10. Permitted range: 0...65535. If you enter 0 (zero), the function is disabled.

Usually in dedicated line networks the value is 0:

### Time options

- **RTS/CTS delay time**

The RTS/CTS delay (ms) can be required when a modem is connected via an RS-485 interface.

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

- Value 0

After setting the RTS signal, (turn transmitter on) transmission only starts when the CTS signal (Clear To Send) was set by the modem.

- Value > 0

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

After the RTS signal has been set, transmission is delayed for the configured time and then started immediately.

- **Send delay time**

The send delay time (ms) is used only when the ready to send (CTS signal) comes from the modem (RTS/CTS delay time = 0).

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

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

- **Polling monitoring time**

Only for interfaces with the Connection mode "Station" / "Node station".

Time (s) after which the TIM expects to be polled. After this time elapses, the TIM sends a message to its local CPU indicating that the master station is disrupted.

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

- Parameters configured:

- After the configured time elapses, the TIM sends a message to its local CPU.

- Parameter not configured at a transmission speed of 9600 bps:

- After 4 seconds without message traffic the TIM outputs a message.

- Parameter not configured at a transmission speed of 1200 bps:

- After 32 seconds without message traffic the TIM outputs a message.

- **Max. allowed disruption time**

Tolerance time (s) for a detected connection disruption.

If there is still a disruption on the connection when the set time has elapsed, the disruption is signaled to all connection partners of the disrupted station.

Default setting: 0. Permitted range: 0...255. If you enter 0 (zero), the function is disabled.

#### Polling parameters

- **Ratio "Polling / Spontaneous"**

Max. number of spontaneous messages that can be sent by a master station between two polls.

Only for interfaces with the Connection mode "Master station".

Default setting: 0. Permitted range: 0...255. If you enter 0 (zero), the function is disabled.

#### Event transmission

- **Type of transmission**

Specifies the form in which data messages are sent.

- As single messages

- Several messages as a block

## 4.9.3 Dialup network

### Settings dialup network

Only the configurable parameters are explained.

#### 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.

- **Operating mode**

The operating mode of the serial interface specifies the mode of the data transfer.

A maximum of one serial interface of a TIM module may be operated in DMA mode.

Range of values:

- Interrupt (block)

This operating mode applies to the transmit and receive mode. The default mode Interrupt (block) is suitable for all connections. 4 characters are transferred per block. Following this, there is an interrupt. The received characters are checked only after a complete message has arrived.

- DMA

This operating mode applies to the transmit and receive mode.

The DMA mode should be used for connections with a high baud rate or a lot of message traffic, however not for GSM networks.

- Interrupt (individual characters)

This operating mode is used only in the receive direction. In the transmit direction, the block mode continues to be used.

The interrupt mode is suitable for extremely bad lines. An interrupt is triggered per transmitted character and each character is analyzed immediately after it is received allowing extremely good diagnostics of transmission errors. This mode is more reliable than the block mode but is slower.

**Number of spontaneous frames**

- **Number of spontaneous frames**

Only for interfaces with the Connection mode "Station" / "Node station".

The parameter decides after how many messages the master station has the opportunity of transferring its pending messages to the station. As maximum, the configured number of spontaneous frames that are pending at the time of the first call frame are transferred.

Default setting: 200. Permitted range: 0...255

If 0 (zero) is set, all spontaneous frames are sent at the call.

- **Limit for locked frames**

Only for interfaces with the Connection mode "Station" / "Node station".

Messages are marked as locked when due to communications problems they cannot be transferred to the communications partner.

The parameter specifies the maximum quota of locked messages in the send buffer. If the value is exceeded, the image procedure is used for new messages to prevent the send buffer from overflowing.

Default setting: 50. Permitted range: 0...90

If 0 (zero) is set, all spontaneous frames are sent at the call.

**Connection**

- **Extra transmission time**

Time offset (s) with slow networks to prevent premature stopping of connection establishment.

Default setting: 10. Permitted range: 0...65535. If you enter 0 (zero), the function is disabled.

The following values are usual:

- Mobile wireless networks: 10
- Wireless or satellite transmission: 0 .. 1

### **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\$S45=3\N0F0&W
- MD4 : AT\$S45=83\$P1\N0&W
- MD720 : For information on the initialization string, refer to the manual /5/ (Page 164).

- **AT string**

Input box for the AT initialization string

### Transmission setting for conditionally spontaneous messages

- **Transmission criterion**

Only for interfaces with the Connection mode "Station" / "Node station".

The transmission criterion controls connection establishment for the transmission of conditional spontaneous messages. This reduces the number of connection retries.

Range of values:

- Standard conditions

No connection will be established due to the existence of conditionally spontaneous messages .

Only in the following cases will a connection be established to send conditional spontaneous messages.

- Threatened overflow of the send buffer
- Connection establishment by the communications partner

- Degree of filling

The TIM only establishes a connection when the configured fill level of the send buffer for conditional spontaneous messages is exceeded.

In the input box, enter the fill level (%) of the send buffer at which when exceeded the TIM establishes a connection.

- Time

The TIM sends conditional spontaneous messages at a configured time of day, configurable with "Hours" / "Minutes".

- Time scheme

The TIM sends the conditional spontaneous messages cyclically at a configurable interval, configurable with "Hours" / "Minutes".

### Time options

- **Call acceptance delay**

Wait time (s) before accepting an incoming call

Due to the wait time acceptance of the call is possible for the TIM when a telephone is connected to a shared telephone connection to the TIM.

Default setting: 0. Permitted range: 0...30

- **Dial test interval**

The test interval (min) is started when no connection could be established by the TIM after 3 attempted repetitions. When the test interval elapses, the TIM re-establishes the connection again.

If the connection establishment fails, the test interval is restarted.

If a new message 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



- **Minimum connection duration**

Only for interfaces with the Connection mode "Master station".

Minimum connection duration (s) for a dial-up connection.

The minimum connection duration may be required in fast dial-up networks to be able to wait for the reply during a general request before the connection is terminated.

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

- **Abort delay time**

Duration (s) a dial-up connection is retained when the send buffer of the TIM is full and the TIM can send no further messages or data to the CPU.

During the abort delay time, received messages are acknowledged negatively and the communications partner repeats sent and negatively acknowledged messages.

When the abort delay time elapses, the connection is terminated.

Default setting: 20. Permitted range: 0...255

#### Event transmission

- **Type of transmission**

Specifies the form in which data messages are sent.

- As single messages
- Several messages as a block

#### Mobile wireless settings

- **PIN**

PIN of the SIM card of the modem MD720

## 4.10 Ethernet interface > Access to the Web server

### 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 41).

You enable the Web server and make further settings in the parameter group "Web server", see section Web server (Page 72). 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".

## 4.11 Creating telecontrol connections

### Single and redundant connections

For ST7 communication of a communications module you need to create at least one telecontrol connection in the "Network data" editor.

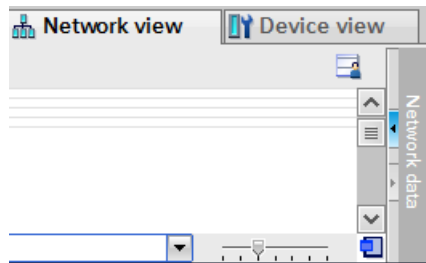
If two subscribers can be reached via different networks, to establish path redundancy you can create a maximum of two connections between the two subscribers. You specify redundant connections in the "Connection path" table (see below).

### 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.

In this tab you configure the telecontrol connections.

### Creating telecontrol connections for the the ST7 communication of the module

For communication between two stations with a module capable of ST7 via classic WAN networks (dedicated line, dialup network) you require at least one telecontrol connection. Follow the steps outlined below:

1. In the "Starting point" box, click on a free row in the "Telecontrol" tab.

The drop-down list shows the configurable starting points that can use the ST7 protocol:

- S7 stations: Assigned CPU
- PC stations: Application (e.g. ST7cc / ST7sc)

For connections between an application on the master station PC and an S7 station, always select the application as the starting point because it can only be selected in the list of starting points.

2. Select the starting point of the connection by double-clicking.

The connection will then be included in the list of telecontrol connections.

The name of the connection is preset, but you can change it.

3. Now in the "Endpoint" box select the connection partner from the drop-down list.

Boxes with a missing or bad configuration are shown on a red background, in the example the representation "TC\_Connection\_3".

Telecontrol-Verbindungen						
Name	Protocol	Starting point	Subscriber num..	Endpoint	Subscriber number - End	
TC_Connection_1	ST7	PLC_11	1	PLC_12	2	
TC_Connection_2	ST7	PLC_21	4	PLC_22	3	
TC_Connection_3	ST7	ST7cc_1	5	PLC_11	1	
<Neu hinzufügen>						

Projektierte Verbindungen			
Priority	Name	Module name	Subscriber number
1	Route_1_Ser	PLC_21 > TIM_21 > TIM_22 > PLC_22	4 > 1021 > 1022 > 3
2	Route_2_IE-S7	PLC_21 > TIM_21 > TIM_22 > PLC_22	4 > 1021 > 1022 > 3


  

Verbindungsweg					
Position	Module name	Subscriber num..	Station name	Interface	Interface t...
	PLC_21	4	S71500/ET200MP-Station	PROFINET-Schnittstelle_1	Ethernet
	TIM_21	1021	TIM_21	Ethernet-Schnittstelle_3	Ethernet
	TIM_21	1021	TIM_21	Serial Interface_1 [X4]	Dial up
	TIM_22	1022	TIM_22	Serial Interface_1 [X4]	Dial up
	TIM_22	1022	TIM_22	Ethernet-Schnittstelle_2	Ethernet

Figure 4-4 "Network data" editor, "Telecontrol" tab

### Specification of the connection sequence

Then specify the connection sequence of the created telecontrol connection.

1. Above the second table "Configured connection paths" click the paths symbol .

The dialog "Add connection paths" opens and the possible connection path are searched for.

2. Select one of the possible connection paths in the top table.

The connection path(s) are shown with details in the second table.

- If several connections are displayed in the upper table, you can select one or two redundant connections.
- If no connection is displayed in the upper 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.

3. If you want to choose the selected connection path as a "configured connection" click on "Add".  
 "Information" in the lower part of the dialog shows whether the connection was added or it is already configured.
4. Close the dialog with the "Close" button if the configured connections correspond to the demands of the project.  
 The connection details of every configured connection are displayed in the lower table "Connection path".

**The "Configured connection paths" and "Connection path" tables**

**"Configured connection paths" table**

This table shows the configured connections (connection paths) of a telecontrol connection.

Priority	Name	Module name	Subscriber number	Networks
1	Route_1	ST7cc_1 > TIM_11 > PLC_11	5 > 1001 > 1	PN > PN/IE_1
2	Route_2	ST7cc_1 > TIM_12 > TIM_11 > PLC_11	5 > 1002 > 1001 > 1	PN > > WAN_1 > PN/IE_1

Position	Module name	Subscriber num..	Station name	Interface	Interface type	Mode	Network
	ST7cc_1	5	PC_1	CP 1616_1, PROFINET int.	Ethernet	None	PN
	TIM_12	1002	TIM_12	Ethernet-Schnittstelle_1 [.	MSC	Station	
	TIM_12	1002	TIM_12	Serial Interface_1 [X4]	Dedicated line	Station	WAN_1
	TIM_11	1001	TIM_11	Serial Interface_1 [X4]	Dedicated line	Master	WAN_1
	TIM_11	1001	TIM_11	Ethernet-Schnittstelle_3 [.	Ethernet	Neutral	PN/IE_1
	PLC_11	1	S71500/ET200MP-Station_1	PROFINET-Schnittstelle_1.	Ethernet	Neutral	PN/IE_1

Figure 4-5 Redundant connection with incorrectly configured connection path (Route\_2)

Connections shown on a red background are invalid.

In the example the PC station was connected via the PC CP to the MSC network between TIM\_11 and TIM\_12 which is not allowed.

**"Connection path" table**

When checking the configured connections. the "Connection path" table supports you.

For every configured connection, the detailed connection path is shown here.

The "Position" column shows a station symbol with a symbol for the connection point (starting point, node, endpoint) Based on the color of the symbols for the connection endpoint you can recognize connections that are not permitted.

- Blue symbols for the connection point: Valid connections
- Red symbols for the connection point: Invalid connections

### Bad connections

In the example the connection path "Route\_2" was originally created from the application "ST7cc\_1" (PC\_1) via the MSC network to TIM\_12. This continued via the dedicated line network from TIM\_12 to TIM\_11.

A connection from the application via an MSC network as well as the connection path via modules with ST7 capability are not permitted.

The connection of the PC station to the MSC network was deleted in the meantime, so that the connection points "ST7cc\_1" and "TIM\_12" are invalid and their symbols are red.

### Redundant telecontrol connections



When different networks between two subscribers have been created in the network configuration the different connection paths are shown in the "Add connection paths" table.

If you only want to use one connection, select only this connection in the table and click "Add".

If you only want to establish a redundant connection, select two connection paths in the table and click "Add". You specify the main and substitute paths between the subscribers after closing the dialog using the "Configured connections" table.

### Main and substitute path of a redundant connection

When you have created two connection paths for a telecontrol connection, the first of the two is the main path and the second the substitute path. This is displayed in the "Priority" column of the "Configured connections" table.

You can change the priority of the two connection paths later, i.e. the specification of the main and substitute path. The arrow keys serve this purpose:  

## Delete invalid or redundant connections

If you have non-permitted or unwanted redundant connections you need to delete one connection. Follow the steps outlined below:

1. To delete a connection in the table "Configured connections", select the connection you do not need.
2. Delete the connection using the shortcut menu "Delete".

## Rules for connection configuration

Note the following rules for connection configuration:

- A connection via an inconsistent network is invalid. Examples:
  - Subscriber with incompatible modems
  - Incompatible settings of two modems in a connection
  - Incompatible settings between modem and network parameters
  - Connections via nodes that are not configured s node stations
- Two connections to one partner (endpoint) via the same interface of a module (start point) are not permitted.

- An MSC connection can only run via the first Ethernet interface [X1] of a TIM or via the serial interface of a module with the setting "IP-based".
- Connections between a PC application and a module can only be of the Network type "Neutral" (S7 connections).
- For connections between a redundant PC application and a module, you need to create two connections.

For a redundant ST7cc control center, in STEP 7 create two PC stations each with an ST7cc application (see below).

Only in this way can you configure a connection from each application.

- A connection via a network in which two MD3 modems communicate with each other and that are configured with 1200 bps / half duplex / AT mode is invalid.

### Connections to redundant control centers and other properties

If you select a connection in the table "Telecontrol connections" at the top in the "Network data" editor, three parameter groups are displayed in the "Properties" tab of the Inspector window. Here you can check and, if necessary, correct the connection configuration and configure the following properties:

- **General**

Here, you will find the basic properties of a telecontrol connection.

You can change the subscriber number of the connection starting point and endpoint. This affects the configuration data of the subscriber.

- **Redundant ST7cc/sc**

If you use a redundant control center in your project (e.g. ST7cc or ST7sc), you must first create two PC stations and the individual connections between the module and the two applications.

Only afterwards you create a redundancy group here for the connection to the redundancy group.

- Add redundant ST7cc/cc partner
- Enable the option for each of the two connections between the redundant application and the module.
- Redundant application

Select the required application from the "Redundant application" drop-down list.

- **Destination subscriber properties**

The parameter group relates to the destination subscriber that was configured as the endpoint of the connection.

- **General request supervision time**

This is the maximum time that may be required by a destination subscriber (communications module capable of ST7) to respond fully to a general request (GR).

If the GR response has not arrived completely at the requesting partner when the supervision time has expired, a message is entered in the diagnostics buffer of the module.

The general request supervision time is 900 seconds.

- **Frames to destination subscriber with time stamp**

Regardless of the configuration all frames are sent to the destination subscriber with a time stamp.

## 4.12 Time stamp

### Time stamp of the ST7 frames

The values of the data points are transferred by the communications module with a time stamp, see also section Creating telecontrol connections (Page 66), subsection "Connections to redundant control centers and other properties".

### Format of the time stamp

The ST7 time stamp is coded in BCD format. The exception is the half byte (nibble) with the time status.

The structure of 8 bytes is assigned as follows:

Table 4- 1 Assignment of the structure of the time stamp

Byte no.	Content	
	High nibble	Low nibble
0	Year * 10	Year * 1
1	Month * 10	Month * 1
2	Day * 10	Day * 1
3	Hour * 10	Hour * 1
4	Minute * 10	Minute * 1
5	Second * 10	Second * 1
6	Millisecond * 100	Millisecond * 10
7	Millisecond * 1	Time status

Table 4- 2 The assignment of the half byte "time status" (low nibble of byte 7)

Bit No.	Value	Meaning
0	0	Time is invalid
	1	Time is valid
1	0	Standard time
	1	Daylight saving time
2		<i>Not used</i>
3		<i>Not used</i>

## 4.13 Web server

### The Web server of the TIM

The TIM provides you with the functionality of a Web server for access using a Web browser. Via the Web server you have the following data available:

- Reading
  - A selection of diagnostics data
  - A selection of configuration data

For a description of the content, refer to the section The Web server (WBM) (Page 117).

### 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:

- Admin
- Standard
- Diagnostics

The rights of the preset roles mean the following for access to the Web server of the TIM:

- Web: Read system configuration  
Reading out configuration and diagnostics data from the Web server of the TIM.
- Web: Write application parameters  
Writing configuration data
- Web: Update firmware  
Loading firmware files via the Web server
- Web: Access Web diagnostics and the file system of the module  
Read and write access to all data in the Web server

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



## Releasing access to the Web server

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 Ethernet interface > Access to the Web server (Page 65). As default access is disabled.

### "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.

#### 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 "Access to the Web server" and "Web server" are adopted reciprocally in the other parameter group.

## 4.14 Communication with the CPU

### Communication with the CPU

Using the first three parameters you specify the CPU access by the TIM in the CPU scan cycle. You will find the structure of the CPU scan cycle in the section Read cycle (Page 102).

The fourth parameter "Frame memory size" decides the size of the send buffer of the TIM for frames of data points that are configured as an event.

- **Cycle pause time**

Wait time between two scan cycles of the CPU memory area

- **Max. number of write jobs**

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

- **Max. number of read jobs**

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

- **Frame memory size**

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

The size of the frame memory is divided equally among all configured communications partners. You will find the size of the frame memory in the section Performance data and configuration limits (Page 23).

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, triggers (Page 99).

## Watchdog bit

- **TIM monitoring**

Via the watchdog bit the CPU can be informed of the status of the telecontrol communication of the TIM.

## 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 the communication response of the two connection paths see section Communication via the SINAUT ST7 protocol (Page 46).

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 4- 3 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
<b>Path redundancy</b>	<b>Connection mode</b>	<b>Temporary connection **</b>	<i>(Reserved)</i>	<b>Message memory *</b>		<b>Path status</b>	<b>Partner status</b>
0: No redundancy 1: Redundancy exists	0: Permanent 1: Temporary	0: Partner not reachable 1: Partner reachable *	-	0: Send buffer OK 1: Memory allocation > 90% 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 'reachable' if the partner itself terminates the connection.

\*\* For the behavior of the message memory, refer to the section "Send buffer" in the section:

Process image, type of transmission, event classes, triggers (Page 99)

### 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 Creating telecontrol connections (Page 66).

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.

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 4- 4 Assignment of byte 1:

Bit 6 + 7	Bit 4 + 5	Bit 2 + 3	Bit 0 + 1
<b>Configured interface</b>		<b>Path status</b>	
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

**Example of 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 4- 5 Coding example 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

## 4.15 Time-of-day synchronization

### Basics of time-of-day synchronization

With telecontrol application that require time-of-day synchronization, you need to synchronize the time of day of the TIM 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 TIM 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 using an external time source, the connected S7 station can obtain the current time of day both via the CPU as well as via the TIM or a CP.

---

**Note**

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

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

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

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

---

### Synchronization method of the TIM

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

- **NTP / NTP (secure)**

Network Time Protocol

Time-of-day synchronization only via Ethernet

The secure method NTP (secure) uses authentication with symmetrical keys according to the hash algorithms MD5 or SHA-1. In the global security settings, you can create and manage 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 absolute time.

- **Time of day from subscriber in the network**

In this case the TIM adopts the time of day from a subscriber in the connected network. Time-of-day masters can for example be:

- A synchronized CPU
- A subscriber with a time receiver
- A master station PC (e.g. ST7cc/ST7sc) connected to the Ethernet network.

## 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.

## General information on configuration

### Parameter groups for time-of-day synchronization

For configuring the time-of-day synchronization the following parameter groups are available:

- **TIM**

- **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, you also configure the NTP servers if the TIM will be synchronized directly via NTP. This is usually only one TIM that functions as time master in the network.

- **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.

- **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 messages is derived automatically from the node type of the connected interfaces:

Master station ⇒ Node station ⇒ Station

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

### 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 via which the time of day will be forwarded by the time master to the time slaves.

## Configuring the synchronization via Ethernet

### 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)
  - Receive time from WAN  
(take the time from a network)
2. Configure the interface of the TIM via which time messages will be forwarded in the parameter group "WAN settings" as network type "Master station".

The function is supported for the Ethernet interface with the MSC protocol and for the serial interface with the setting "network type" = "Neutral".
3. In the parameter group "Send time" for the interface from step 2 enable the option "Forward time to WAN".

Via the connected network the time messages are forwarded in the network.
4. When necessary in the parameter group "Send time" enable the option "To local station" 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 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. When necessary in the parameter group "Send time" enable the option "To local station" if the assigned CPU should also be synchronized.



## Configuring the synchronization via classic WAN networks

### TIM modules (time master and slaves)

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)
  - Receive time from WAN  
(take the time from a network)
2. Configure the interface of the master TIM as network node type "Master station".
3. Configure the interfaces of the other TIM modules (time slaves) as network node type "Node station" or "Station".
4. When necessary in the parameter group "Send time" of the stations enable the option "To local station" if the assigned CPU should also be synchronized.

### 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. There 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

## 4.16 MSC authentication

### MSC authentication on the different interfaces

When using the secure MSC protocol (MSC / MSCsec) for the TIM as MSC station and as MSC node station the authentication data for the interface involved must be configured.

#### Parameter groups

- MSC authentication - Ethernet interface  
Relevant when using MSC on the Ethernet interface X1
- MSC authentication - MD720  
Relevant on the serial interface when using MSC via mobile wireless

**Parameter**

- **User name**  
User name for communication using MSC
- **Password**  
Password for communication using MSC

The user name and password must be different for every MSC station in the network.

## 4.17 SMSC

### Enabling SMSC

If you want to use SMS, enable the SMSC (Short Message Service Center).

Enter the phone number of the SMSC. You will receive the number from your service provider.

## 4.18 E-mail configuration

### Configuring e-mails in STEP 7

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 in STEP 7), you configure the individual e-mails, see section Message configuration (Page 114).

### 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.

### 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 85).

## 4.19 SNMP

### SNMP

The range of functions of the TIM for SNMP can be found in the section SNMP (Page 133).

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

#### SNMP

- **"Enable SNMP"**

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

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

- **"Use SNMPv1"**

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

- **"Use SNMPv3"**

Enables the use of SNMPv3 for the TIM. 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 TIM 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 TIM 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 generally known strings "public" and "private".

---

**SNMPv3**

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

- **"Authentication algorithm"**

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

- **"Encryption algorithm"**

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

**User management**

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

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

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

## 4.20 Security and protection

### 4.20.1 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 in the table below the local security settings of the module.

For a description of the procedure, refer to the section Handling certificates (Page 85).

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

### 4.20.2 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. 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 the a certificate in the table of device certificates and call the shortcut menu "Renew". Properties of the parameter "Alternative name of the certificate owner" changed in STEP 7 are not adopted by the STEP 7 project.

## 4.20.3 Protection

### Protection functions

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

<b>NOTICE</b>
<p><b>Configuring an access level does not replace the know-how protection</b></p> <p>Configuring access levels prevents unauthorized changes to the module by restricting the download rights.</p> <p>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.</p>

### 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.

## 4.20.4 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.

How the password takes effect is shown in the "Access level" column.

**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.

## 4.21 Data points

### 4.21.1 Data point configuration

#### Data point-related communication with the CPU

No program blocks need to be programmed for telecontrol modules with data point configuration to transfer user data between the station and communications 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 in the CPU program to allow configuration of the data points.

The PLC tags for data point configuration can be created in the standard tag table or in a user-defined tag table. 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

Remember the maximum possible number of PLC tags that can be used for data point configuration in the section Performance data and configuration limits (Page 23).

---

The formats and S7 data types of the PLC tags that are compatible with the protocol-specific data point types of the module can be found in the section Datapoint types (Page 97).

#### 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 find this using the project tree:

Project > directory of the relevant station > Local modules > TIM

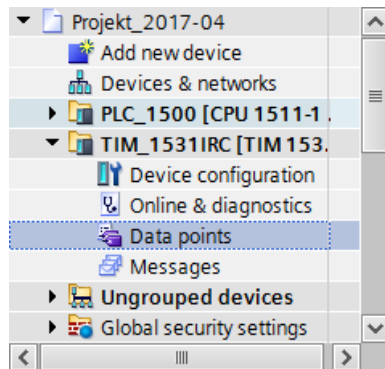


Figure 4-6 Configuring data points and messages

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

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

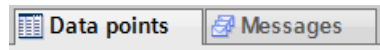


Figure 4-7 Switching over between the two editors

## 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 4-8 Data point table

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

## Assigning data points to their data source

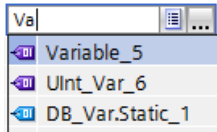
After creating it, you assign a new data point to its data source. Depending on the data type of the data point a PLC tag can serve as the data source.

For the assignment you have the following options:

- Click on the table symbol  in the cell of the "PLC tag" column.  
All configured PLC tags and the tags of the created data blocks are displayed. Select the required data source with the mouse or keyboard.
- Click the symbol .  
A selection list of the configured PLC Tags and the blocks is displayed. From the relevant table, select the required data source.

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

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



Select the required data source.

---

**Note**

**Assignment of parameter values to PLC tags**

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

---

**Arranging and copying objects**

As with many other programs in the data point or message editor you can also arrange the columns, sort the table according to your requirements and copy and insert objects.

- 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.

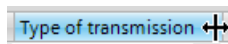
- Adapting the column width

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, pasting, cutting and deleting objects

If you click in a parameter box of an object in the table with the right mouse key, you can use the functions named with the shortcut menu (copy, paste, cut, delete).

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

## 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.

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.

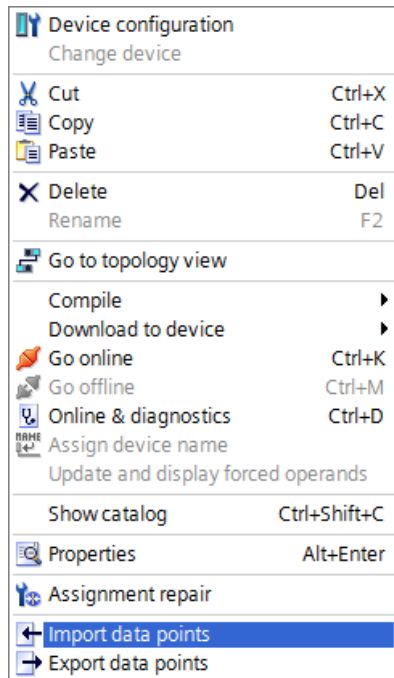


Figure 4-9 Shortcut menu of the module

When it is exported the data point information of a module is written to a 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 at one time.

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 data point information

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.

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.

#### Compatible modules


Data points can be imported and exported between compatible modules.

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

- ST7  
CP 1243-8 IRC, TIM modules with ST7 capability

### 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.

## 4.21.2 "General" tab

### General

You will also the most important parameters in the first tab of the data point editor in the data point table.

- **Data source**

- For the assignment of the PLC tabs, see section Data point configuration (Page 90).
- For the data point type, see Datapoint types (Page 97).

- **Send parameters**

See following sections

- For the type of transmission, see section Process image, type of transmission, event classes, triggers (Page 99).
- For the read cycle see section Read cycle (Page 102).
- High priority

If the option is enabled, the transfer has higher priority (important process data). The values of the data point are transferred before those of lower priority data points.

In dial-up networks the high priority leads to connection establishment only when the value of the data point is transferred with the transfer mode "Spontaneous (direct transfer)" (see "Trigger" tab).



- **Object**

- Object number

- The object number of the data point must be unique. The maximum permitted number of data points per SINAUT object must not be exceeded.

- Refer to the column "Number of data points per SINAUT object" in the section Datapoint types (Page 97).

- Object channel

- Channel number of the SINAUT object

- Partner object number

- Object number of the data point on the partner.

- Per object number, you need to specify a unique object number of the communications partner. This results in unique pairs of "Object number" and "Partner object number".

- See also section Partner stations (Page 113).

### 4.21.3 Datapoint types

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

---

**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

The direction of the data transfer is specified in the "Data point type" column.

- Input = Monitoring direction

- The objects (right column) for the monitoring direction have the abbreviation "\_S".

- Output = Control direction

- The objects (right column) for the control direction have the abbreviation "\_R".

Table 4- 6 Supported data point types and compatible S7 data types

Format (memory requirements)	Data point type	S7 data type	Operand area	Number of data points per object	Object
<b>Bit</b>	Digital input (Status Input)	Bool	I, Q, M, DB	8	Bin08X_S
	Digital output (Status Output)	Bool	Q, M, DB	8	Bin08X_R
<b>Byte</b>	Digital input (Binary Input)	Byte, USInt	I, Q, M, DB	4	Bin04B_S
	Digital output (Binary Output)	Byte, USInt	Q, M, DB	4	Bin04B_R
	Command output (Command Output)	Byte, USInt	Q, M, DB	1	Cmd01B_R
	Command input (Command Input) <sup>1)</sup>	Byte, USInt	Q, M, DB	1	Cmd01B_S <sup>1)</sup>
<b>Integer with sign (16 bits)</b>	Analog input (Analog Input)	Int	I, Q, M, DB	4	Ana04W_S
	Mean value (Mean Value Input)	Int	I, Q, M, DB	4	Mean04W_S
	Analog output (Analog Output)	Int	Q, M, DB	4	Ana04W_R
	Mean value (Mean Value Output)	Int	Q, M, DB	4	Mean04W_R
	Setpoint (Setpoint Output) <sup>2)</sup>	Int	Q, M, DB	1	Set01W_R
	Setpoint (Setpoint Input) <sup>1)</sup>	Int	Q, M, DB	1	Set01W_S <sup>1)</sup>
<b>Counter (16 bits)</b>	Counter input (Counter Input)	UInt, Word	I, Q, M, DB	1	Cnt01D_S
	Counter input (Counter Input)	UInt, Word	I, Q, M, DB	4	Cnt04D_S
	<b>Counter output (Counter Output) <sup>1)</sup></b>	UInt, Word	I, Q, M, DB	1	Cnt01D_R <sup>1)</sup>
	<b>Counter output (Counter Output) <sup>1)</sup></b>	UInt, Word	I, Q, M, DB	4	Cnt04D_R <sup>1)</sup>
<b>Floating-point number (32 bits)</b>	Analog input (Analog Input)	Real	I, Q, M, DB	4	Ana04R_S
	Analog output (Analog Output)	Real	Q, M, DB	4	Ana04R_R
<b>Data block (4 .. 48 bytes)</b>	Data (Data Input)	ARRAY [1...12] of DInt / UInt / DWord / Real <sup>3)</sup>	DB	12	Dat12D_S
	Data (Data Output)		DB	12	Dat12D_R
	Parameter (Parameter Output) <sup>2)</sup>		DB	12	Par12D_R
	Parameter (Parameter Input) <sup>1)</sup>		DB	12	Par12D_S <sup>1)</sup>

<sup>1)</sup> Only as Master station or Node station

<sup>2)</sup> See below, section "Mirroring"

<sup>3)</sup> See below, section "Block of data"

### **Mirroring**

The mirroring back function using the "Value monitoring" parameter can be configured for the following data point types:

- Setpoint output
- Parameter output

The local values of the data points of this type can be monitored for change and the changes transferred to the master with the Value monitoring function.

Changing a local value can, for example, be caused by manual operator input on site.

To allow the value resulting from local events or interventions to be transferred to the master, the Value monitoring function generates a mirroring back channel for the relevant data point via which the locally changed value is mirrored back.

Remember that to use the mirror back function, you need to interconnect the local values in the controller with the relevant PLC tag of the data point.

### **Block of data**

With the ARRAY data type, blocks of data from contiguous memory areas up to a size of 4 .. 48 bytes can be transferred.

Compatible components of ARRAY are DInt, UDint, DWord or Real. The components within an array must be of the same type.

## **4.21.4 Process image, type of transmission, event classes, triggers**

### **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 "Forced image mode" applies.

- If the send buffer reaches a fill level of 90%, the module changes to the forced image mode. New values from data points configured as an event are no longer added to the send buffer but rather they overwrite older existing values in the image memory.
- When the connection to the communications partner returns, the TIM changes back to the send buffer mode if the fill level of the send buffer has fallen below 50%.

## 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.

- **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.

## Trigger

Various trigger types are available for starting event-driven transfer:

- **Threshold value trigger**

The value of the data point is transferred when this reaches a certain threshold. The threshold is calculated as the difference compared with the last stored value, refer to the section Threshold value trigger (Page 104).

- **Time trigger**

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

- **Event trigger**

The value of the data point is transferred when a configurable trigger signal is fired. For the trigger signal, the edge change (0 → 1) of a trigger 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 the trigger tag is in the bit memory or in a data block, the trigger tag is reset to zero when the data point value is transferred.

Whether the value of a data point is transferred to the communications partner immediately after the trigger fires or after a delay depends on the parameter "Transmission mode".

## Transmission mode

The transmission mode of a frame is set in the "Trigger" tab of the data point. With the two options, you specify whether frames of events are sent immediately or following a delay:

- **Spontaneous**

The value is transferred immediately.

- **Conditional spontaneous**  
The value is transferred only when one of the following conditions is fulfilled:
  - The communications partner queries the station.
  - The value of another event with the transmission mode "Unsolicited" is transferred.
  - The fill level of the transmission buffer has reached 80% of its maximum capacity.

#### 4.21.5 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.

Normally it is adequate to assign only data to be acquired quickly such as alarms and contact changeover messages and command, setpoint and parameter objects for the 100n check to the fast cycle.

- **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.

## 4.21.6 "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 104).

- **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

#### **Transferring the value of a data point configured as an event**

You specify whether the value of a data point is transferred to the communications partner immediately after the trigger fires or after a delay in the "Transmission mode" parameter.

### Transmission mode

The transmission mode of a frame is set in the "Trigger" tab of the data point. With the option, you specify whether messages of events are sent immediately or following a delay:

- **Immediate transfer - Spontaneous**  
The value is transferred immediately.
- **Buffered transfer - Conditional spontaneous**  
The value is transferred only when one of the following conditions is fulfilled:
  - The communications partner queries the station.
  - The value of another event with the transmission mode "Spontaneous" is transferred.

### 4.21.7 Threshold value trigger

---

#### Note

#### **Threshold value trigger: Calculation only after "Analog value preprocessing"**

Note that the analog value preprocessing is performed before the check for a configured threshold value and before calculating the threshold value.

This affects the value that is configured for the threshold value trigger.

---

#### Note

#### **No Threshold value trigger if Mean value generation is configured**

If mean value generation is configured, no threshold value trigger can be configured for the analog value event involved.

---

For the time sequence of the analog value preprocessing refer to the section Analog value preprocessing (Page 106).

### Threshold value trigger

#### Function

If the process value deviates by the amount of the threshold value, the process value is saved.

Two methods are used to calculate the threshold value deviation:

- **Absolute method**  
With binary and counter values as well as with analog values with configured mean value generation, the absolute method is used to calculate the threshold value deviation.
- **Integrative method**  
With analog values without configured mean value generation, the integrating method is used to calculate the threshold value deviation.

In the integration threshold value calculation, it is not the absolute value of the deviation of the process value from the last stored value that is evaluated but rather the integrated deviation.



### Absolute method

For each binary value a check is made to determine whether the current (possibly smoothed) value is outside the threshold value band. The current threshold value band results from the last saved value and the amount of the configured threshold value:

- Upper limit of the threshold value band: Last saved value + threshold value
- Lower limit of the threshold value band: Last saved value - threshold value

As soon as the process value reaches the upper or lower limit of the threshold value band, the value is saved. The newly saved value serves as the basis for calculating the new threshold value band.

### Integrative method

The integration threshold value calculation works with a cyclic comparison of the integrated current value with the last stored value. The calculation cycle in which the two values are compared is 500 milliseconds.

(Note: The calculation cycle must not be confused with the scan cycle of the CPU memory areas).

The deviations of the current process value are totaled in each calculation cycle. The trigger is set only when the totaled value reaches the configured value of the threshold value trigger and a new process value is entered in the send buffer.

The method is explained based on the following example in which a threshold value of 2.0 is configured.

Table 4- 7 Example of the integration calculation of a threshold value configured with 2.0

Time [s] (calculation cycle)	Process value stored in the send buffer	Current process value	Absolute deviation from the stored value	Integrated devia- tion
0	<b>20.0</b>	<b>20.0</b>	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	<b>20.5</b>	<b>20.5</b>	+0.5	<b>2.0</b>
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	<b>19.9</b>	<b>19.9</b>	-0.6	<b>-2.1</b>

With the changes in the process value shown in the example, the threshold value trigger configured with 2.0 fires twice:

- At the time 3.5 s: The value of the integrated deviation is at 2.0. The new process value stored in the send buffer is 20.5.

- At the time 6.0 s: The value of the integrated deviation is at 2.1. The new process value stored in the send buffer is 19.9.

In this example, if a deviation of the process value of approximately 0.5 should fire the trigger, then with the behavior of the process value shown here a threshold value of approximately 1.5 ... 2.5 would need to be configured.

### 4.21.8 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 "Fault suppression time", "Limit value calculation" and "smoothing" are not performed if no threshold value trigger is configured for the relevant data point.. In these cases, the read process value of the data point is entered in the image memory 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:

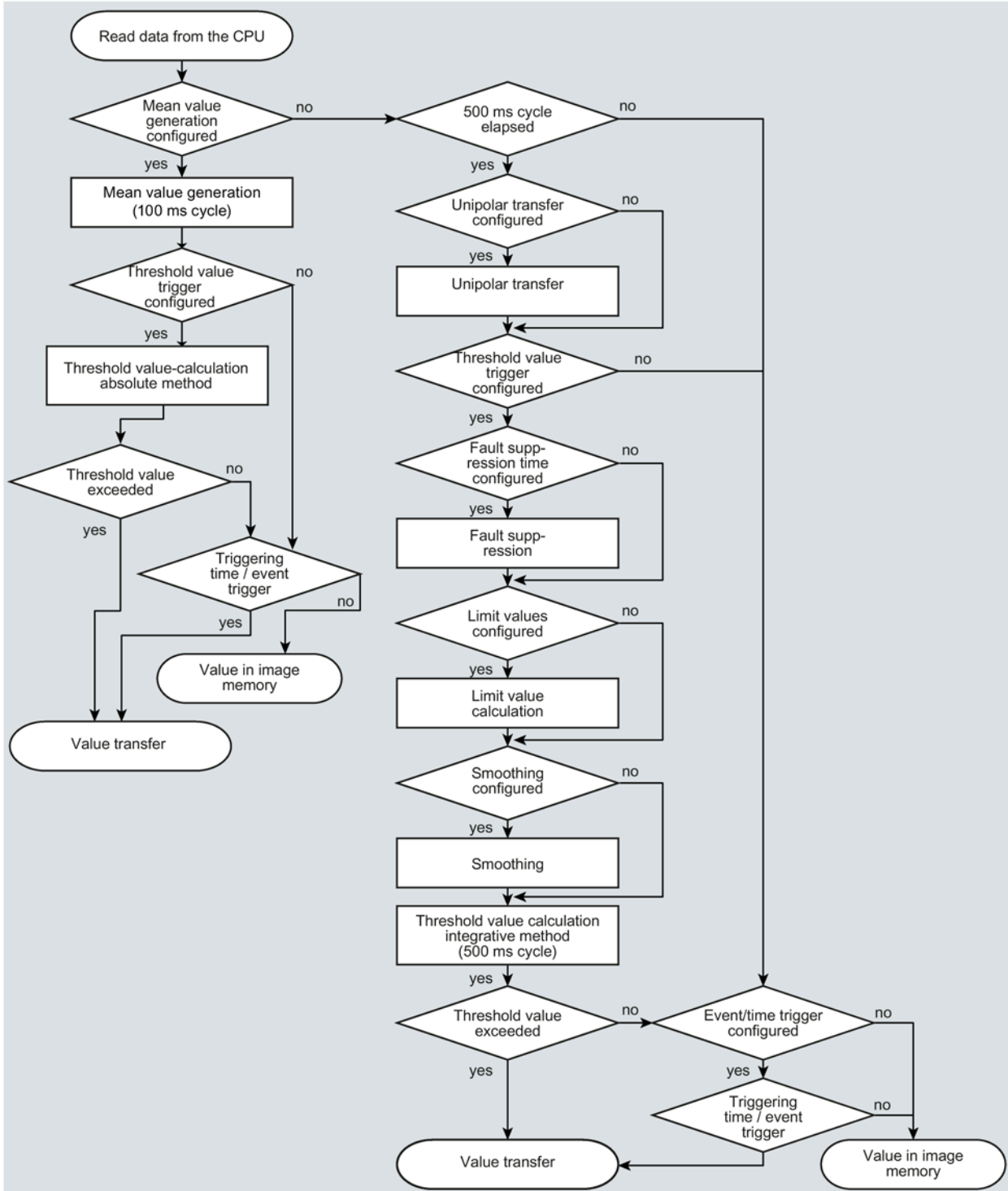


Figure 4-10 Sequence of the analog value preprocessing

The 500 millisecond cycle is started by the integrative threshold value calculation. In this cycle, the values are saved even when the following preprocessing options are enabled:

- Unipolar transfer
- Fault suppression time
- Limit value calculation
- Smoothing

## Mean value generation

---

### Note

#### Restricted preprocessing options if mean value generation is configured

If you configure mean value generation for an analog value event, the following preprocessing options are not available:

- Unipolar transfer
  - Fault suppression time
  - Smoothing
- 

### Function

With this parameter, acquired analog values are transferred as mean values.

If mean value generation is active, it makes sense to configure a time trigger..

The current values of an analog data point are read in a 100 millisecond cycle and totaled. The number of read values per time unit depends on the read cycle of the CPU and the CPU sampling cycle of the TIM.

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<sub>h</sub> or -32768 / 8000<sub>h</sub> 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<sub>h</sub> 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<sub>h</sub>) or underflow range (8000<sub>h</sub>) is suppressed for the specified time. The value 7FFF<sub>H</sub> or 8000<sub>H</sub> 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<sub>h</sub>) or underflow range (-32768 / 8000<sub>h</sub>) 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<sub>h</sub> or -32768 / 8000<sub>h</sub> in the overflow or underflow range. If this is not the case, the parameter should not be configured for preprocessed values.

For finished values preprocess in the CPU, the limits for the overflow and underflow can be freely assigned.

**Smoothing factor**

**Requirements for the function**

Configuration of the threshold trigger for this data point

**Restrictions**

The smoothing factor cannot be configured at the same time as mean value generation. A configured value has no effect when mean value generation is activated.

**Function**

Analog values that fluctuate quickly can be evened out using the smoothing function.

The smoothing factors are calculated according to the following formula as with S7 analog input modules.

$$y_n = \frac{x_n + (k - 1) y_{n-1}}{k}$$

where

- y<sub>n</sub> = smoothed value in the current cycle
- x<sub>n</sub> = value acquired in the current cycle n
- k = smoothing factor

The following values can be configured for the module as the smoothing factor.

- 1 = No smoothing
- 4 = Weak smoothing
- 32 = Medium smoothing
- 64 = Strong smoothing

## Set limit value 'low' / Set limit value 'high'

### Requirements for the function

- Configuration of the threshold trigger for this data point
- PLC tag in the bit memory operand area or data area

The analog value data point must be linked to a PLC tag in the bit memory or data area (data block).

For PLC tags for analog input modules (input operand area) limit value configuration is not possible. With these analog values the limit values of the following table are used automatically.

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.

### Configuration of the limit value

The limit value is configured as a whole decimal number. The range of values is based on the range of values of the raw value of analog input modules.

Range	Raw value (16 bits) of the PLC tag		Module output [mA]			Measuring range [%]
	Decimal	Hexadecimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
Overflow	32767	7FFF	> 23.515	> 23.515	> 22.810	> 117.593
Overrange	32511	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
Nominal range (bipolar)	27648 ...	6C00 ...		20 ...		100 ...
	0	0000		0		0
	... -27648	... 9400		... -20		... -100
Underrange (unipolar / life zero)	-1	FFFF	-0.001		3.999	-0.004
	...	...	...		...	...
	-4864	ED00	-3.518		1.185	-17.59
Underrange (bipolar)	-27649	93FF		-20.001		-100.004
	...	...		...		...
	-32512	8100		-23.516		-117.593
Undershoot / wire break	-32768	8000	< -3.518		< 1.185	< -17.593

Please note: The entry of the value 0 (zero) is interpreted as a deactivated limit value.

**Note**

**Evaluation of the value even when the option is disabled**

If you enable one or both options and configure a value and then disable the option later, the grayed out value is nevertheless evaluated.

To disable the two options, delete the previously configured values limit values from the input boxes and then disable the relevant option.

**Recommendation for quickly fluctuating analog values:**

If the analog value fluctuates quickly, it may be useful to smooth the analog value first if limit values are configured.

**4.21.9 Command outputs**

**Parameters for the data point type "Command output (Cmd01B\_R)"**

The data point type allows receipt of a command with the following control information (control code):

- LATCH\_ON / LATCH\_OFF

or

- PULSE\_ON

When the byte "Control Code" is received with the function "PULSE\_ON" information sent with it by the master "Count", "On-time" and "Off-time" is evaluated and compared to the object parameters "Max. pulse duration", "Pulse duration replacement time" and "Max. number of pulses" (see below).

The following control codes sent by the master station are evaluated.

Table 4- 8 Functions of the data object

Receipt of:			Reaction of the object depends on the configuration	
Control Code	TCC *	Op Type **	Output mode = Pulse on	Output mode = Latch on/off
0x01	NUL	PULSE_ON	The output is set to 1 for the duration of "On-time".	The command is rejected.
0x03	NUL	LATCH_ON	The command is rejected.	The output is set permanently to 1.
0x04	NUL	LATCH_OFF	The command is rejected.	The output is set permanently to 0.
0x41	CLOSE	PULSE_ON	The output is set permanently to 1 (as with LATCH_ON).	The command is rejected.
0x81	TRIP	PULSE_ON	The output is set permanently to 0 (as with LATCH_OFF).	The command is rejected.

\* Trip-Close Code field

\*\* Operation Type field



### Parameter

Name: **Max. number of pulses**

Range of values: 0 ... 255

Default: 0

Explanation: Monitors the number of pulses sent by the master station (Count). If the number of pulses received from the master station exceeds the value configured here, the command is rejected.  
If you enter 0 (zero), the monitoring is disabled.

Name: **Max. pulse duration**

Range of values: 0 ... 2147483647

Default: 0

Explanation: Monitors the pulse duration sent by the master station (On-time). If the pulse duration received from the master station exceeds the value configured here, the command is rejected.  
If you enter 0 (zero), the monitoring is disabled.

Name: **Pulse duration equivalent time**

Range of values: 0 ... 2147483647

Default: 0

Explanation: Substitute value for the pulse duration If the pulse duration received from the master exceeds the value configured in "Max pulse duration". The parameter is only used when "Max. pulse duration" is configured.  
If the value is 0 (zero), no replacement value is used.

## 4.21.10 Partner stations

### Enabling the partner for the ST7 data point

Enable all partners to which a telecontrol connection was configured and with which the selected data point will exchange data. To do this select the relevant "

You can configure or change the partners in the overview table or in the "Partner stations" tab of the module. The data will be adopted at the other point.

## 4.22 Messages

### 4.22.1 Message configuration

#### Configuring e-mails

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

You configure the e-mail in STEP 7 in the editor for the data point and message configuration. You can find this using the project tree:

Project > Directory of the relevant TIM

For the view in STEP 7, refer to the section Data point configuration (Page 90).

#### Requirements and necessary information

Remember the following requirements in the configuration for the transfer of messages:

- Enabling telecontrol communication ("Communication types") parameter group
- SMS: Configuration of the SMSC in the "SMSC" parameter group
- E-mails: Configuration of the "E-mail configuration" parameter group

To do this, you require the following information:

- Access data of the SMTP server: Address, port number, user name, password
- TIM's own e-mail address
- Email address of the recipient

#### "Message parameter"

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

## "Trigger"

In the "Trigger" parameter group you configure triggering for sending the message and other parameters.

- **E-mail trigger / SMS trigger**

Specifies the event for which the sending of the message is triggered.

- Use PLC tag

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

- CPU changes to STOP

- CPU changes to RUN

- Connection to a partner interrupted

Triggers the sending of the message when the connection to a partner is interrupted.

- Connection to a partner established

Triggers the sending of the message when the connection returns.

- Weak mobile wireless network

Only with SMS

Triggers the sending of an SMS when the network is weak and possibly no dialup connection can be established via mobile wireless.

- **PLC tag for trigger**

PLC tag for the message trigger "Use PLC tag"

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

- **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 (diagnostics status) or read it out from the PLC tag.

For the significance of the status output in hexadecimal, refer to the section Processing status of the messages (SMS / e-mail) (Page 135).

- **PLC tag for processing status**

PLC tag of the type DWORD for the processing status

- **Include value**

If you enable the option, the TIM sends a value for the placeholder \$\$ from the memory area of the CPU in the message. To do this enter "\$\$" as a placeholder for the value to be sent in the message text.

Select a PLC tag whose value will be integrated in the message. The value is entered in the message text instead of the placeholder \$\$.

\$\$ can be a placeholder for data point types with a simple data type up to a size of 32 bits.

- **PLC tag for value**

PLC tag in which the value to be sent is written.

## The Web server (WBM)

### 5.1 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 56)
- Firefox (version 51)

You will find these Web browsers, information and any necessary addons on the Internet.

### 5.2 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

The condition for access to the TIM is that the PC is located in the same subnet and that the TIM can be reached.

### 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:

## 5.3 General functions of the WBM

### Symbols of the title bar

The symbols in the title bar have the following significance:

Symbol	Function
	Date and time of the last page update of the WBM in the local time of the RTU (yyyy-mm-dd hh:mm:ss)
	Displays the set WBM language You set the WBM language with the setting of the browser being used. The following languages are supported: <ul style="list-style-type: none"> <li>• German</li> <li>• English</li> </ul>
	Name of the currently logged in user
	Logout of the user
	The automatic update of the WBM display is enabled. The data is called up at 5 second intervals.

Symbol	Function
	The automatic update of the WBM display is disabled.
<a href="#">Turn on</a>	Switches on the automatic update of the WBM display.
<a href="#">Turn off</a>	Switches off the automatic update of the WBM display.
	Prints out the current WBM page

## 5.4 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

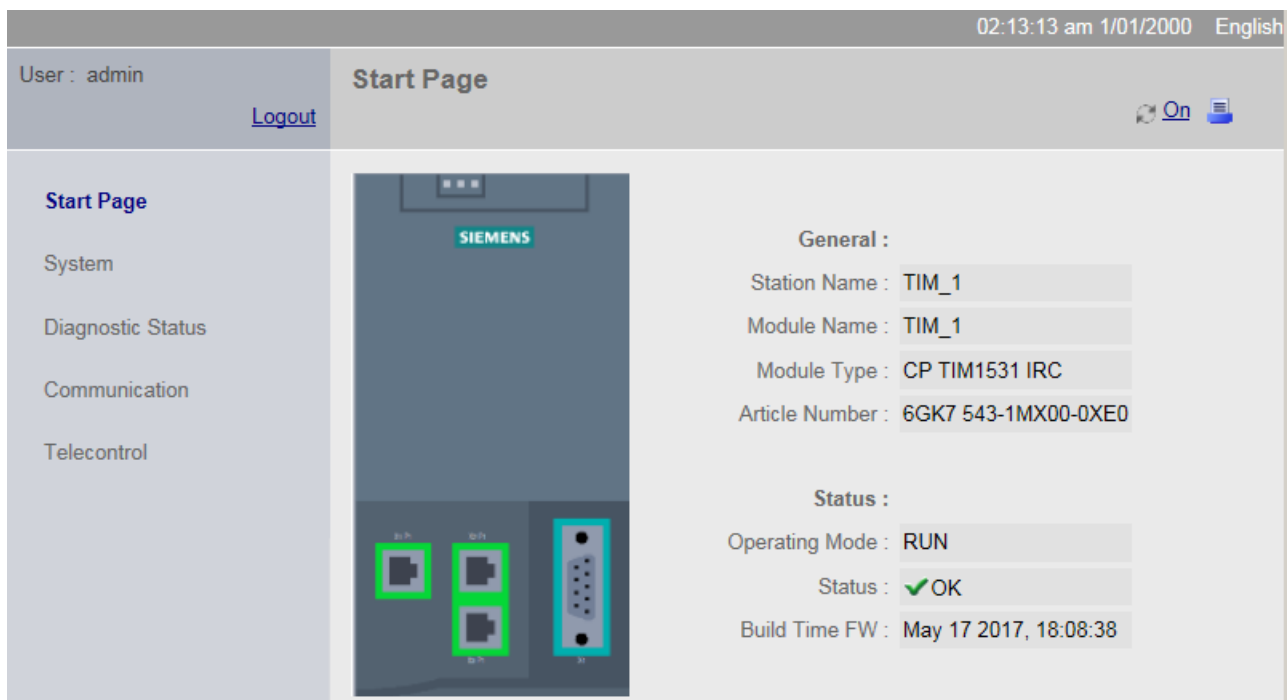


Figure 5-1 Start page of the WBM

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 YY, hh:mm:ss

## 5.5 System

### 5.5.1 Device info

**Module**

- Short designation  
Parameter configured in STEP 7
- Article number
- Hardware product version
- Firmware version
- Rack
- Slot



**Module information**

- Device name  
- *not relevant* -
- Module name  
Parameter configured in STEP 7

**Vendor information**

- Vendor
- Serial number  
Serial number of the device

**5.5.2 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

**5.5.3 NTP****NTP**

- **NTP server list**  
Shows the addresses of the configured NTP servers.

**5.5.4 DNS configuration****DNS server list**

- **List of configured DNS servers**  
Servers configured in STEP 7

## 5.6 Diagnostics

### 5.6.1 Diagnostics messages

#### 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

## 5.6.2 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 135).
- **Type**  
Type of the message

## 5.7 LAN

### 5.7.1 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

- **Network setting**

Behavior of the network setting:

- Automatic
- Manual setting for transmission speed and direction dependency

- **Mode**

Used transmission speed and direction dependency (duplex/half duplex)

- **Medium**

Connected medium (copper / optical)

## IPv6 parameters

- **IPv6 address**

Currently used IPv6 address

- **IPv6 gateway**

Configured default gateway

## 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.

## 5.8 Telecontrol

### 5.8.1 Partner information

The tab shows you information on the communications partners and the connection status of the TIM.

- **Top left**

Here you will find the connection overview with information on the connection partners of the TIM.

⇒ Select a partner in the "Partner type" list e with the mouse.

- **Top right**

Here the information on the selected partner and the connection paths is displayed.

- **Bottom right**

Here information on the frame status of the TIM is displayed.

#### Connection overview

- **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: Not connected**

None of the possible connections is established

- **Partner type**

Possible partner types:

- CPU (local CPU)

The CPU assigned to the TIM in the configuration.

- Application (e.g. WinCC)

- CPU

CPU of the remote station

- TIM

TIM of the remote station

- CP 1243-8 IRC

CP of the remote station

- **Subscriber number**  
Subscriber number of the partner

## Partner: Local CPU

### Local CPU

- **Status**  
Operating status of the local CPU
- **Number of connections**  
Number of connections between the TIM and local CPU

### Transmission path 1

- **Interface no.**  
Number of the Ethernet interface of the TIM (1 / 2 / 3)
- **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

## Partner: Remote partner

### Partner

Information on the partner selected on the left of the WBM page

- **Partner type**
  - Application (e.g. WinCC)
  - CPU
    - CPU of the remote station
  - TIM
  - CP 1243-8 IRC
- **Subscriber number**

Subscriber number of the partner
- **Connection status**
  - Connected
  - Not connected

### Transmission paths

- **Number of transmission paths**

Number of configured telecontrol connections
- **Status transmission paths**
  - All transmission paths OK
  - 1 transmission path OK
  - No transmission path OK
- **Security options**

Display of the configured and active option:  
ON / OFF
- **Time master**

Display of the configured and active option:  
Yes / No

### Transmission path 1 / 2

- **Address**

IP address or WAN address of the interface of the TIM
- **Interface**

Interface of the TIM
- **CFB reference**

Local ID (decimal) of the S7 connection



- **Connection type**

Display of several of the following connection properties:

- PBK connection  
Configured S7 connection
- MSC connection  
Connection of the MSC protocol for which no S7 connections are required.
- CR connection  
Read/write connection to the local CPU that does not require S7 connections.
- 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
- Not connected

## Frame memory status

Display of the frame memory status of the TIM:

- **Normal operation**

The send buffer is working normally. The memory space allocation is between 10 and 90%.

- **90% limit reached**

When the send buffer is 90% full, the TIM switches to the forced image mode.

See also section Process image, type of transmission, event classes, triggers (Page 99).

- **Overflow**

Send buffer 100% full

## 5.8.2 Data points

The tab shows you information on the configured data points of the TIM.

### Data points

- **Data point number**
- **Name and type**  
Name and type of the data point
- **Type identifier**  
Object group of the DNP3 data point or type of the IEC data point
- **Object number**  
Object number of the ST7 data point
- **Status**  
Status of the connection of the data point to the communications partner
- **Current value**  
Currently saved value
- **Historical value**  
Value saved last but one
- **Time stamp**  
Time stamp of the currently saved value

## Diagnostics and upkeep

### 6.1 Diagnostics options

The following diagnostics options are available.

#### LEDs of the module

For information on the LED displays, refer to the section LEDs (Page 28).

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

If your engineering station is connected to the TIM via Ethernet, here you will receive information about the selected module:

- Connection status of the engineering station with the TIM

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

Using the online functions, you can read diagnostics information from the TIM from an engineering station on which the STEP 7 project is stored. You obtain the following static information on the selected module:

- **General information on the module**  
General information on the module
- **Diagnostics status**  
Information on the diagnostics status
- **Ethernet interface[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, a connection statistic and further diagnostics information. Click on a subscriber to display further information.

You will also find information on the partners in the WBM.

- **Data point list**

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

– **Protocol diagnostics**

With this function you can enable the logging of ST7 frames of the TIM and evaluate it using the SINAUT engineering software.

With the function "Enable protocol trace" the frames received and sent by the module are copied for several seconds.

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

With the function "Save", you can save the log file on the engineering station.

To evaluate the file you need to rename it to the format "\*.7dt". You can decode and analyze the renamed file using the TIM frame monitor of the SINAUT diagnostics tool.

– **Device-specific events**

Here you will find diagnostics buffer entries of the TIM and an overview of the sent messages (SMS messages / e-mails).

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

## Web server (WBM) of the TIM

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 The Web server (WBM) (Page 117).

### 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 126).

### 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 the section Communication with the CPU (Page 73).

## SNMP

For information on the functions, refer to the section SNMP (Page 133).

## 6.2 Online functions

### Online functions


Along with STEP 7 on the engineering station (ES) the TIM provides various diagnostics and maintenance functions. The requirement is that the ES and the TIM are located in the same subnet.

## Connection establishment to use the online functions via Ethernet

### Procedure:

1. Connect the ES to the network.
2. Open the relevant STEP 7 project on the ES.
3. Select the TIM that you want to update with new firmware.
4. Enable the online functions using the "Connect online" icon.
5. In the "Connect online" dialog, go to the Choose the entry "TeleService via telecontrol" in the "Type of PG/PC interface" drop-down list.
6. In the "PG/PC interface" drop-down list select the entry "TeleService board".
7. In the table select the TIM if it is not already selected.

The path both via the TIM or also via the CPU is possible.

8. Click on the  icon next to the "PG/PC interface" drop-down list.

The "Establish remote connection via telecontrol" dialog box opens.

9. Make the necessary entries in this dialog (see below) and click on "Connect".

### Terminate online connection

On completion of the online session, terminate the online connection again using the "Disconnect" button.

## 6.3 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 entered in MIB files (MIB = Management Information Base).

### Scope of performance of the TIM as an SNMP agent

The TIM supports data queries in the following SNMP versions:

- SNMPv1 (standard)
- SNMPv3 (Security)

It returns the contents of MIB objects of the standard MIB II according to RFC 1213 and the Siemens Automation MIB.

- **MIB II**

The TIM supports the following groups of MIB objects:

- System
- Interfaces

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

- IP
- ICMP
- TCP
- UDP
- SNMP

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

- Address Translation (AT)
- EGP
- Transmission

- **Siemens Automation MIB**

The following exceptions / restrictions apply to the TIM.

Write access is permitted only for the following MIB objects of the system group:

- sysContact
- sysLocation
- sysName

A set sysName is sent as the host name using DHCP option 12 to the DHCP server to register with a DNS server.

For all other MIB objects / MIB object groups, only read access is possible for security reasons.

Traps are not supported by the TIM.

For more detailed information about the MIB files and SNMP, refer to the manual /11/ (Page 165).

## Configuration

For information on the configuration, refer to the section SNMP (Page 83).

## 6.4 Processing status of the messages (SMS / e-mail)

### Processing status of messages

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

### Processing status of the telecontrol e-mails

The meaning of the statuses is as follows:

Table 6- 1 SMS: Meaning of the status ID output in hexadecimal format

Status	Meaning
0000	Transfer completed free of errors
0001	Error in the transfer, possible causes: <ul style="list-style-type: none"> <li>• SIM card invalid</li> <li>• No network</li> <li>• Wrong destination phone number (number not reachable)</li> </ul>

Table 6- 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.

6.4 Processing status of the messages (SMS / e-mail)

Status	Meaning
8415	An internal error occurred in the cURL module. Execution was aborted.
8416	An internal error occurred in the SMTP module. Execution was aborted.
8417	Requests to SMTP on a channel already being used or invalid channel ID. Execution was aborted.
8418	Sending the e-mail was aborted. Possible cause: Execution time exceeded.
8419	The channel was interrupted and cannot be used before the connection is terminated.
8420	Certificate chain from the server could not be verified with the root certificate of the 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"> <li>• Recipient address ("To" or "Cc").</li> </ul>
8502	Syntax error. Check the following configuration data: Alarm configuration > E-mail data (Content): <ul style="list-style-type: none"> <li>• Email address (sender)</li> </ul>
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"> <li>• Module configuration &gt; E-mail configuration: <ul style="list-style-type: none"> <li>– User name</li> <li>– Password</li> <li>– Email address (sender)</li> </ul> </li> <li>• Alarm configuration &gt; E-mail data (Content): <ul style="list-style-type: none"> <li>– Recipient address ("To" or "Cc").</li> </ul> </li> </ul>
8554	Transfer failed
85xx	Other error message from the e-mail server Apart from the leading "8", the message corresponds to the three-digit error number of the SMTP protocol.



## 6.5 Update firmware

### New firmware versions of the TIM

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/cert>)

Firmware files have the file format \*.upd.

Save the firmware file on your PC.

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

- Loading the firmware with the online functions of STEP 7 via Ethernet / Internet
- Loading the firmware from an SD card

---

**Note****SD card only for firmware file**

For the firmware file you require a separate SD card. This must meet the requirements of the TIM, see section SD cards (Page 153).

You cannot use the SD card with the configuration data.

---

---

**Note****Duration of the firmware update**

Downloading a new firmware file can take several minutes.

Always wait until the completion of the firmware update can be recognized from the LEDs (see below).

---

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

**Requirements:**

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

**Procedure:**

1. Select the TIM that you want to update with new firmware.
2. Enable the online functions using the "Connect online" icon.

3. In the "Connect online" dialog, select the Ethernet interface in the "Type of PG/PC interface" list box.
4. Select the TIM.
5. Click on "Start search" to search for the module in the network and to specify the connection path.

When the module is found it is displayed in the table.

6. Connect using the "Connect" button.

The "Connect online" wizard guides you through the remaining steps in installation.

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

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

## Loading the firmware via the SD card

### Requirements:

- You have copied the new firmware file from your PC to the SD card using a suitable card reader.
- You have saved a backup file of the firmware file currently being used.

### Procedure:

1. Turn off the power supply to the TIM.
2. If you use an optional SD card for the configuration data, take the SD card out of the card slot of the TIM.

See section Switch (Page 31) for information on this.

3. Insert the SD card with the firmware file in the card slot of the TIM.
4. Turn on the power supply to the TIM.

The TIM starts up with the new firmware from the SD card.

Wait until the startup is completed successfully.







5. Turn off the power supply to the TIM.

6. Remove the SD card with the firmware file from the card slot of the TIM.  
If you use an optional SD card for the configuration data, plug this into the card slot of the TIM.
7. Turn on the power supply to the TIM again.  
The TIM starts up with the new firmware and the configuration data on the SD card.

### LED patterns when updating the firmware

The table below describes the LED patterns when transferring a firmware file to the TIM.

Table 6- 3 Meaning of the LED patterns

RUN	ERROR	CONNECT	LED pattern / meaning
			The firmware file is transferred. <ul style="list-style-type: none"> <li>• "RUN" flashes alternately green and yellow.</li> <li>• "ERROR" is off.</li> <li>• "CONNECT" flashes.</li> </ul>
			Startup successfully completed, start of the firmware

For the LED pattern during the restart, refer to the section Startup - LED pattern (Page 40).

## 6.6 Resetting to factory settings

### Resetting to factory settings: Effect

---

#### Note

#### Configuration data is deleted

With the functions for resetting to factory settings described here, all configuration data on the TIM is deleted!

---

- **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

**Note**

**Configuration data when using an SD card**

If you use an SD card and you want to reset the TIM to the factory settings, you must pull the SD card before resetting. If the SD card remains inserted, the TIM starts up again with the configuration data on the SD card.

When pulling the SIM card, remember the information in section Inserting the SD card (Page 38).

**Executing the "Reset to factory settings" function**

To reset to factory settings using the switch, follow the steps outlined below:

1. Put the switch to the position "MRES" and hold it in the "MRES" position for at least 5 seconds.

The TIM restarts.

2. During the restart, continue to hold the switch in the "MRES" position.





If the LED pattern of step 2 occurs (see below) the TIM is reset.

For information on the switch settings, refer to the section Switch (Page 31).

**LED patterns when resetting**

The table below describes the LED patterns when resetting the TIM.

Table 6- 4 Meaning of the LED patterns

Step	LED pattern			Meaning
	RUN	ERROR	CONNECT	
1				After holding the switch in the "MRES" position for 5 seconds, chaser lights of the three LEDs appear (flashing alternately). The TIM restarts. Continue to hold switch.
2				As soon as the three LEDs flash three times synchronously the TIM is reset. It adopts the factory settings. You can release the button:

**Startup after resetting to factory settings**

After resetting return the switch of the TIM back to the "RUN" position.

The TIM restarts again. For the LED pattern see section Startup - LED pattern (Page 40).

When resetting using the WBM, the TIM starts up again automatically.

The remaining behavior depends on the use of an optional SD card:

- **Startup without SD card**

If you do not use an SD card, the TIM starts up without configuration data with an error.

You need to reload the configuration data.

The TIM can be reached via its Ethernet interfaces with default IP address (see above) set in the factory.

Generally, the defaults apply during the first commissioning, refer to the section Commissioning (Page 39).

- **Startup with SD card**

If the SD card remains inserted, the TIM starts up again with the configuration data on the SD card.

## 6.7 Module replacement

### Startup with configuration data from the SD card

Depending on the use of an optional SD card, the STEP 7 configuration data of the TIM are stored differently.

- **No use of an SD card**

The configuration data of the TIM is stored in the work memory of the TIM.

- **Use of an SD card**

If an SD card is used, the configuration data is stored on the SC card and read from there each time the TIM starts up.

If the TIM needs to be replaced, this allows simple replacement of the TIM without needing to download the configuration data again.

If you insert the SD card of the TIM being replaced in the new TIM, when it restarts it reads the configuration data from the SD card of the replaced TIM.



# Technical specifications

## 7.1 Technical specifications

Table 7- 1 Technical specifications - TIM 1531 IRC

<b>Technical specifications</b>		
<b>Article number</b>	6GK7 543-1MX00-0XE0	
<b>Attachment to Industrial Ethernet</b>		
Quantity	<ul style="list-style-type: none"> <li>• 1 x gigabit interface (X1)</li> <li>• 2x Fast Ethernet interface (X2, X3)</li> </ul>	
Design	RJ-45 jack, galvanically isolated	
Properties	Half duplex/full duplex, autocrossover, autonegotiation	
Standard / transmission speed	Gigabit interface (X1)	Fast Ethernet interfaces (X2 / X3)
<ul style="list-style-type: none"> <li>• Standard</li> <li>• Transmission speeds</li> </ul>	<ul style="list-style-type: none"> <li>• 1000BASE-T, IEEE 802.3ab</li> <li>• 10 / 100 / 1000 Mbps</li> </ul>	<ul style="list-style-type: none"> <li>• 100BASE-TX, IEEE 802.3-2005</li> <li>• 10 / 100 Mbps</li> </ul>
<b>Permitted cable lengths (Ethernet)</b>	<b>(Alternative combinations per length range) *</b>	
0 ... 55 m	<ul style="list-style-type: none"> <li>• Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180</li> <li>• Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet</li> </ul>	
0 ... 85 m	<ul style="list-style-type: none"> <li>• Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180</li> <li>• Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet</li> </ul>	
0 ... 100 m	<ul style="list-style-type: none"> <li>• Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180</li> <li>• Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet</li> </ul>	
<b>Serial interface for connection to the transmission device</b>		
Quantity	1 x serial interface (X4)	
Design	9-pin D-sub male connector, isolated	
Standards	RS-232 / RS-485 (can be changed in the configuration)	
Transmission speeds	300 .. 115 200 bps (depending on the connected modem)	
<b>Power supply</b>		
Design	Socket (X80) Terminal block for socket	Two terminals with reverse polarity protection  Two terminals with reverse polarity protection

## Technical specifications

### 7.1 Technical specifications

#### Technical specifications

Power supply	<ul style="list-style-type: none"><li>• Type of voltage</li><li>• Permitted low limit</li><li>• Permitted high limit</li></ul>	<ul style="list-style-type: none"><li>• 24 VDC</li><li>• 19.2 V</li><li>• 28.8 V</li></ul>
Cable cross-section connectable to the terminal block	<ul style="list-style-type: none"><li>• Without wire end ferrule</li><li>• With wire end ferrule</li><li>• With TWIN wire end ferrule</li></ul>	<ul style="list-style-type: none"><li>• 0.2 .. 2.5 mm<sup>2</sup> / AWG 24 .. 13</li><li>• 0.25 .. 1.5 mm<sup>2</sup> / AWG 24 .. 16</li><li>• 0.5 .. 1.0 mm<sup>2</sup> / AWG 20 .. 17</li></ul>

#### Further electrical data

Details for a TIM with all interfaces connected:

Current consumption (typical)	160 mA
Effective power loss (typical)	4 W
Overvoltage category according to IEC / EN 60664-1	Category I

#### Permitted ambient conditions

Ambient temperature	During operation with the rack installed horizontally	0 °C ... +70 °C
	During operation with the rack installed vertically	0 °C ... +50 °C
	During storage	-40 °C to +70 °C
	During transportation	-40 °C to +70 °C
Relative humidity	During operation	≤ 60 % at 25 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3	
	<ul style="list-style-type: none"><li>• SO<sub>2</sub></li><li>• H<sub>2</sub>S</li></ul>	<ul style="list-style-type: none"><li>• &lt; 0.5 ppm</li><li>• &lt; 0.1 ppm</li></ul>

#### Design, dimensions and weight

Module format	Compact module S7-1500
Degree of protection	IP20
Weight	525 g
Dimensions (W x H x D)	70 x 147 x 129 mm
Installation options	DIN rail for SIMATIC S7-1500 (article numbers 6ES7590-1Axx0-0AB0)

#### Product functions \*\*

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

\*\*You will find further characteristics and performance data in the section Application and functions (Page 11).



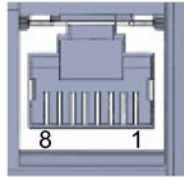
## 7.2 Pinout of the Ethernet interfaces

### Pinout of the Ethernet interfaces

The tables below show the pin assignment of the Ethernet interfaces.

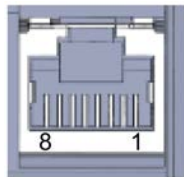
- X1

Gigabit interface

View of the RJ-45 jack	Pin	Signal name	Assignment
	1	D1+	D1+ bidirectional
	2	D1-	D1- bidirectional
	3	D2+	D2+ bidirectional
	4	D3+	D3+ bidirectional
	5	D3-	D3- bidirectional
	6	D2-	D2- bidirectional
	7	D4+	D4+ bidirectional
	8	D4-	D4- bidirectional

- X2 / X3

Fast Ethernet interfaces

View of an RJ-45 jack	Pin	Signal name	Assignment
	1	Tx+	Transmit Data +
	2	Tx-	Transmit Data -
	3	Rx+	Receive Data +
	4	-	
	5	-	
	6	Rx-	Receive Data -
	7	-	
	8	-	

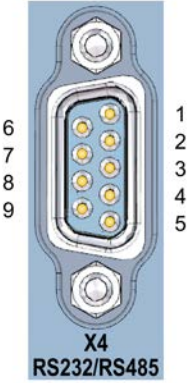
## 7.3 Pin assignment of the serial interface

### Pin assignment of the serial interface X4 (RS-232 / RS-485)

The table below shows the pin assignment of the 9-pin D-sub miniature plug of the serial interface. The interface corresponds to the connector assignment of a standardized PC connector.

7.3 Pin assignment of the serial interface

Table 7- 2 Pinout of the plug of the serial interface

Illustration	Pin no.	Signal name	Meaning / remarks	Signal direction
 <p>The illustration shows a blue plastic connector plug with nine pins. The pins are numbered 1 through 9 from top to bottom. Pin 5 is the ground pin. A shield is located at the bottom of the plug. The text 'X4 RS232/RS485' is printed on the bottom of the plug.</p>	1	DCD	Received signal level The DCE reports the input of data to be sent to the DTE (connection establishment). <sup>1, 2</sup>	Input
	2	RxD	Received data (DCE → DTE) Switchover to RS-485 by configuration <sup>3</sup>	Input
	3	TxD	Send data (DTE → DCE) Switchover to RS-485 by configuration <sup>3</sup>	Output
	4	DTR	DTE signals readiness to sent to DCE.	Output
	5	GND	Reference mass of the interface	
	6	DSR	DCE reports readiness for operation to DTE.	Input
	7	RTS	Turn on transmitter The DTE requests the DCE to send data on the data cable. The DTE waits for confirmation of the readiness to to send (CTS) of the DCE.	Output
	8	CTS	Ready to send The DCE can transfer the data coming from the DTE.	Input
	9	-	-	-
	Schirm	-	On connector housing	-
<p><sup>1</sup> DCE = data communication equipment (connected modem)  <sup>2</sup> DTE = data terminal equipment (TIM / CP)  <sup>3</sup> Fore the switchover RS-232 ↔ RS-485 see section .</p>				

# Approvals

## Approvals issued

---

### Note

#### Issued approvals on the type plate of the device

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

---

## Scope of validity of the approvals

The approvals listed below are only valid for the TIM module.

The products of the accessories program have their own approvals, that are not listed here.

## EC declaration of conformity



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

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

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

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

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

The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft  
 Division Process Industries and Drives  
 Process Automation  
 DE-76181 Karlsruhe  
 Germany

You will find the EC Declaration of Conformity on the Internet at the following address:

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

> Certificate type: "EC declaration of conformity"

## EMC

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

Applied standards:

- EN 61000-6-4

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

- EN 61000-6-2

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

## RoHS

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

Applied standard:

- EN 50581:2012

## c(UL)us



Applied standards:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Certificate Number: 20130830-E85972

## Australia - RCM



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

## Marking for the customs union



EAC (Eurasian Conformity)

Customs union of Russia, Belarus and Kazakhstan

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

**MSIP 요구사항 - For Korea only**

Registration Number: MSIP REI S7M

**A급 기기(업무용 방송통신기자재)**

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

**Current approvals**

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

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

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



# Dimension drawings

# A

All dimensions in the dimension drawings are in millimeters.

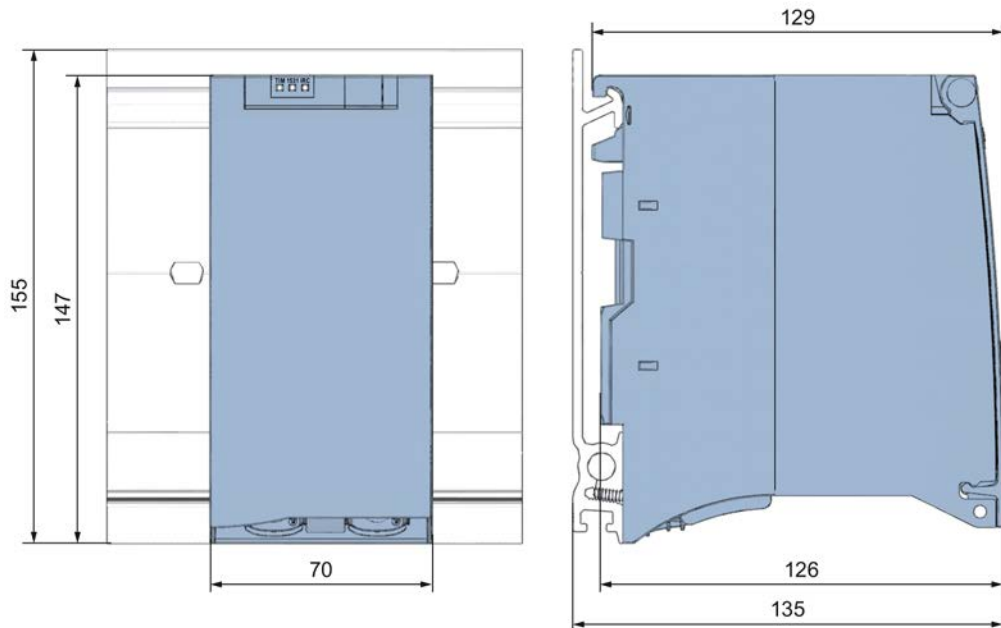


Figure A-1 TIM 1531 IRC: Front view and side view

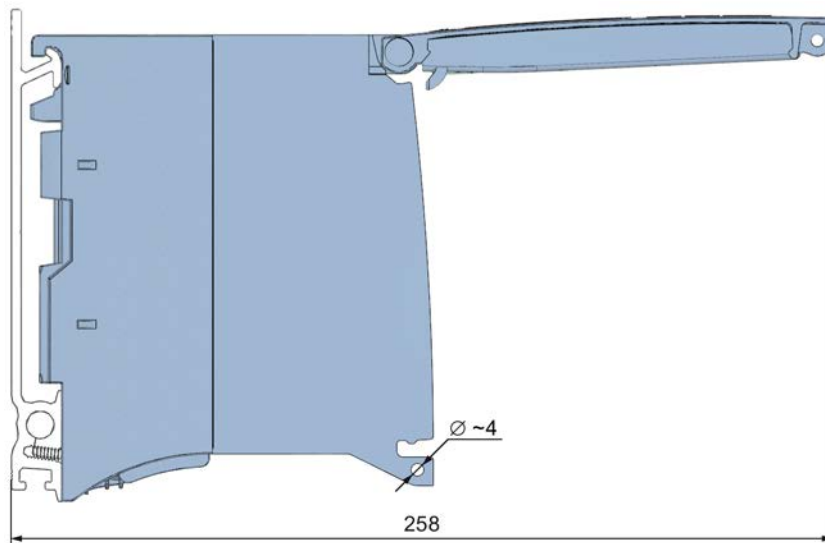


Figure A-2 TIM 1531 IRC: Side view with cover open





## Accessories

### B.1 Power supply

#### Power supplies for the TIM

Excerpt from the Siemens program for power supplies SITOP and S7-1500:

- SITOP PSU100C  
24 V / 0.6 A stabilized power supply, input: AC 120/230 V, output: DC 24 V / 0.6 A  
Article number: 6EP1331-5BA00
- SITOP PSU100L  
24 V / 2.5 A stabilized power supply, input: AC 120/230 V, output: DC 24 V / 2.5 A  
Article number: 6EP1332-1LB00
- SIMATIC PM 1507  
24 V / 3 A stabilized power supply for SIMATIC S7-1500, input: AC 120/230 V, output:  
DC 24 V / 3 A  
Article number: 6EP1332-4BA00

### B.2 SD cards

#### Compatible SD cards

To store configuration data and firmware files you have the option of using an SD card. To achieve the number of frames named in the section Performance data and configuration limits (Page 23), the card should have a minimum size of 24 MB.

---

#### Note

##### Temperature range of the SD card

When using an SD card, make sure that this is suitable for the industrial temperature range from -40 ... +85 °C.

---

The following card formats can be used:

- Size: 24 x 32 mm
- Standard and capacity:
  - SDSC (SD 1.0 / SD 1.1)  
24 MB ... 2 GB
  - SDHC  
4 ... 32 GB
- Speed classes: Class 0, 2, 4, 6, 10
- File system: FAT32

You will find information on using the SD card in the section SD card slot (Page 33).

### **SIMATIC S7 - Memory Card (SMC)**

The SMC is available with various capacities. The recommended memory capacity is in the range between 24 MB and 32 GB. SMCs up to 32 GB memory capacity are supported.

Article numbers: 6ES7954-8Lx02-0AA0

x is a placeholder for: F / L / P / T

You will find the cards on the pages of the Siemens Industry Mall using the search term "6ES7954".

## B.3 Routers, modems, antennas

### B.3.1 Dedicated line and dialup network modems

#### Modems for dedicated line and dialup networks

---

**Note****Discontinuation of modules**

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

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

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

### B.3.2 MODEM MD720

#### MODEM MD720

Article number: 6NH9720-3AA01-0XX0



Use in SIMATIC S7 stations that are part of a telecontrol or remote maintenance system and for communication with other stations in the network or an OPC server in the master station.

The MD720 supports the following types of communication:

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

#### Technical specifications (excerpt)

Connection to Industrial Ethernet		
X1 interface	Number:	1
	Implementation:	D-sub 9-pin, female
	Characteristics:	RS-232 Control using AT commands
	Transmission speed:	19200 bps Permitted range: 300 ... 57600 bps
Wireless interface		
Antenna connector	Number:	1
	Implementation:	SMA socket
	Impedance:	50 Ω nominal
Frequency bands	GPRS / CSD:	Quad band: 850, 900, 1800, 1900 MHz

GPRS	Characteristics:	Maximum of 5 time slots at the same time, of which: <ul style="list-style-type: none"> <li>• Up to 2 uplinks</li> <li>• Up to 4 downlinks</li> </ul>
	Transmission speed <ul style="list-style-type: none"> <li>• Uplink (modem → Internet)</li> <li>• Downlink (Internet → modem)</li> </ul>	Gross values: <ul style="list-style-type: none"> <li>• Max. 42 kbps</li> <li>• Max. 54 kbps</li> </ul> The net values (user data) are approximately 30% lower.
CSD	Characteristics:	MTC (Mobile Terminated Call)
	Transmission speed:	9600 bps
SMS (TX)	Characteristics:	Text mode

### B.3.3 Router SCALANCE M

#### Routers for IP-based communication

To connect a TIM to IP-based infrastructure networks, the following routers are available:

- SCALANCE M812

ADSL router for wired IP communication via the Internet, VPN, firewall, NAT, 1 RJ-45 Ethernet interface, 1 digital input, 1 digital output, ADSL2T or ADSL2+

  - ADSL2T (analog phone connection - Annex A)  
Article number: 6GK5812-1AA00-2AA2
  - ADSL2+ (ISDN connection - Annex B)  
Article number: 6GK5812-1BA00-2AA2
- SCALANCE M816

ADSL router for wired IP communication via the Internet, VPN, firewall, NAT, 1 RJ-45 Ethernet interface with 4-port switch, 1 digital input, 1 digital output, ADSL2T or ADSL2+

  - ADSL2T (analog phone connection - Annex A)  
Article number: 6GK5816-1AA00-2AA2
  - ADSL2+ (ISDN connection - Annex B)  
Article number: 6GK5816-1BA00-2AA2
- SCALANCE M826-2

SHDSL router for IP communication via 2- and 4-wire cables, ITU-T standard G.991.2 / SHDSL.biz, SHDSL topology: Point-to point, bonding, line bridge mode; routing mode with VPN, firewall, NAT, 1 Ethernet interface with 4-port switch, 1 digital input, 1 digital output  
Article number 6GK5826-2AB00-2AB2
- SCALANCE M874-2

2.5G router for wireless IP communication via 2.5G mobile wireless, VPN, firewall, NAT, 1 RJ-45 Ethernet interface with 2-port switch, SMA antenna connector, 1 digital input, 1

digital output

Article number: 6GK5874-2AA00-2AA2

- SCALANCE M874-3

3G router for wireless IP communication via 3G mobile wireless, VPN, firewall, NAT, 1 RJ-45 Ethernet interface with 2-port switch, SMA antenna connector, 1 digital input, 1 digital output

Article number: 6GK5874-3AA00-2AA2

- SCALANCE M876-3

3G router for wireless IP communication via 3G mobile wireless HSPA+/EV-DO, VPN, firewall, NAT, 1 RJ-45 Ethernet interface with 4-port switch, SMA antenna connector, antenna diversity, 1 digital input, 1 digital output

Note network provider approvals!

- International version

Article number: 6GK5876-3AA02-2BA2

- Version for Korea

Article number: 6GK5876-3AA02-2EA2

- SCALANCE M876-4

4G router for wireless IP communication via LTE mobile wireless, VPN, firewall, NAT, 1 RJ-45 Ethernet interface with 4-port switch, 2 SMA antenna connectors, MIMO technology, 1 digital input, 1 digital output

- Version for Europe

Article number: 6GK5876-4AA00-2BA2

- Version for North America

Article number: 6GK5876-4AA00-2DA2

Information on the devices can be found on the Internet pages of Siemens Industry Online Support:

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

## B.3.4 Mobile wireless antennas

### GSM/GPRS antennas

The following antennas are available for use in GSM/GPRS networks and can be installed both indoors and outdoors. The antennas must be ordered separately.

#### Quadband antenna ANT794-4MR

You will find detailed information in the device manual. You will find this on the Internet on the pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/23119005>)



Figure B-1 ANT794-4MR GSM/GPRS antenna

Short name	Article number	Explanation
ANT794-4MR	6NH9 860-1AA00	Quadband antenna (900, 1800/1900 MHz, UMTS); weatherproof for indoor and outdoor areas; 5 m connecting cable connected permanently to the antenna; SMA connector, including installation bracket, screws, wall plugs

**Flat antenna ANT794-3M**

Figure B-2 Flat antenna ANT794-3M

Short name	Article number	Explanation
ANT794-3M	6NH9 870-1AA00	Flat antenna (900, 1800/1900 MHz); weatherproof for indoor and outdoor areas; 1.2 m connecting cable connected permanently to the antenna; SMA connector, including adhesive pad, screws mounting possible

You will find detailed information in the device manual. You will find this on the Internet on the pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/48729835>)

## B.4 Cables, connecting cables

### B.4.1 Connecting cables for connecting modems

#### Standard connecting cables (RS-232)

The following connecting cables do not ship with the TIM.

Table B- 1 Standard connecting cables for connecting TIM and modem

Article number	Description	Illustration
6NH7701-4AL	<p>Connecting cable for connecting the serial interface of the TIM (RS-232) with a modem</p> <p>D-sub male connector</p> <p>Cable length 1.5 m</p> <p>Suitable for the connection of the following modems:</p> <ul style="list-style-type: none"> <li>• Modem for a dedicated line (MD2)</li> <li>• Modem for analog dialup network (MD3)</li> <li>• Modem for analog dialup network (MD4)</li> <li>• GSM mobile wireless modem MODEM MD720</li> </ul> <p>(can be used for MD720 with the supplied gender changer)</p>	
6NH7701-5AN	<p>Connecting cable for connecting the serial interface of the TIM (RS-232) with a GSM mobile wireless modem</p> <p>1 D-sub male connector, 1 D-sub female connector</p> <p>Cable length 2.5 m</p> <p>Suitable for the connection of the following modems:</p> <ul style="list-style-type: none"> <li>• GSM mobile wireless modem MODEM MD720</li> </ul> <p>(can be used without gender changer)</p> <ul style="list-style-type: none"> <li>• Third-party modems with RS-232 connector</li> <li>• Wireless devices with RS-232 connector</li> </ul>	
6NH7701-4BN	<p>Connecting cable open at one end for connecting the serial interface of the TIM (RS-232) with a third-party modem</p> <p>Cable length 2.5 m</p>	
6NH7701-0AR	<p>Test cable</p> <p>Crossover connecting cable for connection of two TIM modules via their RS-232 interface</p> <p>(without connecting a null modem in between)</p> <p>Cable length 6 m</p>	



Plug pin assignment of the standard connecting cables

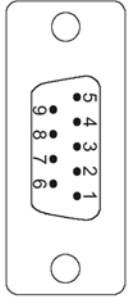
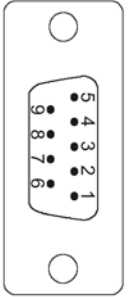
TIM (RS-232)	Pin	Interconnection	Pin	Modem (RS-232)
 <p>D-sub female connector 9-pin</p>	Housing shield		Housing shield	 <p>D-sub female connector 9-pin</p>
	1	DCD	1	
	2	RxD	2	
	3	TxD	3	
	4	DTR	4	
	5	GND	5	
	6	DSR	6	
	7	RTS	7	
	8	CTS	8	
9	RI	9		

Figure B-3 6NH7701-4AL

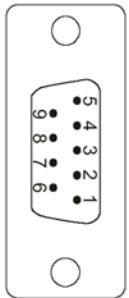
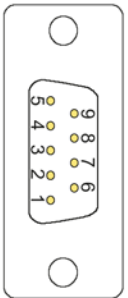
TIM (RS-232)	Pin	Interconnection	Pin	Modem (RS-232)
 <p>D-sub female connector 9-pin</p>	Housing shield		Housing shield	 <p>D-sub male connector 9-pin</p>
	1	DCD	1	
	2	RxD	2	
	3	TxD	3	
	4	DTR	4	
	5	GND	5	
	6	DSR	6	
	7	RTS	7	
	8	CTS	8	
9	RI	9		

Figure B-4 6NH7701-5AN

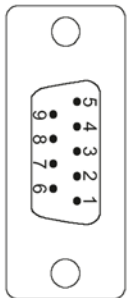
TIM (RS-232)	Pin	Interconnection	Pin	Color code (wires)
 <p>D-sub female connector 9-pin</p>	Housing shield		Housing shield	
	1	DCD	1	white
	2	RxD	2	brown
	3	TxD	3	green
	4	DTR	4	yellow
	5	GND	5	gray
	6	DSR	6	pink
	7	RTS	7	blue
	8	CTS	8	red
9	RI	9	black	

Figure B-5 6NH7701-4BN

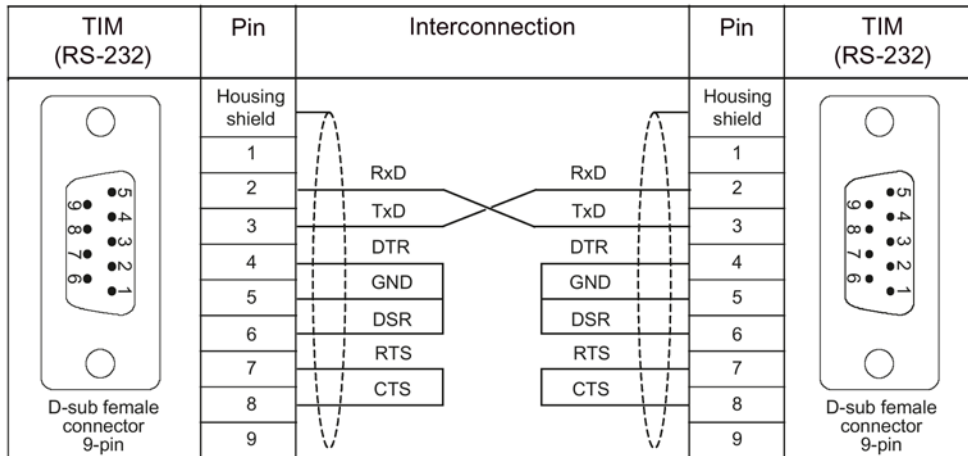


Figure B-6 6NH7701-0AR

### B.4.2 Cable for RS-485 connection

#### Accessories for RS-485 operation of the serial interface

Excerpt from the Siemens accessories program PROFIBUS or RS-485 operation

- **Cable**

- PROFIBUS FC standard cable GP, bus cable 2-wire, shielded, special design for fast installation, sold by the meter

02YSY (ST) CY, 1x2x0.64 / 2.55-150 VI KF 40 FR

Article number: 6XV1830-0EH10

- **Terminating resistor**

In a network in RS-485 operation the terminating resistor of the bus cable is turned on or off by the STEP 7 configuration.

The connecting cable for the serial interface in RS-485 operation must be assigned as follows:

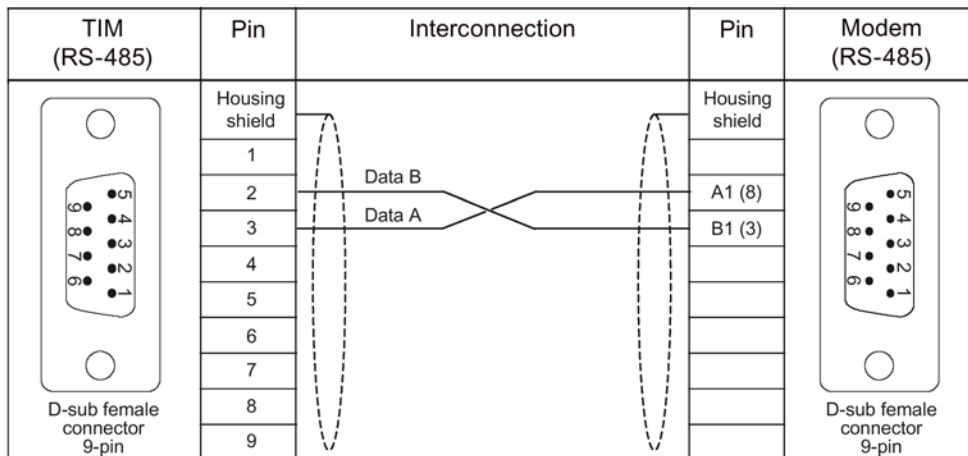


Figure B-7 Assignment of the cable for the RS-485 interface

# Documentation references

## Where to find Siemens documentation

- Article numbers

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

- SIMATIC NET - Industrial Communication / Industrial Identification, catalog IK PI
- SIMATIC - Products for Totally Integrated Automation and Micro Automation, catalog ST 70

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

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

- Manuals on the Internet

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

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

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

Entry type "Manuals"

- Manuals on the data medium

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

/1/

SIMATIC NET  
TIM 1531 IRC  
Operating instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/24710/man>)

**/2/**

SIMATIC  
S7-1500/ET 200MP Manual Collection  
Reference work  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/view/86140384>)

**/3/**

SIMATIC NET  
SCALANCE M812, M816  
Operating Instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15984>)

**/4/**

SIMATIC NET  
Mobilfunkrouter SCALANCE M870  
(M873 / M874 / M875 / M876)  
Operating Instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15987/man>)

**/5/**

SIMATIC NET  
MODEM MD720  
Operating Instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15923/man>)

**/6/**

SIMATIC NET  
MODEM MD2  
Operating Instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/view/17163799>)

**/7/**

SIMATIC NET  
MODEM MD3  
Operating Instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/view/17164329>)

**/8/**

SIMATIC NET  
MODEM MD4  
Operating Instructions  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/view/17165032>)

**/9/**

SIMATIC NET  
Industrial Ethernet Security  
Security basics and applications  
Configuration manual  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15326/man>)

**/10/**

SIMATIC NET  
Industrial Ethernet Security  
SCALANCE S  
Commissioning and Installation Manual  
Siemens AG  
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15327/man>)

**/11/**

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



# Index

## A

Abbreviations/acronyms, 4  
Article number, 3  
Authentication, 15

## C

Classic WAN, 53  
    Creating a network, 44  
Conditional spontaneous, 101, 104  
Connection resources, 23  
Connection status - diagnostics, 132  
Cross references (PDF), 4

## D

Data buffering, 24  
Data point configuration, 90  
Device replacement, 141  
Diagnostics messages, 122  
Direct communication, 13  
Disposal, 6  
Downloading - configuration data, 39

## E

E-mail, 13  
    Configuration, 114  
    Number of messages, 24  
Encryption, 15  
ES - engineering station, 18

## F

Firewall, 16  
Firmware  
    Version, 3  
Forced image mode, 100

## G

General request supervision time, 71  
GET, 14, 14

Glossary, 6  
Grounding, 37

## H

Hardware product version, 3

## I

Image memory, 99  
Importing a certificate - e-mail, 83  
Inter-station communication, 13, 20  
IP configuration, 17  
IPsec, 17

## M

MAC address, 3  
Main path, 46  
Master station types, 11  
Message memory, 24  
MIB, 133  
Mirroring, 99  
MSC, 15  
MSCsec, 15

## N

NTP (secure), 78

## O

Online diagnostics, 131  
Online functions, 18

## P

Partner status - diagnostics, 132  
Path redundancy, 46

## R

READ, 14  
Recycling, 6  
Redundant telecontrol connection, 46

Redundant telecontrol connections, 69  
Replacement situation, 141  
RS-485, 38

## S

Safety notices, 35  
Saving messages, 17  
SD card, 24, 48  
Security  
    Protocols, 15  
Security functions, 44  
Send buffer, 24, 100  
Service & Support, 5  
SIMATIC NET glossary, 6  
SIMATIC PCS 7, 11  
SINAUT ST7cc, 11  
SINAUT system, 12  
SMS, 13  
    Number of messages, 24  
SMTPS, 82  
SNMP, 18, 133  
SNMPv3, 15, 83  
SSL/TLS, 82  
ST7sc, 11  
STARTTLS, 82  
Station address, 47  
STEP 7 - version, 25  
Subscriber number, 47  
Substitute path, 46

## T

Terminating resistor, 38  
Time stamp, 18, 71, 71  
Time-of-day synchronization, 18  
Training, 5  
Transmission mode, 104  
Trigger tag - resetting, 103

## U

Unsolicited, 101, 104

## V

VPN, 17

## W

WAN - creating a network, 52  
WAN address, 47  
WAN network  
    creating, 44  
WinCC TC, 11  
WRITE, 14