SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE XF-200G

Operating Instructions

Introduction

Safety notices 1

Security recommendations 2

Description of the device 3

Installing and removing 4

Connecting up 5

Maintenance and cleaning 6

Error correction 7

Technical specifications 8

Dimension drawings 9

Approvals A

03/2024
C79000-G8976-C676-02

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

C79000-G8976-C676-02
Ⓟ 02/2024 Subject to change

Copyright © Siemens 2023 - 2024.
All rights reserved

Introduction

Purpose of the operating instructions

These operating instructions will help you to install and connect devices of the SCALANCE XF-200G. product group.

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

Scope of validity of the operating instructions

These operating instructions apply to the following devices:

- SCALANCE XF204G

Unless mentioned otherwise, the descriptions in these operating instructions refer to all devices of the SCALANCE XF-200G product group specified in the scope of validity.

Designations used

Classification	Description	Terms used
Product line	The product line includes all devices and variants of all product groups. If information applies to all product groups within the product line, the term SCALANCE X-200 is used.	SCALANCE X-200
Product group	If information applies to all devices and versions of a product group, the term SCALANCE XF-200G is used.	SCALANCE XF-200G
Device	If information relates to a specific device, the device name is used.	e.g. SCALANCE XF204G

Documentation on configuration

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

- SCALANCE Layer 2 Switches Web Based Management (WBM) Vx.x
- SCALANCE Layer 2 Switches Command Line Interface (CLI) Vx.x

You will find the configuration manuals here:

- on the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15291/man).

Further documentation

System manuals for SIMATIC NET products

In the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components", you will find 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 partners that you require for the installation.

You will find the system manuals here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support under the following entry IDs:
  - 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)

Manual Collection "Distributed I/O System ET 200SP"

In the reference manual for the scalable IO system ET 200SP you will find more information on the bus adapters.

You will find the reference manual on the Internet pages of Siemens Industry Online Support:

- SIMATIC ET 200SP Manual Collection (https://support.industry.siemens.com/cs/ww/en/view/84133942)

SIMATIC NET manuals

You will find the SIMATIC NET manuals here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15247).

Supplementary documentation

In addition, note the operating instructions for the Extension Unit box.

You can find the supplementary documentation on the Internet pages of Siemens Industry Online Support.

- Extension Unit box (https://support.industry.siemens.com/cs/ww/en/ps/21639/man)

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection or product DVD
  The DVD ships with certain SIMATIC NET products.
- On the Internet under the following address:
  50305045 (https://support.industry.siemens.com/cs/ww/en/view/50305045)

Cybersecurity notes

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/industrialsecurity).

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

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.

Catalogs

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

- SIMATIC NET Industrial Communication / Industrial Identification, catalog IK PI
- SIMATIC Products for Totally Integrated Automation and Micro Automation, catalog ST 70
- Industry Mall - catalog and ordering system for automation and drive technology, Online catalog (https://mall.industry.siemens.com/goos/WelcomePage.aspx?regionUrl=/de&language=en)

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

Device defective

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

Decommissioning

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

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

Also restore the factory settings on the storage medium.

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.

Trademarks

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

SCALANCE, C-PLUG, OLM

Table of contents

Introduction **3**

1 Safety notices **9**

2 Security recommendations **11**

3 Description of the device **19**

3.1 Product overview 19
3.1.1 Accessories 20
3.1.2 Spare parts 21

3.2 Device view 22

3.3 RESET button 22

3.4 LED display 25
3.4.1 Fault LED "F" 25
3.4.2 "RM" LED 26
3.4.3 LED "L" 26
3.4.4 Port LEDs "P" 26

3.5 C-PLUG 27
3.5.1 Function of the C-PLUG 27
3.5.2 Replacing the C-PLUG 28

4 Installing and removing **31**

4.1 Safety during mounting 31

4.2 Information on mounting 34

4.3 Installing in an Extension unit box 35

4.4 Mounting on DIN rails 39

4.5 Uninstalling 42

5 Connecting up **43**

5.1 Safety when connecting up 43

5.2 Industrial Ethernet 48
5.2.1 Electrical 48

5.3 Wiring rules 50

5.4 Power supply 50

5.5 Serial interface 52

5.6 Grounding 54

6 Maintenance and cleaning **55**

7 Error correction **57**

7.1 Downloading new firmware using TFTP without WBM and CLI 57

7.2 Restoring the factory settings ... 58
8 Technical specifications ... 59
8.1 Technical specifications of SCALANCE XF204G ... 59
8.2 Cable lengths ... 60
8.3 Switching properties ... 60
8.4 Mechanical stability (in operation) ... 61
9 Dimension drawings ... 63
9.1 Dimension drawing XF-200G ... 63
A Approvals ... 65
Index ... 71

Safety notices

1

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".

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING
EXPLOSION HAZARD
Do not open the device when the supply voltage is turned on.

Safety notices when using the device according to Hazardous Locations (HazLoc)

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

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

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

Security recommendations

2

NOTICE
Information security Connect to the device and change the standard password for the user set in the factory "admin" and "" before you operate the device.

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

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 (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- 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).
- Separate connections correctly (WBM, SSH etc.).
- 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.

Physical access

- Restrict physical access to the device to qualified personnel because the plug-in data medium can contain sensitive data.
- Lock unused physical interfaces on the device. Unused interfaces can be used to gain access to the plant without permission.

Software (security functions)

- Keep the firmware up to date. Check regularly for security updates for the device. You can find information on this at the Industrial Security (https://www.siemens.com/industrialsecurity) website.
- Inform yourself regularly about security recommendations published by Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm).
- Only activate protocols that you require to use the device.
- Restrict access to the management of the device with rules in an access control list (ACL).
- The option of VLAN structuring provides protection against DoS attacks and unauthorized access. Check whether this is practical or useful in your environment.
- Use a central logging server to log changes and accesses. Operate your logging server within the protected network area and check the logging information regularly.

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.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 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 passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- 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.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. 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.

Certificates and keys

- The device contains a pre-installed X.509 certificate with key. Replace this certificate with a self-made certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use the certification authority including key revocation and management to sign the certificates.
- 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.
- Use password-protected certificates in the format "PKCS #12".
- Use certificates with a key length of 4096 bits.
- 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, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Secure/non-secure protocols and services

- Avoid or disable non-secure protocols and services, for example HTTP, Telnet and TFTP. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Check whether use of the following protocols and services is necessary:
  - Non authenticated and unencrypted ports
  - HTTP
  - Telnet
  - SNMPv1/v2c
  - NTP
  - MRP, HRP, STP, RSTP and MSTP
  - IGMP snooping
  - LLDP
  - DCP
  - Syslog
  - DHCP Options 66/67
  - TFTP
  - GMRP and GVRP

- The following protocols provide secure alternatives:
  - HTTP → HTTPS
  - Telnet → SSH
  - SNMPv1/v2c → SNMPv3
    Check whether use of SNMPv1/v2c. is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The device provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use the authentication and encryption mechanisms of SNMPv3.
  - TFTP → SFTP
  - NTP → NTPsecure
- Use secure protocols when access to the device is not prevented by physical protection measures.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- If you use RADIUS for management access to the device, activate secure protocols and services.

Interfaces security

- Disable unused interfaces.
- Use IEEE 802.1X for interface authentication.
- Use the function "Locked Ports" to block interfaces for unknown nodes.
- Use the configuration options of the interfaces, e.g. the "Edge Type".
- Configure the receive ports so that they discard all untagged frames ("Tagged Frames Only").

Available protocols

The following list provides you with an overview of the open protocol ports.

The table includes the following columns:

- **Protocol**
- **Port**
- **Default port status**
  - Open
    The factory setting of the port is "Open".
  - Closed
    The factory setting of the port is "Closed".

- **Configurable port**
  - ✓
    The port status can be changed.
  - --
    The port status cannot be changed.
- **Authentication**
  Specifies whether the communication partner is authenticated.
- **Encryption**
  Specifies whether or not the transfer is encrypted.

List of available services

Note

Packet filtering

Packets are processed according to their importance for the operation of the network. Some packets directed to the CPUs of the switch may be discarded due to various security-relevant packet filters. Therefore, it can occur that not all ICMP packets are delivered to the CPUs, for example, and are thus not responded to.

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

The table includes the following columns:

- **Service**
  The services that the device supports
- **Default port status**
  This is the status of the port in the delivery state (factory setting).
- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.
- **Authentication**
  Specifies whether the communication partner is authenticated.
  If optional, the authentication can be configured as required.
- **Encryption**
  Specifies whether the transfer is encrypted.
  If optional, the encryption can be configured as required.

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

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [5)]
			Port	Service		
DHCPv4 Server	UDP/67	Closed	-	✓	-	-
DHCPv4 Client	UDP/68	Open	-	✓	-	-

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [5]
			Port	Service		
EtherNet/IP	TCP/44818 UDP/2222 UDP/44818	Closed (Open with EtherNetIP variants)	-	✓	-	-
HTTP Server/Client [3]	TCP/80	Closed	✓	✓	✓	-
HTTPS WBM Server/ Client	TCP/443	Open	✓	✓	✓	✓
NTP Client	UDP/123	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Closed	✓	✓	✓	-
PROFINET	UDP/34964 UDP/49151 ... 49159 [1]	Open	-	✓	-	-
RADIUS Client	UPD/1812 [4] UPD/1813 [4]	Outbound only	✓	✓	-	-
	UDP/3799	Open	✓	✓	-	-
SFTP Server	UDP/22	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	-	-
SMTP Client (secure)	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c [2] [3]	UDP/161	Open	✓	✓	-	-
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outbound only	-	✓	-	-
SNTP Client	UDP/123	Closed	✓	✓	-	-
SSH CLI Server	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	-	-
Syslog (secure) Client	TCP/6514	Closed	✓	✓	-	✓
Telnet [3]	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outbound only	✓	✓	-	-

1) Port number can be configured via the WBM.

2) Read-only access only.

3) Protocol according to Security by Default.

4) The port is closed by default and is displayed when a RADIUS server is configured. Port number can be configured via the WBM.

5) You can find additional information on the encryption methods used in the WBM appendix "Ciphers used".

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**	**Service configurable**
DCP	Setup mode [1)]	✓
LLDP	Open	✓
RSTP	Closed	✓
MSTP	Open	✓

1) Setting according to Security by Default.

Description of the device

3

3.1 Product overview

Article numbers

Device	Description	Article number
SCALANCE XF204G	4 x 10/100/1000 Mbps ports, PROFINET device	6GK5 204-0GA00-1UF2

Factory settings

- Industrial Ethernet protocol: PROFINET
- Base bridge mode: 802.1D transparent bridge
- Redundancy mechanism: Ring redundancy
- Trust mode: Trust CoS
- IGMP Snooping/IGMP Querier: Off
- IPv4 Address Collision Detection: Never give up

Ring ports

The factory setting defines the following ring ports:

- Ports P1.1 and P2.1

Scope of delivery

The following components are supplied with the device:

- One device
- One 2-pin plug-in terminal block (power supply)
- One product DVD with documentation and software

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
- Damage to the device and other components

Use only undamaged parts.

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

3.1.1 Accessories

The following accessories are available for the devices mentioned in the scope of validity:

Cable

Component	Description	Article number
Connecting cable (RJ-11/RS-232)	Preassembled, serial cable with RJ-11 and RS-232 plug, Length: 3 m pack of 1	6GK5 980-3BB00-0AA5

C-PLUG

Component	Description	Article number
C-PLUG	Configuration plug, exchangeable storage medium for configuration data, 32 MB	6GK1 900-0AB00
	Configuration plug, exchangeable storage medium for configuration data, 256 MB	6GK1 900-0AB10

Mounting plate

Component	Description	Article number
Mounting plate Extension unit box	Mounting plate for mounting in an Extension unit box Including grounding screw Pack of 1	6GK5 980-2HA10-0AA1
Mounting plate, DIN rail	Mounting plate for installation on a DIN rail Including grounding screw Pack of 1	6GK5 980-2HA00-0AA1

3.1.2 Spare parts

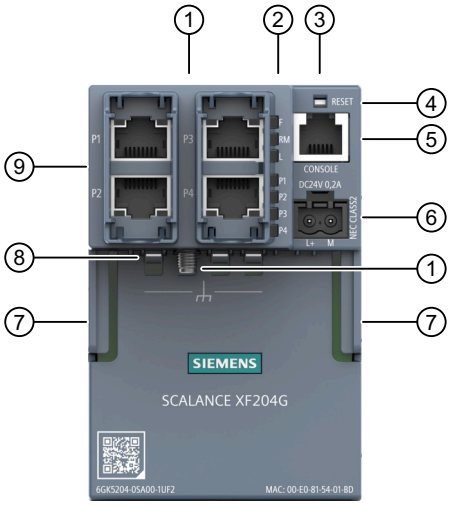
The following spare parts are available for the devices mentioned in the scope of validity:

Terminal block, 2-pin

Component	Description	Article number
2-pin spring-loaded terminal block	2-pin spring-loaded terminal block for connecting the 24 V DC power supply Pack of 5	6GK5980-0BB10-0AA5

3.2 Device view

The following figure shows an overview of the components of the SCALANCE XF-200G.



① Mounting screw
- M4
- Torx T20
- Captive

② LED display
- F: Fault LED
- RM: redundancy manager
- L: Power LED, power supply
- P: Port LEDs

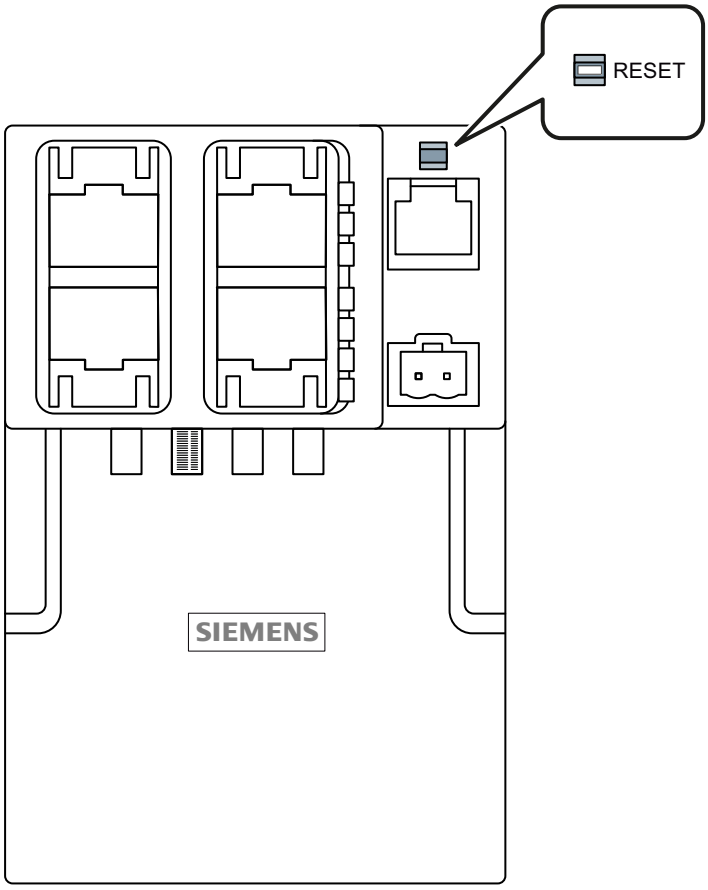
③ Slot for C-PLUG
④ RESET button
⑤ Serial interface
⑥ Connector for power supply
⑦ Guide for mounting plates
⑧ Ground springs (grounding)
⑨ Electrical ports

3.3 RESET button

WARNING
EXPLOSION HAZARD
Do not press the RESET button if there is a potentially explosive atmosphere.

Position

The "RESET" button is located on the front of the device.



Resetting the device to factory defaults

NOTICE
Previous settings If you reset, all the settings you have made will be overwritten by factory defaults.

NOTICE
Inadvertent reset An inadvertent reset can cause disturbances and failures with further consequences in the configured network.

Note

Damage to the button

The RESET button is a short-stroke button with only a slight pressure point. To operate the button, you only need a force 2.5 N (approx. 250 g).

To avoid damaging the button press it with little force. Hold the tool you are using, for example, with only two fingers.

Requirement

- The device is in operation.
- The function "Restore factory defaults" is enabled for the RESET button.

  Note

  Reset despite disabled "RESET" button

  If you have disabled the "Restore factory defaults"function for the "RESET" button in the configuration, this does not apply during the startup phase, see section "Restoring the factory settings (Page 58)"

  If the function has been disabled in the configuration, it is only disabled on completion of the startup phase.

Procedure

To restore the device to the factory defaults during operation, follow the steps below:

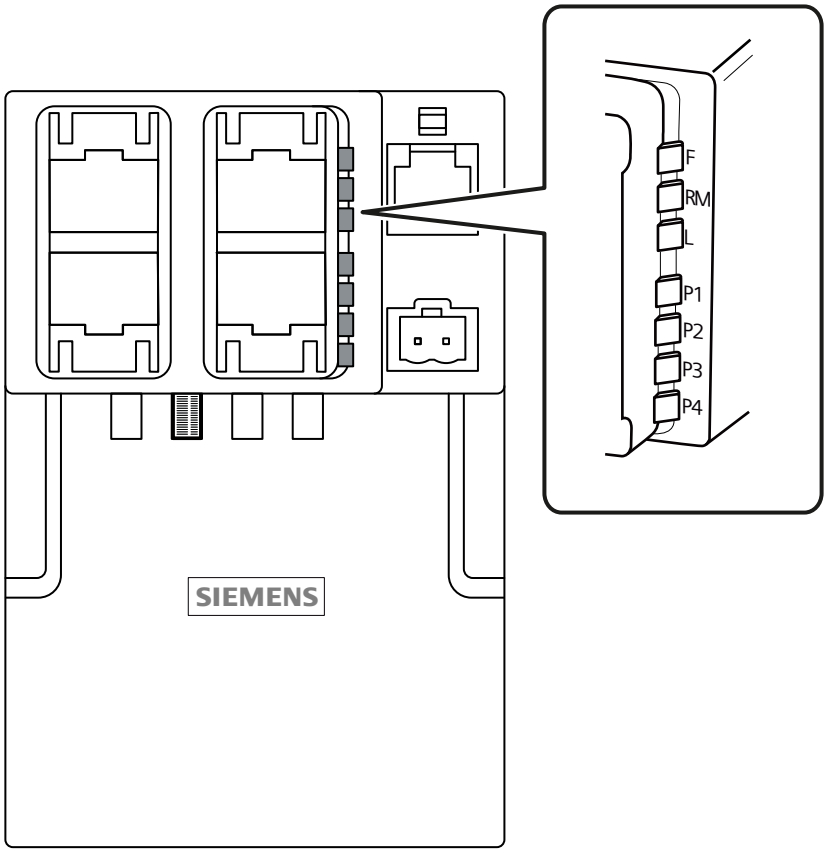
1. Press the "RESET" button with only slight force.
   A screwdriver for example with following size is suitable:
   - Blade thickness 0.8 - 1.8 mm
   - Blade width 4.0 - 4.8 mm
2. Hold down the button for approximately 12 seconds.
   After 9 seconds, the fault LED "F" flashes for 3 seconds.
   - If you release the button after approximately 12 seconds, the device is restarted and the factory settings are restored.
   - If you release the button before the 12 seconds have elapsed, the reset is canceled.

Enabling and disabling the button

In the configuration, you can enable or disable the button function.

3.4 LED display

The following figure shows the arrangement of the LEDs:



3.4.1 Fault LED "F"

The fault LED "F" indicates the incorrect functioning of the device.

LED color	LED status	Meaning
-	Off	The device is switched off or has not detected a problem.
Red	Lit	The device has detected a problem. Using the WBM and CLI, you can set when the device signals an error and which errors should be signaled.

3.4.2 "RM" LED

The "RM" LED indicates whether the device has the Media Redundancy Manager (MRM) role and whether the MRP ring is operating error-free.

LED color	LED status	Meaning
-	Off	The device is not an MRM.
Green	On	The device has the MRM role. The MRP ring is in normal state. The MRM has blocked data traffic on one of its ring ports and is monitoring the MRP ring.
Green	Flashing	The device has the MRM role. The MRP ring is in error state. The MRM has detected an error in the MRP ring or at one of its ring ports and activates an alternative communication path.

3.4.3 LED "L"

The "L" LED shows whether the power supply is connected.

LED color	LED status	Meaning
Green	Lit	The power supply is connected.
-	Off	No external power supply is connected.

3.4.4 Port LEDs "P"

The port LEDs indicate the status of the ports.

LED color	LED status	Meaning
Green	Lit	Link exists
Yellow	Flashing	Link exists and there is data transmission at the port
-	Off	No link exists

3.5 C-PLUG

3.5.1 Function of the C-PLUG

NOTICE
Do not remove or insert a C-PLUG during operation
A C-PLUG may only be removed or inserted when the device is turned off.

A C-PLUG is an exchangeable storage medium for storing the configuration data of the device. This allows fast and uncomplicated replacement of a device. The C-PLUG is taken from the previous device and inserted in the new device. The first time it is started up, the replacement device has the same configuration as the previous device except for the device-specific MAC address set by the vendor. A C-PLUG stores the current information about the configuration of a device.

A C-PLUG can be used to save the firmware. You will find more information under "System > PLUG".

Note

The device can also be operated without a C-PLUG.

How it works

Operating mode

In terms of the C-PLUG, there are three modes for the device:

- Without C-PLUG
  The device stores the configuration in internal memory.
  This mode is active if no C-PLUG is inserted.
- With unwritten C-PLUG
  If an unwritten C-PLUG (factory status or deleted with Clean function) is used, the local configuration already existing on the device is automatically stored on the inserted C-PLUG during startup.
  This mode is active as soon as an unwritten C-PLUG is inserted.
- With written C-PLUG
  A device with a written and accepted C-PLUG uses the configuration data of the C-PLUG automatically when it starts up. The requirement for acceptance is that the data was written by a compatible device type.
  If there is configuration data in the internal memory of the device this is overwritten.
  This mode is active as soon as a written C-PLUG is inserted.

Operation with C-PLUG

The configuration stored on the C-PLUG is displayed over the user interfaces.

If changes are made to the configuration, the device stores the configuration directly on the C-PLUG, if this is in the "ACCEPTED" status and in internal memory.

Response to errors

Inserting a C-PLUG that does not contain the configuration of a compatible device type and inadvertently removing the C-PLUG, or general malfunctions of the C-PLUG are indicated by the diagnostic mechanisms of the device.

- Fault LED
- Web Based Management (WBM)
- SNMP
- Command Line Interface (CLI)
- PROFINET diagnostics

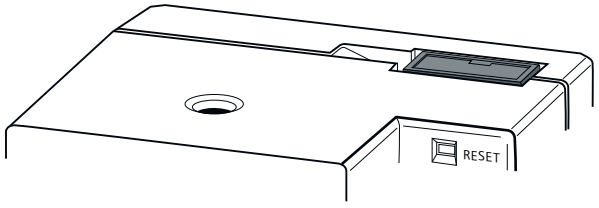
The user then has the choice of either removing the C-PLUG again or selecting the option to reformat the C-PLUG.

3.5.2 Replacing the C-PLUG

Position of the C-PLUG

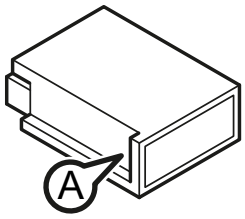
NOTICE
Do not remove or insert a C-PLUG during operation The C-PLUG may only be removed or inserted when the device is turned off.

The C-PLUG slot is on the top of the device.



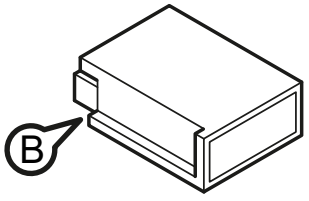
Replacing a C-PLUG.

Removing a C-PLUG



1. Turn off the power to the device.
2. Insert a screwdriver between the front edge of the C-PLUG (A) and the slot and release the C-PLUG.
3. Remove the C-PLUG.

Inserting a C-PLUG



1. Turn off the power to the device.
2. The housing of the C-PLUG has a protruding ridge on the long side (B). The slot has a groove at this position. Insert the C-PLUG correctly oriented into the slot.

Installing and removing

4

4.1 Safety during mounting

Safety notices

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

⚠ 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

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

⚠ WARNING

If the cable or conduit entry point exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 60 °C, only use cables with admitted maximum operating temperature of at least 80 °C.

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

WARNING

EXPLOSION HAZARD

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

WARNING

The device is intended for indoor use only.

WARNING

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

WARNING

Substitution of components may impair suitability of the equipment.

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.

Notes for use in hazardous locations according to ATEX, IECEx, UKEX and CCC Ex

If you use the device under ATEX, IECEx, UKEX or CCC Ex 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

For operation the device is intended to be installed within an enclosure/control cabinet. The inner temperature of the enclosure/control cabinet corresponds to the ambient temperature of the device. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

WARNING

The IP rating marking is not associated with the FM approvals certification.

WARNING

If a device is operated at an ambient temperature of more than 60 °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 60 °C.

Note

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

WARNING

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

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

Substitution of components may impair suitability for Division 2.

WARNING

Do not remove or replace while circuit is live when a flammable or combustible atmosphere is present.

⚠ WARNING

Explosion hazard

Do not disconnect equipment when a flammable or combustible atmosphere is present.

Additional notes

⚠ CAUTION

Use only approved components

If you use components and accessories that are not approved for SIMATIC NET devices or their target systems, this may violate the requirements and regulations for safety and electromagnetic compatibility.
Only use components approved for the SIMATIC NET devices.

NOTICE

Warming and premature aging of the IE switch due to direct sunlight

Direct sunlight can heat up the device and can lead to premature aging of the IE switch and its cabling.

Provide suitable shade to protect the IE switch against direct sunlight.

Note

During installation and operation, keep to the installation guidelines and safety notices described in this document and in the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components".

You will find information on the system manuals in the section "Introduction (Page 3)", under "Further documentation".

4.2 Information on mounting

The devices can be installed in the following ways:

- Installing in an Extension unit box
- DIN-rail mounting

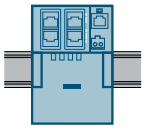
Installation clearances

When mounting on DIN rail, observe the following minimum clearances so that the convection ventilation of the device is not blocked:

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

Installation position

The following mounting position is recommended for DIN-rail mounting:

Horizontal Horizontal installation of the rack (DIN rail)	

4.3 Installing in an Extension unit box

Required tools

To mount the device in an Extension unit box, you need the following:

- 1 mounting plate for mounting in an Extension unit box
- 1 T20 screwdriver, Torx T20
- 4 M4 hexagon nuts (ISO 4032)
- 4 M4 screws (max. penetration depth 9.5 mm)

Installation

Note

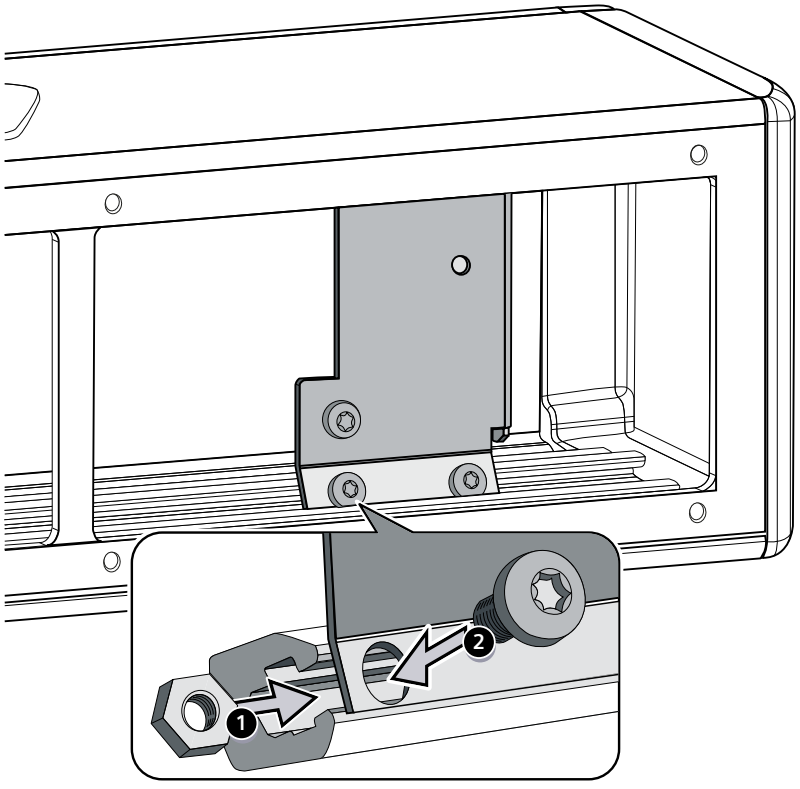
Before mounting, decide whether to connect the following components already before mounting or in the mounted state:

- Electrical ports
- Connector for power supply
- Serial interface

If the device is mounted in an Extension Unit box, the components mentioned are still accessible, but may be more difficult to reach.

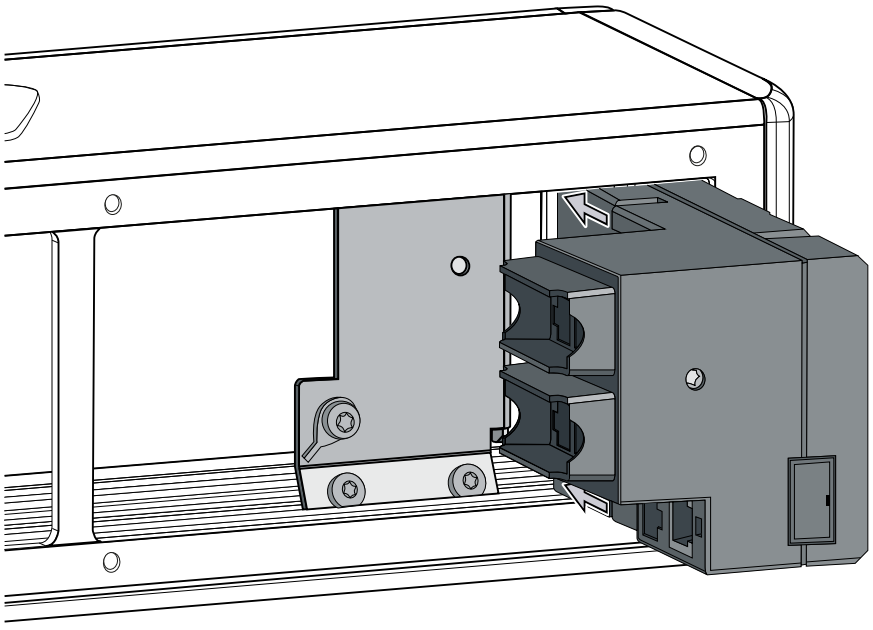
To mount the device inside an Extension Unit box, follow these steps:

1. Remove the rear panel of the Extension Unit box.
   For more information, see the Product information of the Extension Unit box (Page 3).
2. Screw the mounting plate to a screw channel with 4 fixing screws (torque 1.5 Nm).
   The screw channels of the Extension Unit box are suitable for M4 screws with a maximum penetration depth of 9.5 mm and M4 hexagon nuts according to ISO 4032.
   Observe the following schematic diagram.

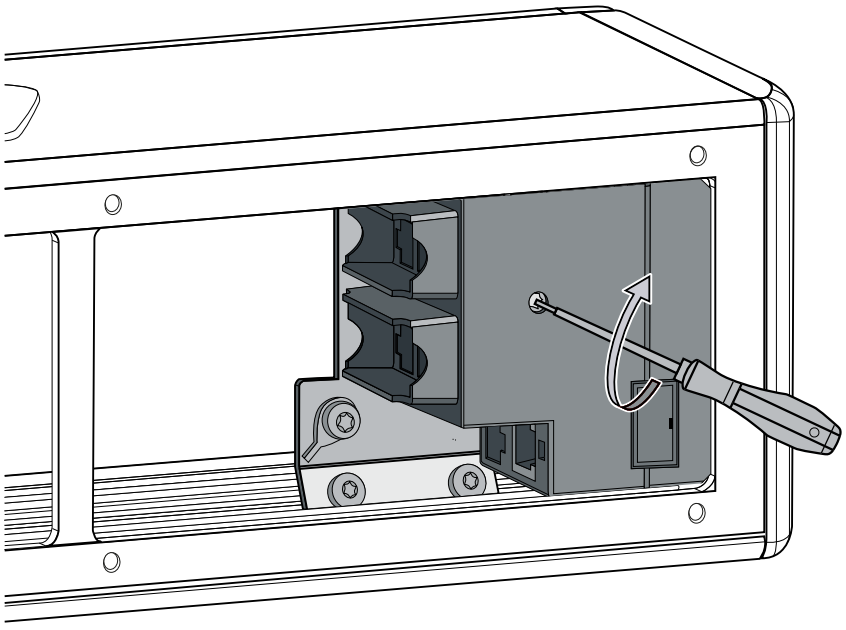


3. Connect the grounding (Page 54) to the mounting plate.

4. Install the device:
   - Insert the device so that the guides on the device connect the device to the mounting plate.
     For an overview of the components of the device, see "Device view (Page 22)
   - Push the device into the Extension unit box until the mounting plate offers resistance. The device is latched on the mounting plate, but not fixed.



5. Screw the mounting screw (torque xx Nm).
   The mounting screw snaps into in a nut on the mounting plate and fixes the device firmly to the mounting plate.
   In this position, the following components are still accessible:
   - Electrical ports
   - Connector for power supply
   - Serial interface
   - RESET button
   - Slot for C-PLUG



6. Fit the connectors for the power supply, see the section "Wiring rules (Page 50)".
7. Insert the terminal blocks into the sockets on the device.
8. Close the rear cover of the Extension Unit box.
9. Tighten the screws of the rear panel cover (torque 1.5 Nm).

Removal

To remove the device from a DIN rail, follow these steps:

1. Remove the rear panel of the Extension Unit box.
2. Disconnect all connected cables.
3. Loosen the mounting screw.
   The device is no longer fixed to the mounting plate.
4. Pull the device out of the Extension Unit box.
5. Remove the mounting plate.
6. Close the rear cover of the Extension Unit box.

4.4 Mounting on DIN rails

Required tools

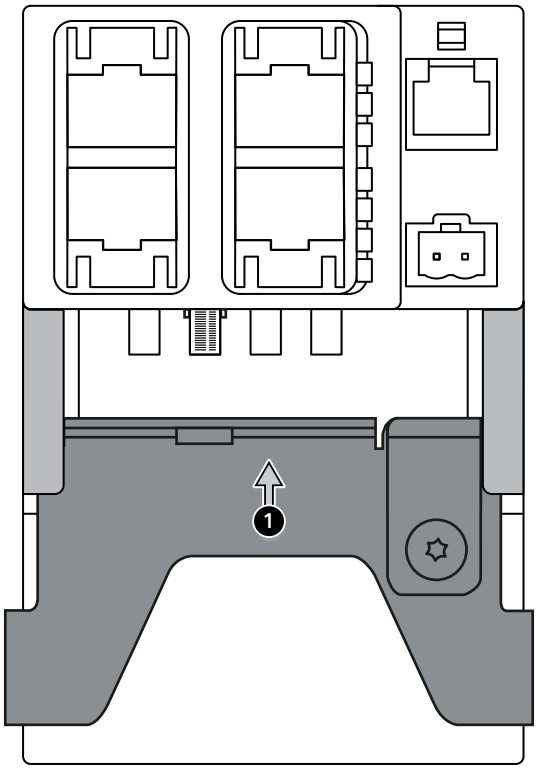
To mount the device on a DIN rail, you need the following:

- 1 mounting plate for DIN-rail mounting
- 1 T20 screwdriver, Torx T20

Installation

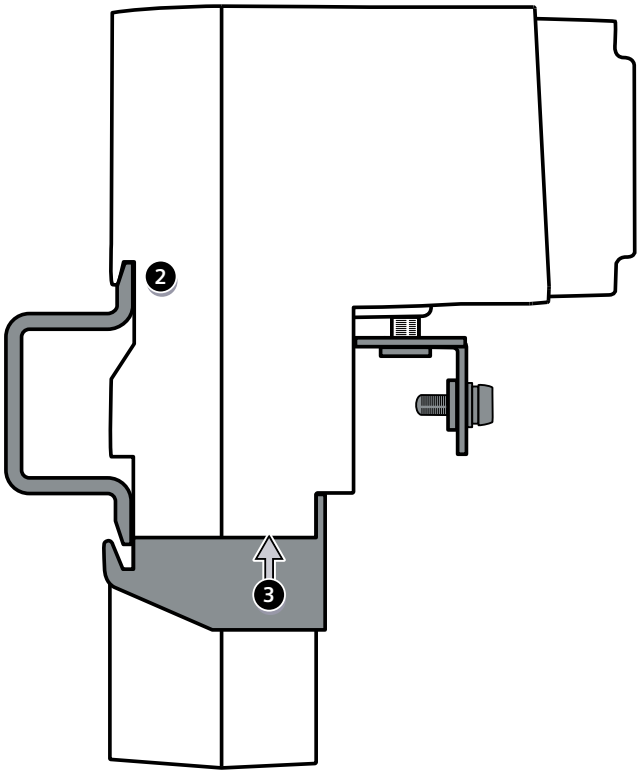
To install the device on a 35 mm DIN rail complying with DIN EN 60715, follow these steps:

1. Mount the mounting plate:
   - Place the mounting plate in the guides on the device.
     For an overview of the components of the device, see "Device view (Page 22)".
   - Push the mounting plate upwards until it snaps into place ①.
     The mounting plate is connected to the device, but not fixed.

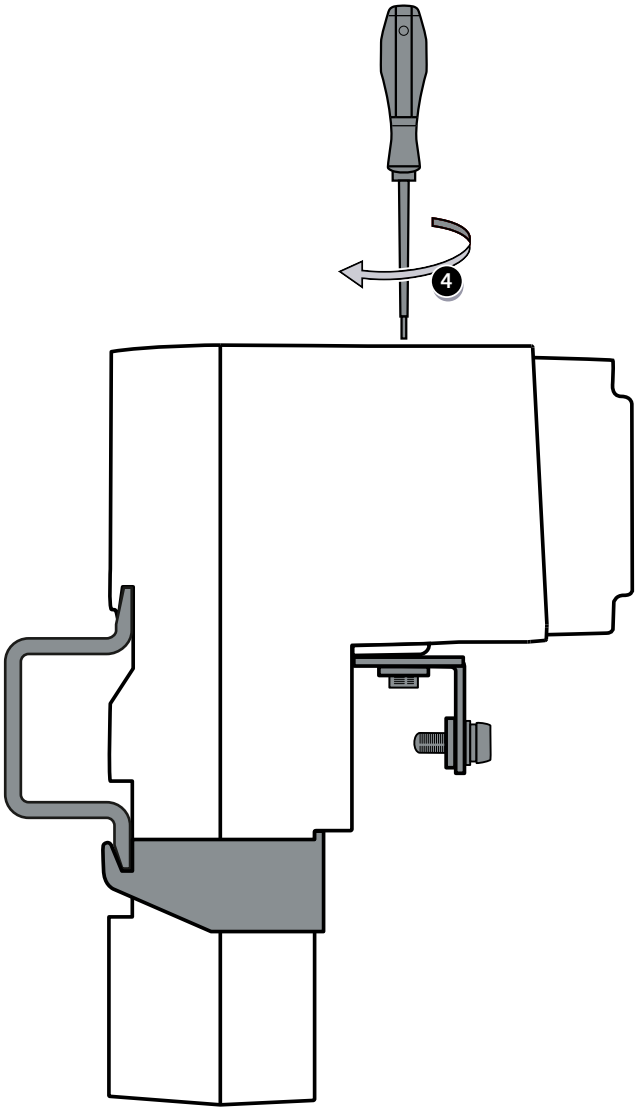


2. Place the housing guide of the device on the top edge of the DIN rail ②.

3. Slide the mounting plate upwards and hold it at the uppermost position ③.



4. Screw the mounting screw ④ (torque xx Nm).
   The mounting screw snaps into in a nut on the mounting plate and fixes the mounting plate firmly to the device. In this position, the mounting plate encloses the lower edge of the DIN rail.



5. Fit the connectors for the power supply, see the section "Wiring rules (Page 50)".
6. Insert the terminal blocks into the sockets on the device.
7. Connect the grounding (Page 54) to the mounting plate.

Removal

To remove the device from a DIN rail, follow these steps:

1. Disconnect all connected cables.
2. Loosen the mounting screw.
   The mounting plate is no longer fixed and releases the lower edge of the DIN rail.

3. Pull the device away from the DIN rail.
4. Remove the mounting plate.

4.5 Uninstalling

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.

Connecting up

5

5.1 Safety when connecting up

Safety notices

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

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 a directly connectable safety extra low voltage (SELV) from a limited power source (LPS).

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

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

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

⚠ 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

Protective ground

A PELV circuit contains a connection to protective ground. Without a connection to protective ground, or in case there is a fault in the connection to the protective ground, the voltage for the circuit is not stabilized.

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 SET 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.

Notes for use in hazardous locations according to ATEX, IECEx, UKEX and CCC Ex

If you use the device under ATEX, IECEx, UKEX or CCC Ex 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 overvoltages of more than 40% of the rated voltage (or more than 119 V). This is the case if you only operate devices with SELV (safety extra-low voltage).

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, GB/T 3836.1.

Safety notices when using the device according to Hazardous Locations (HazLoc)

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

WARNING

EXPLOSION HAZARD

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

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

Do not disconnect while circuit is live unless area is known to be non-hazardous.

⚠ WARNING

Explosion hazard

Do not disconnect equipment when a flammable or combustible atmosphere is present.

⚠ WARNING

Safety notice for connecting with a LAN ID (Local Area Network)

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

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

5.2 Industrial Ethernet

The connection to Industrial Ethernet uses the interfaces of the inserted BusAdapter. Therefore, when connecting to Industrial Ethernet, always take note of the information in the BusAdapter operating instructions. You can find additional information on the operating instructions in the "Introduction" section, paragraphs "Additional documentation" and "Further documentation".

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.

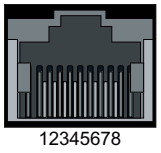
5.2.1 Electrical

R-45 connector technology

The attachment to Industrial Ethernet uses RJ-45 connected technology with MDI-X assignment.

Pin assignment

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

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

MDI / MDI-X autocrossover

With the MDI/MDI-X autocrossover function, the send and receive contacts of an Ethernet port are assigned automatically. The assignment depends on the cable with which the communications partner is connected. This means that it does not matter whether the port is connected using a patch cable or crossover cable. This prevents malfunctions resulting from mismatching send and receive wires. This makes installation much easier for the user.

Note

Formation of loops

Please note that the direct connection of two ports on the IE switch or accidental connection over several IE switches causes an illegal loop. Such a loop can lead to network overload and network failures.

Autonegotiation

Autonegotiation means the automatic detection/negotiation of the transmission rate and the operating mode of ports at the opposite end. This makes it possible to configure different devices automatically.

Two components connected to a link segment can exchange information about the transfer and can adapt their settings to each other. The mode with the highest possible speed is set.

Note

- If a port is set permanently to full duplex, the connected partner port must also be set to full duplex.
- If a port operating in the "Auto negotiation" mode is connected to a partner port that is not operating in the"Auto negotiation" mode, the partner port setting must be fixed at 100 Mbps or 10 Mbps half duplex mode.
- If you disable the "Auto negotiation" function, the "MDI/MDI-X autocrossover" function remains active.

5.3 Wiring rules

When wiring use cables with the following AWG categories or cross sections.

Wiring rules for ...		**Spring-loaded terminals**
connectable cable cross sections for flexible cables ...	without wire end ferrule	0.25 - 2.5 mm^2
		AWG: 24 - 14
	with wire end ferrule**	0.25 - 2.5 mm^2
		AWG: 24 - 14
	with TWIN wire end ferrule**	2 x 0.25 - 2 x 1 mm^2
		AWG: 24 - 18
Stripped length of the cable		8 - 10 mm
Wire end ferrule according to DIN 46228 with plastic ferrule**		8 - 10 mm

* AWG: American Wire Gauge

** See note "Wire end ferrules"

Note

Wire end ferrules

Use crimp shapes with smooth surfaces, such as provided by square and trapeze shaped crimp cross sections.

Crimp shapes with wave-shaped profile are unsuitable.

5.4 Power supply

Notes on the power supply

⚠ WARNING

Incorrect power supply

Never operate the device to alternating voltage.

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

⚠ CAUTION

Damage to the device due to overvoltage

The connector of the external power supply is not protected against strong electromagnetic pulses that can, for example, result from lightning strikes or switching large loads.

One of the tests used to attest the immunity of SCALANCE XF-200G IE switches to electromagnetic interference is the "surge immunity test" according to EN61000-4-5. This test requires overvoltage protection for the power supply lines. A suitable device would be, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422, or a comparable protective element.

Manufacturer: DEHN+SOEHNE GmbH+Co.KG, Hans-Dehn-Str.1, Postfach 1640, D92306 Neumarkt, Germany

Operate the SCALANCE XB-200 with suitable overvoltage protection.

Information on the power supply

- The power supply is connected using a 2-pin plug-in terminal block. The terminal block is included in the scope of delivery (Page 19) of the device and can also be ordered as a spare part (Page 21).
- The power supply is connected over a high resistance with the enclosure to allow an ungrounded set up. The voltage input is non-isolated.
- Note the wiring rules (Page 50).

Position and assignment

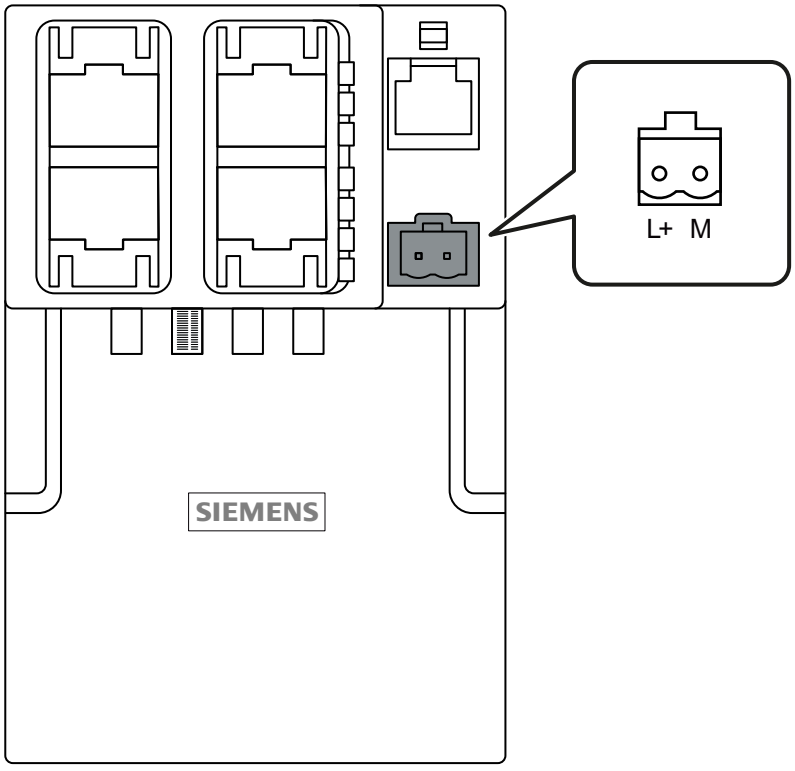


Figure 5-1 Position of the power supply

Contact	Assignment
L+	24 V DC
M	Ground

5.5 Serial interface

Information on the serial interface

- Via the serial interface (RJ-11 jack), you can access the CLI of the device directly via an RS-232 connection (115200 8N1) without assigning an IP address.
- Access to the device is also possible independent of the Ethernet ports.
- To connect the serial interface to the PC, you require a cable with an RJ-11 plug and 9-pin D-sub female connector. You can order the connecting cable for the serial interface as an accessory (Page 20).

Position and assignment

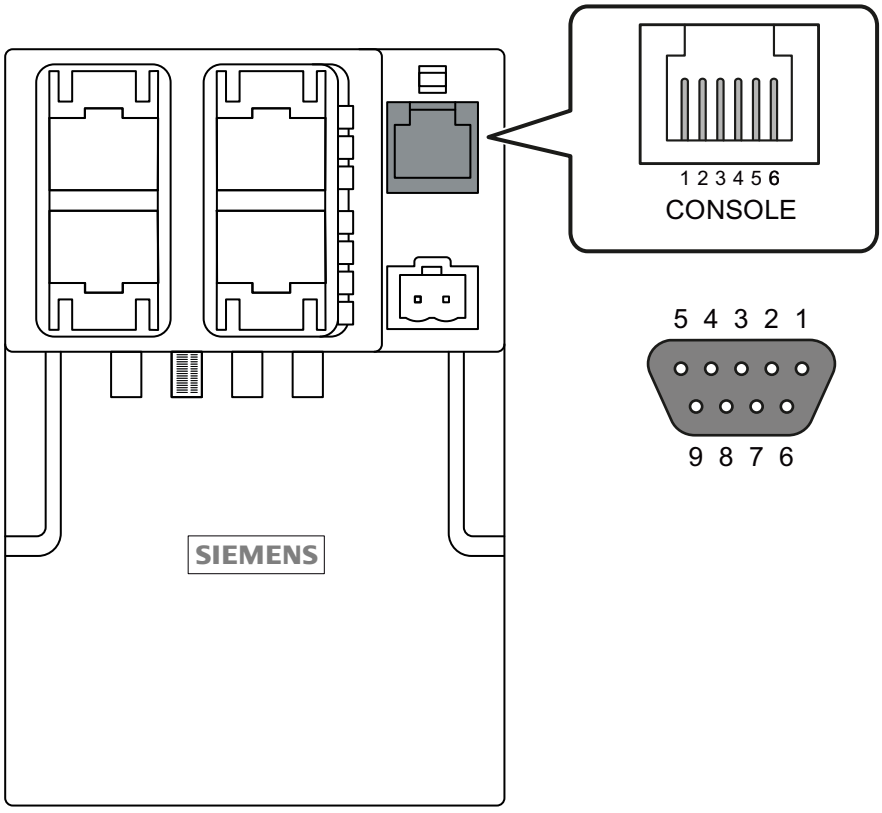


Figure 5-2 Position and pin assignment of the serial interface (RJ-11 jack), for example on the SCALANCE XB213-3

Assignment of the connecting cable

The connecting cable listed in the "Accessories" section has the following pin assignment:

Contact	Pin assignment of the RJ-11 plug	Pin assignment of the D-sub female connector
1	-	-
2	-	TD (Transmit Data)
3	TD (Transmit Data)	RD (Receive Data)
4	SG (Signal Ground)	-
5	RD (Receive Data)	SG (Signal Ground)
6	-	-
7		-
8		-
9		-

Note

Pin assignment of the RJ-11 jack on the device

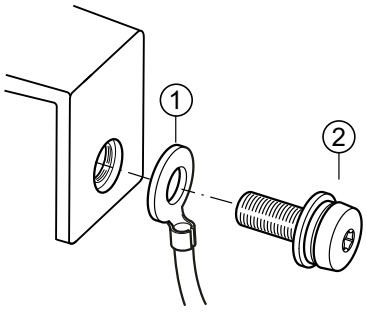
The RJ-11 jack on the device has a pinout to match the RJ-11 plug of the connecting cable mentioned above.

5.6 Grounding

The device is grounded via the mounting plates (Page 20) for mounting the device.

The mounting plates have a grounding screw for connecting a ground terminal. When mounted (mounting screw screwed), the respective mounting plate contacts the ground springs of the device.

Follow the steps below to connect ground:



① Ground terminal with cable
② Fillister head screw with spring washer and washer

Figure 5-3 Grounding screw using the mounting plate for DIN-rail mounting as an example

1. Loosen the grounding screw from the mounting plate.
2. Join the ground terminal and grounding screw together.
3. Tighten the grounding screw on the mounting plate (torque 0.75 Nm).

Maintenance and cleaning

6

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.

WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories (Page 20) and original spare parts (Page 21).
- 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.

Error correction 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.

Pressing the "RESET" button

To load new firmware, you require the "RESET" button. When pressing the button, remember the information in the section "RESET button (Page 22)".

Procedure with Microsoft Windows

Using TFTP, you can supply a device with new firmware even when it cannot be reached using WBM or CLI. This section explains the procedure based on the example of Microsoft Windows.

Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Press the button and reconnect the power supply to the device while holding down the button.
3. Hold down the button until the red fault LED "F" starts to flash.
4. Release the button as long as the red error LED is still flashing..

   Note

   This time only lasts a few seconds.

   The bootloader of the device waits in this status for a new firmware file that you can download by TFTP.
5. Connect a PC to port "P1.1" via an Ethernet cable.
6. Assign an IP address to the device using DHCP or SINEC PNI.
7. Open a Windows command prompt 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>`

   Note

   You can enable TFTP in Microsoft Windows as follows:

   "Control Panel" > "Programs and Features" > "Turn Windows features on or off" > "TFTP Client".
8. Once the firmware has been transferred completely to the device and validated, there is an automatic restart on the device. This may take several minutes.

7.2 Restoring the factory settings

NOTICE
Previous settings If you reset, all the settings you have made will be overwritten by factory defaults.

NOTICE
Inadvertent reset An inadvertent reset can cause disturbances and failures with further consequences in the configured network.

With the button

Restoring the factory settings during the startup phase

NOTICE
Reset despite disabled button Using the button, you can always restore the device parameters to the factory defaults during the startup phase of the device. This applies also if the "Reset factory defaults" function was disabled in the configuration. This allows you to restore the device to the factory defaults in an emergency. If the function has been disabled in the configuration, it is only disabled on completion of the startup phase.

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

1. Turn off the power to the device.
2. Now press the button and reconnect the power supply to the device while holding down the button.
3. Hold down the button until the red error LED "F" stops flashing and is permanently lit.
4. Now release the button and wait until the fault LED "F" goes off again.
5. The device starts automatically with the factory defaults.

Restoring the factory defaults during operation

You can also restore the device to the factory defaults during operation, see section "RESET button (Page 22)".

Via the configuration

You will find detailed information on resetting the device parameters using the web-based management and CLI in the configuration manuals see also section "Introduction (Page 3)":

Technical specifications

8

8.1 Technical specifications of SCALANCE XF204G

The following technical specifications apply to the SCALANCE XF204G.

Technical specifications		
Connection to Industrial Ethernet		
Electrical connectors	Quantity	4
	Connector	RJ45 jack
	Properties	Half/full duplex, MDI-X assignment
	Transmission speed	10 / 100 / 1000 Mbps
Diagnostics interface		
Serial interface	Quantity	1
	Connector	RJ11 jack
Electrical data		
Power supply [1)]	Rated voltage	24 V DC
	Voltage range (incl. tolerance)	16.8 to 31.2 V DC Safe Extra Low Voltage (SELV)
	Design	Terminal block, 2-pin
	Property for an IEC 62368-1 environment	The connected power supply must meet the requirements of NEC Class 2 or PS2/LPS in compliance with UL 62368-1.
Current consumption	24 V DC	200 mA
Effective power loss		4.3 W
Overvoltage category		CAT II
Fusing		1.5 A / 125 V
Permissible ambient conditions		
Ambient temperature	With operation up to 2000 m above sea level	During operation, regardless of the mounting position: 0 °C to +60 °C
	During storage	-40 °C ... +85 °C
	During transportation	-40 °C ... +85 °C
Relative humidity	During operation, at 25 °C	≤ 95% without condensation
Enclosure, dimensions and weight		
Design	Compact	
Housing material	Basic housing	Polycarbonate (PC-GF10)
	Front cover	Polycarbonate (PC-GF10)
Degree of protection	IP 20	
Dimensions (W x H x D)	66 x 100 x 69 mm	
Weight	170 g	

Technical specifications	
Installation options	• DIN-rail mounting • Installing in an Extension unit box
Mean time between failure (MTBF)	
MTBF (EN/IEC 61709; 40 °C)	> 73 years

[1] Note the wiring rules (Page 50).

8.2 Cable lengths

Cable	Permitted cable length
IE TP torsion cable with IE FC Outlet RJ45 + 10 m TP cord	0 to 45 m + 10 m TP cord
IE TP torsion cable with IE FC RJ45 Plug 180	0 to 55 m
IE FC TP Marine / Trailing / Flexible cable with IE FC Outlet RJ45 + 10 m TP cord	0 to 75 m + 10 m TP cord
IE FC TP Marine / Trailing / Flexible cable with IE FC RJ45 Plug 180	0 to 85 m
IE FC TP standard cable with IE FC Outlet RJ45 + 10 m TP cord	0 to 90 m + 10 m TP cord
IE FC TP standard cable with IE FC RJ45 Plug 180	0 to 100 m

8.3 Switching properties

Switching properties	
Aging time	Can be configured (default value: 30 seconds)
Maximum frame size	10240
Max. number of learnable addresses	16000
Response to LLDP frames	Blocking
Response to spanning tree BPDU frames	Forwarding
CoS acc. to IEEE 802.1Q	Yes
QoS priority queues	8
Switching technique	Store and forward
Latency	10 microseconds

Full wire speed switching		
Frame length (bytes)	**Number of frames per second**	
	At 100 Mbps	At 1000 Mbps
64	148810	1488095
128	84459	844594
256	45290	452898
512	23496	234962
1024	11973	119731
1280	9615	96153
1518	8127	81274

Note

The number of SCALANCE XF-200G modules connected in a line influences the frame delay. When a frame passes through the IE switch, this is delayed by the store-and-forward function of the SCALANCE XF-200G by 10-130 microseconds (at 100 Mbps).

8.4 Mechanical stability (in operation)

Mechanical stability (in operation)

Device	**IEC 60068-2-27 shock**	**IEC 60068-2-6 vibration**
	15 g, 11 ms duration 6 shocks per axis	**10 - 58 Hz: 0.075 mm 85 - 150 Hz: 1 g 1 octave/min, 20 sweeps**
SCALANCE XF204G	●	●

Dimension drawings

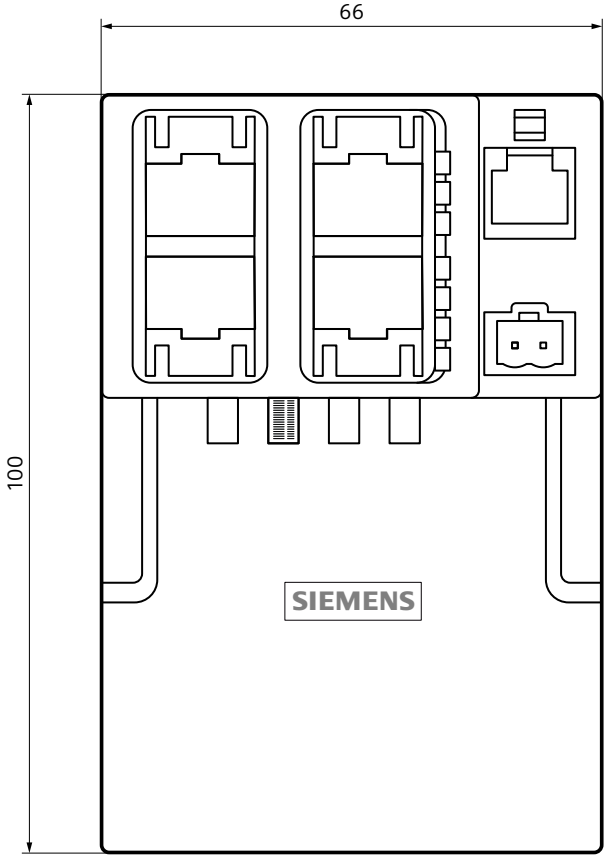
9

Note

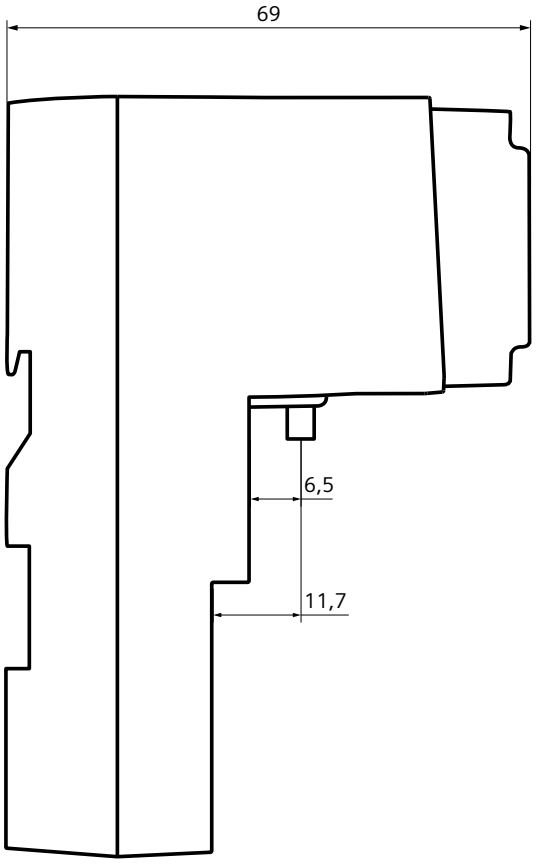
The dimensions are specified in mm.

9.1 Dimension drawing XF-200G

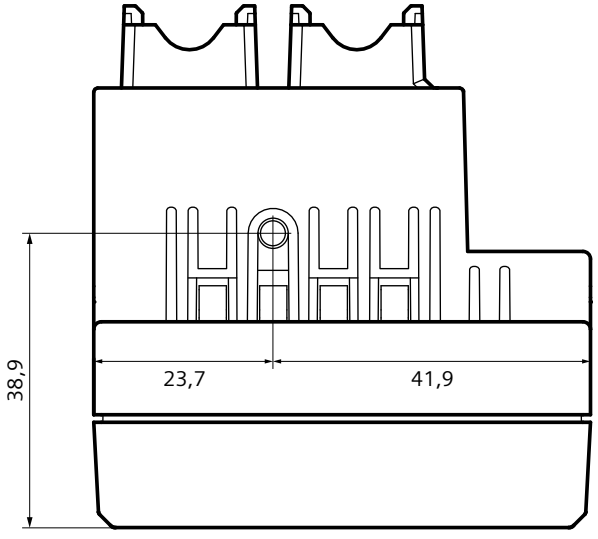
Front view



Side view



Underside



Approvals

A

The SIMATIC NET products described in these Operating Instructions have the approvals listed below.

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.

Current approvals on the Internet

You will find the current approvals for the product on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15273/cert).

Notes for the manufacturers of machines

This product is not a machine in the sense of the EC Machinery Directive or the Supply of Machinery (Safety) Regulations (UK).

There is therefore no declaration of conformity relating to the EC Machinery Directive 2006/42/EEC or the Supply of Machinery (Safety) Regulations 2008 (UK) for this product.

If the product is part of the equipment of a machine, it must be included in the procedure for obtaining the EU/UK conformity assessment by the manufacturer of the machine.

Machinery directive

The product is a component in compliance with the EC Machinery Directive 2006/42/EEC and the Supply of Machinery (Safety) Regulations 2008 (UK).

According to the Machinery Directive respectively the Supply of Machinery (Safety) Regulations (UK), we are obliged to point out that the product described is intended solely for installation in a machine.

Before the final product can be put into operation, it must be tested to ensure that it conforms with the Machinery Directive 2006/42/EEC and the Supply of Machinery (Safety) Regulations 2008 (UK).

EC declaration of conformity

CE

The SIMATIC NET products described in these operating instructions meet the requirements and safety objectives of the following EC directives and comply with the harmonized

European standards (EN) which are published in the official documentation of the European Union and here.

- **2014/34/EU (ATEX explosion protection directive)**
  Directive of the European Parliament and the Council of 26 February 2014 on the approximation of the laws of the member states concerning equipment and protective systems intended for use in potentially explosive atmospheres, official journal of the EU L96, 29/03/2014, pages. 309-356
- **2014/30/EU (EMC)**
  EMC directive of the European Parliament and of the Council of February 26, 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, pages. 79-106
- **2011/65/EU (RoHS)**
  Directive of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment, official journal of the EC L174, 01/07/2011, pages 88-110

You will find the EC declaration of conformity for these products on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15273/cert).

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

Siemens Aktiengesellschaft

Digital Industries
DE-76181 Karlsruhe
Germany

UK Declaration of Conformity

UK CA

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

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76181 Karlsruhe
Germany

Importer UK:

Siemens plc,
Manchester M20 2UR

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/15273/cert).

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

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

ATEX, IECEx, UKEX and CCC Ex certification

⚠ WARNING

Risk of explosion in hazardous areas

When using SIMATIC NET products in hazardous area zone 2, make absolutely sure that the associated conditions in the following document are adhered to:

"SIMATIC NET Product Information Use of subassemblies/modules in a Zone 2 Hazardous Area".

You will find this document

- on the data medium that ships with some devices.
- on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/view/78381013).

Enter the document identification number "C234" as the search term.

The markings of the electrical devices are:

II 3 G Ex ec IIC T4 Gc
DEKRA 18ATEX0025 X
IECEx DEK 18.0017X

II 3 G Ex ec IIC T4 Gc
DEKRA 21UKEX0001 X

Importer UK:
Siemens plc,
Manchester, M20 2UR, UK

(Ex ec IIC T4 Gc, not on the nameplate)

The products meet the requirements of the following standards:

- EN/IEC 60079-7, GB/T 3836.3
- EN IEC/IEC 60079-0, GB/T 3836.1

You will find the current versions of the standards in the currently valid certificates.

EMC (electromagnetic compatibility)

The SIMATIC NET products described in these operating instructions meet the electromagnetic compatibility requirements according to the EU Directive 2014/30/EU as well as the UK-Regulation SI 2016/1091 and their associated amendments.

Applied standards:

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

You will find the current versions of the standards in the currently valid EC/UK Declaration of Conformity.

RoHS

The SIMATIC NET products described in these operating instructions meet the requirements on the restriction of the use of certain hazardous substances in electrical and electronic equipment according to the EU Directive 2011/65/EU as well as the UK-Regulation SI 2012/3032 and their associated amendments.

Applied standard:

- EN IEC 63000

FM

The product meets the requirements of the standards:

- Factory Mutual Approval Standard Class Number 3611
- 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

cULus Approval for Information Technology Equipment

cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

- UL 62368-1 (information/communication technology)
- CSA C22.2 No. 62368-1 (information/communication technology)

Report no. E115352

cULus Approval Hazardous Location

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

Underwriters Laboratories Inc. complying with

- UL 62368-1 (information/communication technology)
- CSA C22.2 No. 62368-1 (information/communication technology)
- ANSI/ISA 12.12.01
- CSA C22.2 No. 213

Approved for use in
Cl. 1, Div. 2, GP A, B, C, D T4
Cl. 1, Zone 2, GP IIC T4

Report no. E240480

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

- AS/NZS CISPR11 (Industrial, scientific and medical equipment - Radio-frequency disturbance characteristics - Limits and methods of measurement).
- EN 61000-6-4 Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

You will find the current versions of the standards in the currently valid RCM SDoCs (Self-Declaration of Conformity).

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

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

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)

FDA and IEC marking

The following devices meet the FDA and IEC requirements listed below:

Device	CLASS 1 LASER Product
SCALANCE XF204G	-

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 SIMATIC NET 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.

Index

A

Accessories, 20
Ambient conditions, 59
Approvals, 65
Article numbers, 19
Autonegotiation, 49
AWG, 50

B

Button, 57, 58

C

Cable cross section, 50
CE mark, 65
CLI, 52
Command Line Interface, 52
Command Line Interface (CLI), 28, 57
Configuration, 24
Connection to Industrial Ethernet, 59
C-PLUG, 20
    Configuration, 27
Cross section, 50

D

Dimensions, 59
DIN-rail mounting, 39

E

Electrical data, 59
Extension Unit box, 4

F

Factory default, 23, 58
Factory setting, 23, 58
Fault LED, 25
Firmware, 57

G

Glossary, 5

H

Housing, 59

I

Installation, 59
    DIN-rail mounting, 39
    Extension unit box, 36

L

LED display
    Fault LED, 25
    Port LED, 26
    RM LED, 25

M

MDI / MDI-X autocrossover, 49
MTBF, 60

P

Permissible ambient conditions, 59
Pin assignment, 49
PLUG, 27
Port LED, 26
Power supply, 51

R

RESET button, 23
Reset device, 23, 58
Restore factory defaults, 24, 58
RM LED, 25

S

Safety notices
for installation, 31
general, 9
Use in hazardous areas, 9, 31, 43, 44
when connecting up, 43, 44
Scope of delivery, 19
Serial interface, 52
SIMATIC NET glossary, 5
SIMATIC NET manual, 4
Spare parts, 21
Startup phase, 24, 58
System manual, 4, 34, 70

W

Web Based Management (WBM), 28, 57
Weight, 59
Wiring, 50
Wiring rules, 51