SIEMENS

SIMATIC NET

Industrial Ethernet switches SCALANCE XM-400

Operating Instructions

Introduction 1

Safety notices 2

Recommendations on network security 3

Description of the device 4

installing and removing 5

Connecting up 6

Upkeep and maintenance 7

Troubleshooting 8

Technical specifications 9

Dimension drawings 10

Approvals A

04/2024
C79000-G8976-C306-14

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-C306-14
Ⓟ 04/2024 Subject to change

Copyright © Siemens 2013 - 2024.
All rights reserved

Table of contents

1 Introduction 5

1.1 Cybersecurity information 7

2 Safety notices 11

3 Recommendations on network security 13

4 Description of the device 21

4.1 Properties and functions 21

4.2 Product overview 22

4.3 Accessories 24

4.4 Spare parts 27

4.5 Device views 29
4.5.1 SCALANCE XM408-4C 29
4.5.2 SCALANCE XM408-8C 30
4.5.3 SCALANCE XM416-4C 31

4.6 SELECT / SET button 32

4.7 LED display 34
4.7.1 Overview 34
4.7.2 "RM" LED 34
4.7.3 "SB" LED 35
4.7.4 "F" LED 35
4.7.5 LEDs "DM1" and "DM2" 35
4.7.6 LEDs "L1" and "L2" 36
4.7.7 Port LEDs 37

4.8 C-PLUG/KEY-PLUG 38
4.8.1 Function of the C-PLUG/KEY-PLUG 38
4.8.2 Replacing the C-PLUG/KEY-PLUG 40

4.9 Functions 41
4.9.1 Combo ports 41
4.9.2 Power over Ethernet (PoE) 42

5 installing and removing 43

5.1 Safety notices for installation 43

5.2 Types of installation 45

5.3 Mounting on DIN rails 46

5.4 Installation on a standard S7-300 rail 47

5.5 Installation on a standard S7-1500 rail 48

5.6 Fitting an extender 49

5.7 General notes for SFP transceivers 52

5.8 Disassembly ... 52
6 Connecting up ... 53
6.1 Safety when connecting up ... 53
6.2 Spring-loaded terminal ... 56
6.3 Power supply ... 57
6.4 Signaling contact ... 58
6.5 Serial interface ... 59
6.6 Out-of-band interface ... 60
6.7 Functional ground ... 61
7 Upkeep and maintenance ... 63
8 Troubleshooting ... 65
8.1 Downloading new firmware using TFTP without WBM and CLI ... 65
8.2 Restoring the factory settings ... 66
9 Technical specifications ... 67
9.1 Technical specifications of the SCALANCE XM408-4C ... 67
9.2 Technical specifications of the SCALANCE XM408-8C ... 68
9.3 Technical specifications of the SCALANCE XM416-4C ... 70
9.4 Switching properties ... 71
10 Dimension drawings ... 73
10.1 SCALANCE XM-400 dimension drawings ... 73
10.2 Extender dimension drawings ... 75
A Approvals ... 79
Index ... 87

Introduction

1

Purpose of the Operating Instructions

These operating instructions support you when installing and connecting up devices of the SCALANCE XM-400 product group.

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

Validity of the Operating Instructions

These operating instructions apply to the following devices:

- SCALANCE XM408-4C
- SCALANCE XM408-8C
- SCALANCE XM416-4C

Unless mentioned otherwise, the descriptions in these operating instructions refer to all devices of the SCALANCE XM-400 product group named above in the section on 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-400 is used.	SCALANCE X-400
Product group	If information applies to all devices and variants of a product group, the term SCALANCE XM-400 is used.	SCALANCE XM-400
Device	If information relates to a specific device, the device name is used.	SCALANCE XM408-4C SCALANCE XM408-8C SCALANCE XM416-4C

Additional documentation

In addition, note the Operating Instructions of the extenders and pluggable transceivers.

When working with the port extender PE408PoE, note the documentation of the PoE power supplies SCALANCE PS9230 PoE and SCALANCE PS924 PoE.

You will find the supplementary documentation 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/15315)

When using the Function Extender BUS ANALYZER Agent XM-400, note the documentation of the BUS ANALYZER Agent XM-400 on the Siemens Industry Online Support website:

- Product announcement (https://support.industry.siemens.com/cs/de/en/view/109745817)
- Application example (https://support.industry.siemens.com/cs/de/en/view/109762541)

Documentation on configuration

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

- SCALANCE XM-400/XR-500 Web Based Management
- SCALANCE XM-400/XR-500 Command Line Interface

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/15315/man)

Further documentation

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 partner 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:
  - 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)

SIMATIC NET manuals

You will find the SIMATIC NET manuals here:

- On the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15247).

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

1.1 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/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=/en&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.

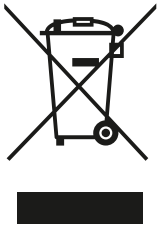
Decommissioning

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

Safety notices

2

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.

Recommendations on network security

3

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.
  - The memory card or the PLUG (C-PLUG, KEY-PLUG) contains sensitive data such as certificates, keys etc. that can be read out and modified.
  - Using the button, you can reset the device to the factory defaults.
- If the device is publicly accessible, disable the functions of the button using the software.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.

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

- There is a preset SSL/TLS (RSA) certificate with 2048 bit key length 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 via the WBM ("System > Load and Save").
- Use certificates with a key length of 4096 bits.
- 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".
- 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.

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.

Protocol	Protocol/ Port number	Default port status	Configurable		Authenti-cation	Encryption [6]
			Port	Service		
DHCPv4 Server	UDP/67	Closed	-	✓	-	-
DHCPv4 Client (IPv4)	UDP/68	Open	-	✓	-	-
DHCPv6 Client (IPv6)	UDP/546	Closed	-	✓	-	-
EtherNet/IP [2]	TCP/44818 UDP/2222 UDP/44818	Closed	-	✓	-	-

Protocol	Protocol/ Port number	Default port status	Configurable		Authenti-cation	Encryption [6]
			Port	Service		
HTTP Server/Client [4]	TCP/80	Closed	✓	✓	✓	-
HTTPS WBM Server/Client	TCP/443	Open	✓	✓	✓	✓
MSDP	TCP/639	Closed	-	✓	-	-
NTP Client	UDP/123	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Closed	✓	✓	✓	-
PROFINET	UDP/34964 UDP/49151 ... 49159 [1]	Open	-	✓	-	-
RADIUS Client	UDP/1812 [5] UDP/1813 [5]	Outbound only	✓	✓	-	-
	UDP/3799	Open	✓	✓	-	-
RIP	UDP/520	Closed	-	✓	-	-
RIPng IPv6	UDP/521	Closed	-	✓	-	-
SFTP Server	UDP/22	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	-	-
SMTP Client (secure)	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c [3] [4]	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 [4]	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outbound only	✓	✓	-	-
VRRP	TCP/50000	Open, filtered	-	✓	-	-

1) Port number can be configured via the WBM.

2) Service disabled by default.

3) Read-only access only.

4) Protocol according to Security by Default.

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

6) 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

4

4.1 Properties and functions

SCALANCE XM-400 product group

The product group SCALANCE XM-400 consists of basic devices (compact switches) and extenders (port extenders and function extender).

SCALANCE XM-400 basic device

Basic properties

The SCALANCE XM-400 basic devices are modular compact switches with fixed RJ-45 ports (10/100/1000 Mbps) and SFP transceiver slots that can be equipped individually. The SFP transceiver slots are combo ports.

A SCALANCE XM-400 can manage a maximum of 24 ports with 10/100/1000 Mbps.

The following components exist only on the basic device:

- CPU
- Power supply
- Signaling contact
- Out-of-band port
- Serial interface
- "SELECT / SET" button

Expansions

The basic devices can be expanded with additional ports and functions by using an extender. The extenders are connected to the side of the basic device. Each basic device has an expansion interface to the left for function extenders and to the right an expansion interface for port extenders.

Depending on the number of ports of the basic device (10/100/1000 Mbps) up to 2 port extenders can be added. Further port extenders are not supplied with power. There is no particular order in which the port extenders need to be added.

Example:

- The basic device SCALANCE XM408-8C has 8 ports. It can therefore be expanded by 2 port extenders each with 8 ports.
- The basic device SCALANCE XM416-4C has 16 ports. It can therefore be expanded by one port extender with 8 ports.

A function extender can be added.

Port extender PE-400

Port extenders are modular network components with RJ-45 ports (10/100/1000 Mbps) or SFP transceiver slots. To the left they have an expansion interface to connect to the basic device or to another port extender and to the right they have an expansion interface for additional port extenders. Each port extender functions with every basic device.

Note

Port extenders function only in conjunction with a basic device.

Function Extender BUS ANALYZER Agent XM-400

Function extenders are modular network components, that expand the range of functions of the basic device.
To the right they have an expansion interface to connect to the basic device. Function extenders can be used with every basic device.

The BUS ANALYZER Agent XM-400 can be used as a function extender for SCALANCE XM-400.

As a function extender the BUS ANALYZER Agent XM-400 is a modular network component with 4 internal monitor ports for port mirroring. On the internal ports of the BUS ANALYZER Agent XM-400, ports of the basic device can be mirrored and their data traffic recorded. The BUS ANALYZER Agent XM-400 has an expansion interface to the right to connect to the basic device. It can be used with every basic device.

In standalone mode, the BUS ANALYZER Agent XM-400 is an independent hardware module for recording and sending Ethernet and PROFINET data without any consequences.

You will find detailed information in the operating instructions of the BUS ANALYZER Agent XM-400, see section "Introduction (Page 5)", subsection "Additional documentation".

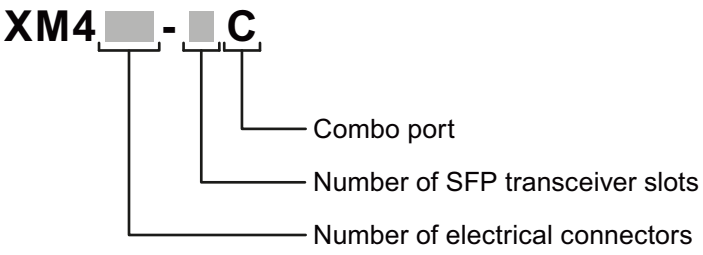
4.2 Product overview

Article numbers

Type	Properties	Article number
SCALANCE XM408-4C	8 RJ-45 ports, 4 pluggable transceiver slots, up to 2 port extenders and 1 function extender, layer 3 with KEY-PLUG	6GK5 408-4GP00-2AM2
	8 RJ-45 ports, 4 pluggable transceiver slots, up to 2 port extenders and 1 function extender, layer 3 integrated	6GK5 408-4GQ00-2AM2
SCALANCE XM408-8C	8 RJ-45 ports, 8 pluggable transceiver slots, up to 2 port extenders and 1 function extender, layer 3 with KEY-PLUG	6GK5 408-8GS00-2AM2
	8 RJ-45 ports, 8 pluggable transceiver slots, up to 2 port extenders and 1 function extender, layer 3 integrated	6GK5 408-8GR00-2AM2
SCALANCE XM416-4C	16 RJ-45 ports, 4 pluggable transceiver slots, max. 1 port extender and 1 function extender, layer 3 with KEY-PLUG	6GK5 416-4GS00-2AM2
	16 RJ-45 ports, 4 pluggable transceiver slots, max. 1 port extender and 1 function extender, layer 3 integrated	6GK5 416-4GR00-2AM2

Type designation

The type designation of a SCALANCE XM-400 is made up of several parts that have the following meaning:



Interfaces

Device	Number of electrical connectors	Number of combo ports	Number of slots for pluggable transceivers
SCALANCE XM408-4C	8	4	4
SCALANCE XM408-8C	8	8	8
SCALANCE XM416-4C	16	4	4

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.

Components of the product

The following components are supplied with a SCALANCE XM-400:

- One IE switch with exchangeable storage medium C-PLUG (article number: 6GK1 900-0AB10)
- One product DVD with documentation and software

- Securing screw for mounting on an S7 standard rail
- A 4-pin terminal block for the power supply (spring-loaded terminal)
- A 2-pin terminal block for the signaling contact (spring-loaded terminal)
- A connecting cable for the serial interface with RJ-11 plug and 9-pin D-sub female connector
- Covers for the pluggable transceiver slots
  - SCALANCE XM408-8C: 8 covers
  - SCALANCE XM416-4C: 4 covers

4.3 Accessories

The following accessories are available for SCALANCE XM-400:

KEY-PLUG

Type	Article number
KEY-PLUG XM400 Layer 3	6GK5 904-0PA00

See also

Technical specifications (Page 67)

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

Pluggable transceiver SFP (100 Mbps)

Type	Property	Article number
SFP991-1	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5 991-1AD00-8AA0
	10 packing unit (VPE 10)	6GK5 991-1AD00-8AC0
SFP991-1 (C)	1 x 100 Mbps, LC port optical, for glass FO cable (multimode), up to max. 5 km, varnished	6GK5 991-1AD00-8FA0
SFP991-1LD	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5 991-1AF00-8AA0
	10 packing unit (VPE 10)	6GK5 991-1AF00-8AC0
SFP991-1LD (C)	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km, varnished	6GK5 991-1AF00-8FA0

Type	Property	Article number
SFP991-1LH+	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 991-1AE00-8AA0
SFP991-1ELH200	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 200 km	6GK5 991-1AE30-8AA0

The SFP plug-in transceiver (100 Mbps) cannot be operated in SFP+ slots.

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Pluggable transceiver SFP (1000 Mbps)

Type	Property	Article number
SFP992-1	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 750 m	6GK5 992-1AL00-8AA0
	10 packing unit (VPE 10)	6GK5 992-1AL00-8AC0
SFP992-1 (C)	1 x 1000 Mbps, LC port optical, for glass FO cable (multimode), up to max. 750 m, varnished	6GK5 992-1AL00-8FA0
SFP992-1+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 2 km	6GK5 992-1AG00-8AA0
SFP992-1LD	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AM00-8AA0
	10 packing unit (VPE 10)	6GK5 992-1AM00-8AC0
SFP992-1LD (C)	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km, varnished	6GK5 992-1AM00-8FA0
SFP992-1LD+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 30 km	6GK5 992-1AM30-8AA0
SFP992-1LH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 40 km	6GK5 992-1AN00-8AA0
SFP992-1LH+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 992-1AP00-8AA0
SFP992-1ELH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 120 km	6GK5 992-1AQ00-8AA0

Pluggable transceivers with the supplement (C) in the type name have varnished printed circuit boards (conformal coating).

Note

Restriction for pluggable transceivers

The maximum ambient temperature changes if you use pluggable transceivers:

- If you use transceivers of the types multimode and LD, the maximum ambient temperature is reduced to 60 °C.
- If you use transceivers of the types LH, LH+, ELH or ELH200, the maximum ambient temperature is reduced to 50 °C.
  You can only use up to 4 pluggable transceivers of the types LH, LH+, ELH or ELH200 in the basic device.

For the values of the ambient temperature without pluggable transceivers, refer to the section "Technical specifications (Page 67)".

Bidirectional plug-in transceiver SFP

Bidirectional plug-in transceivers feature only one fiber connection. They transmit and receive on two different wavelengths. To establish a connection, you need two matching bidirectional SFPs. The connected SFPs must respectively transmit on the wavelength at which the connection partner receives.

Type	Properties	Article number
SFP992-1BXMT	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AL00-8TA0
SFP992-1BXMR	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AL00-8RA0

Port extender

Type	Properties	Article number
PE408	8 x 10/100/1000 Mbps RJ-45 ports	6GK5 408-0GA00-8AP2
PE408PoE	8 x 10/100/1000 Mbps, RJ-45 ports with PoE	6GK5 408-0PA00-8AP2
PE400-8SFP	8 x 100/1000 Mbps, SFP ports	6GK5 400-8AS00-8AP2

Function Extender BUS ANALYZER Agent XM-400

Device	Properties	Article number
BUS ANALYZER Agent XM-400 as function extender	4 x internal monitor ports for port mirroring	9AE 4140-2AA00

PoE power supply

Type	Input voltage	Output voltage	Output current	Article number
SCALANCE PS9230 PoE	100/240 VAC 50/60 Hz	54 VDC	1.6 A	6GK5 923-0PS00-3AA2
SCALANCE PS924 PoE	24 VDC	54 VDC	1.6 A	6GK5 924-0PS00-1AA2

SCP / STP transceiver

Type	Properties	Article number
SCP992-1	1 x 1000 Mbps SC port optical for glass FO cable (multimode) up to max. 750 m	6GK5 992-1AJ00-8AA0
SCP992-1LD	1 x 1000 Mbps SC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AK00-8AA0
STP991-1	1 x 100 Mbps ST port optical for glass FO cable (multimode) up to max. 3 km	6GK5 991-1AB00-8AA0
STP991-1LD	1 x 100 Mbps ST port optical for glass FO cable (single mode) up to max. 26 km	6GK5 991-1AC00-8AA0

Can only be operated in SCP and STP slots.

4.4 Spare parts

The following spare parts are available for SCALANCE XM-400:

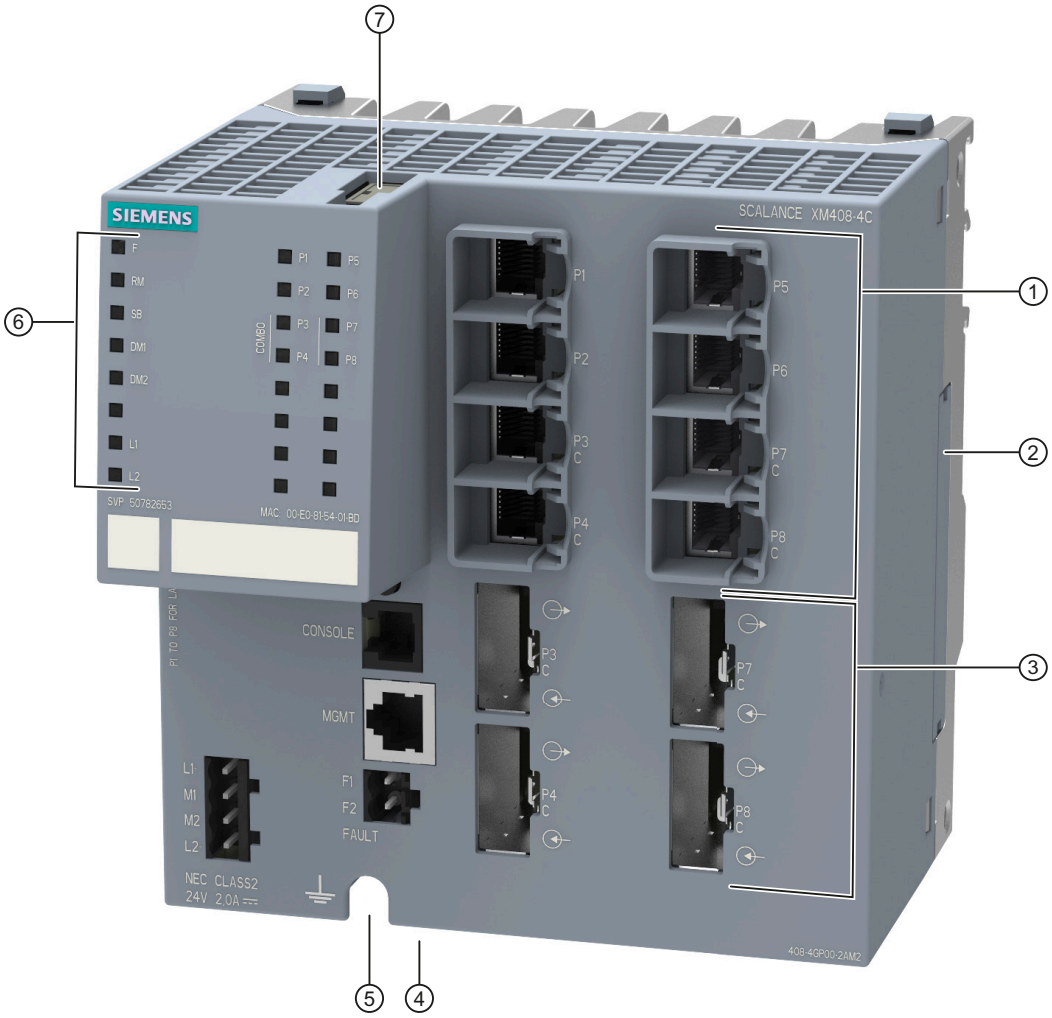
Component	Description	Article number
C-PLUG	Configuration plug, exchangeable storage medium for configuration data	6GK1 900-0AB00
Spring-loaded terminal block, 4 terminals	4-terminal spring-loaded terminal block to connect the power supply (24 VDC), for SCALANCE X/W/S/M, pack of 5	6GK5 980-1DB10-0AA5
Spring-loaded terminal block, 2 terminals	2-terminal spring-loaded terminal block to connect the signaling contact (24 VDC), for SCALANCE X/W/S/M, pack of 5	6GK5 980-0BB10-0AA5
Screw terminal block, 4 terminals	4-terminal screw terminal block to connect the power supply (24 VDC), for SCALANCE X/W/S/M, pack of 5	6GK5 980-1DB00-0AA5
Screw terminal block, 2 terminals	2-terminal screw terminal block to connect the power supply (24 VDC), for SCALANCE X/W/S/M, pack of 5	6GK5 980-0BB00-0AA5

Component	Description	Article number
Securing screw	Screw for mounting on an S7-1500 and S7-300 standard rail, for SCALANCE X/W, pack of 5	6GK5 980-4AA00-0AA5
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

4.5 Device views

4.5.1 SCALANCE XM408-4C

The following figure shows an overview of the components of the SCALANCE XM408-4C.



① Electrical ports
② Expansion interface with cover
③ Slots for pluggable transceivers (STP and DCP)
④ Location for securing to an S7 standard rail (on the underside of the device, not in figure)
⑤ Grounding (on rear of device, not shown in figure)
⑥ LED display
⑦ Slot for C-PLUG / KEY-PLUG

4.5.2 SCALANCE XM408-8C

The following figure shows an overview of the components of the SCALANCE XM408-8C.



① Electrical ports
② Expansion interface with cover
③ Slots for SFP transceivers
④ Location for securing to an S7 standard rail (on the underside of the device, not in figure)
⑤ Grounding (on rear of device, not shown in figure)
⑥ LED display
⑦ Slots for C-PLUG / KEY-PLUG

4.5.3 SCALANCE XM416-4C

The following figure shows an overview of the components of the SCALANCE XM416-4C.



① Electrical ports
② Expansion interface with cover
③ Slots for SFP transceivers
④ Location for securing to an S7 standard rail (on the underside of the device, not in figure)
⑤ Grounding (on rear of device, not shown in figure)
⑥ LED display
⑦ Slot for C-PLUG / KEY-PLUG

4.6 SELECT / SET button

Position

The "SELECT/SET" button is located on the front of the SCALANCE XM-400.

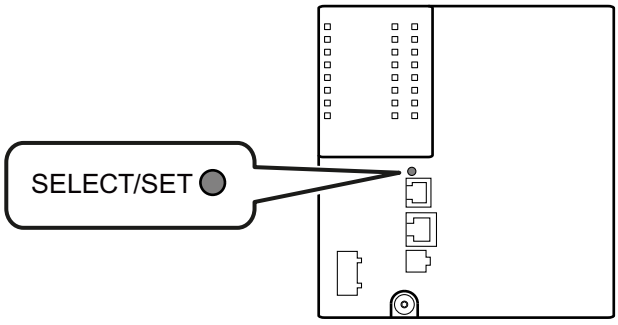


Figure 4-1 Position of the "SELECT/SET" button on the SCALANCE XM-400

Setting the display mode

To set the required display mode, press the "SELECT/SET" button.

For more detailed information on the display modes, refer to the section "LEDs "DM1" and "DM2" (Page 35)".

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 in a configured network with further consequences.

Requirement

- The device is in operation.
- The function "Restore Factory Defaults" is enabled for the "SELECT / SET" button.

Note

Reset despite disabled "SELECT/SET" button

If you have disabled the "Restore Factory Defaults" function for the "SELECT/SET" button in the configuration, this does not apply during the startup phase, see section "Restoring the factory settings (Page 66)".

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

Procedure

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

1. Switch to display mode A.
   Display mode A is active if the LEDS "DM1" and "DM2" are unlit.
   If the "DM1" and "DM2" LEDs are lit or flashing, you will need to press the "SET/SELECT" repeatedly until the "DM1" and "DM2" LEDs go off.
   If you do not press the "SELECT/SET" button for longer than 1 minute, the device automatically changes to display mode A.
2. Hold down the "SELECT/SET" button for 12 seconds.
   After 9 seconds,the "DM1" and "DM2" LEDs start to flash for 3 seconds. At the same time, the port LEDs go on one after the other.
   After you have held down the button for 12 seconds, the factory defaults 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.

Defining the fault mask

Using the fault mask, you specify an individual "good status" for the connected ports and the power supply. Deviations from this status are displayed as errors/faults.

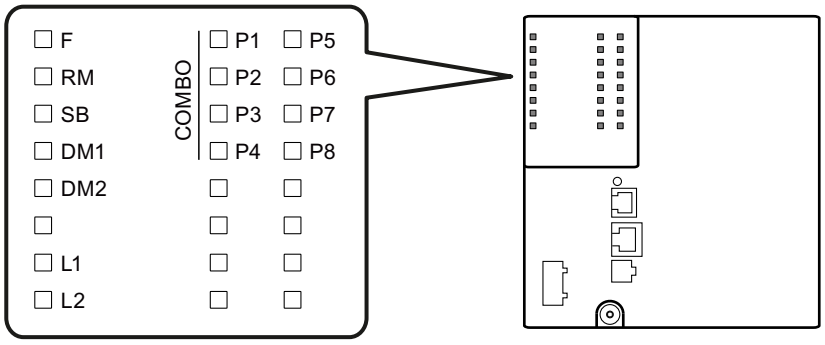
To define the fault mask, follow the steps below:

1. Switch to display mode D.
   Display mode D is active if the "DM1" and "DM2" LEDs are lit green..
   If another display mode is active, you will need to press the "SET/SELECT" button repeatedly until the "DM1" and "DM2" LEDs are lit green.
2. Hold down the "SELECT/SET" button for 5 seconds.
   After 2 seconds,the "DM1" and "DM2" LEDs start to flash for 3 seconds. At the same time, the port LEDs go on one after the other.
   After you have held down the button for 5 seconds, the current settings are stored as the "good status".
   If you release the button before the 5 seconds have elapsed, the previous fault mask will be retained.

4.7 LED display

4.7.1 Overview

The following figure shows the arrangement of the LEDs.



F	LED for displaying the fault/error status
RM	LED for displaying the "redundancy manager" function
SB	LED for display of redundantly linked rings
DM1/DM2	LEDs for displaying the display mode
L1/L2	LEDs for displaying the power supply
P	LEDs for displaying the port status *)
COMBO	Indicates that the LEDs belong to combo ports

*) The number of port LEDs depends on the device.

4.7.2 "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.

4.7.3 "SB" LED

With a redundant linking of rings, the "SB" LED shows the status of the redundant connection. The available options of a redundant link are as follows:

- Standby Function
- MRP Interconnection

Standby Function

LED color	LED status	Meaning
-	Off	The standby function is disabled.
Green	On	The standby function is enabled. The standby section is passive.
Green	Flashing	The standby function is enabled. The standby section is active.

MRP Interconnection

LED color	LED status	Meaning
-	Off	MRP Interconnection is disabled.
Green	On	MRP Interconnection redundancy is available.
Green	Flashing	MRP Interconnection redundancy is not available.

4.7.4 "F" LED

The "F" LED shows the fault/error status of the device.

Meaning during device startup

LED color	LED status	Meaning during device startup
-	Off	Device startup was completed successfully.
Red	On	Device startup is not yet completed or errors have occurred.
Red	Flashing	There are errors in the firmware.

Meaning during operation

LED color	LED status	Meaning during operation
-	Off	The device is operating free of errors. The signaling contact is closed.
Red	On	The device has detected a problem. The signaling contact has opened.

4.7.5 LEDs "DM1" and "DM2"

The "DM1" and "DM2" LEDs indicate which display mode is set.

There are 5 display modes (A, B, C, D, and E). Display mode A is the default mode.

Depending on the set display mode, the "L1", "L2" LEDs and the port LEDs show different information.

LED color	LED status		Meaning
	DM1 LED	DM2 LED	
-	Off		Display mode A
Green	On	Off	Display mode B
Green	Off	On	Display mode C
Green	On		Display mode D
Green	Flashing	Off	Display mode E

Setting the display mode

To set the required display mode, press the "SELECT/SET" button.

If you do not press the "SELECT/SET" button for longer than 1 minute, the device automatically changes to display mode A.

Pressing SELECT/SET button starting at display mode A	LED status		Display mode
	DM1	DM2	
-	Off		Display mode A
Press once	On	Off	Display mode B
Press twice	Off	On	Display mode C
Press three times	On		Display mode D
Press four times	Flashing	Off	Display mode E

4.7.6 LEDs "L1" and "L2"

The "L1" and "L2" LEDs indicate the current range of the power supply at connectors L1 and L2.

The meaning of the "L1" and "L2" LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 35)".

Meaning in display modes A, B, C and E

In display modes A, B, C and E, from the "L1" and "L2" LEDs you can see whether the power supply is higher or lower than 17 V.

L1/L2 LED		L1/L2 connector
LED color	LED status	
-	Off	Power supply lower than 17 V
Green	On	Power supply higher than 17 V

Meaning in display mode D

In display mode D, the "L1" and "L2" LEDs indicate whether the power supply is monitored.

L1/L2 LED		L1/L2 connector
LED color	**LED status**	
-	Off	Power supply is not monitored. If the power supply falls below 17 V, the signaling contact does not respond.
Green	On	Power supply is monitored. If the power supply falls below 17 V, the signaling contact responds.

4.7.7 Port LEDs

The port LEDs "P1", "P2" etc. show information about the corresponding ports.

The meaning of the Port LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 35)".

Meaning in display mode A

In display mode A, the port LEDs indicate whether a valid link exists.

LED color	LED status	Meaning
-	Off	No valid link to the port (for example communications partner turned off or cable not connected).
Green	On	Link exists and port in normal status. In this status, the port can receive and send data.
	Flashes once per period*	Link exists and port in "Blocking" status. In this status, the port only receives management data (no user data).
	Flashes three times per period*	Link exists and port turned off by management. In this status, no data is sent or received via the port.
	Flashes four times per period*	Link exists and is in the "Monitor Port" status. In this status, the data traffic of another port is mirrored to this port.
Yellow	Flashing / lit	Receiving data at port

* 1 period ≙ 2.5 seconds

Meaning in display mode B

In display mode B, the port LEDs indicate the transmission speed.

LED color	LED status	Meaning
-	Off	Port operating at 10 Mbps
Green	On	Port operating at 100 Mbps
Orange	On	Port operating at 1000 Mbps
Green	Flashing	Port operating at 10 Gbps

If there is a connection problem and the type of transmission is fixed (auto negotiation off), the desired status, in other words the set transmission speed (10 Gbps, 1000 Mbps,

100 Mbps, 10 Mbps) continues to be displayed. If there is a connection problem and auto negotiation is active, the port LED goes off.

Meaning in display mode C

In display mode C, the port LEDs indicate the mode.

LED color	LED status	Meaning
-	Off	Port operating in half duplex mode
Green	On	Port operating in full duplex mode

Meaning in display mode D

In display mode D, the port LEDs indicate whether the port is monitored.

LED color	LED status	Meaning
-	Off	Port is not monitored. If no link was established at the port the signaling contact does not indicate an error.
Green	On	Port is monitored. If no link was established at the port the signaling contact indicates an error.

Meaning in display mode E

In display mode E, the port LEDs indicate whether the connected device is supplied using PoE.

LED color	LED status	Meaning
-	Off	The connected device is not supplied using PoE.
Green	On	The connected device is supplied via PoE.

4.8 C-PLUG/KEY-PLUG

4.8.1 Function of the C-PLUG/KEY-PLUG

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

Saving configuration data and enabling layer 3 functionality

A PLUG is an exchangeable storage medium for storing the configuration data of the device. This allows fast and uncomplicated replacement of a device. The 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.

In addition to the configuration, a KEY-PLUG also contains a license with which layer 3 functionality is enabled.

Note

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

How it works

Operating mode

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

- Without C-PLUG/KEY-PLUG
  The device stores the configuration in internal memory.
  This mode is active if no C-PLUG/KEY-PLUG is inserted.
- With unwritten C-PLUG/KEY-PLUG
  If an unwritten C-PLUG/KEY-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/KEY-PLUG during startup.
  This mode is active as soon as an unwritten C-PLUG/KEY-PLUG is inserted.
- With written C-PLUG/KEY-PLUG
  A device with a written and accepted C-PLUG/KEY-PLUG ("ACCEPTED" status) automatically uses its configuration data during startup.
  Acceptance is only possible if the data was written by a compatible device type.
  This mode is active as soon as a written C-PLUG/KEY-PLUG is inserted.

Operation with C-PLUG/KEY-PLUG

The configuration stored on the C-PLUG/KEY-PLUG is displayed via the user interfaces.

If changes are made to the configuration, the device stores the configuration directly on the C-PLUG/KEY-PLUG, if this is in the "ACCEPTED" status. The internal memory is neither read nor written.

Response to errors

Inserting a C-PLUG/KEY-PLUG that does not contain the configuration of a compatible device type, accidentally removing the C-PLUG/KEY-PLUG or general malfunctions of the C-PLUG/KEY-PLUG are signaled by the diagnostics mechanisms of the device (LEDs, Web-based management (WBM), SNMP, Command Line Interface (CLI) and PROFINET diagnostics).

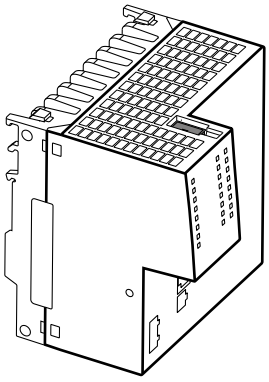
The user then has the choice of either removing the C-PLUG/KEY-PLUG again or selecting the option to reformat the C-PLUG/KEY-PLUG.

4.8.2 Replacing the C-PLUG/KEY-PLUG

Position of the C-PLUG/KEY-PLUG

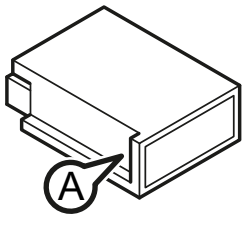
NOTICE
Do not remove or insert a C-PLUG/KEY-PLUG during operation A C-PLUG/KEY-PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a C-PLUG/KEY-PLUG is inserted at one second intervals. If it is detected that the C-PLUG/KEY-PLUG was removed, there is a restart. If a KEY-PLUG was inserted in the device, the device changes to a defined error state following the restart.

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



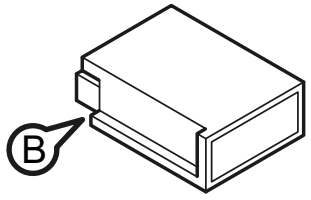
Replacing a C-PLUG/KEY-PLUG

Removing a C-PLUG/KEY-PLUG



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

Inserting a C-PLUG/KEY-PLUG



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

4.9 Functions

4.9.1 Combo ports

Characteristics

Combo port is the name for two communication ports. A combo port has the two following jacks:

- a fixed RJ-45 port
- an SFP transceiver slot that can be equipped individually

Of these two ports, only one can ever be active. Using the mode, you can decide how the ports are prioritized.

The port name is the same on both jacks of the combo port, for example "PxC".

There is an LED for each combo port. The LEDs for the combo ports can be identified by a vertical line and the word "COMBO". The labeling of the combo port LEDs does not differ from that of the other LEDs, e.g. "P3".

Setting the mode

The following modes can be configured for a combo port:

- Mode 1: **auto**
  The SFP transceiver port has priority. As soon as an SFP transceiver is plugged in, an existing connection at the fixed RJ-45 port is terminated. If no SFC transceiver is plugged in, a connection can be established via the fixed RJ-45 port.
- Mode 2: **rj45**
  The fixed RJ-45 port is independent of the SFP transceiver port.
- Mode 3: **sfp**
  The pluggable transceiver port is used independent of the fixed RJ-45 port.

The factory setting for the combo ports is mode 1: auto

You configure the mode with Web Based Management or the Command Line Interface.

4.9.2 Power over Ethernet (PoE)

Function

The "Power over Ethernet" function supplies connected devices with power via the Ethernet cable. Devices supplied with power via an Ethernet cable do not require a separate voltage source.

PoE-compliant devices can be divided into the following groups:

- Power source (PSE - Power Sourcing Equipment)
  These inject power onto the Ethernet cable.
- Power consumer (PD - Powered Device)
  These are supplied with power via the Ethernet cable.

Power over Ethernet with SCALANCE XM-400

With a SCALANCE XM-400, you can use the "Power over Ethernet" function via the port extender PE408PoE as the power generator.

You will find suitable PoE power supplies in the section "Accessories (Page 24)".

You will find detailed information on the port extender PE408PoE in the operating instructions "Extenders for SCALANCE XM-400".

You will find the Operating Instructions 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 (http://support.automation.siemens.com/WW/view/en/79730528/133300)

installing and removing

5

5.1 Safety notices for installation

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 temperature of the cable or housing socket exceeds 70 °C or the temperature at the branching points of the cables exceeds 80 °C, special precautions must be taken. If the device is operated at max. ambient temperature, only use cables with permitted maximum operating temperature of at least 90 °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 equipment shall only be used in an area with pollution degree 1 or 2 (see also EN/IEC 60664-1, GB/T 16935.1).

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.

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.

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", under "Further documentation".

5.2 Types of installation

Types of installation

You have the following options for the device:

- DIN rail
- S7-300 standard rail
- S7-1500 standard rail

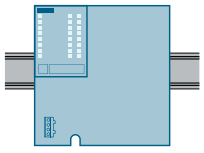
Installation clearance

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 location

Mount the devices horizontally so that the LED display is at the top left and the ventilation openings are oriented up and down.

Horizontal Horizontal installation of the rack (DIN rail).	 Example of mounting position on standard rail

5.3 Mounting on DIN rails

Installation

WARNING

Danger of injury by falling objects

The 35 mm DIN rail does not provide adequate support in shipping or when there is severe vibration (> 10 g). When used under these conditions, the device can detach itself and may cause injury to persons.
When used in shipbuilding or when extreme vibration can be expected, mount the device on a S7 standard rail.

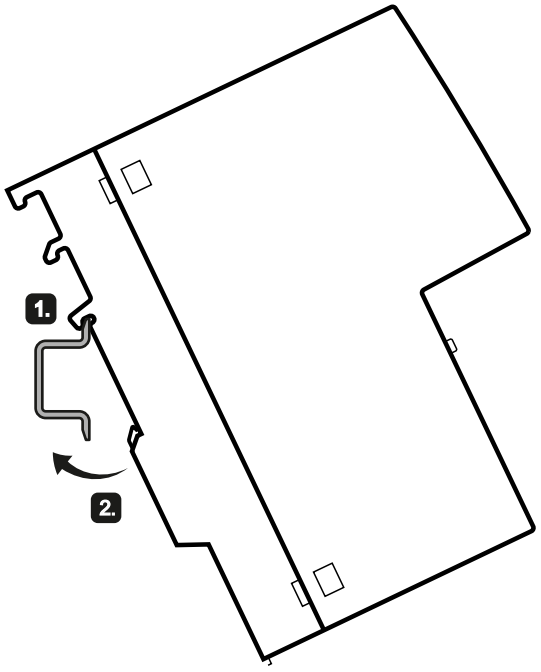


Figure 5-1 DIN rail mounting

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

1. Place the third housing guide of the device on the top edge of the DIN rail ①.
2. Press the device down against the DIN rail until the spring catch locks in place ②.
3. Connect the electrical connecting cables; refer to the section "Connecting up (Page 53)".

Removal

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

1. Disconnect all connected cables.
2. Release the DIN rail catch on the bottom of the device using a screwdriver.
3. Pull lower part of the device away from the DIN rail.

5.4 Installation on a standard S7-300 rail

Installing on an S7-300 standard rail

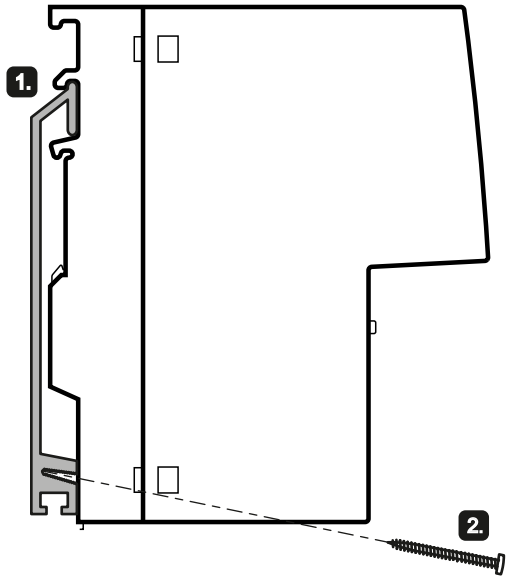


Figure 5-2 S7-300 standard rail mounting

To screw the device to an S7-300 standard rail, you require a securing screw with the following properties:

- Self-tapping screw 4 x 45 mm
- Screw head diameter: max. 7 mm

To install the device on an S7-300 standard rail, follow the steps below:

1. Place the second housing guide of the device on the top edge of the standard rail ①.
2. Screw the device to the lower part of the standard rail with the supplied securing screw ② (tightening torque 1.5 Nm), see also "Device views (Page 29)".
3. Connect the electrical connecting cables; refer to the section "Connecting up (Page 53)".

Removal

To remove the device from a standard rail, follow the steps below:

1. Disconnect all connected cables.
2. Release the screw on the underside of the standard rail.
3. Remove the device from the standard rail.

5.5 Installation on a standard S7-1500 rail

Installing on an S7-1500 standard rail

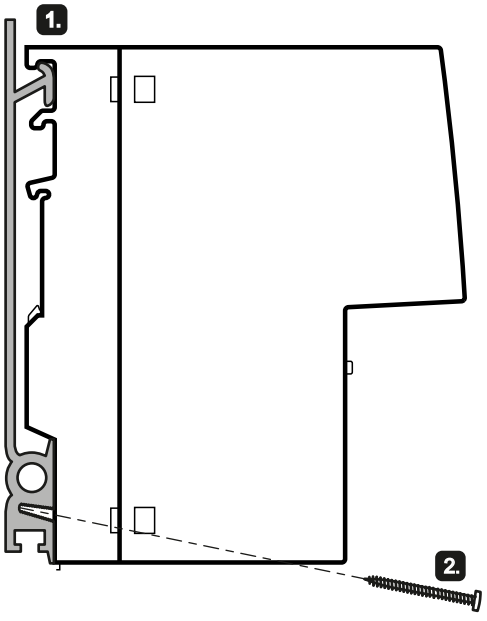


Figure 5-3 S7-1500 standard rail mounting

To screw the device to an S7-1500 standard rail, you require a securing screw with the following properties:

- Self-tapping screw 4 x 45 mm
- Screw head diameter: max. 7 mm

To install the device on an S7-1500 standard rail, follow the steps below:

1. Place the first housing guide of the device on the top edge of the standard rail ①.
2. Screw the device to the lower part of the standard rail with the supplied securing screw ② (tightening torque 1.5 Nm), see also "Device views (Page 29)".
3. Connect the electrical connecting cables; refer to the section "Connecting up (Page 53)".

Removal

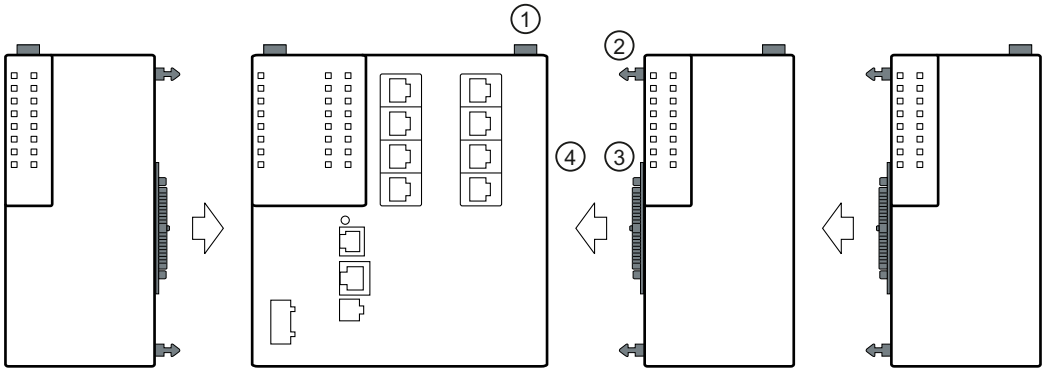
To remove the device from a standard rail, follow the steps below:

1. Disconnect all connected cables.
2. Release the screw on the underside of the standard rail.
3. Remove the device from the standard rail.

5.6 Fitting an extender

Position

The following figure shows the elements required to connect two devices.



① Locking mechanism (on the rear of the device)
② Centering pin
③ Multipole connector for connection to the expansion interface
④ Expansion interface with cover

Via the expansion interface, the basic device supplies the extenders with power and manages the ports of the extenders.

The power provided by the PE408PoE port extender for Power over Ethernet does not come from the basic device. Connect an external power source, see e.g. section "Accessories (Page 24)".

Types of installation

You have the following options when connecting devices:

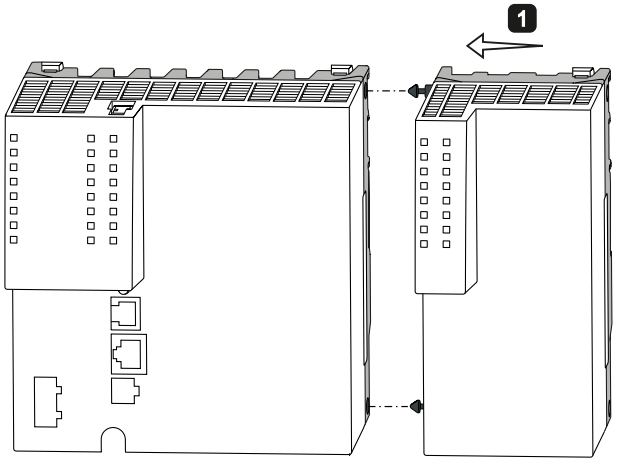
- You can connect the devices and mount them together on a DIN or S7 standard rail.
- You can mount a device on a DIN or S7 standard rail and expand it later.

Note

For mounting on a rail as well as for removing from the rail, plan enough space between the devices, see section "Extender dimension drawings (Page 75)".

Fitting and removing an extender

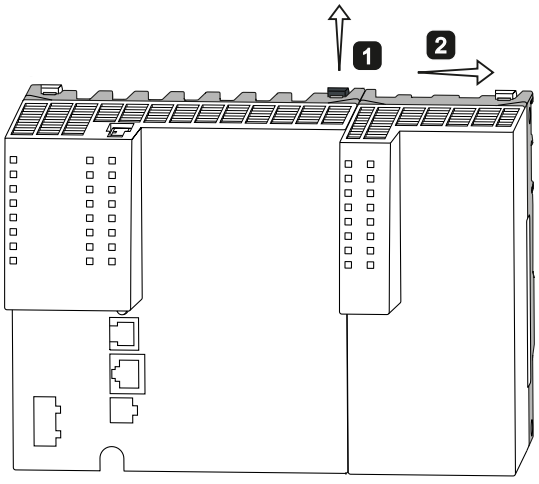
Fitting an extender



To fit an extender, follow the steps below:

1. Remove the cover of the expansion interface on the basic device.
2. Fit the two devices together so that the two centering pins are accommodated by the opposing openings ①.
3. Press the devices together until they are flush.
   The centering pins click audibly into place. The locking device is automatically pressed up briefly as this happens.

Removing an extender



To remove an extender, follow the steps below:

1. Release the locking device using a screwdriver ①.
   The two devices are separated from each other.
2. Pull the two devices apart in a straight line ② until the two centering pins are completely out of the openings.

Exchanging extenders - with change of medium

Exchanging extenders

If you replace an electrical extender with an optical extender (or vice versa), this can lead to malfunctions.

The IE switch therefore reacts as follows:

- The extender is disabled.
- The red fault LED "F" lights up.
- The event is shown in the log table in WBM.

Enabling the extender

To activate the replacement extender, restart the IE switch:

- The extender is active.
- The red fault LED "F" goes off.

5.7 General notes for SFP transceivers

WARNING

Use only approved plug-in transceivers

If you use plug-in transceivers that have not been approved by Siemens AG, there is no guarantee that the device will function according to its specifications.
If you use unapproved plug-in transceivers, this can lead to the following problems:

- Damage to the device
- Loss of the approvals
- Violation of the EMC regulations

Use only approved plug-in transceivers.

Note

Plugging and pulling during operation

You can plug and pull plug-in transceivers with the device in operation.

Note

LASER Class 1

All plug-in transceivers you use in the devices must comply with LASER Class I according to IEC/EN 60825-1. All plug-in transceivers from Siemens AG comply with LASER Class I according to IEC/EN 60825-1.

Documentation for plug-in transceivers

You will find detailed information in the operating instructions of the plug-in transceivers, see the chapter "Introduction (Page 5)" section "Additional documentation".

5.8 Disassembly

WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

Connecting up

6

6.1 Safety when connecting up

Safety notices

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.

NOTICE

Failure of the data traffic due to contamination of optical plug-in connections

Optical sockets and plugs are sensitive to contamination of the end face. Contamination can lead to the failure of the optical transmission network. Take the following precautions to avoid functional impairments:

- Clean the end face of field-assembled connectors carefully before connecting. No residues of processing may remain on the connector.
- Only remove the dust caps of optical transceivers and pre-configured cables shortly before connecting the cables.
- Close unused optical sockets and plugs as well as pluggable transceivers and slots with the supplied protective caps.

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

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.

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.

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

If the device is operated at max. ambient temperature, only use cables with permitted maximum operating temperature of at least 90 ℃. The cable entries used on the enclosure must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB 3836.1.

Further notes

⚠ WARNING

Commissioning devices and replacement devices

If you use redundancy mechanisms (HRP/MRP ring redundancy and/or redundant coupling of rings with standby), open the redundant path before you insert a new or replacement device in an operational network. A bad configuration or attachment of the Ethernet cables to incorrectly configured ports causes overload in the network and a breakdown in communication.

A device may only be inserted in a network and connected in the following situations:

- With HRP/MRP:
  - Ring redundancy must be activated
  - The mode must be selected correctly.
  - The ring ports of the device being inserted in the HRP/MRP ring must be configured as ring ports.
- With standby link:
  - The standby connection must be activated.
  - The "Standby Connection Name" must match the name of the partner device.
  - The port must be configured as a standby port.

For further information, refer to the configuration manuals (Page 5).

In areas subject to the NEC or CEC:

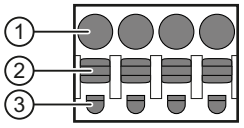
⚠ WARNING

Safety notice for connectors with LAN (Local Area Network) marking

A LAN or LAN segment, with all its associated interconnected equipment, shall be entirely contained within a single low-voltage power distribution and within a single building. The LAN is considered to be in an "environment A" according to IEEE802.3 or "environment 0" according to IEC TR 62102, respectively. Never connect directly to TNV-circuits (Telephone Network) or WAN (Wide Area Network).

6.2 Spring-loaded terminal

The following figure shows the individual components of a spring-loaded terminal:



①	Wire inlet	For connecting the wire
②	Button	For releasing the wire
③	Test contact	For measuring the voltage

6.3 Power supply

Notes on the power supply

⚠ WARNING

Incorrect power supply

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

Never operate the device with AC voltage or 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 devices of the SCALANCE CM-400 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 is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element.

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

Operate the SCALANCE XM-400 with suitable overvoltage protection.

Note

The extenders and pluggable transceivers are supplied with power via the basic device.

Information on the power supply

- The "L1" and "L2" LEDs indicate the current range of the power supply, see the section "LEDs "L1" and "L2" (Page 36)".
- The power supply is connected using a 4-pin plug-in terminal block (spring-loaded terminal). The terminal block ships with the device and can also be ordered as a spare part.
- The power supply can be connected redundantly. Both inputs are isolated. There is no distribution of load. When a redundant power supply is used, the power supply unit with the higher output voltage supplies the SCALANCE XM-400 alone.
- The power supply is connected over a high resistance with the enclosure to allow an ungrounded set up. The two power inputs are non-floating.
- To wire up the power connector, use a copper cable of category 18-12 AWG or cable with a cross-section of 0.75 to 2.5 mm^2.

Position and assignment

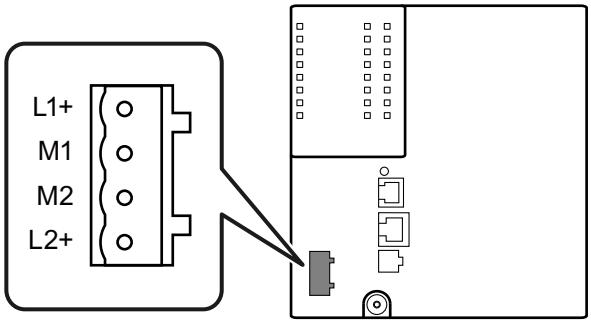


Figure 6-1 Position of the power supply on the SCALANCE XM-400 and the assignment of the terminal block

Contact	Assignment
L1+	24 VDC
M1	Ground
M2	Ground
L2+	24 VDC

6.4 Signaling contact

Information on the signaling contact

- The signaling contact is a floating switch that signals error statuses by opening the contact. The signaling contact must be operated within the range of the operating voltage. If an error/fault occurs, the signaling contact opens. In normal operation, the signaling contact is closed.
- The signaling contact is connected using a 2-pin plug-in terminal block (spring-loaded terminal). The terminal block ships with the device and can also be ordered as a spare part.
- To wire up the signaling contact, use a copper cable of category 18-12 AWG or a cable with a cross-section of 0.75 to 2.5 mm^2.

NOTICE
Damage due to voltage being too high
The signaling contact can be subjected to a maximum load of 100 mA (safety extra-low voltage SELV, 24 VDC).
Higher voltages or currents can damage the device!

Position and assignment

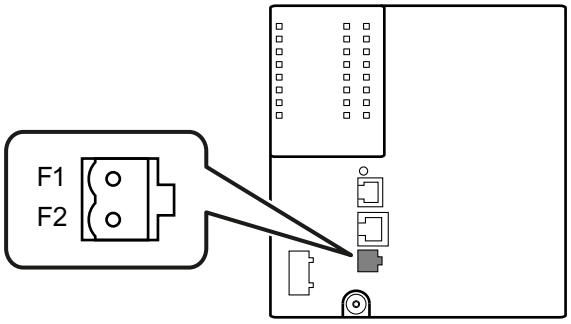


Figure 6-2 Position of the signaling contact on the SCALANCE XM-400 and the assignment of the terminal block

Pin number	Assignment
Pin 1	F1
Pin 2	F2

Signaling faults

- The signaling of errors by the signaling contact is synchronized with the fault LED "F", see section ""F" LED (Page 35)".
  All errors that the fault LED "F" indicates (freely configurable) are also signaled by the signaling contact.
- If an internal fault occurs, the fault LED "F" lights up and the signaling contact opens.
- If you connect a communications node to an unmonitored port or disconnect it, this does not cause an error message.
- The signaling contact remains open until one of the following events occurs:
  - The problem is eliminated.
  - The current status is entered in the fault mask as the new desired status.

6.5 Serial interface

Information on the serial interface

- Via the serial interface on the device (RJ-11 jack), you can access the CLI of the device directly via an RS-232 (115200 8N1) connection 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. The connecting cable for the serial interface ships with the device and can also be ordered as a spare part.

Position and assignment

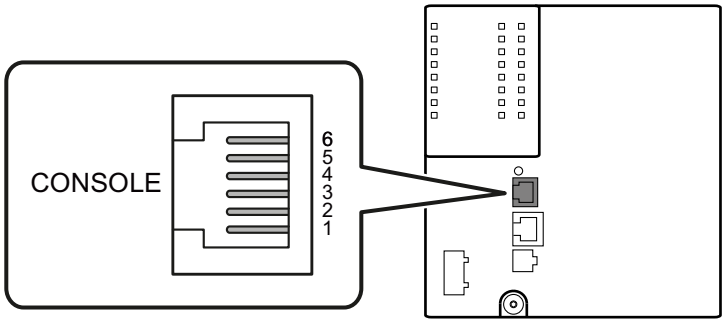


Figure 6-3 Position and pin assignment of the serial interface (RJ-11 jack) on the SCALANCE XM-400 and the pin assignment of the D-sub female connector.

Assignment of the terminal block

The supplied connecting cable has the following 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 supplied connecting cable.

6.6 Out-of-band interface

Information on the out-of-band interface

- The out-of-band interface is an RJ-45 Ethernet port on the CPU module. The out-of-band interface is not used for routing or switching.
- Access to the device is also possible independent of the other Ethernet ports.
- The out-of-band interface allows direct IP access to the WBM of the device.

Position and assignment

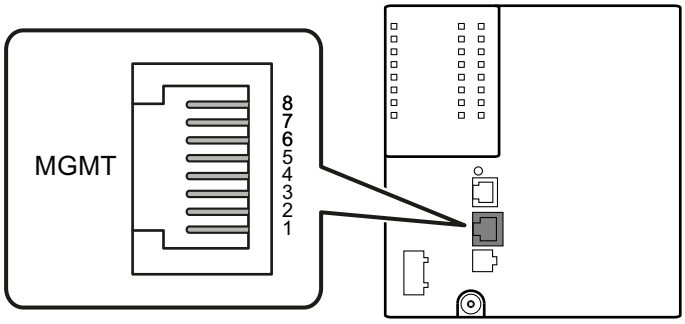


Figure 6-4 Position and pin assignment of the out-of-band interface (RJ-45 jack) on the SCALANCE XM-400.

6.7 Functional ground

Position

The functional ground is established via a grounding screw.

The connector for the grounding cable is in the center of the underside of the device.

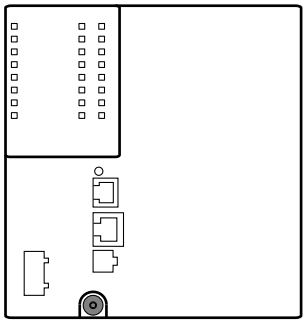
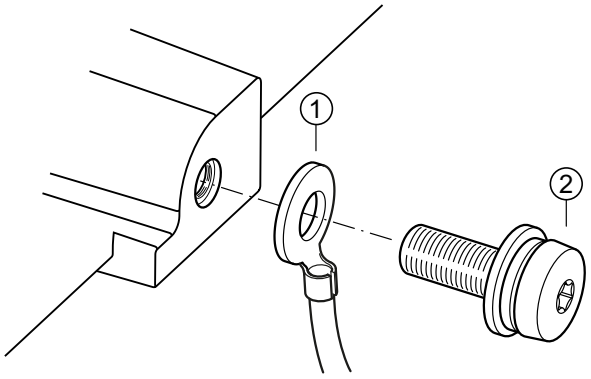


Figure 6-5 Position of the grounding bolt on the SCALANCE XM-400

Connecting up functional ground



① Grounding terminal with cable
② Bolt with spring washer and washer

Follow the steps below to connect the functional ground:

1. Loosen the grounding screw.
2. Put the grounding terminal ①, and the bolt ② together as shown in the drawing.
3. Screw in the bolt ② with a maximum tightening torque of 1.5 Nm.

Upkeep and maintenance

7

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 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.

Troubleshooting

8

8.1 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.

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. Now press the "SELECT/SET" button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red fault LED "F" starts to flash after approximately 30 seconds.
4. Now release the button. 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 the out-band interface of the device via an Ethernet cable.
6. Assign an IP address to the device using DHCP or SINEC PNI.
7. In a Windows command prompt, navigate 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.

8.2 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 in the configured network.

Restoring the factory settings during the startup phase

NOTICE
Reset despite disabled "SELECT/SET" button
Using the "SELECT/SET" button, you can always reset the device parameters to the factory defaults during the startup phase of the device. This applies also if the "Reset to Factory Defaults" function was disabled in the configuration. This allows you to reset 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 reset 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 "SELECT/SET" button and reconnect the power 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 reset the device to the factory defaults during operation, see section "SELECT / SET button (Page 32)".

Technical specifications

9

9.1 Technical specifications of the SCALANCE XM408-4C

The following technical specifications apply to the SCALANCE XM408-4C.

Technical specifications				
Attachment to Industrial Ethernet				
Electrical connectors		Quantity	4	
		Connector	RJ45 jack	
		Transmission speed	10 / 100 / 1000 Mbps	
Combo port	Quantity		4	
	Electrical connectors	Quantity	4	
		Connector	RJ45 jack	
		Transmission speed	10 / 100 / 1000 Mbps	
	Slots for pluggable transceivers	Quantity	4	
		Connector	• STP transceiver (ST port) • SCP transceiver (SC port)	
		Transmission speed	100 / 1000 Mbps	
Diagnostics interface				
Serial interface		Quantity	1	
		Connector	RJ-11 jack	
Out-of-band interface		Quantity	1	
		Connector	RJ45 jack	
Electrical data				
Power supply		Rated voltage	24 V DC	
		Voltage range	19.2 V DC - 28.8 V DC	
		Design	Terminal block, 4 terminals	
		Cable cross-section		
		• Minimum	• 0.75 mm^2 (18 AWG)	
		• Maximum	• 2.5 mm^2 (12 AWG)	
		Properties	Implemented redundantly	
Fusing			3.15 A / 125 V	
			Maximum	**XM408-8C**
			incl. extender	8 x RJ-45 with 1000 Mbps
Current consumption		at 24 V DC	2 A	0.6 A
Effective power loss		at 24 V DC	48 W	14.4 W

Technical specifications		
Signaling contact	Quantity	1
	Design	Terminal block, 2 terminals
	Permitted voltage range	24 V DC
	Load capability	max. 100 mA
Permitted ambient conditions		
Ambient temperature/ In areas according to UL508 or CSA C22.2 No.142: Temperature of the ambient air	During operation up to 2000 m	-40 °C to +70 °C
	During operation up to 3000 m	-40 °C to +65 °C
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation at 25 °C	≤ 95%, no condensation
Design, dimensions and weight		
Weight	1150 g	
Degree of protection	IP20	
Dimensions (W x H x D)	140 x 150 x 125 mm	
Installation options	• Installation on a DIN rail • Installation on an S7-300 standard rail • Installation on an S7-1500 standard rail	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	28 years

9.2 Technical specifications of the SCALANCE XM408-8C

The following technical specifications apply to the SCALANCE XM408-8C.

Technical specifications			
Attachment to Industrial Ethernet			
Combo ports	Quantity		8
	Electrical connectors	Quantity	8
		Connector	RJ45 jack
		Transmission speed	10 / 100 / 1000 Mbps
	Slots for pluggable transceivers	Quantity	8
		Connector	SFP transceivers (LC port)
		Transmission speed	100 / 1000 Mbps
Diagnostics interface			
Serial interface		Quantity	1
		Connector	RJ-11 jack
Out-of-band interface		Quantity	1
		Connector	RJ45 jack
Electrical data			

Technical specifications			
Power supply	Rated voltage	24 V DC	
	Voltage range	19.2 V DC - 28.8 V DC	
	Design	Terminal block, 4 terminals	
	Cable cross-section		
	• Minimum	• 0.75 mm^2 (18 AWG)	
	• Maximum	• 2.5 mm^2 (12 AWG)	
	Properties	Implemented redundantly	
Fusing		3.15 A / 125 V	
		Maximum	**XM408-8C**
		incl. extender	8 x RJ-45 with 1000 Mbps
Current consumption	at 24 V DC	2 A	0.6 A
Effective power loss	at 24 V DC	48 W	14.4 W
Signaling contact	Quantity	1	
	Design	Terminal block, 2 terminals	
	Permitted voltage range	24 V DC	
	Load capability	max. 100 mA	
Permitted ambient conditions			
Ambient temperature/ In areas according to UL508 or CSA C22.2 No.142: Temperature of the ambient air	During operation up to 2000 m	-40 °C to +70 °C	
	During operation up to 3000 m	-40 °C to +65 °C	
	During storage	-40 °C to +85 °C	
	During transportation	-40 °C to +85 °C	
Relative humidity	During operation at 25 °C	≤ 95%, no condensation	
Design, dimensions and weight			
Weight	1150 g		
Degree of protection	IP20		
Dimensions (W x H x D)	140 x 150 x 125 mm		
Installation options	• Installation on a DIN rail		
	• Installation on an S7-300 standard rail		
	• Installation on an S7-1500 standard rail		
Mean time between failure (MTBF)			
	at 40 °C ambient temperature	28 years	

9.3 Technical specifications of the SCALANCE XM416-4C

The following technical specifications apply to the SCALANCE XM416-4C.

Technical specifications				
Attachment to Industrial Ethernet				
Electrical connectors		Quantity	12	
		Connector	RJ45 jack	
		Transmission speed	10 / 100 / 1000 Mbps	
Combo ports	Quantity		4	
	Electrical connectors	Quantity	4	
		Connector	RJ45 jack	
		Transmission speed	10 / 100 / 1000 Mbps	
	Slots for pluggable transceivers	Quantity	4	
		Connector	SFP transceivers (LC port)	
		Transmission speed	100 / 1000 Mbps	
Diagnostics interface				
Serial interface		Quantity	1	
		Connector	RJ-11 jack	
Out-of-band interface		Quantity	1	
		Connector	RJ45 jack	
Electrical data				
Power supply		Rated voltage	24 V DC	
		Voltage range	19.2 V DC - 28.8 V DC	
		Design	Terminal block, 4 terminals	
		Cable cross-section		
		• Minimum	• 0.75 mm^2 (18 AWG)	
		• Maximum	• 2.5 mm^2 (12 AWG)	
		Properties	Implemented redundantly	
Fusing			3.15 A / 125 V	
			Maximum incl. extender	**XM416-4C** 16 x RJ-45 with 1000 Mbps
Current consumption		at 24 V DC	2 A	0.7 A
Effective power loss		at 24 V DC	48 W	16.8 W
Signaling contact		Quantity	1	
		Design	Terminal block, 2 terminals	
		Permitted voltage range	24 V DC	
		Load capability	max. 100 mA	
Permitted ambient conditions				
Ambient temperature/ In areas according to UL508 or CSA C22.2 No.142: Temperature of the ambient air		During operation up to 2000 m	-40 °C to +70 °C	
		During operation up to 3000 m	-40 °C to +65 °C	
		During storage	-40 °C to +85 °C	
		During transportation	-40 °C to +85 °C	

Technical specifications		
Relative humidity	During operation at 25 °C	≤ 95%, no condensation
Design, dimensions and weight		
Weight	1250 g	
Degree of protection	IP20	
Dimensions (W x H x D)	140 x 150 x 125 mm	
Installation options	• Installation on a DIN rail • Installation on an S7-300 standard rail • Installation on an S7-1500 standard rail	
Mean time between failure (MTBF)		
	at 40 °C ambient temperature	22 years

9.4 Switching properties

The switching properties listed below apply to the SCALANCE XM-400.

Switching properties			
Aging time	Can be configured (default value: 40 seconds)		
Max. number of learnable addresses	16000		
Maximum frame size	9194 bytes (configurable)		
Forwarding of PRP frames (Parallel Redundancy Protocol)	Yes		
Switching technique	Store and forward		
Latency	25 - 70 microseconds		
Reconfiguration times for redundancy methods:			
	Redundancy method		**Reconfiguration time**
	HRP		300 ms
	Standby link		300 ms
	MRP		200 ms
Full wire speed switching:			
	Number of frames per second		**Frame length**
	At 100 Mbps	At 1000 Mbps	
	148810	1488095	64 bytes
	84459	844595	128 bytes
	45290	452899	256 bytes
	23496	234962	512 bytes
	11973	119732	1024 bytes
	9615	96154	1280 bytes
	8127	81274	1518 bytes

Note

The number of SCALANCE XM-400 modules connected in a line influences the frame delay. When a frame passes through the switch, this is delayed by the store-and-forward function of the SCALANCE XM-400 by 25-70 microseconds (at 1000 Mbps).

Dimension drawings

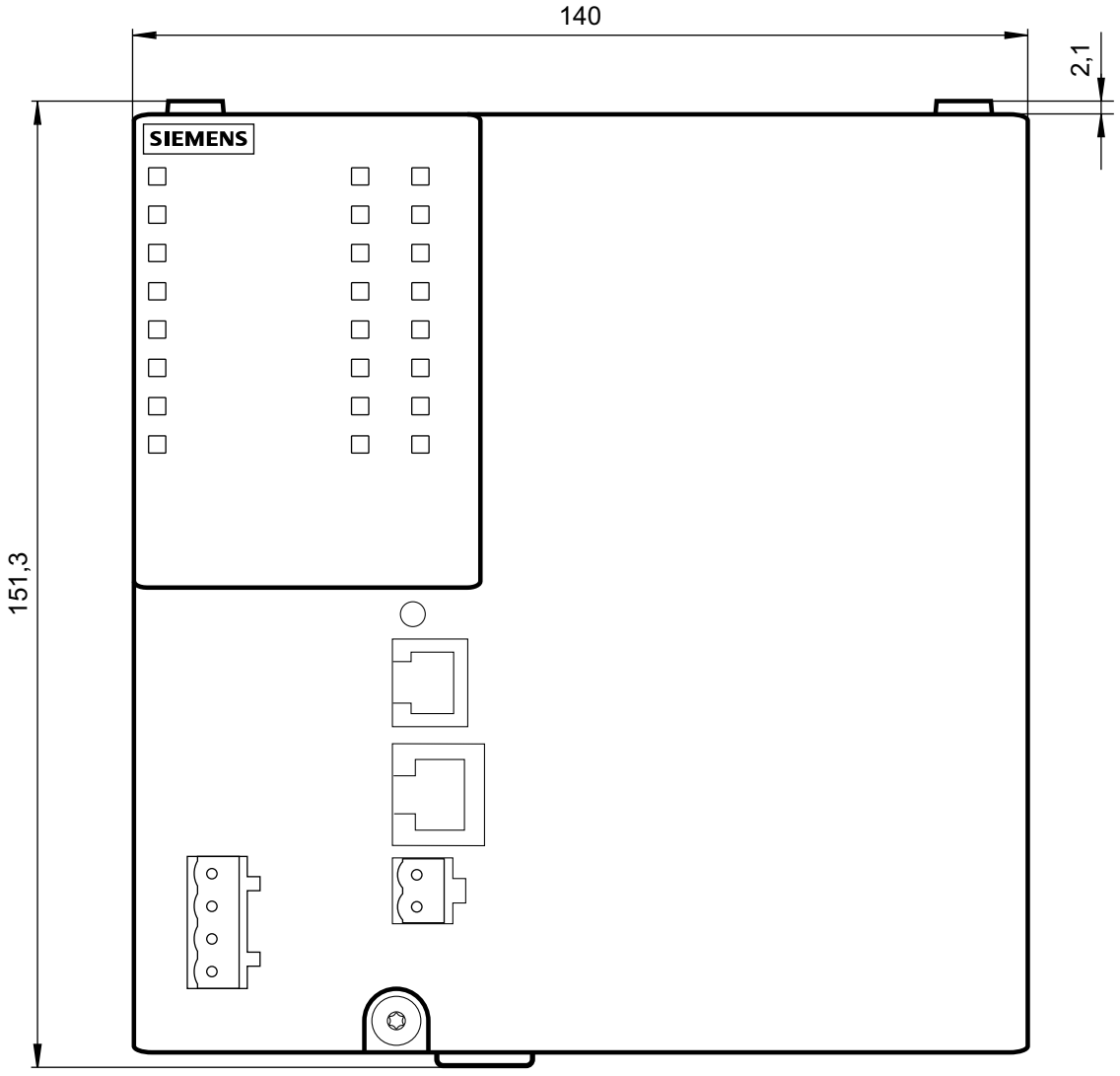
10

10.1 SCALANCE XM-400 dimension drawings

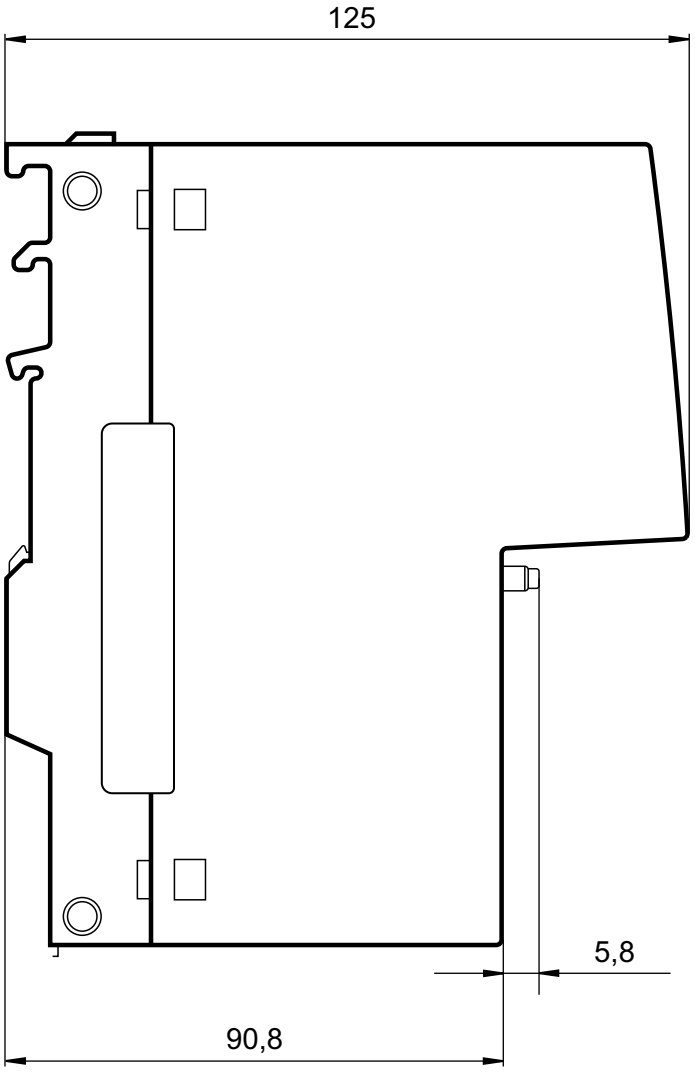
Note

Dimensions are specified in mm.

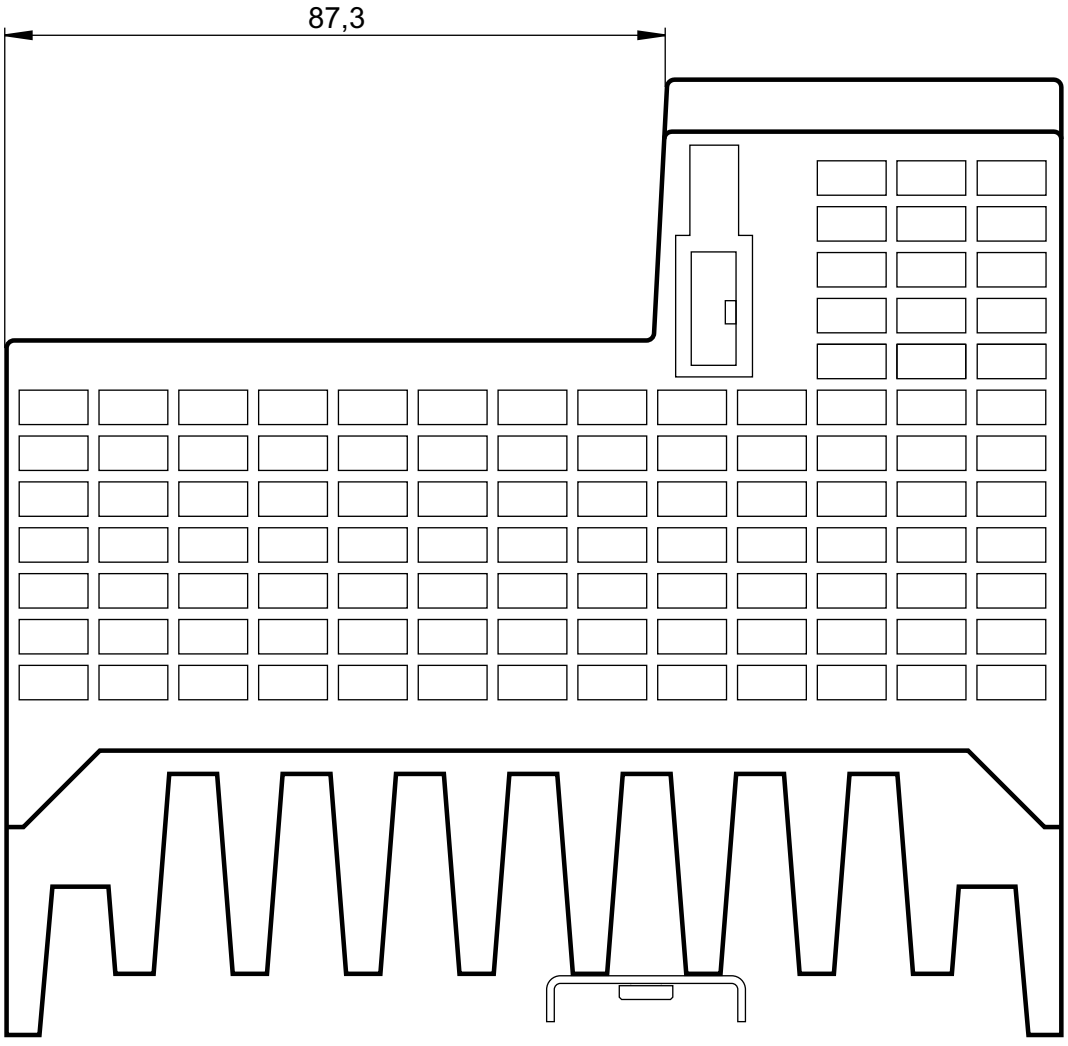
Front view



Side view



From above



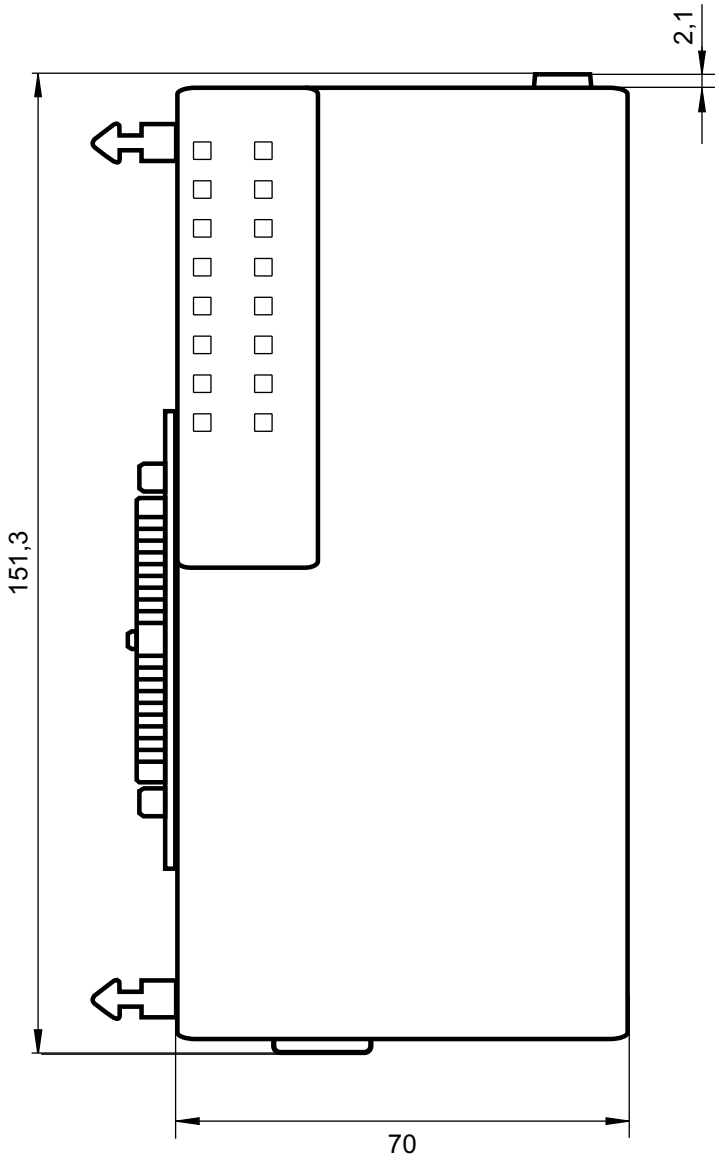
10.2 Extender dimension drawings

Note

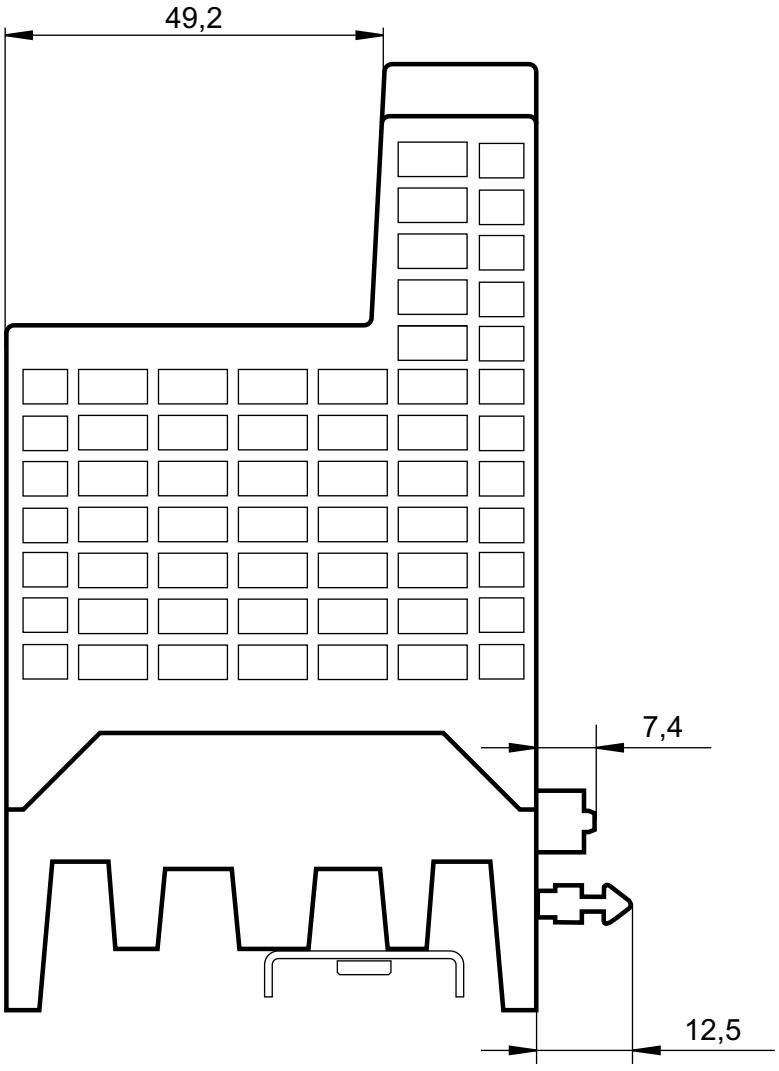
Installing on a rail

Remember the following dimensions if you want to mount two devices on a rail.

Front view



From above



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/15315/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/15312/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 industrial control equipment

cULus Listed IND. CONT. EQ.

Underwriters Laboratories Inc. complying with

- UL 508
- CSA C22.2 No. 142-M1987

Report no. E85972

cULus Approval for Information Technology Equipment



cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

- UL 60950-1 (Information Technology Equipment)
- CSA C22.2 No. 60950-1-03

Report no. E115352

cULus Approval Hazardous Location



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

Underwriters Laboratories Inc. complying with

- UL 60950-1 (Information Technology Equipment)
- ANSI/ISA 12.12.01-2007
- CSA C22.2 No. 213-M1987

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).

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 XM408-4C	(*)
SCALANCE XM408-8C	(*)
SCALANCE XM416-4C	(*)
* In modular devices, you can find the marking in the operating instructions for the plug-in transceiver or extender used.	

CAUTION

Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Mechanical stability (in operation)

Device	IEC 60068-2-6 vibration *	IEC 60068-2-6 vibration	IEC 60068-2-27 shock
	5 - 9 Hz: 3.5 mm 9 - 150 Hz: 1 g 1 octave/min, 20 sweeps	**10 - 58 Hz: 0.075 mm 85 - 150 Hz: 1 g 1 octave/min, 20 sweeps**	**15 g, 11 ms duration 6 shocks per axis**
SCALANCE XM408-4C	●	●	●
SCALANCE XM408-8C	●	●	●
SCALANCE XM416-4C	●	●	●

* Note: When installing on an S7-300 or S7-1500 standard rail

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, 24
Approvals, 79
Article number, 22, 26, 27

B

Basic device, 21
BUS ANALYZER, 6
BUS ANALYZER Agent XM-400, 6, 22, 26

C

CE mark, 79
Centering pin, 49
CLI, 6, 39, 59, 65
Combo port, 34, 41
Command Line Interface, 6, 39, 59, 65
Components of the product, 23
Configuration, 33, 39
Configuration manual, 6, 56
Connecting cable, 59
C-PLUG, 24, 27, 29, 30, 31, 39

D

Defining the fault mask, 33
Display mode, 32, 35

E

Expansion, 21
Expansion interface, 21, 29, 30, 31, 49
Extender, 5, 21

F

Factory defaults, 32, 66
Factory setting, 32, 66
Factory settings, 66
Fault mask, 33
Fault/error status, 35
Firmware, 35, 65
Function extender, 22, 26
Function Extender BUS ANALYZER Agent XM-400, 22, 26
Functional ground, 61

G

Glossary, 7
Grounding, 29, 30, 31, 61

I

Installation
  Installation on a DIN rail, 47
  Installation on a standard rail, 48, 49
Installation on a DIN rail, 47
Installation on a standard rail, 48, 49

K

KEY-PLUG, 24, 29, 30, 31, 39

L

Layer 3, 39
Layer 3 functionality, 39
LED, 34
License, 39
Locking mechanism, 49

O

Out-of-band interface, 60, 65

P

PE408PoE, 5, 42, 49
PLUG, 39
Pluggable transceiver, 5
  SCP, 27, 29
  SFP, 24, 25, 30, 31
  STP, 27, 29
PoE, 42, 49
  Port extender PE408PoE, 42, 49
PoE power supply, 5, 27, 42, 49
PoE power supply unit, 5, 27, 42, 49
Port extender, 5, 22

Port extender PE408PoE, 42, 49
Power over Ethernet, 42, 49
  Port extender PE408PoE, 42, 49
Power supply, 5, 27, 42, 49, 57
Power supply unit, 5, 27, 42, 49
PS9230 PoE, 5, 27, 42, 49
PS924 PoE, 5, 27, 42, 49

R

Reset device, 32, 66
Reset to Factory Defaults, 66
Restore Factory Defaults, 33

S

S7-1500, 49
S7-300, 48
Safety notices
  for installation, 43
  general, 11
  Use in hazardous areas, 11, 43, 53
  when connecting up, 53
SCALANCE PS9230 PoE, 5
SCALANCE PS924 PoE, 5
SCP, 5
SCP transceiver, 27, 29
Securing location, 29, 30, 31, 48, 49
Securing screw, 24, 27, 29, 30, 31, 48, 49
SELECT/SET button, 32, 36, 65, 66
Serial interface, 59
SFP, 5
SFP plug-in transceiver, 24
SFP transceiver, 25, 30, 31
SFP transceiver slots, 21
SFP+, 5
Signaling contact, 35, 58
SIMATIC NET glossary, 7
SIMATIC NET manual, 7
Spare parts, 27
Spring-loaded terminal, 24, 27, 56, 57, 58
Startup phase, 33, 35, 66
STP, 5
STP transceiver, 27, 29
System manual, 7, 45, 84

T

Transceiver, 5

W

WBM, 6, 39, 60, 65
Web Based Management, 6, 39, 60, 65