SIEMENS

SIMATIC NET

# Industrial Remote Communication Remote Networks SCALANCE MUM853-1

Operating Instructions


Introduction 1

Safety notices 2

Security recommendations 3

Description of the device 4

Installation and removal 5

Connection 6

Troubleshooting 7

Maintenance and cleaning 8

Technical specifications 9

Dimension drawings 10

Approvals 11



10/2024
C79000-G8976-C650-10

## Legal information

### Warning notice system

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

**⚠ DANGER**

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

**⚠ WARNING**

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

**⚠ CAUTION**

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

**NOTICE**

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

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

### Qualified Personnel

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

### Proper use of Siemens products

Note the following:

**⚠ WARNING**

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

### Trademarks

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

### Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: C79000-G8976-C650
Ⓟ 12/2024 Subject to change

Copyright © Siemens 2022 - 2024.
All rights reserved

# Table of contents


**1 Introduction ..... 7**

1.1 Purpose of the operating instructions ..... 7

1.2 Scope of validity ..... 7

1.3 QR code ..... 7

1.4 Supplementary documentation ..... 8

1.5 Service & Support ..... 9

1.6 Training ..... 10

1.7 Cybersecurity information ..... 10

1.8 Firmware ..... 11

1.9 Error/fault ..... 11

1.10 Decommissioning ..... 11

1.11 Recycling and disposal ..... 11

1.12 Open source license conditions ..... 12

1.13 SIMATIC NET glossary ..... 12

1.14 Trademarks ..... 12

**2 Safety notices ..... 13**

**3 Security recommendations ..... 15**

3.1 Security recommendations ..... 15

3.2 Available services ..... 20

**4 Description of the device ..... 25**

4.1 Structure of the type designation ..... 25

4.2 Product characteristics ..... 25

4.3 Device view ..... 26

4.4 Components of the product ..... 27

4.5 Antennas and accessories ..... 28

4.5.1 Installation ..... 28

4.5.2 CLP ..... 28

4.5.3 Industrial Ethernet ..... 28

4.5.4 Antennas and antenna accessories ..... 29

4.6 Terminals ..... 31

4.7 LED display ..... 32

4.8 Reset button ..... 35

4.9 Configuration License PLUG ... 36

**5 Installation and removal ... 39**

5.1 Safety when mounting ... 39

5.2 Types of installation ... 42

5.3 Wall mounting ... 43

5.4 Installing on the DIN rail ... 45
5.4.1 Mounting directly on the DIN rail ... 45
5.4.2 Mounting rotated by 90° with DIN rail mounting adapter ... 47

5.5 Installing on an S7-300 mounting rail ... 50

5.6 Installing on an S7-1500 mounting rail ... 51

**6 Connection ... 53**

6.1 Safety when connecting ... 53

6.2 Power supply ... 58

6.3 Ethernet ... 59

6.4 Antennas ... 61

6.5 SIM card ... 64

6.6 Grounding ... 67

6.7 Digital input/output ... 68

6.8 Replacing a CLP ... 71

**7 Troubleshooting ... 73**

7.1 Downloading new firmware using TFTP without WBM and CLI ... 73

7.2 Restoring the factory settings ... 74

**8 Maintenance and cleaning ... 77**

**9 Technical specifications ... 79**

**10 Dimension drawings ... 85**

**11 Approvals ... 87**

11.1 EC declaration of conformity ... 88
11.1.1 RoHS ... 89
11.1.2 RED ... 89
11.1.2.1 Protection of health and safety ... 89
11.1.2.2 EMC ... 89
11.1.2.3 Efficient use of the radio spectrum ... 90
11.1.3 Other technical standards ... 90

11.2 UK Declaration of Conformity ... 91
11.2.1 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 ... 91
11.2.2 The Radio Equipment Regulations 2017 ... 92
11.2.2.1 Protection of health and safety ... 92
11.2.2.2 EMC ... 92

11.2.2.3 Efficient use of the radio spectrum ..... 93
11.2.3 Other technical standards ..... 93
11.3 Supplier's declaration of conformity ..... 93
11.4 General approvals ..... 94
11.5 Country-specific notes ..... 96
11.5.1 Note for Australia and New Zealand ..... 96
11.5.2 Note for Brazil ..... 97
11.5.3 Notes for Mexico ..... 97
11.5.4 Notes for the United States (FCC approval) ..... 97
**Index ..... 99**

# 1 Introduction

## 1.1 Purpose of the operating instructions

Based on the operating instructions, you will be able to install and connect the SCALANCE device correctly. The instructions are aimed primarily at planning, commissioning, maintenance and service personnel.

The configuration and the integration of the device in a network are not described in these instructions.

## 1.2 Scope of validity

These operating instructions cover the following products:

| Product | Article numbers | Model |
|---|---|---|
| SCALANCE MUM853-1 | 6GK5853-2EA00-2DA1 | MS5G15R-30-M1-RJ-E4-1 |
| | 6GK5853-2EA10-2AA1 (A1) | MS5G16R-30-M1-RJ-E4-1 |
| | 6GK5853-2EA10-2BA1 (B1) | MS5G16R-30-M1-RJ-E4-2 |

These operating instructions apply to the following firmware version:

- SCALANCE M-800/S615 as of version V8.2

You will find the article numbers for the Siemens products of relevance here in the following catalogs:

- Industry Mall - catalog and ordering system for automation and drive technology, Online catalog (https://mall.industry.siemens.com)

You can request the catalogs and additional information from your Siemens representative.

## 1.3 QR code

### Identification Link

There are multiple scannable codes, including a QR code, on the product. The QR code is an Identification Link (ID-Link), a globally unique product identifier according to IEC 61406-1. You can recognize the ID-Link from the frame, which has a black corner at the bottom right.

Disconnect the device from the power and scan the QR code with a smartphone camera, a bar code scanner or a read app. Open the ID-Link. The Siemens web page corresponding to the product opens with the digital nameplate.

In the digital nameplate, you will find product data, manuals, declarations of conformity, certificates, and other helpful information about your product.

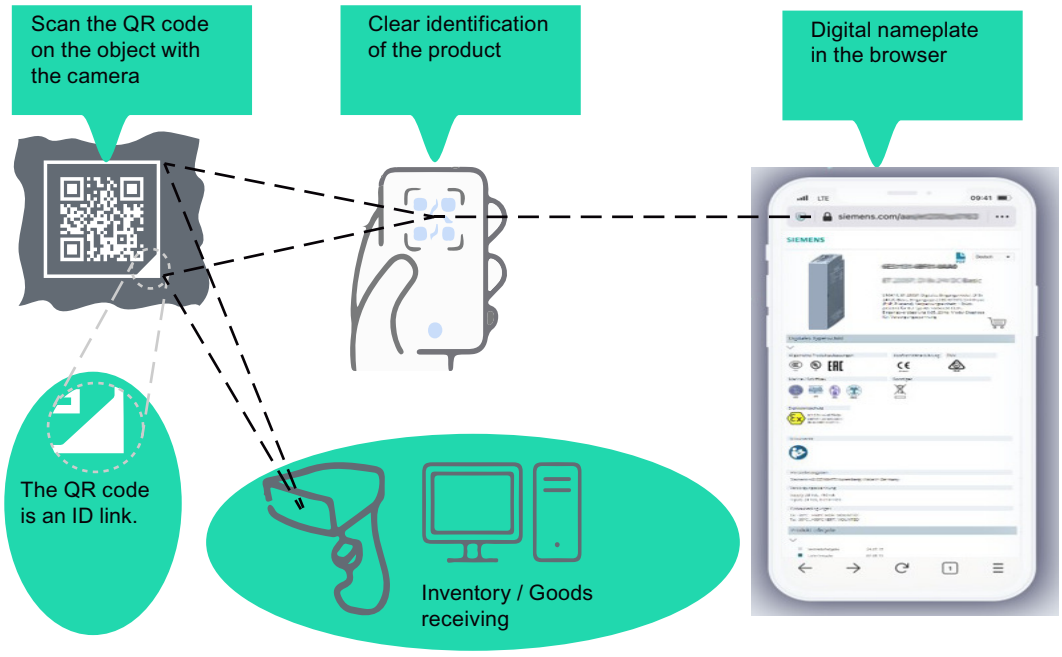



Figure 1-1 Application & functions of the Identification Link

## 1.4 Supplementary documentation

### Documentation on the Internet

You can find the current version of the document on the Internet at. (https://support.industry.siemens.com/cs/ww/en/ps/15982/man)

Enter the name or article number of the product in the search filter.

### Documentation on configuration

You will find detailed information on configuring the devices in the following configuration manuals:

- SCALANCE M-800 Web Based Management
- SCALANCE M-800 Command Line Interface

### Further documentation

- System manual "Industrial Ethernet"
  The system manual contains information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network. There, you will find among other things optical performance data of the communications partner that you require for the installation.
  The "SIMATIC NET Industrial Ethernet" system manual can be found on the Internet pages of Siemens Industry Online Support under the following entry ID: 27069465 (https://support.industry.siemens.com/cs/ww/en/view/27069465)
- "Passive network components" system manual
  This system manual contains installation instructions for several of the most common components and guidelines for setting up networked automation plants in buildings.
  The "Passive network components" system manual can be found on the Internet pages of Siemens Industry Online Support under the following entry ID: 84922825 (https://support.industry.siemens.com/cs/ww/en/view/84922825)

### SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- using the search function:
  Link to Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/)
  Enter the entry ID of the relevant manual as the search item.
- In the navigation panel on the left hand side in the area "Industrial Communication":
  Link to the area "Industrial Communication" (https://support.industry.siemens.com/cs/ww/en/ps/15982/man)
  Go to the required product group and make the following settings:
  tab "Entry list", Entry type "Manuals"

## 1.5 Service & Support

### Industry Online Support

In addition to the product documentation, you are supported by the comprehensive online information platform of Siemens Industry Online Support at the following Internet address:
Link: (https://support.industry.siemens.com/cs/de/en/)

Apart from news, there you will also find:

- Project information: Manuals, FAQs, downloads, application examples etc.
- Contacts, Technical Forum
- The option submitting a support query:
  Link: (https://support.industry.siemens.com/cs/my?lc=en-WW)
- Our service offer:
  Right across our products and systems, we provide numerous services that support you in every phase of the life of your machine or system - from planning and implementation to commissioning, through to maintenance and modernization.

You will find contact data on the Internet at the following address:
Link: (https://www.automation.siemens.com/aspa_app/?ci=yes&lang=en)

## 1.6 Training

### SITRAIN - Training for Industry

The training offer includes more than 300 courses on basic topics, extended knowledge and special knowledge as well as advanced training for individual sectors - available at more than 130 locations. Courses can also be organized individually and held locally at your location.

You will find detailed information on the training curriculum and how to contact our customer consultants at the following Internet address:

Link: (https://new.siemens.com/global/en/products/services/industry/sitrain/personal.html)

### Industrial Networks Education

Training and certification for Industrial Networks

In our Industrial Networks Education courses you'll learn to design and implement wired and wireless data networks and connect them to a corporate network. You will also receive instruction on how to secure, diagnose and optimize communication networks. Certification can also be offered to supplement almost all training courses.

Link: (https://www.siemens.com/industrial-networks-education)

## 1.7 Cybersecurity information

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

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

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

For additional information on industrial cybersecurity measures that may be implemented, please visit
https://www.siemens.com/cybersecurity-industry (https://www.siemens.com/cybersecurity-industry).

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no

longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

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

## 1.8 Firmware

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/en/ps/28821/dl)

### Note on firmware/software support

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

## 1.9 Error/fault

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

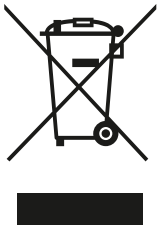
## 1.10 Decommissioning

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

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

Also restore the factory settings on the storage medium.

## 1.11 Recycling and disposal



The products are low in pollutants, can be recycled and meet the requirements of the WEEE directive 2012/19/EU for the disposal of electrical and electronic equipment.

Do not dispose of the products 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 (Product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Note the different national regulations.

## 1.12 Open source license conditions

**Note**

**Open source software**

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

The license terms and copyright information can be downloaded from the WBM or CLI as a zip file.

- WBM: System > Load&Save > HTTP / TFTP / SFTP > LicenseCondition
- CLI: `sftp save filetype LicenseConditions / tftp save filetype LicenseConditions`

## 1.13 SIMATIC NET glossary

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

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

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

## 1.14 Trademarks

The following and possibly other names not identified by the registered trademark sign ® are registered trademarks of Siemens AG:

- SCALANCE
- SINEMA
- SINEC

# Safety notices

# 2

**CAUTION**

To prevent injury and damage, read the manual before using the device.

## Read the safety notices

Note the following safety notices. These relate to the entire working life of the device.

You should also read the safety notices relating to handling in the individual sections, particularly in the sections "Installation" and "Connecting up".



**WARNING**

**Hot surfaces**

Electric devices have hot surfaces. Do not touch these surfaces. They could cause severe burns.

- Allow the device to cool down before starting any work on it.

**WARNING**

**EXPLOSION HAZARD**

Do not open the device when the supply voltage is turned on.

# Security recommendations

# 3

## 3.1 Security recommendations

To prevent unauthorized access to the device and/or network, observe the following security recommendations.

**Note**

Note that GNSS signals can be obfuscated or blocked by malicious third-party devices.

### General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products. For more information, refer to:
  Link: (https://www.siemens.com/industrialsecurity)
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. If possible, operate the device only within a protected network area.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

### Authentication

**Note**

**Accessibility risk - Risk of data loss**

Do not lose the passwords for the device. Access to the device can only be restored by resetting the device to factory settings which completely removes all configuration data.

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device. Create a separate user account for each user that will receive access to the device.
- Define rules for the assignment of passwords.

- Use passwords with a high password strength. Avoid weak passwords, (e.g. Passwort1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the user account details in a safe location to have them available if they are lost. You can use password managers or encrypted files/drives for this purpose.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel. Use a RADIUS connection with changing passwords, expiry time, etc.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.
- Use TOTP-based two-factor authentication of the user. You can find more information on this under "Security > Passwords > Two-Factor Authentication".

### Certificates and keys

- There is a pre-installed Web server certificate and an SSH Private Key in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate in the WBM via "System > Load & Save".
- Use the certification authority including key revocation and management to sign the certificates.
- Use password-protected certificates in the format "PKCS #12".
- Use certificates with a key length of 4096 bits.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- SSH and SSL keys are available for admin users. Make sure that you take appropriate security measures when shipping the device outside of the trusted environment:
  - Reset the device to the factory settings. Replace the SSH and SSL keys with disposable keys prior to shipping to Siemens.
  - Decommission the existing SSH and SSL keys. Create and program new keys when the device is returned.

- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, reset it to factory settings and replace the current certificates and keys with temporary throwaway certificates and keys that can be destroyed when the device is returned.

### Physical/remote access

- If possible, operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention".
- If possible, use the VPN functionality to encrypt and authenticate communication for communication via non-secure networks.
- When you establish a secure connection to a server (for example for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 11)".
- We recommend formatting a PLUG that is not being used.

### Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device using firewall rules.
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
  For more information on available services, see "List of available services (Page 20)".
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).

- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products at the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert/en/cert-security-advisories.htm) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.
- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur.
    For more information, see WBM "System > SNMP > Notifications".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access.
- The names of the configuration files can be changed. To improve security, do not use spaces in the TFTP file name.

### Secure/non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, RSTP, etc.).
  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.

- Check whether use of the following protocols is necessary:
  - Telnet
  - HTTP
  - Broadcast pings
  - Non authenticated and unencrypted interfaces
  - ICMP (redirect)
  - LLDP
  - DHCP Options 66/67
  - SNTP
  - NTP
  - TFTP
  - TIA Portal Cloud Connector (not available with SCALANCE MUx85x)
  - VRRPv3
  - DNS
  - SNMPv1/V2c
- If a secure alternative is available for a protocol, use it.
  The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3
    Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options. If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
  - HTTP → HTTPS
  - Telnet → SSH
  - NTP → Secure NTP
  - TFTP → SFTP
  - TIA Portal Cloud Connector using a secure connection (not available with SCALANCE MUx85x). Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
    Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector" to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server").
  - DNS > DNSSec
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- Select a trusted DNS provider.
  Enable the DNSSec option on the WBM page "System > DNS client" or with the CLI command `dnssec`.

- SCALANCE MUM85x, SCALANCE M87x and RUGGEDCOM RM1224:
  For command SMS, use the identifier to secure your SMS messages. You can set a configurable value for a SCALANCE M device that, in addition to the phone number, must match the received identifier of the SMS. You configure the identifier on the WBM page "System > SMS > SMS Command" or with the CLI commands `sms-cmd idx identifier` and `sms-cmd sender`.
- The TCP Diagnostics Stream is considered non-secure without encryption. As of V8.1, encryption that enables secure use in productive operation is supported. Enable encryption of the function to use it securely.
- Only use the TCP Event function in secured networks or VPN. The firewall must be activated beforehand.
- With authentication on the RADIUS server and RADIUS client, use the Message Authenticator attribute to check packets.

## 3.2 Available services

### List of available services

The following is a list of all available protocols and services as well as their ports through which the device can be accessed.

The table includes the following columns:

- **Service**
  The services that the device supports.
- **Protocol / Port number**
  Port number assigned to the protocol.
- **Default port status**
  The port status on delivery (factory setting) distinguishes between local and external access.
  - Local access: The port is accessed via a local connection (vlan1).
  - External access: The port is accessed via an external connection (vlan2).
- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
  Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption can be configured.

| Service | Protocol/ Port number | Default port status | | Configurable | | Authentication | Encryption [2] |
|---|---|---|---|---|---|---|---|
| | | Local access | External access [1] | Port | Service | | |
| DHCPv4 Client | UDP/68 | Closed [3] | Closed | -- | ✓ | -- | -- |
| DHCPv6 Client | TCP/546<br>UDP/546 | Open | Open | -- | -- | -- | -- |
| DHCPv4-Server | UDP/67 | Closed | Closed [4] | -- | ✓ | -- | -- |
| DNS Client | TCP/53<br>UDP/53 | Outgoing only | Outgoing only | -- | ✓ | -- | -- |
| DNS Server | TCP/53<br>UDP/53<br>UDP/49000 ...<br>UDP/65535 | Open [5] | Closed | -- | ✓ | -- | -- |
| DynDNS | TCP/80<br>UDP/80<br>TCP/443<br>UDP/443 | Outgoing only | Outgoing only | -- | ✓ | ✓ | -- |
| HTTP | TCP/80 | Open | Closed | ✓ | ✓ | ✓ | -- |
| HTTP Proxy | TCP/3128<br>TCP/8080 | Outgoing only | Outgoing only | ✓ | ✓ | Optional | -- |
| HTTPS WBM Server/Client | TCP/443 | Open | Closed | ✓ | ✓ | ✓ | ✓ |
| IPsec/IKE | UDP/500<br>UDP/4500 | Closed | Closed | -- | ✓ | ✓ | ✓ |
| iperf3 [8] | TCP/5201 | Closed | Closed | ✓ | ✓ | -- | -- |
| NTP Client | UDP/123 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| NTP Client (secure) | UDP/123 | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | -- |
| NTP Server | UDP/123 | Closed | Closed | ✓ | ✓ | -- | -- |
| NTP Server (secure) | UDP/123 | Closed | Closed | ✓ | ✓ | ✓ | -- |
| OpenVPN [10] | UDP/1194<br>TCP/1194 | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | ✓ |
| Packet Capture [11] | TCP/2002 | Disabled | Disabled | ✓ | ✓ | -- | -- |
| Ping | ICMP | Open | Closed | -- | ✓ | -- | -- |
| RADIUS Client | UDP/1812 | Closed | Closed | ✓ | ✓ | ✓ | Optional |
| | UDP/1813 | | | | | | -- |
| SFTP Server | TCP/22 | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | ✓ |
| Siemens Remote Service (cRSP/SRS) [10] | TCP/443 | Outgoing only | Outgoing only | -- | ✓ | Optional | ✓ |
| SINEMA RC | HTTPS/443 and TCP/UDP depending on the server configuration | Outgoing only | Outgoing only | ✓ | ✓ | ✓ | ✓ |
| SMS Relay [7] | TCP/26864 | Closed | Closed | ✓ | ✓ | -- | -- |

| Service | Protocol/ Port number | Default port status | | Configurable | | Authentication | Encryption [2] |
|---|---|---|---|---|---|---|---|
| | | Local access | External access [1] | Port | Service | | |
| SMTP Client | TCP/25 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| SMTP (secure) | TCP/465<br>TCP/587 | Outgoing only | Outgoing only | ✓ | ✓ | Optional | ✓ |
| SNMPv1/v2c [12] | UDP/161 | Open | Closed | ✓ | ✓ | -- | -- |
| SNMPv3 Server | UDP/161 | Open | Closed | ✓ | ✓ | Optional | Optional |
| SNMP Trap | UDP/161 | Open | Closed | ✓ | ✓ | Optional | Optional |
| SNTP Client | UDP/123 | Closed | Closed | ✓ | ✓ | -- | -- |
| SSH CLI | TCP/22 | Open | Closed | ✓ | ✓ | ✓ | ✓ |
| Syslog Client | UDP/514 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| Syslog Client TLS | TCP/6514 | Outgoing only | Outgoing only | ✓ | ✓ | -- | ✓ |
| Telnet | TCP/23 | Closed | Closed | ✓ | ✓ | ✓ | -- |
| TFTP | UDP/69 | Outgoing only | Outgoing only | ✓ | ✓ | -- | -- |
| TIA Portal Cloud Connector [6] | TCP/9023 | Closed | Closed | ✓ | ✓ | -- | -- |
| TCP Diagnostic Stream [11] | TCP/5510<br>TCP/5511 | Closed | Closed | ✓ | ✓ | -- | ✓ |
| TCP Event | TCP/26864 | Closed | Closed | ✓ | ✓ | -- | -- |
| VXLAN [9] | UDP/4789 | Closed | Closed | ✓ | ✓ | -- | -- |

[1] With SCALANCE M826 and M804PB, only access via vlan1 is possible in the delivery state (factory setting).

[2] You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

[3] Only open with SCALANCE M826

[4] Only open with SCALANCE S615

[5] Only closed with SCALANCE S615

[6] Not available with SCALANCE MUx85x

[7] Only available with SCALANCE M87x, MUM85x and RUGGEDCOM RM1224

[8] Only available with SCALANCE MUM85x

[9] Only available with SCALANCE M87x, MUx85x, S615 and RUGGEDCOM RM1224

[10] Not available with SCALANCE MUB852

[11] Only available with SCALANCE MUx85x

[12] Read Only

The following is a list of all available Layer 2 services through which the device can be accessed.

The table includes the following columns:

- **Layer 2 service**
  The Layer 2 services that the device supports**.**
- **Default status**
  The default status of the service (open or closed).
- **Service configurable**
  Indicates whether the service can be configured via WBM / CLI.

| Layer 2 service | Default port status | Configurable |
|---|---|---|
| DCP | Open (when configured) | ✓ |
| LLDP | Open (when configured) | ✓ |
| SIMATIC NET TIME | Open (when configured) | ✓ |
| VLAN | Open (when configured) | ✓ |
| VXLAN [1)] | Open (when configured) | ✓ |

[1)] Only available with SCALANCE M87x, MUx85x, S615 and RUGGEDCOM RM1224

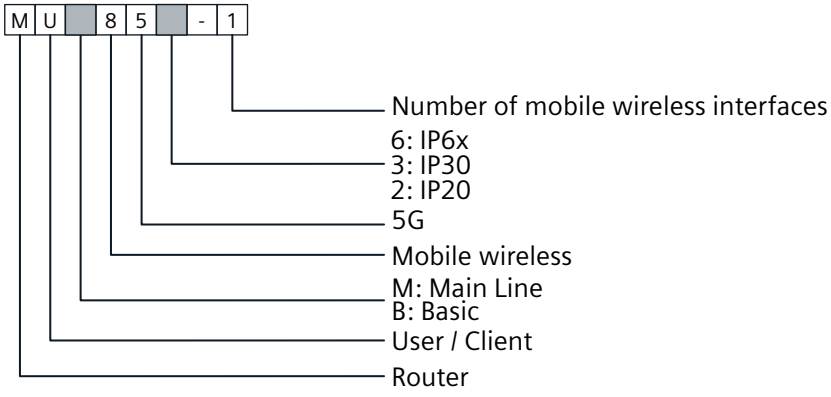
# Description of the device

4

## 4.1 Structure of the type designation

### Structure of the type designation

The type designation of the device is made up of several parts that have the following meaning:

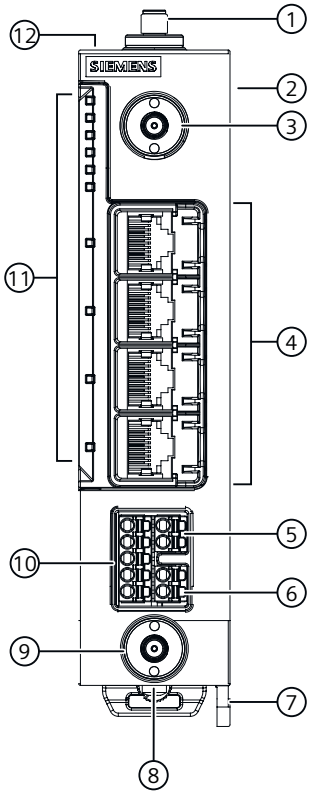



## 4.2 Product characteristics

### Interfaces

| **Functionality** | SCALANCE MUM853-1 |
|---|---|
| Connectors for external antennas | 4 x SMA connectors female |
| Ethernet interface | 4 x RJ45 connectors with 10/100/1000 Mbps |
| Power supply | Plug-in terminal block, 5-pin |
| Digital input | Plug-in terminal block, 2-pin |
| Digital output | Plug-in terminal block, 2-pin |

## 4.3 Device view




① 2 x antenna connectors A3/A4, type SMA female
② Slot for the micro SIM card 3FF on the device rear (covered)
③ Antenna connector A1, type SMA female
④ Ethernet connectors (P1, P2, P3, P4)
⑤ Digital input (DI)
⑥ Digital output (DO)
⑦ Eye for grounding (diameter 4.6 mm) / wall mounting
⑧ On the bottom of the device behind the screw-on cover:
- Reset button
- PLUG slot (CLP)

For the position, see "Reset button (Page 35)".
⑨ Antenna connector A2, type SMA female
⑩ Power supply connection
⑪ LED display
⑫ ID link on the top of the device
For more information, see "Identification Link (Page 7)".

## 4.4 Components of the product

The following components are supplied with the product:

- One SCALANCE MUM853-1
- One cover for CLP slot
- One 5-pin plug-in terminal block for the power supply
- One 2-pin plug-in terminal block for the digital input
- One 2-pin plug-in terminal block for the digital output
- An additional tray for the SIM card with M3 screw

Please check that the consignment you have received is complete. If the consignment is incomplete, contact your supplier or your local Siemens office.

**Note**

**Not included with the product**

The following components do not ship with the product:

- CLP
  You will find more detailed information in "CLP (Page 28)".
- Antennas and connecting cables
  You will find more detailed information in "Antennas and antenna accessories (Page 29)".
- Micro SIM card
  Use the SIM card from the chosen mobile wireless provider.

### Unpacking and checking

**WARNING**

**Do not use any parts that show evidence of damage**

If you use damaged parts, there is no guarantee that the device will function according to the specification.

If you use damaged parts, this can lead to the following problems:

- Injury to persons
- Loss of the approvals
- Violation of the EMC regulations

Use only undamaged parts.

1. Make sure that the package is complete.
2. Check all the parts for transport damage.

# 4.5 Antennas and accessories

Technical data subject to change.

You will find further information on the range of accessories in the Industry Mall (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10022025)

Use the TIA Selection Tool (https://mall.industry.siemens.com/tst/) for configuring the device.

## 4.5.1 Installation

| Component | Description | Article number |
|---|---|---|
| DIN rail mounting adapter | Adapter for mounting on a 35 mm DIN rail according to DIN EN 50 022, with fixing screws | 6GK5798-8MF00-0AA1 |

## 4.5.2 CLP

| Type | Properties | Article number |
|---|---|---|
| SCALANCE CLP 2GB SINEMA RC | Removable data storage medium for enabling connection to SINEMA Remote Connect for SCALANCE MUM85x, for simple device replacement in the event of a fault, and for storing configuration data | 6GK5908-0UA00-0AA0 |

## 4.5.3 Industrial Ethernet

You will find information on the cabling for communication networks in the industry on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/109766358).

### Cables Industrial Ethernet (pre-assembled)

| Component | Description | Article number |
|---|---|---|
| IE TP XP Cord RJ45/RJ45 | Industrial Ethernet TP XP Cord RJ45/RJ45, CAT 6A, crossed TP cable 4x2, pre-assembled with 2 x RJ45 plugs | 6XV1870-3R* |
| IE TP Cord RJ45/ RJ45 | Industrial Ethernet TP Cord RJ45/RJ45, CAT 6A, TP 4x2 cable, pre-assembled with 2 x RJ45 plugs | |
| | Green | 6XV1870-3Q* |
| | Blue | 6XV1870-4B* |
| | Yellow | 6XV1870-4G* |
| | Red | 6XV1870-4R* |
| | Gray | 6XV1870-4U* |
| IE TP Cord M12-90/RJ45-180 | Industrial Ethernet Flexible Cable, pre-assembled with 1 x M12 plug (X-coded) 90 degree cable outlet and 1 x RJ45 plug 180 degree cable outlet | 6XV1878-5S* |
| IE TP Cord M12-180/RJ45-180 | Industrial Ethernet Flexible Cable, pre-assembled with 1 x M12 plug (X-coded) 180 degree cable outlet and 1 x RJ45 plug 180 degree cable outlet | 6XV1878-5T* |

* Available in different lengths

You can find detailed information and accessories on the Siemens Industry Online Support website under (https://mall.industry.siemens.com/mall/en/en/Catalog/Products/9300175).

## 4.5.4 Antennas and antenna accessories

| Type | Properties | Article number |
|---|---|---|
| **Antennas** | | |
| ANT795-6MN | Antenna with omnidirectional characteristic for WLAN 2.4/ 5 GHz and private 5G networks, incl. N-Connect connector (female); IP65, -40 ... +70 °C, for mounting on roof and vehicles with the mounting kit 6GK5795-6MN01-0AA6<br>Frequency range: **2.4 ... 7.125 GHz** [1]<br>Antenna gain: **6 ... 8 dBi** [2] | 6GK5795-6MN10-0AA6 |
| ANT897-4MA | Mobile wireless antenna with omnidirectional characteristics for public and private LTE 4G/5G mobile wireless networks worldwide; incl. SMA connector (male); IP65, -20 ... +65 °C, for direct mounting on SCALANCE devices with SMA connection system<br>Frequency range: **600 ... 5000 MHz** [1]<br>Antenna gain: **1 ... 2 dBi** [2] | 6GK5897-4MA00-0AA3 |

| Type | Properties | Article number |
|---|---|---|
| ANT897-4ME | Mobile wireless antenna with omnidirectional characteristic for public 3/4/5G mobile wireless networks and private 5G networks worldwide, incl. N-Connect connector (female), IP65; -40 ... +85°C; note country approvals; mounting on wall or mast, scope of delivery: 1x ANT897-4ME, 1x mounting bracket<br>Frequency range: **600 ... 6000 MHz** [1)]<br>Antenna gain: **2 ... 6 dBi** [2)] | 6GK5897-4ME00-0AA0 |
| ANT897-1NY | Mobile wireless antenna with omnidirectional characteristic for public and private 5G/4G/3G/2G mobile networks with 2 antenna elements, incl. 2 x 3 m cable with SMA connector (male); IP69K; -30 ... +70°C; note country approvals; mounting on non-conductive surface on roof and vehicle<br>Frequency range: **700 ... 4200 MHz** [1)]<br>Antenna gain: **0 ... 2 dBi** [2)] | 6GK5897-1NY00-0AA0 |
| ANT897-5PN | Omnidirectional antenna with 4 antenna elements for WLAN 2.4/5 GHz and private 5G mobile networks; 4x cable with N-Connect female in staggered lengths 20 ... 27 cm; IP69K; -30 ... +70°C; note country approvals; mounting on roof, vehicle and ceiling<br>Frequency range: **2300 ... 7200 MHz** [1)]<br>Antenna gain: **4 ... 6 dBi** [2)] | 6GK5897-5PN00-0AA0 |
| **Antenna accessories** | | |
| Flexible Connection Cable N-Connect male/male | Flexible connecting cable, e.g. for connecting antennas, suitable for IWLAN and mobile wireless; different lengths | |
| | 1 meter | 6XV1875-5AH10 |
| | 2 meters | 6XV1875-5AH20 |
| | 5 meters | 6XV1875-5AH50 |
| | 10 meters | 6XV1875-5AN10 |
| Flexible Connection Cable N-Connect/SMA male/male | Flexible connecting cable SCALANCE M antenna, preassembled, various lengths | |
| | 0.3 meters | 6XV1875-5LE30 |
| | 1 meter | 6XV1875-5LH10 |
| | 2 meters | 6XV1875-5LH20 |
| | 5 meters | 6XV1875-5LH50 |
| | 10 meters | 6XV1875-5LN10 |
| Lightning Protector mit N-Connect female/female LP798-1N | Lightning protection element with two N-Connect female/female connectors, 0 ...6 GHz, IP65, -40 ... +100 °C, 0 ... 6 GHz, with gas discharge technology for SCALANCE W and M antennas | 6GK5798-2LP00-2AA6 |
| N-Connect/SMA female/ female Panel Feedthrough | Panel feedthrough for wall thicknesses up to a maximum of 5.5 mm, two N-Connect/SMA female/female connectors | 6GK5798-0PT00-2AA0 |

| Type | Properties | Article number |
|---|---|---|
| N-Connect female/female Panel Feedthrough | Cabinet feedthrough for wall thicknesses up to 4.5 mm, two N-Connect female-female connectors | 6GK5798-2PP00-2AA6 |
| SMA/SMA male/female angle adapter | 90° angle adapter with SMA male/female connectors | 6GK5898-1CV00-4AA0 |

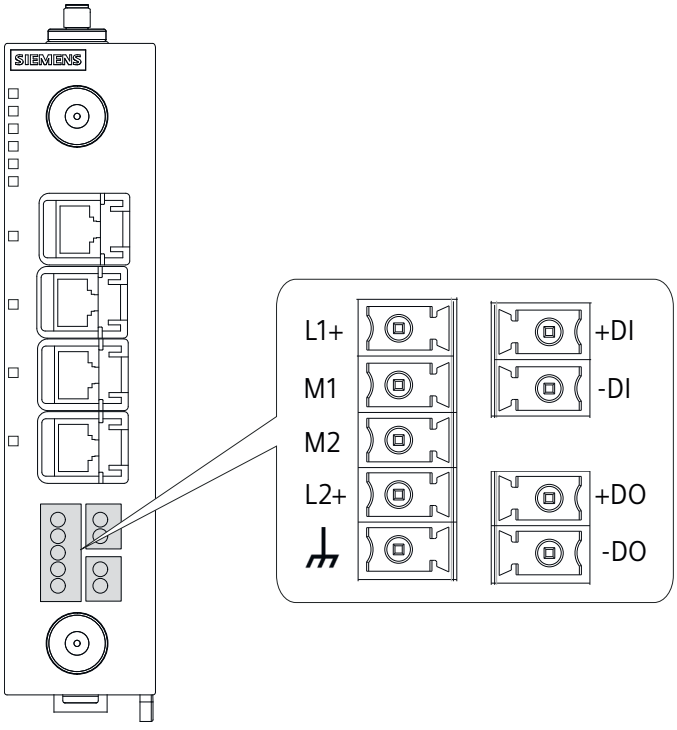
1) You will find information on the supported frequency ranges and antenna gains in the respective band in the operating instructions for the antenna.

2) Depending on the frequency band; see operating instructions for the antenna.

## 4.6 Terminals

### Position

The device has a 5-pin plug-in terminal block for the power supply and two 2-pin plug-in terminal blocks for the digital input and output.




### Connectors and terminal markings

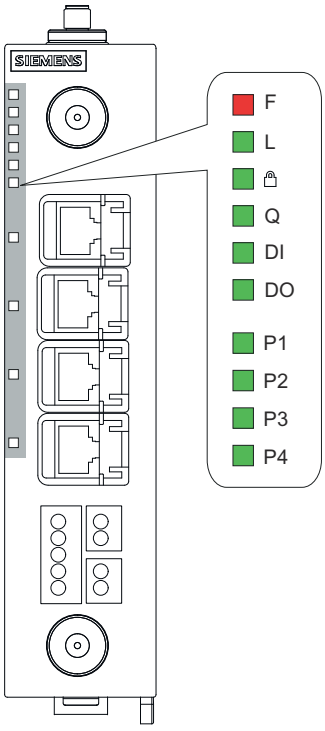
| | | |
|---|---|---|
| L1, M1, L2, M2 | Input for the power supply | Terminal block with five terminal connectors |
| ⏚ | Functional grounding | |

| | | |
|---|---|---|
| +DI, -DI | Digital input | Terminal block with two terminal connectors |
| +DO, -DO | Digital output | Terminal block with two terminal connectors |

### Terminals and wiring

| | | |
|---|---|---|
| Connectors | +DI, -DI /+D0, -DO | L1, M1, L2, M2 |
| AWG | 28 AWG | 16 AWG |
| Wire end ferrule without plastic collar to DIN 46228/1 | 0.2 $mm^2$ | 1.5 $mm^2$ |
| Wire end ferrule with plastic collar to DIN 46228/4 | 0.2 $mm^2$ | 1.5 $mm^2$ |
| Stripped length | 7 mm | 7 mm |

## 4.7 LED display



| LED | Status | Meaning |
|---|---|---|
| F | OFF  | No fault/error. |
| | Yellow  | Sleep mode is active. |
| | Red  | The device is starting up or an error has occurred.<br>Possible errors/faults:<br>• Wrong PIN number<br>• The inserted CLP has an invalid or incompatible configuration.<br>• Errors due to configured system events, e.g. SIM card missing |
| | Flashing  at the interval: 1 s on/ 1 s off | The device is starting up for the first time or has been reset to factory settings. The password of the default user "admin" has not yet been changed. |
| | Flashing red  Interval: 2000 ms on / 200 ms off | Firmware on CLP<br>The device is performing a firmware update or downgrade. |
| L | OFF  | Device turned off, no power supply. |
| | Green  | Device turned on, power supply present. |
| 🔒 | OFF  | No VPN connection is established. |
| | Green  | All configured VPN connections are established. |
| | Flashing green  | Only some of the configured VPN connections are established. |

| LED | Status | Meaning |
|---|---|---|
| P1-P4 | OFF  | There is no connection over the Ethernet interface P1. |
| | Green  | There is a connection over the Ethernet interface P1 (link). |
| | Flashing green and yellow  | Data transfer over the Ethernet interface P1 |
| Q | OFF  | No reception or mobile wireless disabled. |
| | Red  | Wrong PIN number or SIM card error |
| | Flashing red  | Signal strength very poor:<br>• LTE / 5G: < -109 dBm<br>• UMTS: < -99 dBm |
| | Flashing yellow  | Signal strength poor:<br>• LTE / 5G: -99 dBm to -109 dBm<br>• UMTS: -91 dBm to -99 dBm |
| | Yellow  | Signal strength medium:<br>• LTE / 5G: -92 dBm to -99 dBm<br>• UMTS: -81 dBm to -91 dBm |
| | Flashing green  | Signal strength good:<br>• LTE / 5G: -70 dBm to -92 dBm<br>• UMTS: -65 dBm to -81 dBm |
| | Green  | Signal strength very good:<br>• LTE / 5G: ≥ -70 dBm<br>• UMTS: ≥ -65 dBm |
| DI | OFF  | Digital input inactive. |
| | Green  | Digital input active. |

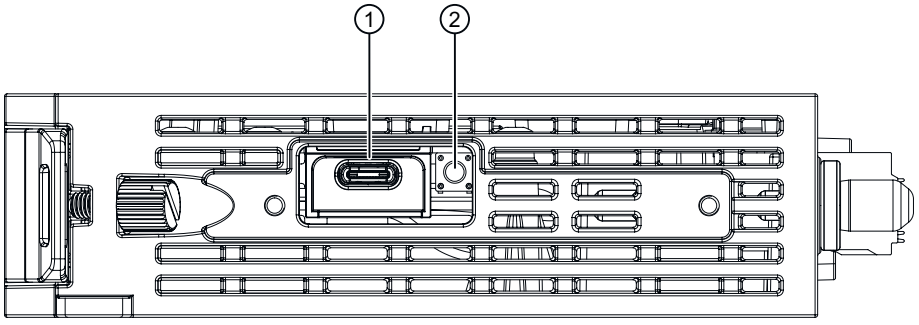
| LED | Status | Meaning |
|---|---|---|
| DO | OFF  | Digital output inactive. |
| | Green  | Digital output active. |
| P1-P4, Q, DI, DO and  | Flashing green  | The LEDs flash for detection of device location.<br>The "Flash LED" function is activated<br>• Either with SINEC PNI<br>• Or via the WBM page "Discovery and Set via DCP". |

## 4.8 Reset button

### Position

| NOTICE |
|---|
| **Loss of the degree of protection** |
| When the cover is not mounted correctly, the device loses its degree of protection IP30. |

The Reset button is located behind the screw-on cover on the underside of the housing.




① PLUG slot (CLP)
② Reset button

### Function

The reset button has the following functions:

- **Restarting the device**
  To restart the device, press the reset button briefly.

  **Note**

  If you make changes to the configuration and restart immediately afterwards with the reset button, the changes may be lost. If you restart the device using the WBM (menu command "System > Restart") or using the CLI (command "restart" in the Privileged EXEC Modus), the configuration changes are always retained.

- **Loading a firmware file via TFTP**
  If the normal procedure with the "Load & Save" menu of Web Based Management is unsuccessful, the reset button can be used to load new firmware. This situation can occur if there is a power outage during the normal firmware update. You can find more detailed information in the section "Downloading new firmware using TFTP without WBM and CLI (Page 73)".
- **Resetting the device to factory settings**
  If you reset, all the settings you have made will be overwritten by factory defaults. If a PLUG has been inserted in the device, the PLUG is also reset to default settings. You can find more detailed information in the section "Restoring the factory settings (Page 74)".

| NOTICE |
| --- |
| **Inadvertent reset** |
| An inadvertent reset can cause disturbances and failures in a configured network with further consequences. |

## 4.9 Configuration License PLUG

The CLP (Configuration License PLUG) is used to transfer the configuration of the old device to the new device when a device is replaced. The CLP is also referred to as PLUG in the description.

The PLUG is available in the following variants:

- PLUG Configuration: The exchangeable storage medium only saves the configuration data of the device.
- PLUG License: In addition to the configuration data, the exchangeable storage medium contains a license with which special functions are enabled, e.g. iFeatures.

| NOTICE |
| --- |
| **Loss of the degree of protection** |
| When the cover is not mounted correctly, the device loses its degree of protection IP30. |

## Position

The CLP slot is at the bottom of the device enclosure under a cover, see Reset button (Page 35).

## Function

Devices with a CLP slot support the following operating modes:

- **Without CLP**
  The device saves the configuration data in the internal memory. This mode is active when no CLP is inserted.
- **With CLP**
  In the startup phase:
  - When an **empty** CLP (delivery state) is inserted into the device, the device automatically backs up the configuration data on the CLP during startup. After that, it behaves like a CLP with data.
  - When a CLP **with data** is plugged into a device, the device automatically adopts the configuration of the CLP during the startup phase. The prerequisite for this is that the configuration data was written by a compatible device type.
    One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.
  - If the CLP contains a license, additional functions are also enabled.

    **Note**

    If the device was configured at some time with a CLP license, the device can no longer be used without this CLP. To be able to use the device again, reset the device to the factory settings.

  During operation:
  - During operation, changes to the configuration are saved on the CLP and in the internal memory.
  - The configuration data of the device is stored in a secured memory area of the CLP. This secured memory area can only be accessed via the authentication of the Siemens device.
  - The device checks whether a CLP is inserted at one second intervals. If the device detects that the CLP has been removed, it restarts automatically.

    | **NOTICE** |
    |---|
    | **Operating risk - Danger of data loss** |
    | Only pull and plug the CLP when the device is de-energized. |

  - The device signals deviations from normal operation of the CLP (e.g., incompatible data, incorrect operation or malfunctions) via the existing diagnostics mechanisms (e.g., LEDs or user interfaces).

The procedure for inserting and removing the CLP can be found in the section "Replacing a CLP (Page 71)".

# Installation and removal

# 5

## 5.1 Safety when mounting

### Safety notices

When installing the device, keep to the safety notices listed below.

| NOTICE |
| --- |
| **Improper mounting**<br>Improper mounting may damage the device or impair its operation.<br>• Before mounting the device, always ensure that there is no visible damage to the device.<br>• Mount the device using suitable tools. Observe the information in the respective section about mounting. |

| ⚠ CAUTION |
| --- |
| **Minimum distance to antennas**<br>Fit the device so that there is a minimum clearance of 20 cm between antennas and persons. |

| ⚠ WARNING |
| --- |
| If a device is operated in an ambient temperature of more than 50 °C, the temperature of the device housing may be higher than 70 °C. The device must therefore be installed so that it is only accessible to service personnel or users that are aware of the reason for restricted access and the required safety measures at an ambient temperature higher than 50 °C. |

| ⚠ WARNING |
| --- |
| The device is intended for indoor use only. |

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

## Safety notices on use in hazardous areas

### General safety notices relating to protection against explosion

**WARNING**

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

**WARNING**

**EXPLOSION HAZARD**

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

**WARNING**

The device shall only be used in an area with pollution degree 1 or 2 (according to EN/IEC 60664-1, GB/T 16935.1).

### Information on use in hazardous areas according to ATEX, IECEx and UKEX

If you use the device under ATEX, IECEx or UKEX conditions, you must also keep to the following safety instructions in addition to the general safety instructions for protection against explosion:

**WARNING**

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

### Safety notices when using according to FM

If you use the device under FM conditions you must also keep to the following safety notices in addition to the general safety notices for protection against explosion:

**WARNING**

**EXPLOSION HAZARD**

The equipment is intended to be installed within an enclosure/control cabinet. The inner service temperature of the enclosure/control cabinet corresponds to the ambient temperature of the module. Use cables with a maximum permitted operating temperature of at least 20 °C higher than the maximum ambient temperature.

**WARNING**

Wall mounting is only permitted if the requirements for the housing, the installation regulations, the clearance and separating regulations for the control cabinets or housings are adhered to. The control cabinet cover or housing must be secured so that it can only be opened with a tool. An appropriate strain-relief assembly for the cable must be used.

**WARNING**

Wall mounting outside of the control cabinet or housing does not fulfill the requirements of the FM approval.

**WARNING**

The IP30 degree of protection marking is not associated with FM approval.

**Note**

You must not install the device on a wall in hazardous areas.

**Safety notices when using the device as industrial control equipment according to UL 61010-2-201**

If you use the device under UL 61010-2-201 conditions you must also keep to the following safety notices in addition to the general safety notices for protection against explosion:

**WARNING**

**Open equipment**

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

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

**WARNING**

If the temperature at the cable or housing socket or at the branching points of the cables exceeds 60 °C, special precautions must be taken. If the equipment is operated at ambient temperatures in excess of 40 °C, only use cables with permitted operating temperature of at least 80 °C.

**⚠ WARNING**

**Improper disassembly**

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

For proper disassembly, observe the following:

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

## 5.2 Types of installation

For the device, you have the following options:

- Wall mounting
- Installation on a 35 mm DIN rail
  - direct
  - rotated by $90^0$ with a DIN rail mounting adapter (see Accessories (Page 28))
- Installation on the S7-300 mounting rail
- Installation on the S7-1500 mounting rail

**⚠ CAUTION**

**Danger of injury by falling objects**

If the SCALANCE MUM is subjected to very strong vibration (> 10 $m/s^2$), mounting on a DIN rail or S7-300 / S7-1500 mounting rail does not provide adequate support. Under such conditions, the device can come out of the mounting and may cause injury.

In this case, install the device on a wall.

**Permitted mounting position**

- Vertical mounting position (ventilation openings at the top and bottom)
- Horizontal mounting position (ventilation openings to the right and left)

**Strain relief for the cables**

Regardless of the type of installation, make sure that there is suitable strain relief for the connecting cable.

**Shielding of cables**

If cables are installed permanently, it is advisable to remove the insulation of the shielded cable and to establish contact on the shield/PE conductor bar.

**Permitted mounting position**

You can find information about the ambient temperature under Permitted ambient conditions. (Page 79)

Keep to the minimum clearances to other components or to walls of a housing so that the convection ventilation of the device is not blocked.

- Above at least 10 cm
- Below at least 10 cm

**Note**

Antennas, in particular directional antennas, must be mounted in keeping with their characteristics (refer to the technical specifications of the antenna --> Radiation pattern diagrams).

## 5.3 Wall mounting

**Note**

The wall mounting must be capable of supporting at least four times the weight of the device.

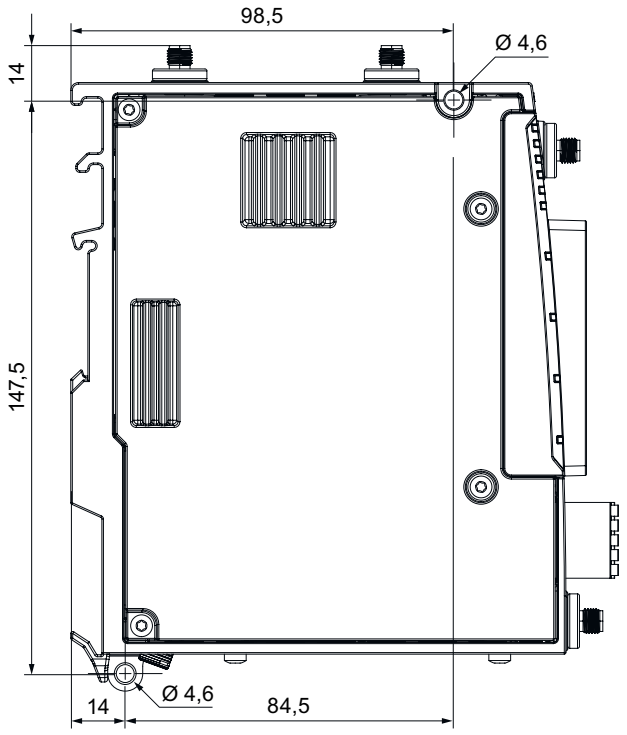
Use suitable fittings depending on the mounting surface.

### Requirement

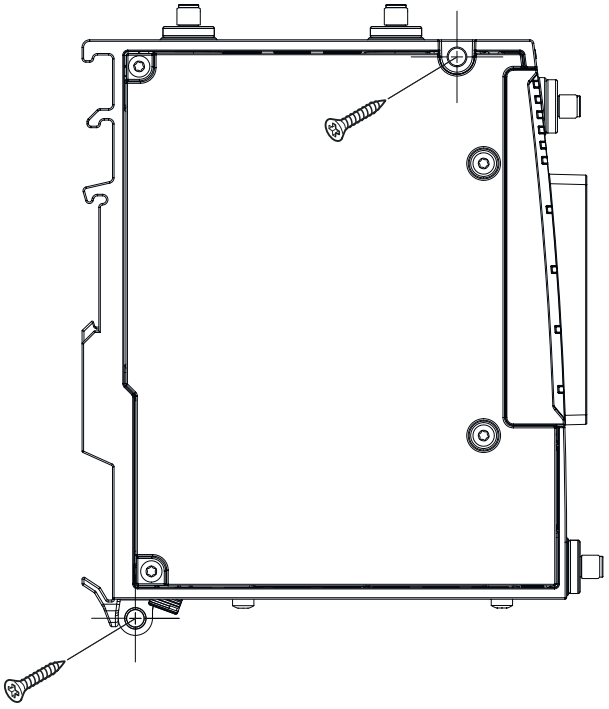
The SIM card is inserted. You can find more information on this in the section "SIM card (Page 64)".

## Drilling template

The figure shows the location of the holes for wall mounting of the device:



**Procedure**



Follow the steps below to mount the device to the wall:

1. Prepare the drill holes for wall mounting. The precise dimensions are listed in the drilling template, refer to section "Drilling template".
2. Secure the device to the wall with two screws. The screws are not supplied with the device. The type and length of the screws depend on the type of wall.
3. Connect the device; see section "Connecting (Page 53)".

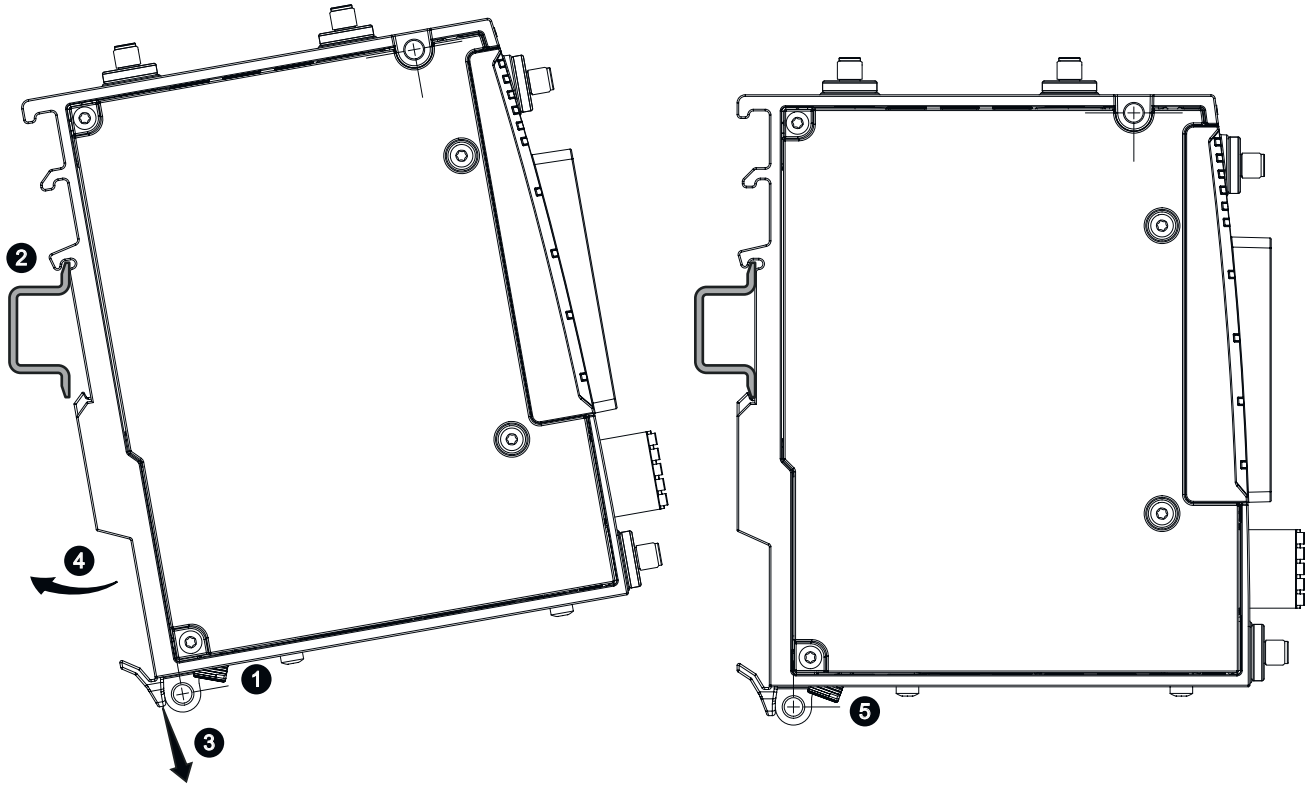
## 5.4 Installing on the DIN rail

### 5.4.1 Mounting directly on the DIN rail

**Requirement**

The SIM card is inserted. You can find more information on this in the section "SIM card (Page 64)".

## Installation




Follow the steps below to mount the device on a DIN rail:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the third housing guide of the device on the top edge of the DIN rail.
3. Using a screwdriver, pull the securing bar down as far as it will go.
4. With the securing bar pulled, swivel the device to the DIN rail and press it against the DIN rail until the spring-mounted securing bar locks into place.
5. Tighten the knurled screw to secure the device additionally (torque 0.5 Nm).
6. Connect the device; see section "Connecting (Page 53)".

## Uninstalling

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. If necessary, loosen the knurled screw with your hand or a screwdriver.
4. Using a screwdriver, pull down the catch on the rear of the device.
5. Pull lower part of the device away from the DIN rail.

### 5.4.2 Mounting rotated by 90° with DIN rail mounting adapter

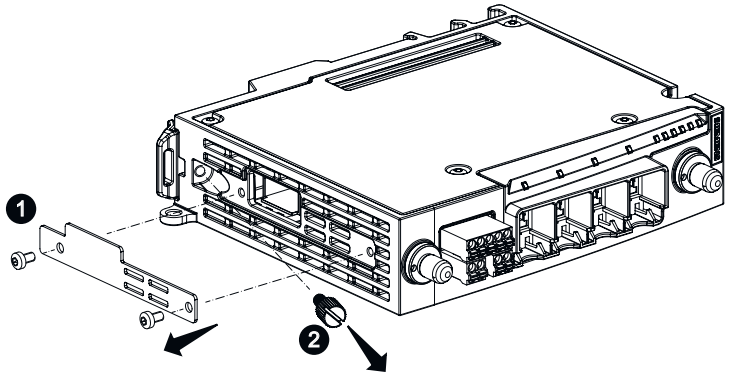
The DIN rail mounting adapter is not included with the product, see Accessories (Page 28).

#### Requirement

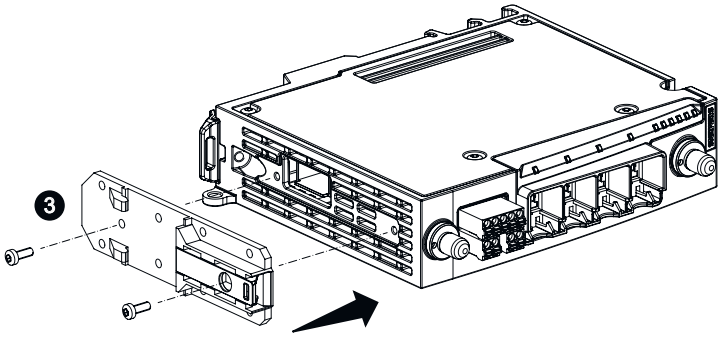
The SIM card is inserted. You can find more information on this in the section "SIM card (Page 64)".

#### Installation

1. Loosen the two M3 screws and remove the cover of the CLP slot ❶.
2. Remove the knurled screw ❷.

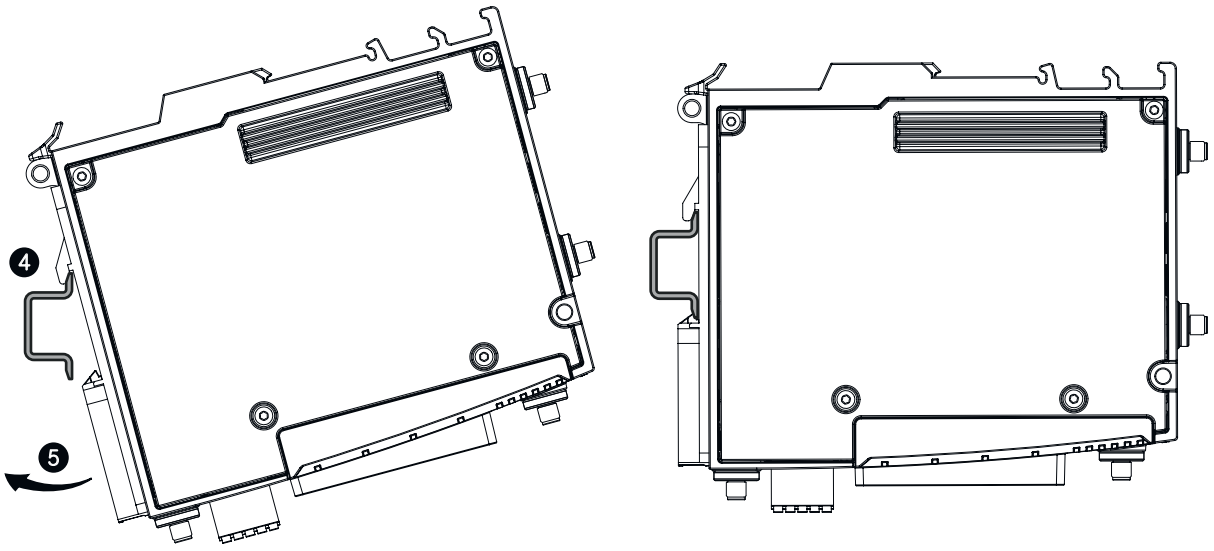



3. Screw the DIN rail mounting adapter ❸ to the bottom of the device (M3 x 8, tightening torque 0.8 Nm). The mounting material is supplied with the DIN rail mounting adapter.




4. Place the device on the upper edge of the DIN rail ❹.

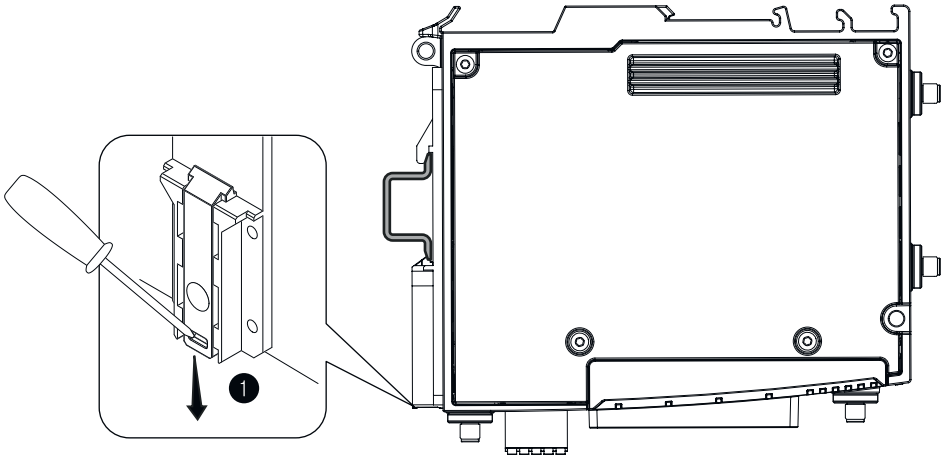
5. Press the device against the DIN rail ❺ until the DIN rail slider catch locks in place.



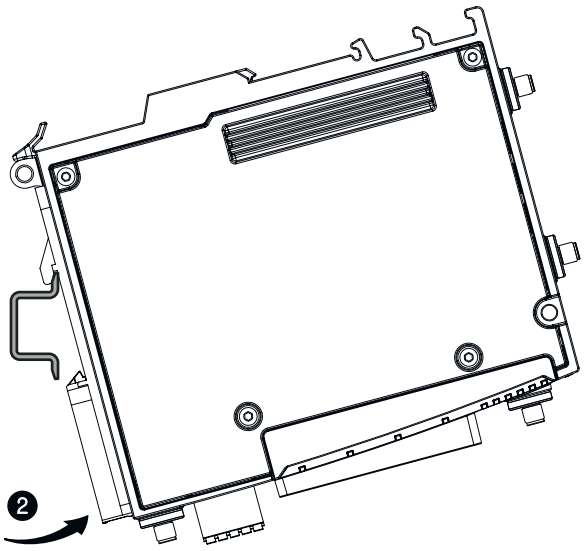

6. Connect the power supply, refer to the section "Power supply (Page 58)".
7. Fit the antennas, refer to the section "Antennas (Page 61)".

## Uninstalling

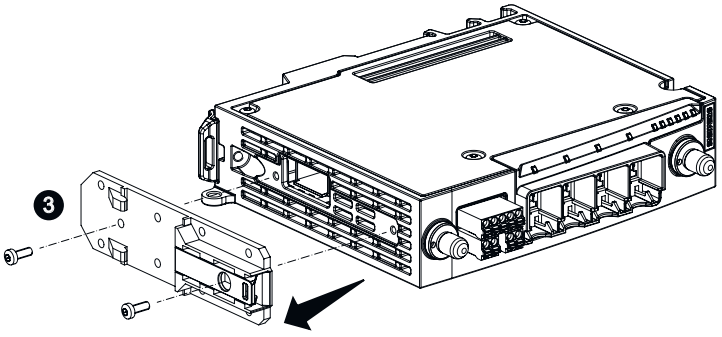
1. Turn off the power to the device.
2. Disconnect all connected cables.
3. Pull the DIN rail slider down with a screwdriver ❶.



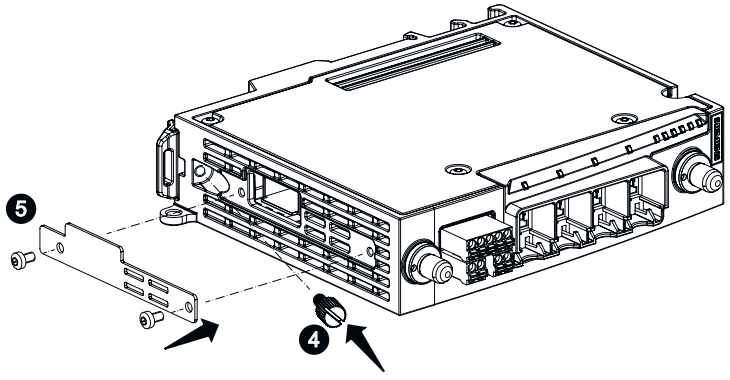
4. Tilt the device forward ❷ and remove the device from the DIN rail.




5. Loosen the screws of the DIN rail mounting adapter ❸ completely and remove it.




6. Install the knurled screw ❹.
7. Attach the cover of the CLP slot ❺ again.

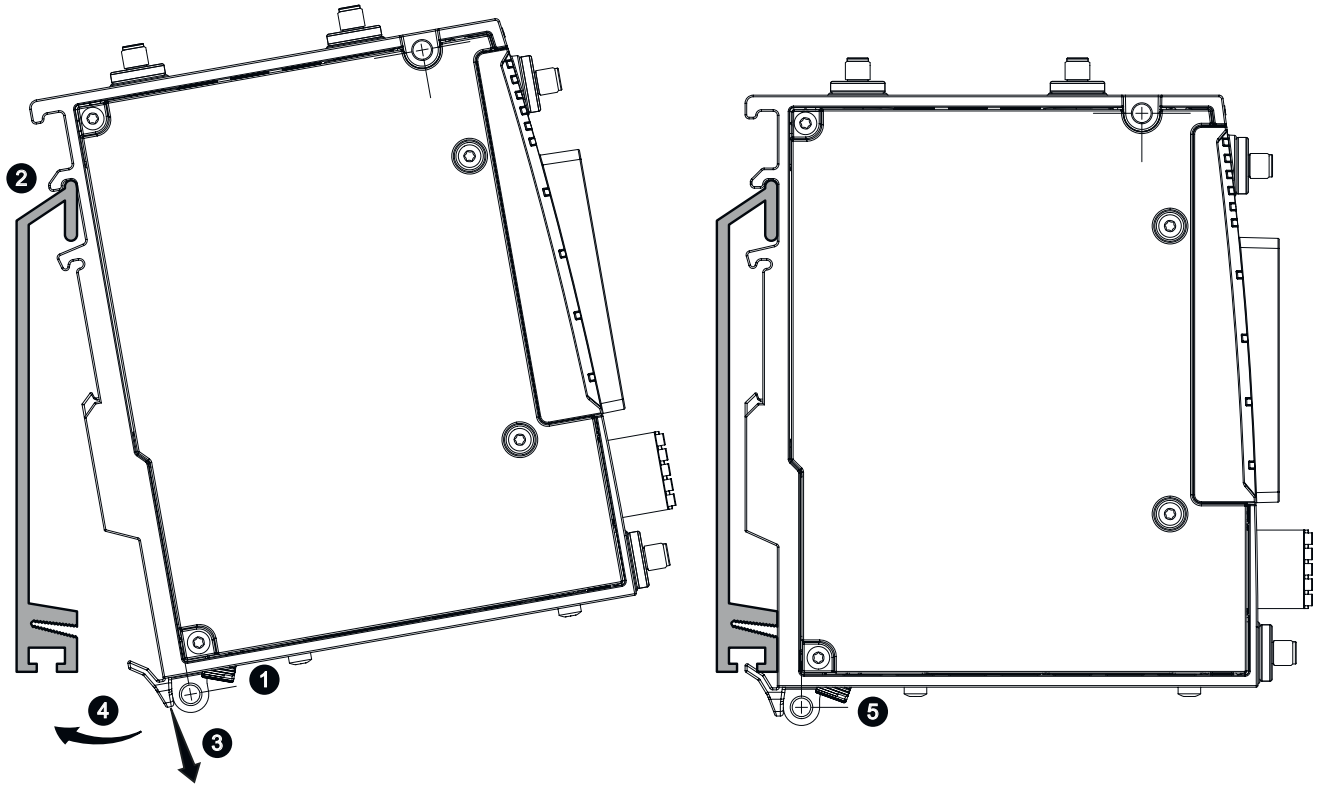


## 5.5 Installing on an S7-300 mounting rail

### Requirement

The SIM card is inserted. You can find more information on this in the section "SIM card (Page 64)".

### Installation




Follow the steps below to mount the device on an S7-300 mounting rail:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the first housing guide of the device on the top edge of the mounting rail.
3. Using a screwdriver, pull the securing bar down as far as it will go.
4. With the securing bar pulled, swivel the device to the mounting rail and press it against the mounting rail until the spring-mounted securing bar locks into place.
5. Tighten the knurled screw to secure the device additionally (torque 0.5 Nm).
6. Connect the device; see section "Connecting (Page 53)".

### Uninstalling

To remove the device from the mounting rail, follow these steps:

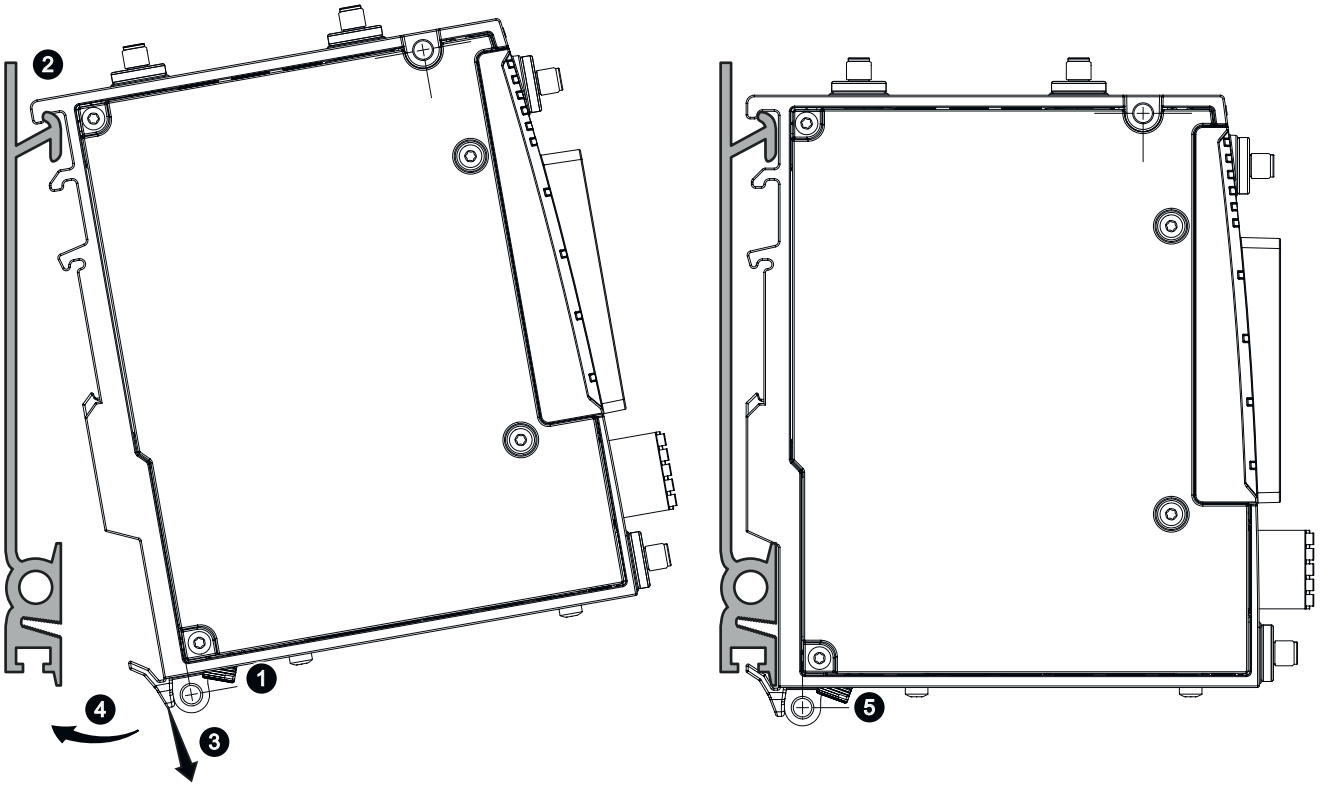
1. Turn off the power to the device.
2. Disconnect all connected cables.
3. If necessary, loosen the knurled screw with your hand or a screwdriver.
4. Using a screwdriver, pull the securing bar down as far as it will go.
5. Remove the device from the mounting rail with the bar pulled.

## 5.6 Installing on an S7-1500 mounting rail

### Requirement

The SIM card is inserted. You can find more information on this in the section "SIM card (Page 64)".

### Installation



Follow the steps below to mount the device on an S7-1500 mounting rail:

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the first housing guide of the device on the top edge of the mounting rail.
3. Using a screwdriver, pull the securing bar down as far as it will go.
4. With the securing bar pulled, swivel the device to the mounting rail and press it against the mounting rail until the spring-mounted securing bar locks into place.
5. Tighten the knurled screw to secure the device additionally (torque 0.5 Nm).
6. Connect the device; see section "Connecting (Page 53)".

### Uninstalling

To remove the device from the mounting rail, follow these steps:

1. Turn off the power to the device.
2. Disconnect all connected cables.
3. If necessary, loosen the knurled screw with your hand or a screwdriver.
4. Using a screwdriver, pull the securing bar down as far as it will go.
5. Remove the device from the mounting rail with the bar pulled.

# Connection

# 6

## 6.1 Safety when connecting

### Safety notices

When connecting up the device, keep to the safety notices listed below.

**Note**

**Strain relief for the Ethernet cables**

In order to avoid mechanical stress on the Ethernet cables and resulting interruption of the contact, fasten the cables at a short distance from the connector using a cable guide or busbar.

### Safety notices for operation with a power supply according to NEC Class 2

Operate the device with a power supply according to NEC Class 2. When connecting up the device, keep to the safety notices listed below.

**⚠ WARNING**

**Power supply**

The device is designed for operation with Safety Extra-Low Voltage (SELV) that can be connected directly by a Limited Power Source (LPS).

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

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

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

**⚠ WARNING**

**Insulation of external power supplies**

Ext. circuits intended to be connected to this device shall be galv. separated from hazardous live voltage by reinforced or double insulation.

**Note**

Minimum temperature rating of the cable to be connected to the field wiring terminals, 90 °C.

## Safety notices for operation with a power supply not complying with NEC Class 2

If you operate the device in a control cabinet, you can use a power supply that does not comply with NEC Class 2. When connecting up the device, keep to the safety notices listed below.

**WARNING**

**Safety extra low voltage**

The device is designed for operation with a directly connectable safety extra-low voltage (SELV) according to UL/IEC 61010-1 and UL/IEC 61010-2-201 whose output power corresponds to "Limited Energy" according to UL/IEC 61010-1.

**NOTICE**

**Suitable fuse for the power supply cables (corresponds to "Limited Energy")**

The current on the terminal may not exceed 3 A. Use a fuse for the power supply that is suitable for protection of AC/DC power supply circuits *) and protects against currents > 3 A.

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for AC/DC *) (min. 60 V / 3 A)
  - Breaking current at least 10 kA
  - Approval according to ANSI/UL 248-14 (suppl. fuses), ANSI/UL 248-4 (Class CC), ANSI/UL 248-8 (J), ANSI/UL 248-15 (T), or CSA C22.2-4 No. 248.14 (suppl. fuses), No. 248-4 (Class CC), No. 248-8 (J), No. 248-15 (T)
- In other areas, the fuse must meet the following requirements:
  - Suitable for AC/DC *) (min. 60 V / 3 A)
  - Breaking current at least 10 kA
  - Approval according to IEC/EN 60947-1/2/3 or IEC/EN 60898-1/2 for circuit breakers
  - Breaking characteristics: B or C
  - Approval according to IEC/EN 60127-1 for fuses
  - Breaking characteristics: max. 120 s at 2 x $I_n$ (corresponds to melting integral $I^2t < 4320$)

If the properties of the supplying current source are known, the following fuse is also possible:

- In areas subject to the NEC or CEC, the fuse must meet the following requirements:
  - Suitable for AC/DC *) (min. 60 V / 3 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to UL 1077 or CSA C22.2 No. 235
- In other areas, the fuse must meet the following requirements:
  - Suitable for AC/DC *) (min. 60 V / 3 A)
  - Breaking current > highest possible current of the current source (incl. short circuit current and fault)
  - Approval according to IEC/EN 60934
  - Breaking characteristics: max. 120s at 2 x $I_n$

*) AC or DC depending on availability

## Safety notices on use in hazardous areas

### General safety notices relating to protection against explosion

**WARNING**

**EXPLOSION HAZARD**

Do not connect or disconnect cables to or from the device when a flammable or combustible atmosphere is present.

**⚠ WARNING**

**EXPLOSION HAZARD**

Do not press the reset button if there is a potentially explosive atmosphere.

**⚠ WARNING**

**Unsuitable cables or connectors**

Risk of explosion in hazardous areas

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

**⚠ WARNING**

**Lack of equipotential bonding**

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

- Ensure that equipotential bonding is available for the device.

**⚠ WARNING**

**Unprotected cable ends**

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

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

**⚠ WARNING**

**Improper installation of shielded cables**

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

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

**WARNING**

**Insufficient isolation of intrinsically safe and non-intrinsically safe circuits**

Risk of explosion in hazardous areas

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

**Information on use in hazardous areas according to ATEX, IECEx and UKEX**

If you use the device under ATEX, IECEx or UKEX conditions, you must also keep to the following safety instructions in addition to the general safety instructions for protection against explosion:

**WARNING**

**Transient overvoltages**

Take measures to prevent transient surges of more than 40% of the rated voltage. Under no circumstances may transient surges exceed 119 V. This is the case if you only operate devices with SELV (safety extra low voltage).

**WARNING**

**Suitable cables at high ambient temperatures in hazardous area**

At an ambient temperature of ≥ 60 °C, use heat-resistant cables designed for an ambient temperature at least 20 °C higher. The cable entries used on the housing must comply with the IP degree of protection required by EN IEC / IEC 60079-0.

**General notes on use in hazardous areas according to UL-HazLoc**

If you use the device under UL-HazLoc conditions, you must also adhere to the following safety notices in addition to the general safety notices for protection against explosion:

**WARNING**

**WARNING - EXPLOSION HAZARD -**

DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

**WARNING**

**Restricted area of application**

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

**⚠ WARNING**

**Restricted area of application**

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

## 6.2 Power supply

**⚠ WARNING**

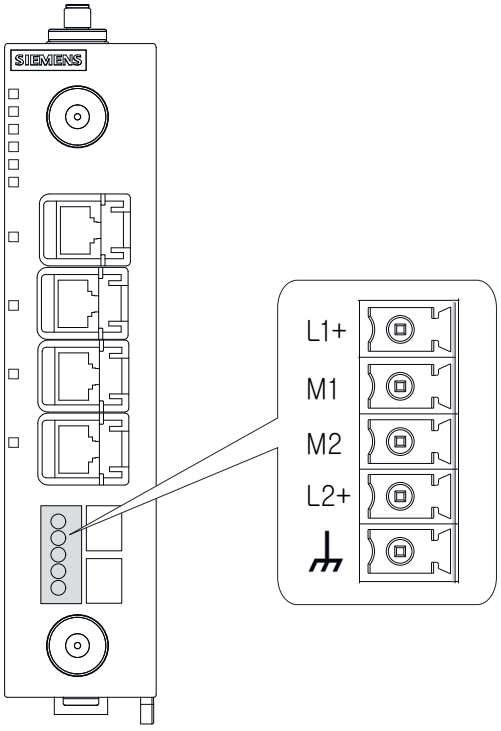
**Impermissible power supply**

Never operate the device with AC voltage or DC voltage higher than 32 V DC.

**Note**

The device can be disconnected from the power supply by removing the terminal block.

The power supply is connected using a 5-pin plug-in terminal block. The power supply is non-floating.




| Contact | Assignment |
|---|---|
| L1+ | 24 VDC |
| M1 | Ground |
| M2 | Ground |

| Contact | Assignment |
|---|---|
| L2+ | 24 VDC |
| ⏚ | Functional grounding, refer to the section "Grounding (Page 67)" |

Use copper cables with the following properties to wire the power connector:

- Two-wire cable with 0.5 to 1.5 $mm^2$ Cross-section per wire
- Permitted tensile load at least 10 N. - UL
- List of cables according to the national installation regulations. In areas where NEC or CEC applies: Type PTLC or ITC

You can find more information in the section "Terminals (Page 31)".

The "L1" and "L2" LEDs indicate the current range of the power supply, see the section "LED display (Page 32)".

**Note**

The requirements of EN61000-4-5, "Surge Immunity Test" on power supply lines with 24 VDC are met only when a Blitzductor is used:

24 VDC: BVT AVD 24 type no. 918 422

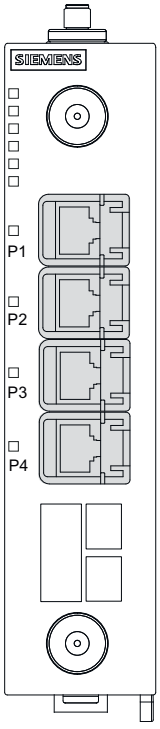
Vendor: DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str. 1, Postfach 1640, D - 92306 Neumarkt, Germany

## 6.3 Ethernet

The device has four Ethernet interfaces located on the front of the device. Connection to Industrial Ethernet uses RJ45 connection technology with MDI-X assignment.

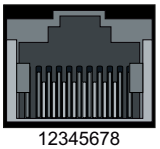
## Position

The figure shows the position of the connectors to Industrial Ethernet with 10/100/1000 Mbps.




## Pin assignment

The following table shows the pin assignment of the RJ45 connectors.

| Pin number | Pin assignment | RJ45 connector |
|---|---|---|
| | **10/100/1000 Mbps** | |
| Pin 1 | D1+ |  12345678 |
| Pin 2 | D1- | |
| Pin 3 | D2+ | |
| Pin 4 | D3+ | |
| Pin 5 | D3- | |
| Pin 6 | D2- | |
| Pin 7 | D4+ | |
| Pin 8 | D4- | |

## 6.4 Antennas

The SCALANCE MUM853-1 has 4 antenna ports of the type SMA female.

**Note**

Use the antennas from the range of accessories for the device. You will find more detailed information in "Accessories (Page 29)". If you use a different antenna, there is no guarantee that the device will function according to the specification.

You can either connect an external antenna directly to the device or connect it with a flexible connecting cable.

**⚠ CAUTION**

**Minimum clearance to the device**

The device may only be operated when the distance between the device (or antenna) and user is at least 20 cm.

### Notes on lightning protection



**⚠ WARNING**

**Danger due to lightning strikes**

Antennas installed outdoors must be within the area covered by a lightning protection system. Make sure that all conducting systems entering from outdoors are protected by lightning protection electrical bonding.

When implementing your lightning protection concept, make sure you adhere to the requirements of the VDE 0182 or IEC 62305 standards.

- A suitable lightning conductor LP798-1N (article no. 6GK5798-2LP00-2AA6) is available in the range of accessories of SIMATIC NET Industrial WLAN:
  Depending on the connector, an adapter cable is required to connect to SMA.



**⚠ WARNING**

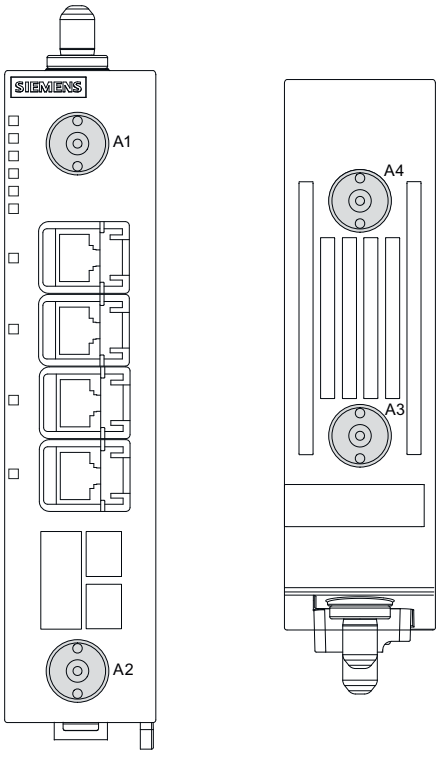
**Danger due to lightning strikes**

Installing this lightning protector between an antenna and a SCALANCE M device is not adequate protection against a lightning strike. The LP798-1N lightening protector only works within the framework of a comprehensive lightning protection concept. If you have questions, ask a qualified specialist company.

### Connecting antennas

You can connect an external antenna to the device directly or using a flexible connecting cable.

Antenna ports A1 and A2 are located on the front of the device (left picture) and antenna ports A3 and A4 on the top of the device (right picture).




| | | | |
|---|---|---|---|
| A1 | Antenna port A1 | A3 | Antenna port A3 |
| A2 | Antenna port A2 | A4 | Antenna port A4 |

**Note**

**Antennas**

- An antenna must always be connected to all antenna ports in order to use 3/4/5G connectivity.
- For GNSS operation, use the A4 antenna. This must have a clear view of the sky.

**Protective caps**

Keep the removed protective caps for later use.

To connect an antenna, follow these steps:

1. Remove the protective cap from the relevant antenna port on the device.
2. Insert the connector of the antenna or the flexible connecting cable into the SMA socket and tighten the sleeve nut of the connector on the socket (key size SW8, tightening torque 1 Nm).

**NOTICE**

**The SMA socket may be damaged**

When securing an antenna to the device, only the screw cap of the antenna can be rotated. Rotating the entire antenna could damage the SMA connector on the device.

**NOTICE**

**UL approval only for use in buildings**

Where NEC and CEC apply, the device and the antennas connected to it may only be used in a closed building. For this reason, do not lead antennas into the outdoor area if you need to meet UL requirements.

**Note**

**Cabinet installation**

When installing the device in a cabinet, you need to use detached antennas. A suitable flexible connecting cable for the connection between the device and a detached antenna are available from SIMATIC NET. You will find detailed information in the section "Accessories (Page 29)".

## Frequency bands

| | | |
|---|---|---|
| 6GK5853-2EA00-2DA1 | 5G Standalone (SA) | n1, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n71, n77, n78, n79 |
| | 5G Non-Standalone (NSA) | n1, n3, n5, n7, n8, n20, n28, n38, n40, n41, n48, n66, n77, n78, n79 |
| | LTE | B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29, B30, B32, B66, B71, B34, B38, B39, B40, B41, B42, B43, B46, B48 |
| | UMTS | B1, B2, B3, B4, B5, B8 |
| | GNSS | GPS L1 (1575.42 MHz)<br>GPS L5 (1176.45 MHz)<br>For GNSS operation, the A4 antenna must have a clear view of the sky. |

| | | |
|---|---|---|
| 6GK5853-2EA10-2AA1 (A1) | 5G Standalone (SA) | n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n75(DL), n77, n78, n79 |
| | 5G Non-Standalone (NSA) | n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n66, n71, n77, n78, n79 |
| | LTE | B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B29(DL), B30, B32(DL), B34, B38, B39, B40, B41, B42, B43, B46(DL), B48, B66, B71 |
| | UMTS | B1, B2, B4, B5, B6, B8, B19 |
| | GNSS | GPS L1 (1575.42 MHz)<br>Galileo E1 (1575.42 MHz)<br>For GNSS operation, the A4 antenna must have a clear view of the sky. |
| 6GK5853-2EA10-2BA1 (B1) | 5G Standalone (SA) | n1, n3, n5, n8, n28, n41, n77, n78, n79 |
| | 5G Non-Standalone (NSA) | n41, n77, n78, n79 |
| | LTE | B1, B3, B5, B8, B34, B38, B39, B40, B41 |
| | UMTS | B1, B5, B8 |
| | GNSS | Not supported |

Depending on the frequency bands used by your mobile wireless provider, antennas must be tuned to the suitable frequencies. Check with your mobile wireless provider for the frequency bands.

### Signal quality

During installation make sure that there is a good signal strength of > -73 dBm.

If the "Q" LED is lit permanently, the signal quality is good. For more detailed information, refer to the section "LED display (Page 32)".

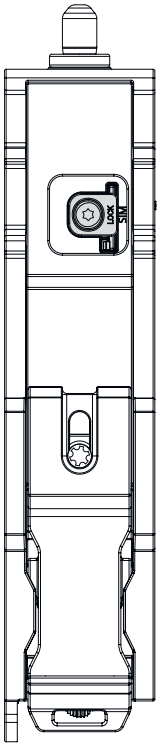
Avoid large metallic objects in the immediate vicinity.

## 6.5 SIM card

| NOTICE |
|---|
| **Turn off the power supply before replacing SIM cards** |
| Before you insert or remove the SIM card, turn off the power supply of the device. |
| Do not open the SIM card tray during operation. This can damage the SIM card and the device. |

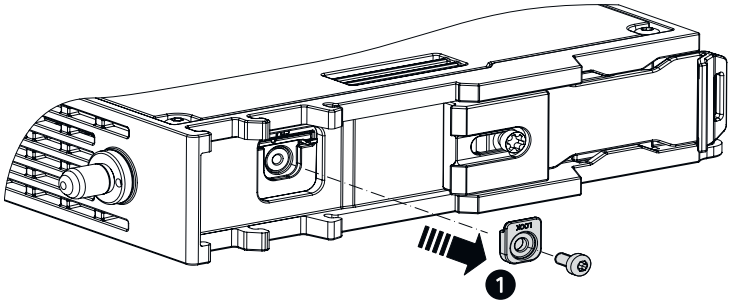
## Position

The tray for the micro SIM card is located on the back of the device. The tray is secured with an M3 screw.

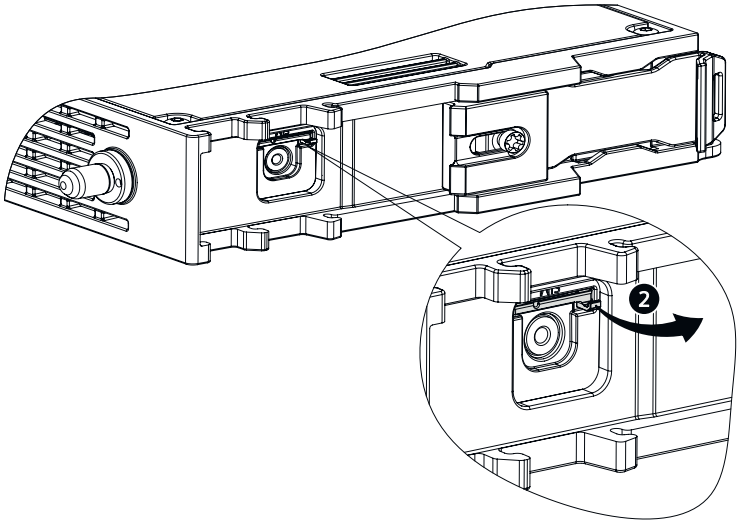


### Inserting the SIM card

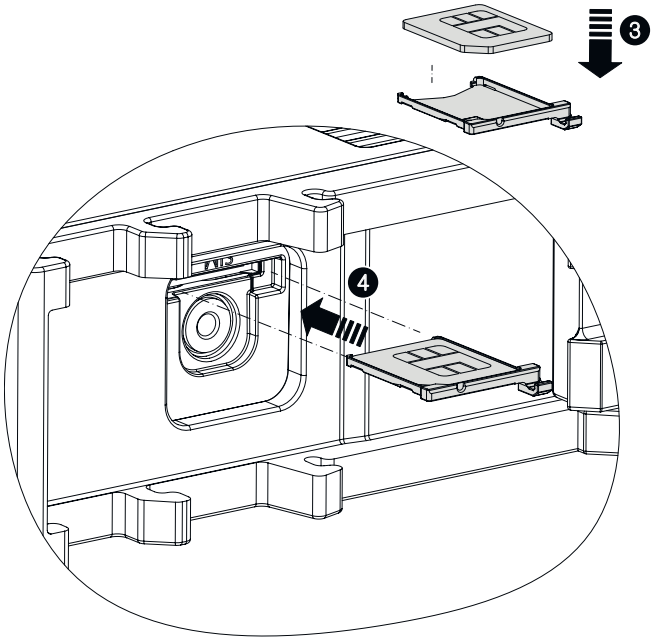
1. Loosen the M3 screw and remove the tray cover.



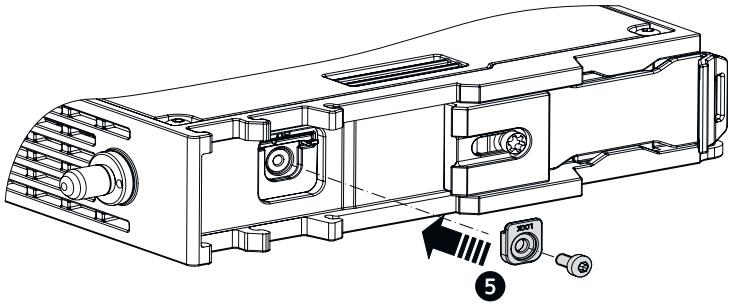

2. Press on the tab of the drawer with your index finger and pull it out.




3. Insert the SIM card into the tray with the golden contact surface facing up.



4. Then push the tray with the SIM card back into the housing as far as it will go.
5. Replace the cover and carefully tighten the M3 screw ④ with a maximum torque of 0.4 Nm.




## 6.6 Grounding

### Grounding for wall mounting

The device is grounded by the fixing screw via the unpainted eyelet, position see section "Device view (Page 26)".

In addition to grounding via the fixing screw, you can also ground the device using the terminal block. The terminal is identified by the symbol for the functional ground ⏚; for the position, see section "Terminals (Page 31)". Connect the terminal of the device with as short a cable as possible ≤ 150 mm and with the required cross-sectional area to a grounded part of the system.

If the device is mounted on a non-conductive base, grounding must be connected either via the functional ground on the terminal block or via a grounding cable.

The grounding cable is not supplied with the device. Connect the paint-free surface of the device to the nearest grounding point using the grounding cable.

### Grounding when installing on a DIN rail / S7 mounting rail

The device is grounded via the rear of the device.

You can also ground the device via the terminal block. The terminal is identified by the symbol for the functional ground ⏚; for the position, see section "Terminals (Page 31)". Connect the terminal of the device with as short a cable as possible ≤ 150 mm and with the required cross-sectional area to a grounded part of the system.

## 6.7 Digital input/output

The digital input and output are connected using a 2-pin plug-in terminal block in each case. Two terminal blocks ship with the device.

| NOTICE |
| --- |
| **Damage due to voltage being too high or too low**<br>The voltage at the digital input/output must not exceed 30 VDC and not fall below -30 VDC, otherwise the digital input/output will be destroyed. |

**Note**

**Interference pulse**

To avoid evaluating an interference pulse, the pulse for the signal 1 (TRUE / HIGH) must be at least 200 ms.

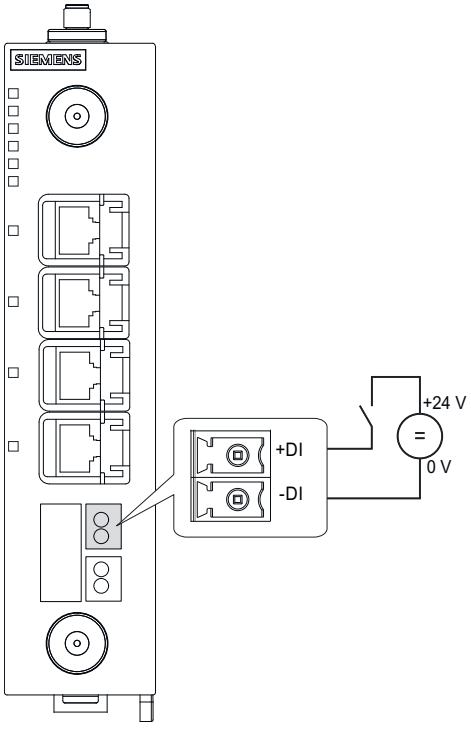
### Wiring rules

- To wire the digital input/output, use a copper cable of category AWG18-16 or a cable with a cross-section of 0.75 to 1.5 $mm^2$.
- Always wire the digital input/output in pairs.
- The maximum permitted cable length is 30 m.

You can find additional information in the section "Terminals (Page 31)".

## Digital input

The 2-pin terminal block has the following assignment:




| Contact | Assignment |
|---|---|
| +DI | Input |
| -DI | Ground |

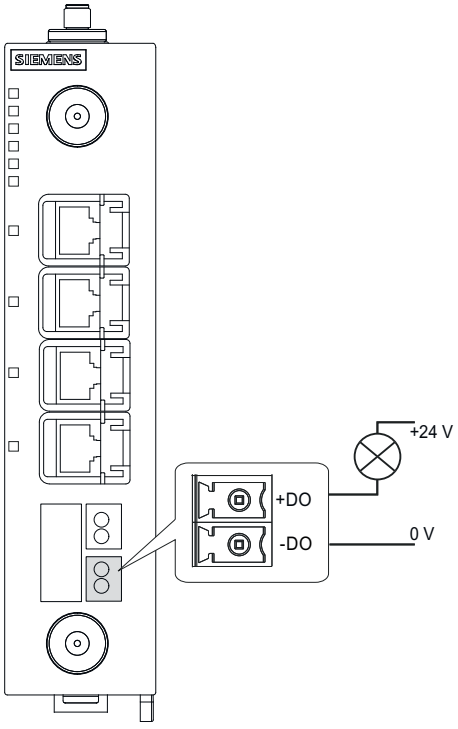
If there is an adequate switching voltage at the digital input, the digital input is active and the "DI" LED is lit.

The voltage applied to the "DI" contact is converted to a digital status by the device as follows:

| Voltage | Status |
|---|---|
| -30 to +3 V DC | 0 |
| +13 to +30 V DC | 1 |

## Digital output

The 2-pin terminal block has the following assignment:



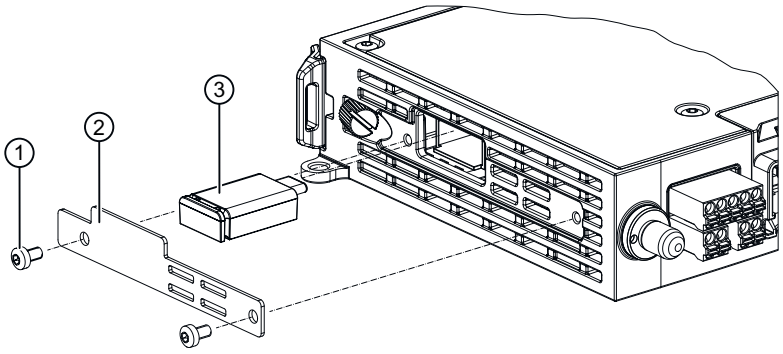

| Contact | Assignment |
|---|---|
| +DO | Switching signal<br>Relay 24 V DC / 0.5 A |
| -DO | Ground |

The output is a switch that switches the signal at +DO to -DO.

## 6.8 Replacing a CLP

### Position

The CLP slot is at the bottom of the device under a cover, see Reset button (Page 35).




① M3 screws (Torx T10)
② Slot cover
③ CLP

### Removing a CLP

**Note**

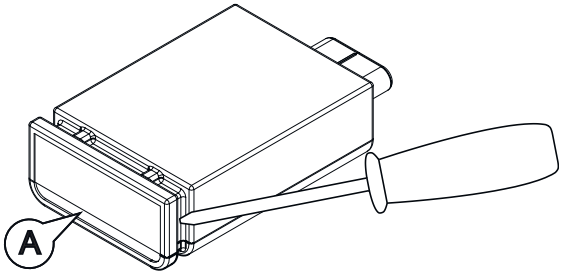
**Loss of the configuration**

The reset button is located directly beside the slot for the CLP. The reset button cannot be used to remove the CLP.

If you press and hold down the reset button you reset all the settings of the device to the factory defaults.

To remove a CLP from the device, follow the steps below:

1. Turn off the power to the device.
2. Loosen the screws M3 ① with a Torx screwdriver T10 and remove the slot cover ②.
3. To release the CLP ③, insert a screwdriver between the front edge of the CLP (A) and the slot.

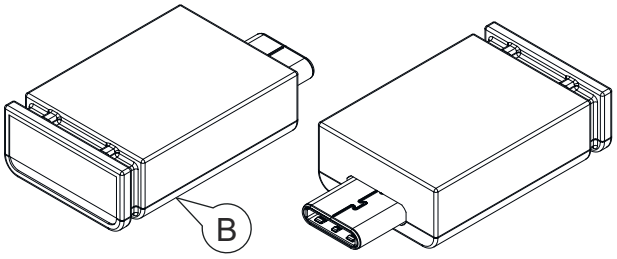


4. Remove the CLP from the slot.
5. Close the slot cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

### Inserting the CLP

To insert a CLP into the device, follow the steps below:

1. Turn off the power to the device.
2. Loosen the screws M3 ① with a Torx screwdriver T10 and remove the slot cover ②.
3. The housing of the CLP has a rounded underside (B). Accordingly, the slot opening has a rounded edge. Note this orientation when inserting the CLP.
   Insert the CLP ③ in the correct orientation into the slot.




4. Close the slot cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

# Troubleshooting

# 7

## 7.1 Downloading new firmware using TFTP without WBM and CLI

### Firmware

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

You can download new firmware to the device using TFTP. To do this, the device does not need to be reachable either using Web Based Management (WBM) or using the Command Line Interface (CLI). This can be the case if there was a power failure during a firmware update.

When pressing the button, make sure you adhere to the instructions in the section "Reset button (Page 35)".

To load a new firmware via TFTP, follow these steps:

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Press and hold down the reset button.
5. Connect the device to the power supply again while holding down the button.
6. Hold down the button until the red fault LED "F" starts to flash after approximately 2 seconds (500ms on/500ms off).
7. Release the button. The F-LED lights continuously red.
   The bootloader waits in this state for a new firmware file that you can download using TFTP.
8. Connect a PC to the device over the Ethernet interface.
9. Assign an IP address to the device using DHCP or the SINEC PNI.
10. Open a DOS box and change to the directory where the file with the new firmware is located and then execute the following command:
    `tftp -i <IP address> put <firmware file>`
    As an alternative, you can use a different TFTP client.
    Once the firmware has been transferred completely to the device, there is an automatic restart on the device. This process can take several minutes.
11. Close the cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

## 7.2 Restoring the factory settings

| NOTICE |
| --- |
| **Previous settings**<br>If you reset, all the settings you have made will be overwritten by factory defaults. |

| NOTICE |
| --- |
| **Inadvertent reset**<br>An inadvertent reset can cause disturbances and failures in a configured network with further consequences. |

### With the reset button

When pressing the button, make sure you adhere to the instructions in the section "Reset button (Page 35)".

To reset the device to the factory defaults during the startup phase, follow the steps below:

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Press the reset button and reconnect the device to the power supply while holding down the button.
5. Hold down the button until the red error LED "F" stops flashing after approximately 10 seconds and is permanently lit.
6. Release the button and wait until the fault LED "F" goes off.
   The device starts automatically with the factory settings.
7. Close the cover (torque 0.8 Nm) to ensure that the device maintains the degree of protection IP30.

### With SINEC PNI

Follow the steps below to reset the device parameters to the factory settings with the SINEC PNI:

1. Select the device whose parameters you want to reset.
2. Click the "Reset device" button.
3. Select the "Reset to factory settings" option in the following dialog.

### Via the configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals:

- Web Based Management, section "Restart"
- Command Line Interface, section "Reset and Defaults"

# Maintenance and cleaning

# 8

**WARNING**

**Unauthorized repair of devices in explosion-proof design**

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.
- For function checks, maintenance and servicing work, you need to observe the requirements on checking and maintaining plants in hazardous areas according to the standards EN / IEC 60079-17.

**WARNING**

**Impermissible accessories and spare parts**

Risk of explosion in hazardous areas

- Only use original accessories (Page 28) and original spare parts.
- Observe all relevant installation and safety instructions described in the manuals for the device or supplied with the accessories or spare parts.



**CAUTION**

**Hot surfaces**

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

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

**NOTICE**

**Cleaning the housing**

If the device is not in a hazardous area, only clean the outer parts of the housing with a dry cloth.

If the device is in a hazardous area, use a slightly damp cloth for cleaning.

Do not use solvents.

# Technical specifications

# 9

The following technical specifications apply to the following devices:

- SCALANCE MUM853-1 (Model MS5G15R-30-M1-RJ-E4-1)
- SCALANCE MUM853-1 (Model MS5G16R-30-M1-RJ-E4-1)
- SCALANCE MUM853-1 (Model MS5G16R-30-M1-RJ-E4-2)

| **Technical specifications** | | | |
|---|---|---|---|
| **Data transfer** | | | |
| Ethernet transfer rate | | | 10/100/1000 Mbps |
| Wireless transfer rate | 5 G | | • Downlink: up to 1000 Mbps<br>• Uplink: up to 500 Mbps |
| | LTE | | • Downlink: up to 1000 Mbps<br>• Uplink: up to 200 Mbps |
| | UMTS | | • Downlink: up to 42 Mbps<br>• Uplink: up to 5.76 Mbps |
| **Connection to Industrial Ethernet** | | | |
| | Quantity | | 4 |
| | Design | | RJ45 socket |
| | Properties | | Half duplex/full duplex, autocrossover, autonegotiation, autosensing, floating |
| **Permissible cable lengths (Ethernet)** | **Alternative combinations per length range** | | |
| | IE TP Torsion Cable | | 0 ... 55 m<br>0 ... 45 m + 10 m TP cord |
| | IE FC TP Marine Cable<br>IE FC TP Trailing Cable<br>IE FC TP Flexible Cable | | 0 ... 85 m<br>0 ... 75 m + 10 m TP cord |
| | IE FC TP Standard Cable | | 0 ... 100 m<br>0 ... 90 m + 10 m TP cord |
| **Radio interface** | | | |
| Device | Mobile wireless standard | Max. conducted power | |
| | | 23 dBm (200 mW) | 26 dBm (400 mW) Downlink only |

| **Technical specifications** | | | | |
|---|---|---|---|---|
| 6GK5853-2EA10-2AA1 (A1) | 5G NR | n1, n2, n3, n5, n7, n8, n20, n25, n28, n30, n38, n40, n41, n48, n66, n71, n77, n78, n79 | n41, n77, n78, n79 | n75 |
| | LTE | B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B30, B34, B38, B39, B40, B41, B42, B43, B48, B66, B71 | B41 | B29, B32, B46 |
| | WCDMA | B1, B2, B4, B5, B6, B8, B19 | - | - |
| 6GK5853-2EA10-2BA1 (B1) | 5G NR | n1, n3, n5, n8, n28, n41, n77, n78, n79 | n41, n77, n78, n79 | - |
| | LTE | B1, B3, B5, B8, B34, B38, B39, B40, B41 | - | - |
| | WCDMA | B1, B5, B8 | - | - |
| 6GK5853-2EA00-2DA1 | 5G NR | n1, n2, n3, n5, n7, n8, n12, n20, n28, n38, n40, n41, n48, n66, n71, n77, n78, n79 | - | - |
| | LTE | B1, B2, B3, B4, B5, B7, B8, B12, B13, B14, B17, B18, B19, B20, B25, B26, B28, B30, B34, B38, B39, B40, B41, B42, B43, B48, B66, B71 | - | B29, B32 |
| | WCDMA | B1, B2, B3, B4, B5, B8 | - | - |
| Antenna port | Quantity | | 4 | |
| | Design | | SMA female | |
| | Impedance | | 50 Ω nominal | |
| **Electrical data** | | | | |
| Direct 24 V DC supply | Supply voltage from socket | | 24 V DC Safety Extra Low Voltage (SELV) | |
| | Type of current | | ⎓ | |
| | Permissible range | ±30% | 16.8 to 31.2 V DC | |
| | Design | | Terminal block, 5-pin | |
| | Properties | | Not galvanically isolated | |
| Current consumption | 24 V DC/maximum | | 550 mA | |
| | 24 V DC Sleep Mode / maximum | | 12.5 mA | |
| Active power loss | 24 V DC/maximum | | 13.2 W | |
| | 24 V DC Sleep Mode / maximum | | 300 mW | |

| **Technical specifications** | | |
|---|---|---|
| Digital input | Quantity | 1 |
| | Design | Terminal block, 2-pin |
| | Status "0" | -30 to 3 V DC |
| | Status "1" | 10 ... 30 V DC |
| | Max. input current | 8 mA |
| | Max. cable length | < 30 m<br>Cables should be routed in pairs |
| | Properties | Input isolated from electronics |
| Digital output | Quantity | 1 |
| | Design | Terminal block, 2-pin |
| | Rated voltage | 24 V DC<br>safety extra-low voltage (SELV) |
| | Fuse | 0.5 A |
| | Max. cable length | < 30 m<br>Cables should be routed in pairs |
| | Properties | Output isolated from electronics |
| **Permissible ambient conditions** | | |
| Ambient temperature | During operation | -30 °C to +60 °C |
| | During storage | -40 °C to +85 °C |
| | During transportation | -40 °C to +85 °C |
| Relative humidity | During operation | ≤ 95% at 25 °C, no condensation |
| Operating altitude | During operation | ≤ 2000 m above sea level |
| Contaminant concentration | | According to ISA-S71.04.-2013 Class G3 |
| Degree of pollution | | 2 |
| Degree of protection | | IP30 |
| **Dimensions and weight** | | |
| Dimensions | W x H x D | 35 x 157 x 137 mm |
| Weight | | 0.68 kg |
| **Installation options** | | |
| | • Wall mounting<br>• Mounting on a DIN rail<br>– direct<br>– rotated by 90° with accessories<br>• Installation on S7-300 mounting rail<br>• Installation on S7-1500 mounting rail | |
| **Mean time between failure (MTBF)** | | |
| | at 40 °C ambient temperature | 26 years |
| **Product functions** | | |
| Configuration / management | • Web-based management (WBM) via HTTPS<br>• Command Line Interface (CLI) via SSH | |

| **Technical specifications** | |
|---|---|
| Security | • Router with NAT function<br>– IP masquerading<br>– NAPT<br>– SourceNAT<br>– NETMAP<br>• Password protection<br>• Firewall function<br>– Port forwarding<br>– IP firewall with stateful packet inspection (layer 3 and 4)<br>– Global and user-defined firewall rules<br>• VPN functions<br>To establish a VPN (Virtual Private Network), the following functions are available:<br>– Up to 20 connections<br>– IPsec VPN, OpenVPN (as client)<br>• SINEMA RC client<br>• Proxy server<br>• Siemens Remote Service (SRS) |

| **Technical specifications** | |
|---|---|
| Monitoring / diagnostics / maintenance | • LEDs<br>Display of operating statuses via the LED display<br>• Logging<br>For logging events<br>• SNMPv1/v2/v3<br>For monitoring and controlling network components<br>• Packet Capture<br>For network diagnostics via a connected PC |
| Other functions | • Time-of-day synchronization<br>– NTP client and NTP server<br>– Secure NTP server<br>– SIMATIC time client<br>– SNTP client<br>– GPS time<br>• DHCP<br>– DHCP server (internal network)<br>• Virtual networks (VLAN)<br>To structure Industrial Ethernet networks with a fast growing number of devices, a physical network can be divided into several virtual subnets<br>• Digital input/digital output<br>• Dynamic DNS client<br>• DNS client and DNS proxy<br>• SMTP client<br>• Location determination via GPS (not available with the 6GK5853-2EA10-2BA1 (B1) device variant)<br>• Geofencing<br>• eSIM<br>• Secure Boot |

# Dimension drawings

# 10

**Note**

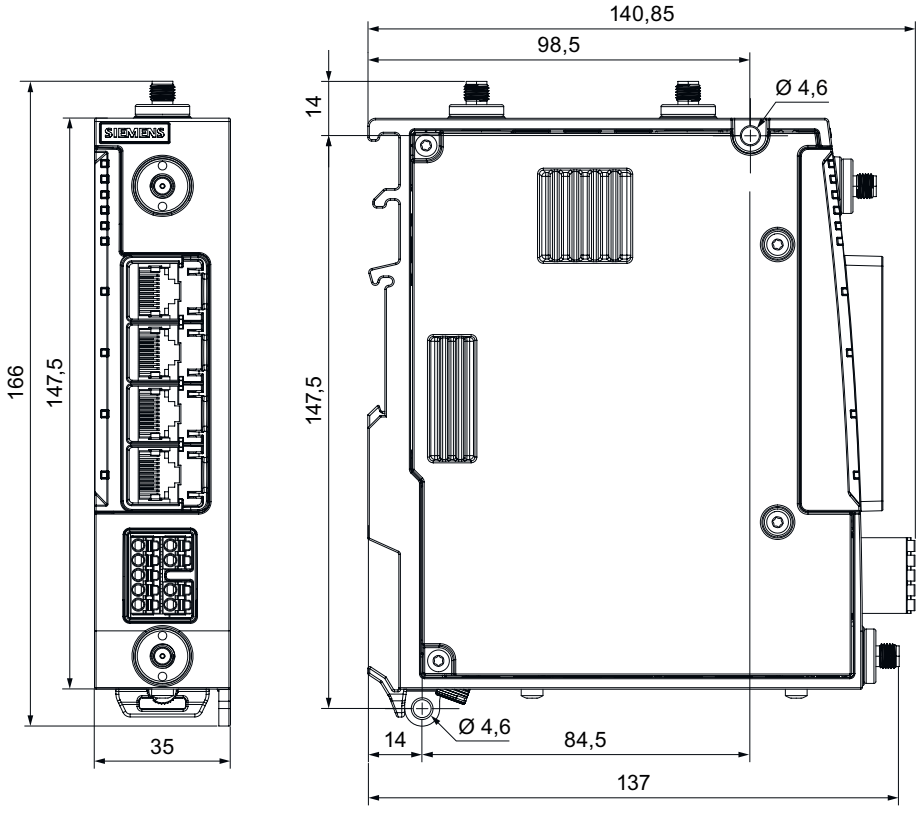
**CAx data**

You can find the CAx data on the Internet at (https://www.automation.siemens.com/bilddb/index.aspx?lang=en)

1. Click on the "CAx data" link in the "Direct Links" area.
   The Industry Image Database page is loaded.
2. Enter the name or article number of the product in the search filter.
   You can refine your search using the "Motif type" selection list.

**Note**

Dimensions are specified in mm.



# Approvals

# 11

## 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.

Approvals for shipbuilding are not printed on the device type plate.

## Current approvals on the Internet

You will find the current approvals for the product on the Internet pages of Siemens Industry Online Support at the following link: (https://support.industry.siemens.com/cs/ww/en/ps/15982/cert)

## National approvals

You can find an overview of the country-specific wireless approvals of SIMATIC NET devices on the Internet pages of Siemens Industry Online Support. You can find the link to the document on the following page

ik-Info (https://www.siemens.com/mobilenetwork-approvals)

## Installation guidelines

The devices meet the requirements if you adhere to the installation and safety instructions contained in this documentation and in the following documentation when installing and operating the devices.

- "Industrial Ethernet / PROFINET Industrial Ethernet" System Manual (https://support.industry.siemens.com/cs/ww/en/view/27069465)
- "Industrial Ethernet / PROFINET - Passive Network Components" System Manual (https://support.industry.siemens.com/cs/ww/en/view/84922825)
- "EMC Installation Guidelines" configuration manual (https://support.industry.siemens.com/cs/ww/en/view/60612658)

**⚠ WARNING**

**Personal injury and property damage can occur**

The installation of expansions that are not approved for products or their target systems may violate the requirements and regulations for safety and electromagnetic compatibility.

Only use expansions that are approved for the system.

**Note**

The test was performed with a device and a connected communications partner that also meets the requirements of the standards listed above.

When operating the device with a communications partner that does not comply with these standards, adherence to the corresponding values cannot be guaranteed.

## 11.1 EC declaration of conformity

CE

The EC Declaration of Conformity is available for all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76187 Karlsruhe
Germany

You can find the current EU declaration of conformity for these products on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15982/cert).

The products described in this document meet the requirements of the following EC directives:

- RoHS directive 2011/65/EU
  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 EU L174, 01/07/2011, pages 88-110
- Radio equipment directive 2014/53/EU (RED, Radio Equipment Directive)
  Directive of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment; official journal of the EU L153, 22/05/2014, pages 62-106

| | |
|---|---|
| Name, address and identification number of the notified body: | American Certification Body, Inc.<br>6731 Whittier Avenue, Suite C110<br>McLean, VA 22101<br>USA<br>1588 |
| Number of the EU type examination certificate: | ATCB031204 (6GK5853-2EA10-2AA1) |

### 11.1.1 RoHS

**RoHS directive (restriction of the use of certain hazardous substances)**

The SIMATIC NET products described in these operating instructions meet the requirements of the EC directive 2011/65/EC for the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Applied standard:

- EN IEC 63000
  Technical documentation for the assessment of electrical and electronic products with respect to restriction of hazardous substances

### 11.1.2 RED

#### 11.1.2.1 Protection of health and safety

- EN IEC 62368-1
  Equipment for audio, video, information and communication technology - Part 1: Safety requirements
- EN IEC 62311
  Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz – 300 GHz)

#### 11.1.2.2 EMC

- ETSI EN 301 489-1
  Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 1: Common technical requirements
- ETSI EN 301 489-52
  Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 52: Specific conditions for cellular communication mobile and portable (UE) radio and ancillary equipment
- EN 55011
  Industrial, scientific and medical (ISM) radio-frequency equipment – Electromagnetic disturbance characteristics – Limits and methods of measurement
- EN 55032
  Electromagnetic compatibility of multimedia equipment – Emission requirements
- EN 55035
  Electromagnetic compatibility of multimedia equipment - Immunity requirements
- EN IEC 61000-6-1
  Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments

- EN IEC 61000-6-2
  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN IEC 61000-6-3
  Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments
- EN IEC 61000-6-4
  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
- EN IEC 61000-6-8
  Electromagnetic compatibility (EMC) - Part 6-8: Generic standards - Emission standard for professional equipment in commercial and light-industrial locations

#### 11.1.2.3 Efficient use of the radio spectrum

- ETSI EN 301 908-1
  IMT cellular networks - Harmonized standard for access to radio spectrum - Part 1: Introduction and common requirements for Release 15
- ETSI EN 301 908-2
  IMT cellular networks - Harmonized standard for access to radio spectrum - Part 2: CDMA Direct Spread (UTRA FDD) User Equipment (UE)
- ETSI EN 301 908-13
  IMT cellular networks - Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive - Part 13: Further developed universal terrestrial wireless access (E-UTRA) end devices (UE)
- ETSI EN 301 908-25
  IMT cellular networks - Harmonised Standard for access to radio spectrum - Part 25: New Radio (NR) User Equipment (UE) Release 15
- ETSI EN 303 413
  Satellite Earth Stations and Systems (SES) - Global Navigation Satellite System - Radios for operation in the frequency bands from 1164 MHz to 1300 MHz and from 1559 MHz to 1610 MHz

### 11.1.3 Other technical standards

- CISPR 11
  Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement
- CISPR 32
  Electromagnetic compatibility of multimedia equipment - Emission requirements
- CISPR 35
  Electromagnetic compatibility of multimedia equipment - Immunity requirements
- NAMUR NE21
  Automation engineering of modular systems in the process industry - Modelling of module services

## 11.2 UK Declaration of Conformity

The UK declaration of conformity is available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76187 Karlsruhe
Germany

**Importer UK:**
Siemens plc,
Manchester M20 2UR
United Kingdom

You can find the current UK Declaration of Conformity for these products on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15982/cert).

The SIMATIC NET product described in these operating instructions meets the requirements of the following directives:

- RoHS Regulation
  SI 2012/3032 Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments
- Radio Equipment Regulation
  SI 2017/1206 The Radio Equipment Regulations 2017

### 11.2.1 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012

#### Restriction of the use of certain hazardous substances

The SIMATIC NET products described in these operating instructions meet the requirements of "The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012".

Applied standard:

- EN IEC 63000
  Technical documentation for the assessment of electrical and electronic products with respect to restriction of hazardous substances

## 11.2.2 The Radio Equipment Regulations 2017

### 11.2.2.1 Protection of health and safety

- EN IEC 62368-1
  Equipment for audio, video, information and communication technology - Part 1: Safety requirements
- EN IEC 62311
  Assessment of electronic and electrical equipment related to human exposure restrictions for electromagnetic fields (0 Hz – 300 GHz)

### 11.2.2.2 EMC

- ETSI EN 301 489-1
  Electromagnetic compatibility and radio spectrum matters (ERM) - Electromagnetic compatibility for radio equipment and services - Part 1: Common technical requirements
- ETSI EN 301 489-52
  Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 52: Specific conditions for cellular communication mobile and portable (UE) radio and ancillary equipment
- EN 55011
  Industrial, scientific and medical (ISM) radio-frequency equipment – Electromagnetic disturbance characteristics – Limits and methods of measurement
- EN 55032
  Electromagnetic compatibility of multimedia equipment – Emission requirements
- EN 55035
  Electromagnetic compatibility of multimedia equipment - Immunity requirements
- EN IEC 61000-6-1
  Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments
- EN IEC 61000-6-2
  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN IEC 61000-6-3
  Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments
- EN IEC 61000-6-4
  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments
- EN IEC 61000-6-8
  Electromagnetic compatibility (EMC) - Part 6-8: Generic standards - Emission standard for professional equipment in commercial and light-industrial locations

#### 11.2.2.3 Efficient use of the radio spectrum

- ETSI EN 301 908-1
  IMT cellular networks - Harmonized standard for access to radio spectrum - Part 1: Introduction and common requirements for Release 15
- ETSI EN 301 908-2
  IMT cellular networks - Harmonized standard for access to radio spectrum - Part 2: CDMA Direct Spread (UTRA FDD) User Equipment (UE)
- ETSI EN 301 908-13
  IMT cellular networks - Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive - Part 13: Further developed universal terrestrial wireless access (E-UTRA) end devices (UE)
- ETSI EN 301 908-25
  IMT cellular networks - Harmonised Standard for access to radio spectrum - Part 25: New Radio (NR) User Equipment (UE) Release 15
- ETSI EN 303 413
  Satellite Earth Stations and Systems (SES) - Global Navigation Satellite System - Radios for operation in the frequency bands from 1164 MHz to 1300 MHz and from 1559 MHz to 1610 MHz

### 11.2.3 Other technical standards

- CISPR 11
  Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement
- CISPR 32
  Electromagnetic compatibility of multimedia equipment - Emission requirements
- CISPR 35
  Electromagnetic compatibility of multimedia equipment - Immunity requirements
- NAMUR NE21
  Automation engineering of modular systems in the process industry - Modelling of module services

## 11.3 Supplier's declaration of conformity



The RCM declaration of conformity is available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76187 Karlsruhe
Germany

You can find the current Supplier's declaration of conformity for these products on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15982/cert)

As required by the following Notices:

- Radiocommunications (Compliance Labelling - Devices) Notice 2014 made under section 182 of the Radiocommunications Act 1992;
- Radiocommunications Labelling (Electromagnetic Compatibility) Notice 2017 made under section 182 of the Radiocommunications Act 1992
- Radiocommunications (Compliance Labelling – Electromagnetic Radiation) Notice 2014 made under section 182 of the Radiocommunications Act 1992
- Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015 made under section 407 of the Telecommunications Act 1997.

### Including the standard

- ETSI EN 301 489-1
- ETSI EN 301 489-19
- ETSI EN 301 489-52
- ETSI EN 301 908-13
- ETSI EN 301 908-25
- ETSI EN 303 413

## 11.4 General 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.

Approvals for shipbuilding are not printed on the device type plate.

### FM




The product meets the requirements of the standards:

- FM Class 3600, FM Class 3611, FM Class 3810
- ANSI/UL 121201, ANSI/UL 61010-1
- FM Hazardous (Classified) Location Electrical Equipment:
  Non Incendive / Class I / Division 2 / Groups A,B,C,D / T4 and
  Non Incendive / Class I / Zone 2 / Group IIC / T4

You can find the temperature class on the nameplate of the product. The permissible temperature range of the product is -30 °C to +60 °C.

### cULus Approval for Information Technology Equipment




cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

- UL 62368-1
- CSA C22.2 No. 62368-1

Report no. E115352

### cULus approval for industrial control equipment




cULus Listed PROG-CNTLR.

Underwriters Laboratories Inc. complying with

- UL 61010-1
- UL 61010-2-201
- CSA C22.2 NO 61010-1
- CSA C22.2 NO 61010-2-201

Report no. E85972

### cULus Approval Hazardous Location




cULus Listed I. T. E. FOR HAZ. LOC.

Underwriters Laboratories Inc. complying with

- UL 121201 (Non Incendive electrical equipment) approved for use in Class I, Division 2, Groups A, B, C, D, T4.
- UL CSA C22.2 NO 213 (Non Incendive electrical equipment) approved for use in Class I, Zone 2, Group IIC, T4.

### Marking for the customs union



EAC (Eurasian Conformity)

Eurasian Economic Union of Russia, Belarus, Armenia, Kazakhstan and Kyrgyzstan

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

## 11.5 Country-specific notes

### 11.5.1 Note for Australia and New Zealand

#### RCM (C-Tick)

Australian Communications and Media Authority, for compliance levels 1, 2 and 3 in Australia and levels of conformity 1, 2 and 3 in New Zealand. As required by notices under:

- Section 182 of the Australian Radiocommunications Act 1992
- Section 407 of the Australian Telecommunications Act 1997
- Section 134 of the New Zealand Radiocommunications Act 1989
- Radiocommunications (Compliance Labelling - Devices) Notice 2014 made under section 182 of the Radiocommunications Act 1992
- Radiocommunications Labelling (Electromagnetic Compatibility) Notice 2008 made under section 182 of the Radiocommunications Act 1992
- Radiocommunications (Compliance Labelling – Electromagnetic Radiation) Notice 2014 made under section 182 of the Radiocommunications Act 1992 and
- Telecommunications (Labelling Notice for Customer Equipment and Customer Cabling) Instrument 2015 made under section 407 of the Telecommunications Act 1997

You can find the current declaration of conformity for these products on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15914/cert)

The SIMATIC NET products described in this document meet the requirements of the standards designated under Product:

| | |
|---|---|
| 1a | EN 60950-1 |
| 1b | EN 60950-1 + A11 + A1 + a12 |
| 2 | ETSI EN 301 489-1 |
| 3 | ETSI EN 301 489-7 |
| 4 | ETSI EN 301 489-24 |
| 5 | ETSI EN 301 489-52 |
| 6 | ETSI EN 301 511 |
| 7 | ETSI EN 301 908-1 |
| 8 | ETSI EN 301 908-13 |

9 1999/519/EC
10 EN 62311
11 FCC part 22
12 FCC part 24
13 FCC part 27
14 AS/CA S042.1
15 AS/ACIF S042.3
16 AS/CA S042.4
17 AS/NZS 60950.1 + Amdt

**Products**

| Product name | Standards | |
|---|---|---|
| | Australia | New Zealand |
| SCALANCE MUM853-1 | -- | -- |

## 11.5.2 Note for Brazil

**Brazil**

Para maiores informações, consulte o site da ANATEL – www.anatel.gov.br

## 11.5.3 Notes for Mexico

Este equipo NO cuenta con la tecnología VoLTE incorporada.

**Instrucciones para localizar el IMEI**

Usted podrá visualizar el IMEI del equipo en su respectiva etiqueta exterior.

## 11.5.4 Notes for the United States (FCC approval)

**FCC Part 15**

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy.

If not installed and used in accordance with the instructions, this may cause harmful interference to wireless communications. There can be no guarantee, however, with certain

installations, even when complying with the instructions, that no interference will be caused. If this equipment does cause harmful interference to radio or television reception that can be determined by turning the equipment off and on, the user is recommended to try to combat the interference with the following measures.

- Change the orientation of the receiving antenna or install it at a different location.
- Increase the distance between the SCALANCE M and the radio or television receiver.
- Connect the device to an outlet on a circuit different from that to which the receiver is connected.
- Consult a dealer / installer or an experienced radio / TV technician.

### FCC Part 15.19

This device complies with Part 15 of the FCC Rules. Operation is subject to the following conditions:

- This device must not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

### FCC Part 15.21

Modifications to the device not expressly approved by the manufacturer could void the user's right to operate the equipment.

The SCALANCE M may only be used with an antenna from the range of accessories of the SCALANCE M.

The installation of the SCALANCE M and the antenna as well as servicing must be performed by qualified technical personnel only. When servicing the antenna, or working at distances closer than those listed below, make sure that the device has been turned off.

This device contains GSM, GPRS Class 12, EGPRS Class 10, and UMTS functions in the 900 and 1800 MHz band that must not be used in territories of the USA.

This device can be used for mobile and fixed applications. The internal/external antennas used with this device must be at least 26 cm away from people and must be positioned or operated in such a way that they work in conjunction with another antenna or transmitter.

Users and installers must be provided with antenna installation instructions and transmitter operating conditions that must be followed to avoid exceeding the permitted RF exposure.

Antennas for the transmitter module used must not exceed the following antenna gains in operating configurations for mobile and fixed applications, see Maximum antenna gain.

This device is approved as a module for installation in other devices.

### Conformity with FCC

The FCC approval applies to the following SCALANCE device:

| Product | FCC ID |
|---|---|
| SCALANCE MUM853-1 | RI7FN990A28 |

# Index


## A

Accessories, 28
Antennas, 62
Article numbers, 7

## B

Button
  Reset, 35

## C

Cables
  Permissible lengths, 79, 80, 81, 82, 83
CAx data, 85
CLP, 36
  Function, 37
  Replacing, 71
Configuration manuals, 8, 75
Connecting
  Antennas, 62
  Digital input, 69
  Digital output, 70
  Ethernet, 59
  Grounding, 67
  Power supply, 31, 58

## D

Device view, 26
Digital input, 69
Digital output, 70
Dimension drawing, 85
DIN rail, 46
Documentation on the Internet, 8
Drilling template, 44

## E

Ethernet
  Connectors, 59

## F

Factory defaults, 74
Factory setting, 74

## G

Grounding, 67

## I

Installation
  DIN rail, 46
  S7-1500 mounting rail, 51
  S7-300 mounting rail, 50
  Wall mounting, 44
Interfaces, 79, 80, 81, 82, 83

## L

LED display, 33, 34, 35

## M

Model, 7

## P

Pin assignment, 60
PLUG, 36
  Function, 37
  Replacing, 71
Power supply, 31, 58
Product property, 25

## R

Reset button, 35
Reset device, 74

## S

S7-1500 mounting rail, 51
S7-300 mounting rail, 50

Safety notices
for installation, 39
general, 13
Use in hazardous areas, 13, 39, 53, 54
when connecting up, 53, 54
Scope of delivery, 27
Scope of validity, 7
Signal quality, 64
SIM card, 65, 66
System manual, 87

## T

Technical specifications, 79, 80, 81, 82, 83
Terminals, 31
Type designations, 25

## W

Wall mounting, 44
Wiring, 32