SIEMENS

SIMATIC NET

Network components SCALANCE LPE9403

Operating Instructions

Introduction 1

Safety notices 2

Security recommendations 3

Description of the device 4

Installation and removal 5

Connecting up 6

Maintenance and cleaning 7

Troubleshooting 8

Technical specifications 9

Dimension drawings 10

Certifications and approvals 11

06/2024
C79000-G8976-C599-06

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-C599-06
Ⓟ 09/2024 Subject to change

Copyright © Siemens 2021 - 2024.
All rights reserved

Table of contents

1 Introduction 7

1.1 Scope of validity 7

1.2 Designations used 7

1.3 Supplementary documentation 7

1.4 Trademarks 8

1.5 SIMATIC NET glossary 9

1.6 Cybersecurity information 9

1.7 Error/fault 9

1.8 Decommissioning 10

1.9 Recycling and disposal 10

1.10 Electrostatic discharge 10

2 Safety notices 11

3 Security recommendations 13

4 Description of the device 21

4.1 Article numbers 21

4.2 Type designation 21

4.3 Device view 22

4.4 Components of the product 22

4.5 Spare parts 23

4.6 Accessories 23

4.6.1 Configuration License PLUG 23

4.6.2 Serial USB cable 24

4.6.3 SFP transceivers 24

4.7 LED display 25

4.7.1 "A" LED 25

4.7.2 Port LEDs 26

4.7.3 "L" LED 27

4.8 SET button 27

4.9 Configuration and License PLUG (CLP) 28

4.10 Combo port 29

4.11 Function extender interface 30

4.11.1 Compatible SCALANCE switches 30

5 Installation and removal ... 33
5.1 Safety during installation and removal ... 33
5.2 Mounting types ... 36
5.3 Mounting on DIN rails ... 37
5.4 Installation on a standard S7-300 rail ... 38
5.5 Installation on a standard S7-1500 rail ... 40
5.6 Wall mounting ... 41
5.7 Changing the position of the securing bar ... 42
5.8 Connecting a SCALANCE switch with a SCALANCE LPE9403 ... 43
5.9 General notes for SFP transceivers ... 46
6 Connecting up ... 47
6.1 Safety when connecting up ... 47
6.2 Wiring rules ... 53
6.3 24 V DC power supply ... 54
6.4 Functional ground ... 56
6.5 Industrial Ethernet ... 58
6.5.1 Electrical ... 58
6.5.2 Optical ... 59
6.6 USB console interface ... 60
6.7 USB interface ... 61
7 Maintenance and cleaning ... 63
8 Troubleshooting ... 65
8.1 System time and firmware update ... 65
8.2 Downloading the firmware in the Rescue system via TFTP ... 67
8.3 Starting the Rescue system when using the Function Extender Interface ... 68
8.4 Error messages when downloading the firmware in the Rescue system ... 69
8.5 Resetting the configuration ... 71
9 Technical specifications ... 73
9.1 Technical specifications of SCALANCE LPE9403 ... 73
9.2 Mechanical stability (in operation) ... 75
9.3 RF radiation according to NAMUR NE21 ... 75
9.4 Cable lengths ... 76
10 Dimension drawings ... 77
10.1 SCALANCE LPE9403 dimension drawings ... 77
10.2 Dimension drawings SCALANCE XCM-300 ... 79

11 Certifications and approvals 83
Index 91

Introduction 1

These operating instructions support you when installing and connecting up devices of the SCALANCE LPE9403 product group.

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

1.1 Scope of validity

These operating instructions apply to the following devices:

- SCALANCE LPE9403

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

1.2 Designations used

This section describes the conventions used in this document to clearly and efficiently portray information.

Classification	Description	Terms used
Product group	If information applies to all devices and variants of a product group, the term SCALANCE LPE is used.	SCALANCE LPE
Device	If information relates to a specific device, the device name is used.	e.g. SCALANCE LPE9403

1.3 Supplementary documentation

The following additional documents may be of interest. Unless specified otherwise, the documents are available in the Siemens Industry Online Support (SIOS) (https://support.industry.siemens.com/cs/ww/en/ps/15247).

Note

The listed documents are the documents that were available at the time of the publication. Newer versions of these documents or the associated products may be available. Additional information is available in the SIOS or contact your Siemens customer service.

Product notes

Product notes are available online in the SIOS (https://support.industry.siemens.com/cs/ww/en/ps/15247).

Manuals

Document title	Link
"SCALANCE LPE9403 V3.0" configuration manual	Visit (https://support.industry.siemens.com/cs/ww/en/ps/26683/man)
"Pluggable transceiver SFP/SFP+/SCP/STP" operating instructions	Visit (https://support.industry.siemens.com/cs/ww/en/ps/25547/man)
"SCALANCE XCH-300/XCM-300" equipment manual	Go to one of the following links: • SCALANCE XCH-300 (https://support.industry.siemens.com/cs/ww/en/ps/29449/man) • SCALANCE XCM-300 (https://support.industry.siemens.com/cs/ww/en/ps/29448/man)

Catalogs

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

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

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

1.4 Trademarks

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

- SCALANCE
- SINEC

Linux® is the registered trademark of Linus Torvalds in the United States and other countries.

The registered trademark Linux® is used according to a sublicense of LMI, the exclusive licensee of Linus Torvalds, owner of the trademark on a global basis.

1.5 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)

1.6 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).

1.7 Error/fault

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

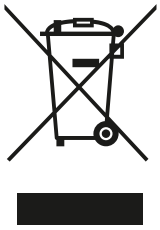
1.8 Decommissioning

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

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

Also restore the factory settings on the storage medium.

1.9 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).

Note the different national regulations.

1.10 Electrostatic discharge

NOTICE
Electrostatic sensitive devices (ESD) Electronic modules contain electrostatic sensitive components These components can easily be destroyed if handled incorrectly. Note the following instructions to avoid damage. • Touch electronic modules only when you absolutely need to work on them. • If electronic modules need to be touched, the body of the person involved must first be electrostatically discharged and grounded. • Do not bring electronic modules in contact with electrically isolating materials such as plastic film, isolating table top pads or clothing made of synthetic fibers. • Place the modules only on conductive surfaces. • Pack, store and transport electronic modules and components only in conductive packaging such as metalized plastic or metal containers, conductive foam or household aluminum foil.

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 instructions for use in hazardous locations according to UL/FM HazLoc

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

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

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

Security recommendations

3

NOTICE
Information security Connect to the device and change the default password and the name of the default user "admin" before operating the device.

To prevent unauthorized access, note 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.
- 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.
- 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

- Operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Restrict physical access to the device to trusted personnel.
- Lock unused physical ports on the device. Unused ports can be used to access the system without authorization.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device.
- For communication via non-secure networks, use additional devices with VPN functionality to encrypt and authenticate communication.

- When you establish a secure connection to a server (e.g. for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTP, HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it.

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 website.
- Inform yourself regularly about security recommendations published by Siemens ProductCERT.
- Only activate protocols that you require to use the device.
- Disable encryption methods with a low security level.
- 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.
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches. You can find the latest information on security patches for Siemens products on the Industrial Security or ProductCERT Security Advisories website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.

Security by Default

Security by Default is a concept in which the configuration possibilities of the device are adapted automatically depending on the status of the device. All necessary configuration steps can be performed without restrictions in delivery state or after a reset to factory settings. After the first login and during operation, only users with administrator rights can configure security-relevant parameters. Non-secure management interfaces are either unavailable (Telnet) or disabled (HTTP, SNMPv1).

NOTICE

Security risk - risk of unauthorized access and/or misuse

By definition, DCP is not secure. The access rights of DCP depend on the status of the device.

- In the delivery state and after reset to default settings, DCP is enabled. Device parameters can be both read and modified. The access rights of DCP correspond to the `read-write` option.
  The `read-write` setting could potentially be used to change the functionality of the device and thus cause the data communication to fail. Users with malicious intent who are in the same local network segment can change IP parameters and/or the PROFINET device name without authentication.
- After the first login with the default user profile **admin** and the assignment of a new password, the device changes the access rights automatically. Only read access is then possible with DCP. The device parameters can be read but not modified. From that point on, the access rights of DCP correspond to the `read-only` option.

To prevent unauthorized access and/or misuse, configure write-protected access rights for DCP (`read-only`).

Security by Default affects configuration with DCP as follows:

- **In delivery state or after a reset to factory settings**
  - Read and write access is possible via ports **P3C** and **EXTENDER1**.
  - DCP is disabled for ports **P1** and **P2** or **EXTENDER2** and **EXTENDER3**.
- **In operating state and after changing the default password**
  - Only read access is possible via ports **P3C** and **EXTENDER1**.
  - DCP is disabled for ports **P1** and **P2** or **EXTENDER2** and **EXTENDER3**.

Security by Default has no effect on DHCP. DHCP is enabled for ports **P1** to **P3C** and **EXTENDER1**. Ports **EXTENDER2** and **EXTENDER3** are disabled by default.

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 X.509 TLS certificate in the device. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed either by a reliable external or by an internal certification authority.
- Use a certification authority including key revocation and management to sign certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- It is recommended that you use password-protected certificates in the PKCS #12 format.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- It is recommended to use certificates with sufficient cryptographic security.
- Change certificates and keys immediately if there is a suspicion of compromise.
- 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.

Handling certificates on the SCALANCE LPE

When the user does not have their own certificate saved in the device, SCALANCE LPE automatically uses the device certificate that is available on each device. For security reasons, this certificate is not visible in the file system.

When a user certificate with the name **server_certificate_custom.pem** exists in the **/etc/ssl/certs/edgebox_web_app/https** directory, the device uses this certificate instead of the module certificate with login via the Web UI. With login via the Linux shell, the module certificate is always used. During a reset of the configuration, all user certificates in the **/etc/ssl/certs/edgebox_web_app/https** directory are deleted.

Secure/non-secure protocols and services

- Check whether use of the following protocols and services is necessary:
  - Non-authenticated and unencrypted ports
  - Syslog
  - DHCP options 66/67
  - TFTP (The TFTP service is only active in the Rescue system.)
- The following protocols provide secure alternatives:
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP
  - NTP → NTPsecure
- Use secure protocols when access to the device is not secured by physical protection measures.
- If you require non-secure protocols and services, operate them 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, enable secure protocols and services.
- After commissioning, the Discovery and Basic Configuration Protocol (DCP) access rights are automatically set to write-protected. If your environment does not require DCP, it is recommended that the protocol be completely disabled.

Interface security

- Disable unused interfaces.
- Use IEEE 802.1X for interface authentication.

List of available protocols

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

- **Protocol/service**
  The protocols/services supported by the device.
- **Protocol**
  The protocol used by the service.

- **Port number**
  The port number assigned to the service.

  Note

  The table contains the preset ports. Additional ports can be opened for protocols with a configurable port number.

- **Default port status/protocol status**
  The default state (i.e. open, closed, active).
- **Protocol/service configurable**
  Specifies whether or not the protocol or service can be configured.
- **Port number configurable**
  Specifies whether the port number can be configured.
- **Authentication**
  Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption can be configured.

Service	Protocol	Port number	Default port status	Protocol/ service configurable	Port number configurable	Authentication	Encryption
Edgeboxwebapp	TCP	8080	Open	✓	✓	-	-
HTTP[1)]	TCP	80	Open	✓	✓	-	-
HTTPS	TCP	443	Open	✓	✓	✓	✓
NTP	UDP	123	Closed	✓	✓	-	-
NTP secure	UDP	123	Closed	✓	✓	✓	-
SFTP	TCP	22	Open	✓	✓	✓	✓
SNMP	UDP	161	Open	✓	✓	Configurable	-
SSH	TCP	22	Open	✓	✓	✓	✓
TFTP	UDP	69	Open[2)]	-	-	-	-

1) Serves only as a reference to the HTTPS service.

2) The TFTP service is only active in the Rescue system.

Outbound connections

Service	Protocol	Port number	Default port status	Protocol/ service configurable	Port number configurable	Authentication	Encryption
DHCP	UDP	68	Closed	✓	-	-	-
Syslog	UDP	(zufällig)[1)]	Closed	✓	-	-	-

1) Needed to send outbound datagrams to the remote syslog server. The port number is not used for inbound traffic.

Service	Protocol	Default protocol status	Protocol/service configurable	Authentication	Encryption
DCP	PROFINET	Active	✓	-	-
LLDP	Ethernet	Active	✓	-	-
Ping	ICMP	Active	-	-	-

Secure Boot

Secure Boot is a security standard that allows a device to start only with trusted software components (bootloader, operating system etc.). Secure Boot is part of the UEFI (Unified Extensible Firmware Interface), an interface between the hardware and the operating system.

During booting with Secure Boot, each involved component is checked for authenticity and integrity. Use of software not signed by the manufacturer is not possible. Furthermore, Secure Boot allows additional security functions for which a secure boot process is essential, such as fTPM with SCALANCE LPE, to be activated.

With Secure Boot, it is no longer possible to use self-generated components for the system test (bootloader, kernel etc.). There are not restrictions during operation; any applications can be installed, updated, modified or deleted as before.

SCALANCE LPE supports the Secure Boot function as of hardware release 2. You will find the hardware release of your device on the type plate. On the type plate, the hardware release is printed as a placeholder "X". "X 2 3 4 5 6" designates a device with hardware release 1.

Description of the device

4

The SCALANCE LPE (Local Processing Engine) is an industrial IoT (Internet of Things) device with a Debian GNU/Linux operating system. The device provides computing power for a wide range of Edge applications (Edge Computing). A further main application is the use of Docker containers in industrial environments. The rugged housing in SIMATIC S7-1500 format and the fanless design enable use in direct manufacturing environments.

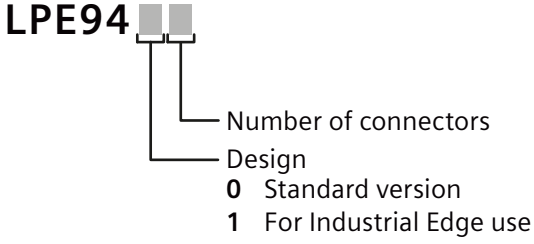
4.1 Article numbers

Device	Description	Article number
SCALANCE LPE9403	The SCALANCE LPE9403 can be operated either standalone or connected with a SCALANCE switch. In **standalone operation**, the SCALANCE LPE9403 has the following ports: • 2 x 10/100/1000 Mbps RJ45 ports • 1 x combo port (1 x 10/100/1000 Mbps RJ45 port / 1 x pluggable transceiver slot with 100/1000 Mbps) When the SCALANCE LPE9403 is **connected to a SCALANCE switch**, the ports of the SCALANCE LPE9403 work as function extender interface (FEI) ports of the SCALANCE switch with the following speeds: • 2 x 1 Gbps • 1 x 10 Gbps The three FEI ports are available as bridge ports within the SCALANCE switch.	6GK5 998-3GS00-2AC2

For a list of SCALANCE switches with which a SCALANCE LPE can be connected, see "Compatible SCALANCE switches (Page 30)".

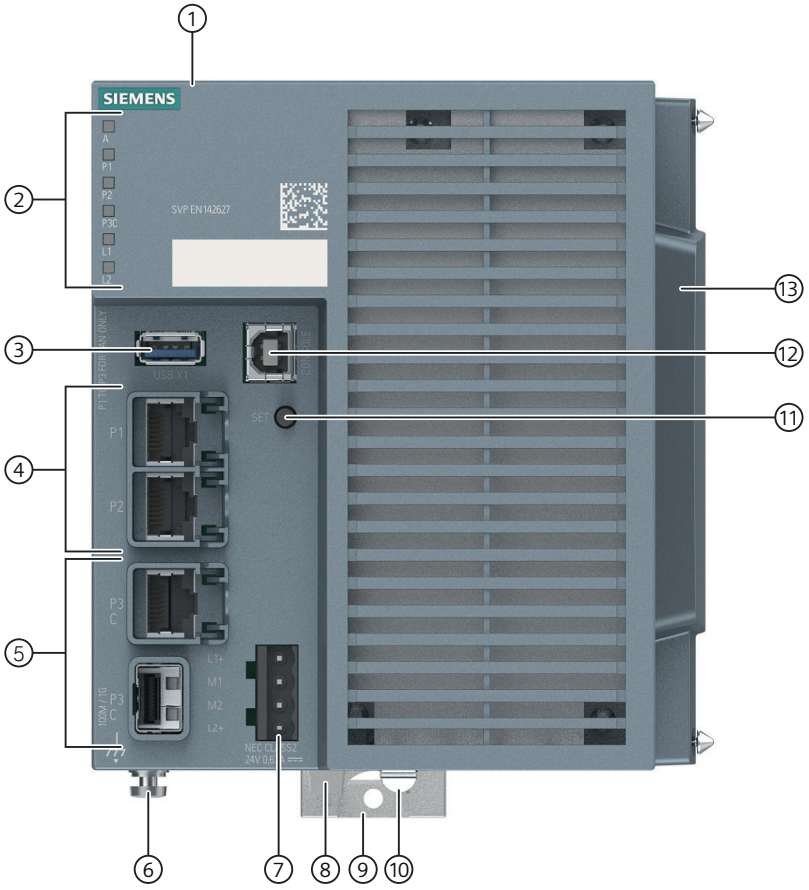
4.2 Type designation

LPE is the acronym for "Local Processing Engine". The type designation of a SCALANCE LPE has the following structure:



4.3 Device view

The following figure shows an overview of the components of the device.



①	CLP slot	⑧	Levering aid for moving the securing bar with a screwdriver
②	LED display	⑨	Securing bar
③	USB 3.0 port (Type A)	⑩	Knurled screw
④	Electrical ports	⑪	"SET" button
⑤	Combo port	⑫	USB 2.0 interface (Type B, serial via USB)
⑥	Grounding screw	⑬	Function extender interface
⑦	Power supply		

4.4 Components of the product

The following components are supplied with the device:

- A SCALANCE LPE
- Two 2-pin terminal blocks for the power supply
- One cover for the pluggable transceiver slot

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.

4.5 Spare parts

The following spare parts are available for the device:

Component	Description	Article number
Spring-loaded terminal block, 4-pin	4-pin spring-loaded terminal block to connect the power supply (24 V DC) Pack of 5	6GK5 980-1DB10-0AA5
Spring-loaded terminal block, 2-pin	2-pin spring-loaded terminal block to connect the power supply (24 V DC) Pack of 5	6GK5 980-0BB10-0AA5

4.6 Accessories

The following accessories are available for the device:

4.6.1 Configuration License PLUG

Component	Description	Article number
SCALANCE CLP 32GB	Configuration License PLUG, removable data storage medium for configuration data, 32 GB	6GK1900-0UB40-0AA0

4.6.2 Serial USB cable

Component	Description	Article number
Connecting cable (USB Type A / USB Type B)	Preassembled USB cable with USB Type A and USB Type B connector, length: 2 m Pack of 1	7ML1930-1FN

4.6.3 SFP transceivers

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 packaging unit (PU 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, coated	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 packaging unit (PU 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, coated	6GK5 991-1AF00-8FA0
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

Pluggable transceivers with the suffix (C) in the type name have coated 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
SFP992-1LD	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

Type	Property	Article number
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

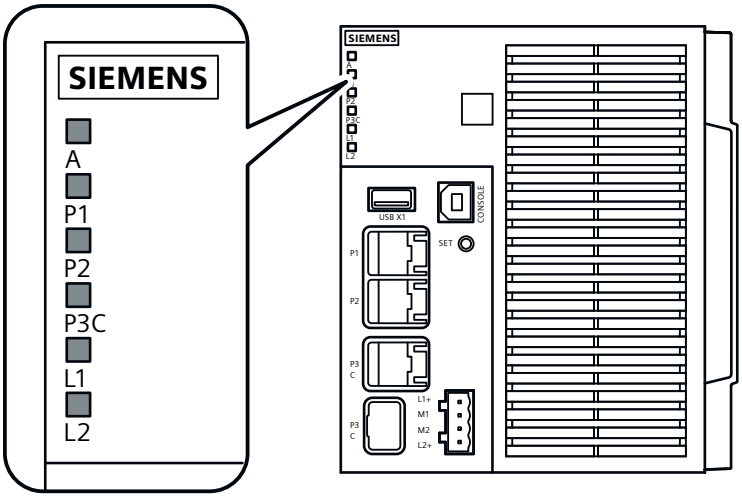
Restriction for pluggable transceivers

The maximum ambient temperature changes if you use pluggable transceivers.

You can find the corresponding values for the ambient temperature in the section "Technical specifications (Page 73)".

4.7 LED display

The following figure shows the arrangement of the LEDs:



A LED for displaying an alarm

P LEDs for displaying the port status

L LEDs for displaying the power supply

4.7.1 "A" LED

The "A" LED indicates an alarm status of the device.

Meaning during device startup without pressing the "SET" button

LED color	LED status	Meaning during device startup
-	Off	Device startup was completed successfully.
Red	On	Device startup is not complete yet or errors have occurred.

Note

When using the function extender interface, LED "A" has the following meaning during device startup:

- LED "A" remains ON until the device startup of the SCALANCE LPE is complete and a connection to a SCALANCE switch has been established.
- LED "A" remains ON permanently if no connection to a SCALANCE switch is possible.

It can take several minutes to establish a connection between a SCALANCE switch and SCALANCE LPE.

Meaning during device startup with pressing the "SET" button

LED color	LED status	Meaning during device startup
-	Off	Reset to factory settings is complete.
Red	Flashing	The device was connected to the power supply while pressing the "SET" button and is in the Rescue system.
Red	On	The device was connected to the power supply while pressing the "SET" button and is being reset to factory settings.

Meaning during operation

LED color	LED status	Meaning during operation
-	Off	The device is operating free of errors.
Red	On	The device has detected an error.

4.7.2 Port LEDs

The port LEDs "P1", "P2" and "P3C" show information about the corresponding ports.

LED color	LED status	Meaning
-	Off	No valid link to the port (for example, communications partner turned off or cable not connected). When using the Function Extender Interface, the port LEDs are always off.
Green	On	A link is established and the port is working in normal status. In this status, the port can receive and send data. The data transmission rate is 10/100/1000 Mbps.
Orange	Flashing / lit	Receiving data at port

4.7.3 "L" LED

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

LED color	LED status	Meaning
-	Off	No power supply connected.
Green	On	Power supply connected to L1 or L2. When using the function extender interface, these LEDs indicate the input via which the SCALANCE switch receives the supply voltage.

4.8 SET button

Position

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

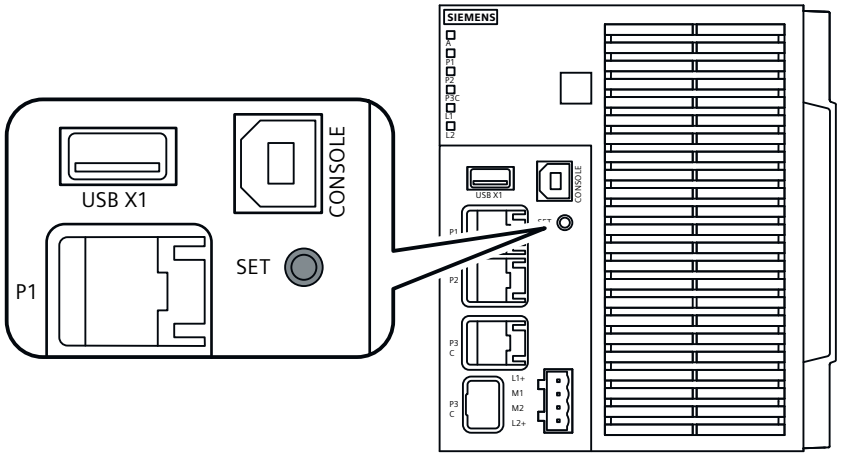


Figure 4-1 Position of the "SET" button on a SCALANCE LPE9403

Function

The **SET** button has the following functions:

- Starting the Rescue system
- Resetting the configuration

Refer to section "Resetting the configuration (Page 71)" for the procedure for resetting the device to the factory settings.

4.9 Configuration and License PLUG (CLP)

SCALANCE LPE has a slot for a CLP on the top of the enclosure. For more information about suitable CLPs for SCALANCE LPE, refer to the "Accessories" section, under "Configuration License PLUG (Page 23)".

NOTICE
Only use approved CLPs Only the CLPs listed in the "Accessories" section are approved for SCALANCE LPE. Any other use of the USB interface (Type C) in the CLP slot can result in malfunctions of the SCALANCE LPE and damage to the device.

NOTICE
Do not remove the CLP during operation The CLP may not be removed during operation of the SCALANCE LPE without further measures. To remove the CLP during operation, follow these steps: 1. Finish any pending write operations with the command **sync**. 2. Unmount the CLP drive with the command **umount**. 3. Remove the CLP from the slot.

After a CLP is inserted in the CLP slot, you need to mount the CLP in the file system of the device. Follow these steps to mount the CLP:

1. Create a directory for access to the CLP:
   `mkdir <Verzeichnisname>`
2. Mount the CLP:
   `sudo mount <Gerätename des CLP> <Verzeichnisname>`
   The following convention applies to the device name:
   - If no USB stick is connected to the device yet via the Type A USB socket on the front of the device, the device name of the CLP is **/dev/sda1**. You can find more information on the Type A USB socket in section "USB interface (Page 61)".
   - If no USB flash drive is connected to the device yet via the Type A USB socket on the front of the device, the **lsblk** (list block devices) command shows the device name of the CLP.

Example

The USB flash drive inserted in the front of the device (but not yet mounted in the file system) has the device name **/dev/sda1**, the inserted CLP has the device name **/dev/sdb1**, as the **lsblk** command shows. You can only mount devices of the type **part** in the file system.

```
admin@lpe9403-VPM7001325:~$ lsblk
NAME         MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda            8:0    1 58.6G  0 disk
└─sda1         8:1    1 29.3G  0 part
sdb            8:16   1  950M  0 disk
└─sdb1         8:17   1  948M  0 part
mmcblk0      179:0    0 14.6G  0 disk
```

```
├─mmcblk0p1  179:1    0  500M  0 part
├─mmcblk0p2  179:2    0  125M  0 part
...
...
```

To create the **/home/admin/usb** directory and mount the CLP at this location in the file system, perform the following commands:

```
mkdir /home/admin/usb
sudo mount /dev/sdb1 /home/admin/usb
```

To show the mount point for the CLP, perform the **lsblk** command again:

```
admin@lpe9403-VPM7001325:~$ lsblk
NAME         MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda            8:0    1 58.6G  0 disk
└─sda1         8:1    1 29.3G  0 part
sdb            8:16   1  950M  0 disk
└─sdb1         8:17   1  948M  0 part /userdata/home/admin/usb
mmcblk0      179:0    0 14.6G  0 disk
├─mmcblk0p1  179:1    0  500M  0 part
├─mmcblk0p2  179:2    0  125M  0 part
...
...
```

4.10 Combo port

Characteristics

Combo port is the name for two corresponding ports. A combo port has the following two plug-in options:

- a fixed RJ45 port
- a pluggable transceiver slot that can be equipped individually

Of these two ports, only one can ever be active. As long as a pluggable transceiver is inserted and detected, the RJ45 port is disabled.

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

Mode

With firmware versions V1.0 to V2.0, only the following mode is available for a combo port:

- **auto**
  The pluggable transceiver port has priority. As soon as a pluggable transceiver is plugged in, an existing connection at the fixed RJ45 port is terminated. If no pluggable transceiver is plugged in, a connection can be established via the fixed RJ45 port.

4.11 Function extender interface

The right side of the enclosure has an interface for connecting the SCALANCE LPE to a compatible SCALANCE switch. This interface is closed with a cover in the delivery state. Connecting the SCALANCE LPE to a SCALANCE switch via this interface results in the following changes:

- You may only connect the power supply to the SCALANCE switch. Read the information in section "24 V DC power supply (Page 54)".
- The RJ45 sockets and the SFP slot are disabled and are available as internal ports. Read the information in section "Function Extender Interface Ports" of the SCALANCE LPE configuration manual.
- The port LEDs are always off because the RJ45 sockets and the SFP slot are disabled. Read the information in section "Port LEDs (Page 26)".
- The procedure for starting the Rescue system changes. Read the information in section "Starting the Rescue system when using the Function Extender Interface (Page 68)".

4.11.1 Compatible SCALANCE switches

The following SCALANCE switches have a function extender interface via which they can be connected with a SCALANCE LPE.

Device	Description	Article number
SCALANCE XCM323	• 16 x 10 / 100 / 1000 Mbps RJ45 ports • 3 x 1 / 2.5 / 5 / 10 Gbps RJ45 ports • 4 x SFP / SFP+ plug-in transceiver slots with 1 / 10 Gbps • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection • 1 x function extender interface for the SCALANCE LPE • Firmware SINEC OS as of version 2.1	6GK5323-4TS01-2AC2
SCALANCE XCM324	• 16 x 10 / 100 / 1000 Mbps RJ45 ports • 8 x SFP / SFP+ plug-in transceiver slots with 1 / 10 Gbps • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection • 1 x function extender interface for the SCALANCE LPE • Firmware SINEC OS as of version 2.1	6GK5324-8TS01-2AC2

Device	Description	Article number
SCALANCE XCH328	• 24 x 10 / 100 / 1000 Mbps RJ45 ports • 4 x SFP / SFP+ plug-in transceiver slots with 1 / 10 Gbps • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection • 1 x function extender interface for the SCALANCE LPE • Conformal-coated PCBs • Firmware SINEC OS as of version 2.1	6GK5328-4TS01-2EC2
SCALANCE XCM328	• 24 x 10 / 100 / 1000 Mbps RJ45 ports • 4 x SFP / SFP+ plug-in transceiver slots with 1 / 10 Gbps • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection • 1 x function extender interface for the SCALANCE LPE • Firmware SINEC OS as of version 2.1	6GK5328-4TS01-2AC2
SCALANCE XCM332	• 32 x 10 / 100 / 1000 Mbps RJ45 ports • 2 x 2-pin terminal block 24 V DC, power supply connection • 1 x CLP slot • 1 x USB Type B, serial interface connection • 1 x 2-pin terminal block 24 V DC, signaling contact connection • 1 x function extender interface for the SCALANCE LPE • Firmware SINEC OS as of version 2.0	6GK5332-0GA01-2AC2

Installation and removal

5

5.1 Safety during installation and removal

Safety notices

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

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.

⚠ 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.

⚠ WARNING
If a device is operated in an ambient temperature of more than 55 to 60 °C, the temperature of the device housing may be higher than 60 °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 of the required safety measures at an ambient temperature higher than 55 to 60 °C.

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

WARNING

EXPLOSION HAZARD

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

WARNING

The device is intended for indoor use only.

WARNING

The device shall only be used in an area with pollution degree 1 or 2 (according to 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 temperature of the cable or housing socket exceeds 60 °C or the temperature at the branching point of the cables 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.

Devices with approval [op is Gb] for optical interfaces

Some devices have an additional ATEX approval according to II 3 (2) G Ex nA [op is Gb] IIC T4 Gc and an additional approval in compliance with IECEx according to Ex nA [op is Gb] IIC T4

Gc, see section "Certifications and approvals (Page 83)". This is indicated on the type plate. The FO bus connections may run through or in a Zone 1 and Zone 2 hazardous area with these devices.

Safety notices when using according to FM

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

⚠ WARNING

EXPLOSION HAZARD

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

⚠ WARNING

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

⚠ WARNING

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

Safety notices when using the device according to ATEX/IECEx and FM

If you use the device under ATEX/IECEx or FM conditions, you must also observe the following safety notices in addition to the general safety notices for protection against explosion:

Note

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

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

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

WARNING

Open equipment

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

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

WARNING

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

Further notes

NOTICE

Warming and premature aging of the network component due to direct sunlight

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

Provide suitable shade to protect the network component against direct sunlight.

5.2 Mounting types

The following types of installation are intended for the device:

- DIN rail
- S7-300 mounting rail
- S7-1500 mounting rail
- Wall mounting

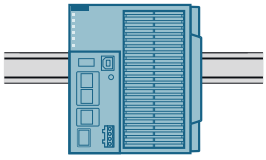
Installation clearance

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 position

The following installation position is recommended in standalone operation:

Horizontal Horizontal installation of the rack (DIN rail)	

A reduced maximum temperature may apply in the event of a different installation position in standalone operation; see section "Technical specifications of SCALANCE LPE9403 (Page 73)".

If the device is connected to a SCALANCE switch, only the horizontal installation position is permitted; see also "Connecting a SCALANCE switch with a SCALANCE LPE9403 (Page 43)".

5.3 Mounting on DIN rails

Installation

Note

Note the position of the securing bar. When supplied, the securing bar is in the wall mounting position. To change the position of the securing bar, refer to the section "Changing the position of the securing bar (Page 42)".

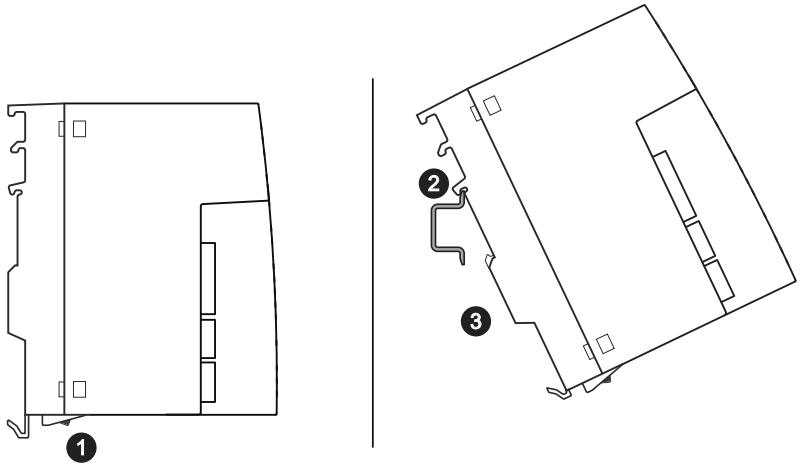


Figure 5-1 DIN rail mounting with securing bar in the wall mounting position

Securing bar in the wall mounting position (as supplied)

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

1. Loosen the knurled screw with your hand or a screwdriver.
2. Place the third housing guide of the device on the top edge of the DIN rail.
3. Press the device down against the DIN rail until the spring-mounted securing bar locks in place.
4. When you tighten the knurled screw. you cannot release the securing bar (torque 0.5 Nm). The device is additionally fixed.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 47)".

Removal

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

1. Disconnect all connected cables.
2. If necessary, loosen the knurled screw with your hand or a screwdriver.
3. Lever the securing bar down using a screwdriver as far as it will go.
4. Pull the device away from the bottom of the DIN rail with the bar pulled.

5.4 Installation on a standard S7-300 rail

Installation on an S7-300 mounting rail

Note

Note the position of the securing bar. When supplied, the securing bar is in the wall mounting position. To change the position of the securing bar, refer to the section "Changing the position of the securing bar (Page 42)".

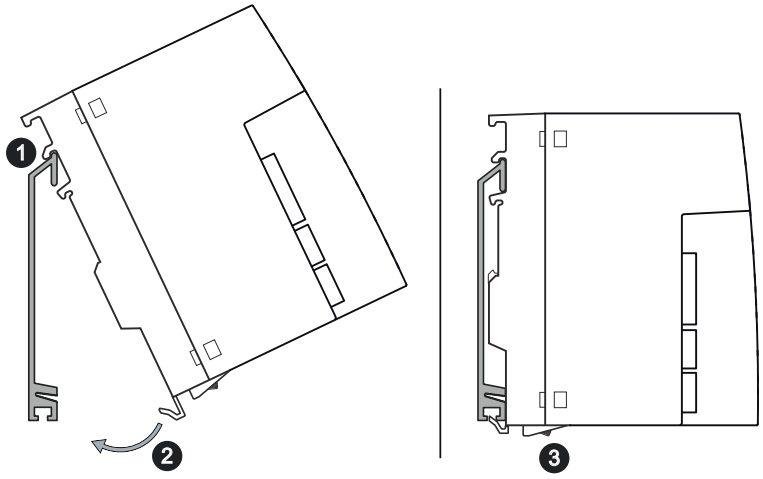


Figure 5-2 S7-300 mounting rail installation with the securing bar in the wall mounting position

Securing bar in the wall mounting position (as supplied)

To install the device on an S7-300 mounting rail, follow these steps:

1. Place the second housing guide of the device on the top edge of the mounting rail.
2. Swing the device down towards the back against the mounting rail.
3. Loosen the knurled screw with your hand or a screwdriver. The spring-mounted securing bar locks into place.
4. When you tighten the knurled screw. you cannot release the securing bar (torque 0.5 Nm). The device is additionally fixed.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 47)".

Removal

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

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

5.5 Installation on a standard S7-1500 rail

Installation on an S7-1500 mounting rail

Note

Note the position of the securing bar. When supplied, the securing bar is in the wall mounting position. To change the position of the securing bar, refer to the section "Changing the position of the securing bar (Page 42)".

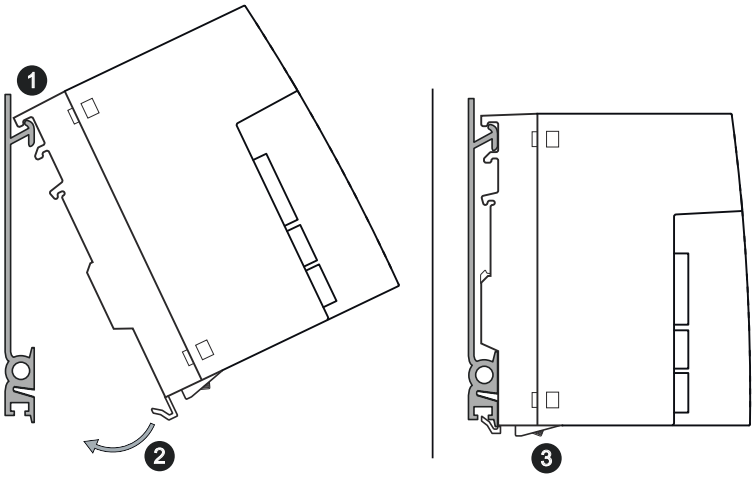


Figure 5-3 S7-1500 mounting rail installation with the securing bar in the wall mounting position

Securing bar in the wall mounting position (as supplied)

To install the device on an S7-1500 mounting rail, follow these steps:

1. Place the first housing guide of the device on the top edge of the mounting rail.
2. Swing the device down towards the back against the mounting rail.
3. Loosen the knurled screw with your hand or a screwdriver. The spring-mounted securing bar locks into place.
4. When you tighten the knurled screw. you cannot release the securing bar (torque 0.5 Nm). The device is additionally fixed.
5. Connect the electrical connecting cables, refer to the section "Connecting up (Page 47)".

Removal

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

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

5.6 Wall mounting

Tools

To mount the device on a wall, you require the following:

- 2 wall plugs with a diameter of 6 mm and a minimum length of 35 mm.
- 2 oval-head screws with a diameter of 3.5 mm to 4 mm and a minimum length of 50 mm.

Note

Depending on the mounting surface, use suitable fittings.

Installation

Note

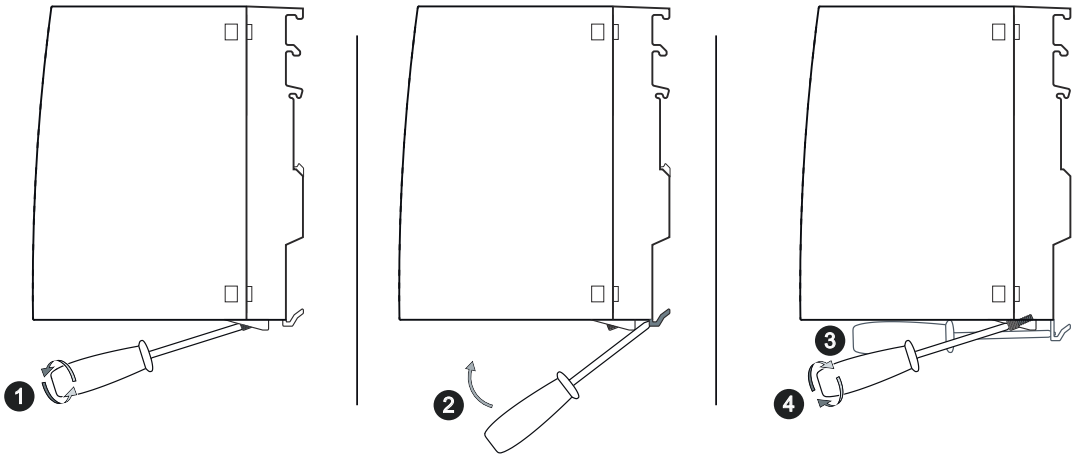
The wall mounting must be capable of supporting at least four times the weight of the device.

To mount the device on a wall, follow the steps below:

1. Prepare the wall mounting with drilled holes and plugs. For the precise dimensions, refer to the section "SCALANCE LPE9403 dimension drawings (Page 77)".
2. Bring the securing bar into position for wall mounting; see section "Changing the position of the securing bar (Page 42)".
3. Turn the upper screw in to the wall so that 10 mm remains jutting out.
4. Hang the device with the keyhole hanging mechanism on the rear on the screw.
5. Fix the device to the wall with the lower screw.
6. Connect the electrical connecting cables, refer to the section "Connecting up (Page 47)".

5.7 Changing the position of the securing bar

Rail mounting position - wall mounting position



To change the securing bar from the rail mounting position to the wall mounting position follow the steps below:

1. If necessary, loosen the knurled screw with your hand or a screwdriver.
2. Move the securing bar down as far as it will go.
   - Use the levering aid and level the securing bar down using a screwdriver into this position.
   - Push the securing bar down using your hand.
3. Hold the securing bar in this position.
   - Hold the securing bar with the screwdriver.
   - Use the gap on the rear of the device and fix the securing bar briefly with a pin.
4. Tighten the knurled screw (torque 0.5 Nm).
   The securing bar is fixed in the wall mounting position.
5. Remove the pin.

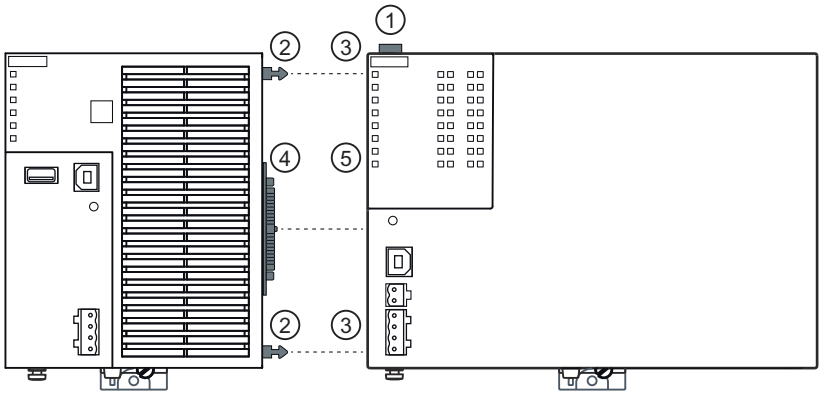
Wall mounting position - rail mounting position

To move the securing bar from the wall mounting position to the rail mounting position, loosen the knurled screw.

5.8 Connecting a SCALANCE switch with a SCALANCE LPE9403

Position

The following figure shows the elements required to connect a SCALANCE switch (Page 30) with a SCALANCE LPE.



① Lock (on the device rear of the SCALANCE switch)
② Centering pin
③ Opening to hold a centering pin
④ Multipole connector for connection to the function extender interface
This connector is closed with a cover in the delivery state.
⑤ Function extender interface
This interface is closed with a cover in the delivery state.

Installation options

You have the following options for connecting the devices:

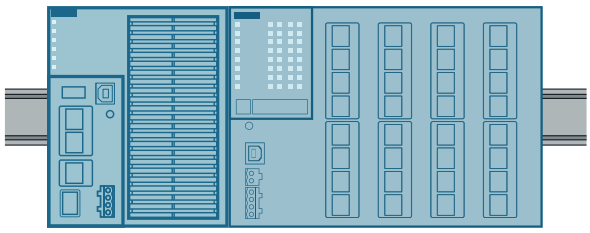
- You can connect the devices and mount them together on a DIN or S7 standard rail.
- You can mount a device on a DIN rail or S7 mounting rail and connect it later.

Note

For mounting on a rail as well as for removing from the rail, plan enough space between the devices, see section "Dimension drawings (Page 77)".

Installation position

If a SCALANCE switch is connected to a SCALANCE LPE, only the following installation position is permitted:

Horizontal Horizontal installation of the rack (e.g. DIN rail)	

Any other installation position can lead to impermissibly high temperatures and damage the devices.

Connecting devices

NOTICE
Danger of damage to property The two devices cannot be connected during operation. Disconnect the two devices from the power supply before connecting the devices.

Follow these steps to connect a SCALANCE switch with a SCALANCE LPE:

1. Disconnect the two devices from the power supply.
2. Remove the function extender interface cover on the SCALANCE switch.
3. Remove the connector cover on the SCALANCE LPE.
4. Fit the two devices together so that the two centering pins ② are accommodated by the opposing openings ③.

5. Press the devices together until they are flush.
   The centering pins click audibly into place. The locking device ① is automatically pressed up briefly as this happens.
6. Connect the SCALANCE switch to the power supply.
   The SCALANCE switch supplies the SCALANCE LPE with power over the function extender interface.

NOTICE
Operating risk - Danger of malfunction during device startup If you have connected a SCALANCE LPE to a SCALANCE switch via the function extender interface, the power for the SCALANCE LPE is supplied exclusively via the SCALANCE switch. This also applies to a redundant power supply. If the SCALANCE switch has a redundant power supply, this redundancy is also provided to the SCALANCE LPE. If you connect both devices to a power supply, this leads to a malfunction during device startup. • Connect the power supply only to the SCALANCE switch. • Do not connect a power supply to the SCALANCE LPE when it is connected to a SCALANCE switch.

Disconnecting devices

NOTICE
Danger of damage to property The two devices cannot be disconnected during operation. Disconnect the SCALANCE switch from the power supply before disconnecting the devices.

Follow these steps to disconnect a SCALANCE switch and a SCALANCE LPE:

1. Disconnect the SCALANCE switch from the power supply.
2. Release the locking device using a screwdriver ①.
   The two devices are separated from each other.
3. Pull the two devices apart in a straight line until the two centering pins ② are completely out of the openings ③.
4. Close the function extender interface on the basic device and the connector on the SCALANCE LPE with the corresponding covers.

5.9 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 7)" section "Additional documentation".

Connecting up 6

6.1 Safety when connecting up

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

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

⚠ WARNING

Power supply

The device is designed for operation with a directly connectable safety extra low voltage (SELV) from a limited power source (LPS). The power supply must meet the requirements for ES1/SELV and PS2/LPS complying with IEC/UL 62368-1.

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

- Only safety extra low voltage (SELV) with limited power source (Limited Power Source, LPS / Power Source Class 2, PS2) complying with IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.
- The power supply unit for the device must meet NEC Class 2 according to the National Electrical Code (r) (ANSI / NFPA 70).

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

⚠ WARNING

Insulation of external power supplies

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

Note

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

Notes on operation with PELV (protective extra-low voltage)

You can operate the device with PELV. When connecting the device, observe the safety information provided below.

Note

Safety extra-low voltage

The supply of the devices by PELV (Protective Extra Low Voltage) according to DIN VDE 0100-410 or IEC 60364-4-41 is permitted when the generated nominal voltage does not exceed the voltage limits 25 VAC or 60 VDC.

⚠ WARNING

Safety extra-low voltage

The relevant standards for the product do not use a PELV concept, which is why product safety-relevant approvals and certifications such as UL ORD LOC, UL HAZ LOC, FM HAZ LOC, ATEX, UKEX, IECEx, CCC-Ex, etc. according to PELV are not possible.

A connection using PELV invalidates the listed approvals and certifications.

⚠ WARNING

Safety extra-low voltage

System power supplies with grounded 24 V DC output voltage require a safe connection to the protective conductor and limiting of the voltage (extra-low voltage) This protection is called PELV (protective extra-low voltage) in accordance with IEC 61131-2 or IEC 61010-2-201. The wiring of PELV circuits must be safely isolated from the wiring of other non-PELV circuits, or the insulation of all conductors must be rated for higher voltage.

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

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

⚠ WARNING

Safety extra low voltage

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

⚠ WARNING

Safety extra low voltage

If the device is operated with a power supply with output power that does not correspond to "Limited Energy" according to UL/IEC 61010-1 or NEC Class 2, the relevant approvals are voided.

⚠ WARNING

Safety notices for operation with a power supply according to "Limited Energy"

1. If the device is supplied by a power supply with limited power (Limited Energy) that complies with IEC/UL61010-1 or VDE 0805-1, no additional power limitation is required according to National Electrical Code (r) (ANSI/NFPA 70).
   If the device is connected to a redundant power supply (two separate power supplies), the combination of the two power supplies must meet these requirements.
   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 3836.3.
2. If the device is operated with a power supply for without power limitation and the entire power requirement does not exceed 100 W, a fuse must be installed between the power supply and each supply input of the device to meet the requirements for limited power (Limited Energy) according to IEC/UL61010-1 or VDE 0805-1. For more information, see "Suitable fusing for the power supply cables" below.
   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 3836.3.
3. If the device is operated with a power supply without power limitation and the entire power requirement exceeds 100 W, the device must be installed in a fire protection housing according to ANSI/UL-61010-1:2018, paragraph 9.3.

NOTICE

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

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

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

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

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

*) AC or DC depending on availability

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

WARNING

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.

WARNING

EXPLOSION HAZARD

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

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 guaranteed if you only operate the devices with SELV (safety extra-low voltage) or PELV (protective extra low voltage).

WARNING

EXPLOSION HAZARD

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

Safety notices when using according to FM

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

WARNING

EXPLOSION HAZARD

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

Safety notices when using the device according to ATEX/IECEx and FM

If you use the device under ATEX/IECEx or FM conditions, you must also observe the following safety notices in addition to the general safety notices for protection against explosion:

⚠ WARNING

Explosion hazard

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

⚠ WARNING

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

Further notes

⚠ WARNING

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

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

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

6.2 Wiring rules

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

Wiring rules for ...		**Screw/spring-loaded terminals**
connectable cable cross sections for flexible cables ...	without wire end ferrule	0.25 - 2.5 mm^2
		AWG: 24 - 13
	with wire end ferrule with plastic ferrule**	0.25 - 2.5 mm^2
		AWG: 24 - 13
	with wire end ferrule without plastic ferrule**	0.25 - 2.5 mm^2
		AWG: 24 - 13
	with TWIN wire end ferrule**	0.5 - 1 mm^2
		AWG: 20 - 17

Wiring rules for ...	Screw/spring-loaded terminals
Stripped length of the cable	8 - 10 mm
Wire end ferrule according to DIN 46228 with plastic ferrule**	8 - 10 mm

* AWG: American Wire Gauge

** See note "Wire end ferrules"

Note

Wire end ferrules

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

Crimp shapes with wave-shaped profile are unsuitable.

6.3 24 V DC power supply

Notes on the power supply

WARNING

Impermissible power supply

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 the SCALANCE LPE to electromagnetic interference is the "surge immunity test" according to EN 61000-4-5. This test requires overvoltage protection for the power supply lines. A suitable device would be, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422, or a comparable protective element.

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

Operate the SCALANCE LPE with appropriate overvoltage protection.

Note

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

Combination of a SCALANCE LPE with a SCALANCE switch via the function extender interface

NOTICE
Operating risk - Danger of malfunction during device startup If you have connected a SCALANCE LPE to a SCALANCE switch via the function extender interface, the power for the SCALANCE LPE is supplied exclusively via the SCALANCE switch. This also applies to a redundant power supply. If the SCALANCE switch has a redundant power supply, this redundancy is also provided to the SCALANCE LPE. If you connect both devices to a power supply, this leads to a malfunction during device startup. • Connect the power supply only to the SCALANCE switch. • Do not connect a power supply to the SCALANCE LPE when it is connected to a SCALANCE switch.

Information on the power supply

- The "L1" and "L2" LEDs indicate whether a power supply is connected or not; see section "LED display (Page 25)".
- The power supply is connected using two 2-pin plug-in terminal blocks (spring-loaded terminal). The terminal blocks ship with the device and can also be ordered as a spare part, see section "Spare parts (Page 23)".
- The power supply can be connected redundantly. Both inputs are isolated. There is no load distribution. When a redundant power supply is used, the power supply unit with the higher output voltage supplies the device alone.
- The power supply is connected over a high resistance with the housing to allow an ungrounded set up. The two power inputs are non-isolated.
- Note the wiring rules (Page 53).

Position and assignment

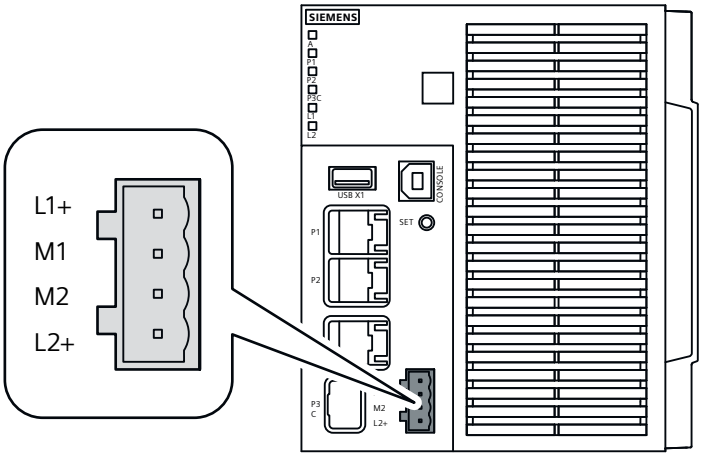


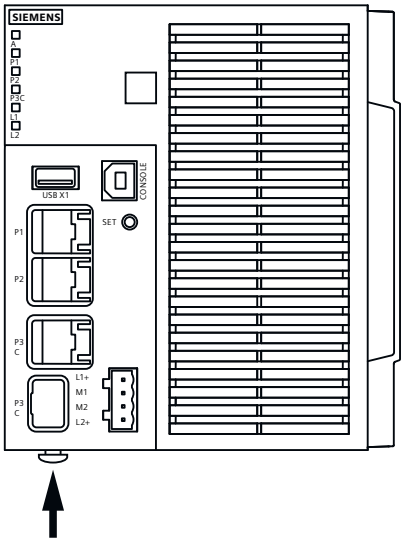
Figure 6-1 Position of the power supply and assignment of the terminal block

Contact	Assignment
L1+	24 V DC
M1	Ground
M2	Ground
L2+	24 V DC

6.4 Functional ground

EMC disturbances are diverted to ground via the functional ground. This ensures the immunity of the data transmission. The functional ground must be implemented with low impedance. The connection of the functional ground must be established directly on the mounting plate or the DIN rail terminal.

The device has a grounding screw (filister head screw with clamping washer and washer) on the bottom of the enclosure for the functional ground:



Follow these steps to connect the functional ground:

1. Loosen the grounding screw.
2. Join the grounding terminal and grounding screw together.
3. Tighten the grounding screw with a maximum torque of 0.75 Nm.

Protective/functional ground

The connection of the reference potential surface with the protective earth system is normally in the cabinet close to the power feed-in. This earth conducts fault currents to ground safely and according to DIN/VDE 0100 is a protective earth to protect people, animals and property from too high contact voltages.

Apart from the protective earth, there is functional ground in the cabinet. According to EN60204-1 (DIN/VDE 0113 T1) electrical circuits must be grounded. The chassis (0 V) is grounded at one defined point. Here, once again the grounding is implemented with the lowest leakage resistance to ground in the vicinity of the power feed-in.

With automation components, functional ground also ensures interference-free operation of a controller. Via the functional ground, interference currents coupled in via the connecting cables are discharged to ground.

6.5 Industrial Ethernet

6.5.1 Electrical

Note

Strain relief for the Ethernet cables

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

Note

Unlocking the plug with a screwdriver

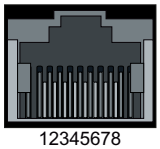
If installation space is limited, you can unlock the connectors using a screwdriver, see also "SIMATIC NET: IE FC RJ45 Plug 4x2 CAT 6A (https://support.industry.siemens.com/cs/ww/en/view/102047916)".

R-45 connector technology

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

Pin assignment

The following table shows the pin assignment of the R-45 connectors.

Pin number	Assignment		R-45 connector
	10/100 Mbps	10/100/1000 Mbps	
Pin 1	RD+	D1+	 12345678
Pin 2	RD-	D1-	
Pin 3	TD+	D2+	
Pin 4	n. c. (Not connected)	D3+	
Pin 5	n. c. (Not connected)	D3-	
Pin 6	TD-	D2-	
Pin 7	n. c. (Not connected)	D4+	
Pin 8	n. c. (Not connected)	D4-	

MDI / MDI-X autocrossover

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

Autonegotiation

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

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

Note

- If a port is set permanently to full duplex, the connected partner port must also be set to full duplex.
- If a port operating in "Autonegotiation" mode is connected to a partner port that is not operating in "Autonegotiation" mode, the partner port must be set permanently to 100 Mbps or 10 Mbps full-duplex mode.
- If you disable the "Auto negotiation" function, the "MDI/MDI-X autocrossover" function is also turned off. Then use a crossover cable.

6.5.2 Optical

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.

LC connector technology

The attachment to Industrial Ethernet uses LC connector technology (Lucent Connector).

Pluggable transceiver slot/
plugged in transceiver

6.6 USB console interface

Information on the USB console interface

- Via the USB console interface on the device (USB socket Type B), you can access the device directly via a virtual serial interface (115200 8N1) without assigning an IP address.
- Access to the device is possible independent of the Ethernet ports.
- To connect the USB console interface to a PC, you require a cable with a USB Type B plug and USB Type A plug. The connecting cable for the USB console interface can be ordered as accessory; see section "Accessories (Page 23)".

Position

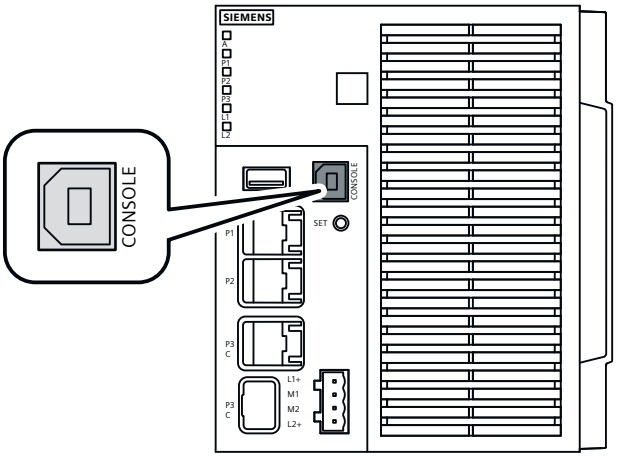


Figure 6-2 Position of the USB console interface (USB socket Type B)

Driver for the USB console interface

To use the USB console interface under Windows, you must download and install the following driver: Driver (https://support.industry.siemens.com/cs/ww/en/view/109798927)

6.7 USB interface

Information on the USB interface

Via the USB interface on the device (USB socket Type A), you can connect storage media to the device.

NOTICE
Only memory expansions allowed The USB interface (Type A) is approved for connection of a storage medium. Any other use of the USB interface (Type A), for example the connection of a USB camera, is at the user's own risk.

NOTICE
Functional disruptions due to cables that are too long The length of the USB cable must not exceed 3 meters to ensure proper function of the USB interface. Longer cables can result in functional disruptions and error messages.

Position

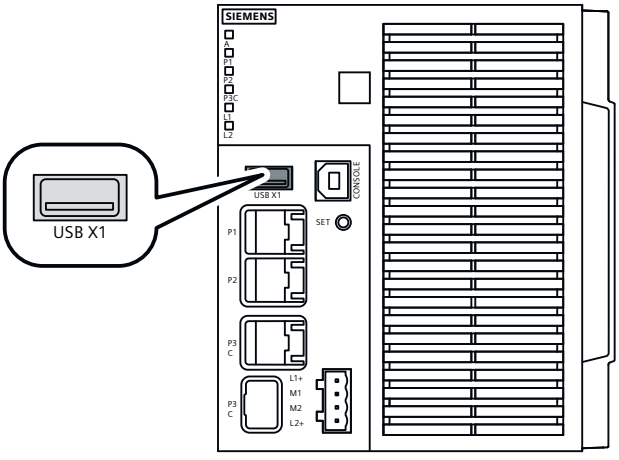


Figure 6-3 Position of the USB interface (USB socket Type A)

Maintenance and cleaning

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.
- For function checks, maintenance and servicing work, you need to observe the requirements on checking and maintaining plants in hazardous areas according to the standards EN / IEC 60079-17.

⚠ WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories 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

This section describes how you load the firmware in the Rescue system of a SCALANCE LPE9403. In addition, possible error messages are addressed and solutions for errors that occur are shown.

8.1 System time and firmware update

The file for updating the firmware of the SCALANCE LPE is protected with a certificate. During a firmware update, the device also checks the date of the certificate. For this purpose, the device must have the current time. After switch-off, the device saves the time for 5 to 7 days.

If the device **is without power for longer than 7 days** and the time is lost, there are the following options to update the time. Except with manual configuration of the system time, the SCALANCE LPE9403 must have a network connection to an NTP server.

DHCP server with option 42

DHCP is enabled by default in the Rescue system for the SCALANCE LPE9403. If the parameters for Option 42 are configured for the corresponding DHCP server, the device receives from the DHCP server a list of IP addresses of the NTP servers in addition to the IP address after starting with the previous firmware.

After a brief time, the device has the correct time and you can update the firmware.

DHCP

If DHCP is enabled in the firmware, the system time can be updated via NTP. The firmware first synchronizes the system time with the NTP server. Then the real time clock (RTC) is synchronized with the system time.

After an operating time of about five minutes, the device has the correct time and you can update the firmware via the Rescue system.

Configuring the NTP server in the Web UI

Start the SCALANCE LPE9403 with the previous firmware initially and configure an NTP server in the Web UI. The firmware first synchronizes the system time with the NTP server. Then the real time clock (RTC) is synchronized with the system time.

After an operating time of about five minutes, the device has the correct time and you can update the firmware via the Rescue system.

Configuring the NTP server in the Linux Shell

Start the SCALANCE LPE9403 with the previous firmware initially and configure an NTP server in the Linux Shell. The firmware first synchronizes the system time with the NTP server. Then the real time clock (RTC) is synchronized with the system time.

After an operating time of about five minutes, the device has the correct time and you can update the firmware via the Rescue system.

Synchronization of the real time clock

Start the SCALANCE LPE9403 with the previous firmware initially. To synchronize the real time clock with the current system time, do the following:

Step	Instruction	Command
1	Restart the **tohwclock** service.	`sudo systemctl restart tohwclock.service`
2	Check if the real time clock has been synchronized with the system time. The **RTC time** row must contain the current time.	`timedatectl`

You can then update the firmware via the Rescue system.

Example

```
admin@lpe9403-VPM7001325:~$ sudo systemctl restart tohwclock.service
[sudo] password for admin: ************
admin@lpe9403-VPM7001325:~$ timedatectl
               Local time: Thu 2024-08-15 09:17:41 CEST
           Universal time: Thu 2024-08-15 07:17:41 UTC
                 RTC time: Thu 2024-08-15 07:17:41
                Time zone: Europe/Berlin (CEST, +0200)
System clock synchronized: no
              NTP service: n/a
          RTC in local TZ: no
```

Configuring the system time manually

Start the SCALANCE LPE9403 with the previous firmware initially and configure the system time manually. Manual configuration is possible in the Linux Shell and in Web UI. You will find more information in the configuration manual for the SCALANCE LPE9403:

- **Linux Shell >> System time >> Configuring the system time manually**
- **Web User Interface ≫ System time >> Configuring the system time manually**

You can then update the firmware via the Rescue system.

8.2 Downloading the firmware in the Rescue system via TFTP

Firmware

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

NOTICE
Observe information on new firmware version The improper use of a new firmware can lead to a malfunction or to failure of the device. When updating to a new firmware version, consider all information to be published for this firmware version. Information on the firmware is available from Siemens Industry Online Support (SIOS) (https://support.industry.siemens.com/cs/ww/en/ps/26683/dl).

Starting the Rescue system in stand-alone mode

NOTICE
Previous configurations and applications are lost When firmware is loaded in this way, the configuration is reset to factory settings and all information saved on the device is deleted. This also affects all Docker components (containers, networks, volumes, images, bind mounts, etc.) present on the device. Back up your previous configurations before you load a new firmware to the device via the Rescue system.

NOTICE
Danger of damage to property If the power supply to the device is lost while a firmware file is being loaded, an error state can occur. Do not disconnect the device from the power supply while a firmware file is being loaded. Do not switch off the device during the reboot after loading the firmware. The firmware update is not complete until you are able to log in after the device has restarted. If the power supply is interrupted during the reboot, the device may not be functional any longer. Such a functional disruption can only be remedied with the help of our technical support.

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

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

To switch to the Rescue system and load a firmware file, follow these steps:

1. Check the firewall settings of the PC on which you start the TFTP client. With incorrect settings, the bidirectional connection establishment can cause communication problems.
2. Turn off the power to the device.
3. Press the button and reconnect the power supply to the device while holding down the button.
4. Hold down the button until the red alarm LED "A" starts to flash.
5. Release the button while the red alarm LED is still flashing, and less than 6 seconds have passed.
   You are now in the Rescue system. The transfer to the Rescue system can take up to 60 seconds. The alarm LED also flashes in this operating state. The device waits in this status for a new firmware file that you can download by TFTP.

   Note

   If you keep the button pressed for more than 6 seconds while the alarm LED is flashing, the Rescue system is not loaded and only parts of the device configuration are reset. You can also identify this state by the permanently lit alarm LED, see Resetting the configuration (Page 71).

6. Connect a PC to port "P3C" via an Ethernet cable. The other ports are not functional in the Rescue system.
7. Assign an IP address to the device using DHCP or SINEC PNI (or any other DCP tool).
8. 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"

   Ensure that the TFTP client is active in the Windows network (domain, private, public) that is connected with the LPE.

9. Once the firmware has been transferred completely to the device and validated, there is an automatic restart on the device. This process can take a few minutes.
10. After the startup, check whether the new firmware is active. To do this, use the `deviceinfo fw` command in the Linux shell or the information on the Web UI start page.

8.3 Starting the Rescue system when using the Function Extender Interface

The function of the **SET** button is independent of whether a SCALANCE LPE is used in combination with a SCALANCE switch or in standalone mode. The Rescue system can therefore also be started on a SCALANCE LPE which is connected to a SCALANCE switch via the function extender interface.

To start the Rescue system of the SCALANCE LPE, perform the following steps:

1. Disconnect the power to the SCALANCE switch.
2. Press the SET button of the SCALANCE LPE and reconnect the SCALANCE switch to the power supply with the button pressed.
3. Keep the SET button pressed until the red alarm LED "A" of the SCALANCE LPE starts flashing.
4. Release the SET button while the red alarm LED is still flashing, and less than 6 seconds have passed. You are now in the Rescue system.

The remaining procedure of the firmware update is the same as for a SCALANCE LPE in standalone mode, described in the previous section: "Downloading the firmware in the Rescue system via TFTP (Page 67)".

In the Rescue system, the port **P3C** is functional even if the SCALANCE LPE is connected to a SCALANCE switch via the function extender interface. Therefore, the PC is connected to the port P3C in this case also.

Note

A SCALANCE LPE connected to a SCALANCE switch via the function extender interface can also be started in the Web User Interface of the switch. For more detailed information, refer to Configuration manual (https://support.industry.siemens.com/cs/document/109964110).

8.4 Error messages when downloading the firmware in the Rescue system

If a firmware update cannot be completed successfully, the Rescue system outputs an error message with a description of the cause. The following sections describe the error messages of the Rescue system.

Bad firmware file

```
Image invalid or corrupted!
Please check <file name> and provide a compatible *.swu file
```

A firmware file is identified as bad if the original contents have been changed or the file format was not recognized.

Measures

- Observe the specific notes for the individual firmware versions in SCALANCE LPE9403 configuration manual (https://support.industry.siemens.com/cs/ww/de/ps/26683/man), section **Firmware update**.
- Check that the firmware file is correct using the SHA-256 checksum. This checksum is specified on the web page for download of the firmware file.

Bad signature

```
CMS signature does not match!
The contents of the sw-description.sig or signature hash value
(sha256) is incorrect.
Please use an officially signed *.swu file.
```

The signature of the firmware file is not recognized as binary coded CMS (**C**ryptographic **M**essage **S**yntax) signature.

Measures

- Only use officially signed firmware files made available by Siemens Industry Online Support.
- Check that the firmware file is correct using the SHA-256 checksum. This checksum is specified on the web page for download of the firmware file.

sw-description file bad

```
Signature verification failed!
sw-description or sw-description.sig file may be corrupted.
Please check and provide a compatible *.swu file.
```

An error occurred when checking the **sw-description** file using the associated **sw-description.sig** signature file. One of the two files is corrupt.

Measures

- Only use officially signed firmware files made available by Siemens Industry Online Support.
- Check that the firmware file is correct using the SHA-256 checksum. This checksum is specified on the web page for download of the firmware file.

The firmware file does not match the device

```
The signature is not compatible with your device.
Please make sure you have the correct *.swu file for your device.
```

The firmware file is not compatible with the device.

Measure

- Use a firmware file that is suitable for the device. Observe the comprehensive information on the Siemens Industry Online Support download page for the affected firmware.

Wrong system time

```
System time is not correct!
Please set the system time. (e.g. usage : date -s \"10 MAY 2025\")
```

The certificate of a firmware file has a specific period of validity. If the system time is wrong, a current certificate can be classified as expired in certain cases.

Measures

- Check the settings for the date, time and time zone. With the `timedatectl` command, you can view this information in the Linux Shell of the firmware.
- If necessary, correct the time setting in the Linux Shell or in the Web UI of the SCALANCE LPE9403.

Incorrect file format

`Unsupported file format (*.sfw) detected!`
`For compatibility, please upload a file in the *.swu format.`

As of firmware version 2.1, the SWU format is used for the firmware files. However, the file used has the SFW format used up to firmware version 2.0 or a different unknown format.

Measure

- Perform the update with a suitable firmware file in SWU format. Firmware files are available in Siemens Industry Online Support.

Connection error

`Firmware installation has been suspended!`
`Please check your connection and try again.`

The firmware update was canceled due to a bad connection between the configuration PC and the SCALANCE LPE or due to a user action.

Measure

- Check the connection between the configuration PC and the SCALANCE LPE.

8.5 Resetting the configuration

NOTICE
Previous configuration settings will be lost By resetting the configuration, all the settings you have made will be overwritten by factory defaults. The software components or applications you have installed will be retained.

Resetting the configuration during the startup phase

To reset the device configuration during the startup phase, follow these steps:

1. Turn off the power to the device.
2. Now press the "SET" button and reconnect the power to the device while holding down the button.
3. Hold down the button until the red alarm LED "A" stops flashing and is permanently lit.

4. Now release the button and wait until the alarm LED "A" goes off again.
5. The device is restarted.

Resetting the configuration during operation

The **SET** button has no function during operation. You can reset the configuration with the console command **configreset** or via the Web UI. You can find more information in the configuration manual chapter "Device management", section "Resetting the configuration".

Technical specifications

9

9.1 Technical specifications of SCALANCE LPE9403

Technical specifications			
Connection to Industrial Ethernet			
Electrical connectors		Quantity	2
		Connector	RJ45 jack
		Properties	Full duplex; MDI-X assignment
		Transmission rate	10 / 100 / 1000 Mbps
Combo ports	Quantity		1
	Electrical connectors	Quantity	1
		Connector	RJ45 jack
		Properties	Full duplex; MDI-X assignment
		Transmission rate	10 / 100 / 1000 Mbps
	Slots for pluggable transceivers	Quantity	1
		Connector	SFP transceiver (LC port)
		Transmission rate	100/1000 Mbps
Maximum packet size (MTU)		All interfaces	1500 bytes (default) 2048 bytes (configurable maximum value)
Transmission speed RDI ports (The SCALANCE LPE is connected to a SCALANCE switch, use of the ports only as internal interfaces via the SCALANCE switch)		extender0/1	1000 Mbps
		extender0/2	1000 Mbps
		extender0/3	10 Gbps
Diagnostics interface			
Serial interface		Quantity	1
		Connector	USB socket Type B (USB 2.0)
USB 3.0 port			
Interface for storage media		Quantity	1
		Connector	USB socket Type A
Processor, RAM and storage medium			
Processor		Type	64-bit ARMv8 A53
		Number of cores	4
		Cycle	1.4 GHz
Work memory		Type and size	4 GB DDR4 RAM
		Design	ECC
Storage medium		Hardware release FS01 [1)]	16 GB eMMC (pSLC)
		Hardware release FS02 [1)]	38 GB eMMC (pSLC)
Electrical data			

Technical specifications		
Power supply [2]	Rated voltage	24 V DC
	Voltage range (incl. tolerance)	19.2 to 28.8 V DC safety extra-low voltage (SELV/PELV)
	Design	Terminal block, 2 x 2-pin
	Properties	Redundant design, galvanically connected to the housing The connected power supply must meet the requirements of NEC Class 2.
Current consumption		800 mA
Effective power loss		19.2 W
Overvoltage category		CAT II
Fusing		3.15 A / 125 V
Voltage buffer	HW clock	After the device is separated from the power supply, the hardware clock of the device continues running for about 5 to 7 days, depending on the ambient temperature.
Permitted ambient conditions		
Ambient temperature [3]	In standalone operation with RJ45 connectors (LAN) up to 2000 m above sea level	During operation in horizontal installation position: -40 °C ... +60 °C During operation in a different installation position: -40 °C ... +50 °C
	In standalone operation with plug-in transceivers of the types: • [-] Standard version • LD Up to 2000 m above sea level	During operation in horizontal installation position: -40 °C ... +60 °C During operation in a different installation position: -40 °C ... +50 °C
	In standalone operation with plug-in transceivers of the types: • LH • LH+ • ELH Up to 2000 m above sea level	During operation in horizontal installation position: -40 °C ... +60 °C During operation in a different installation position: -40 °C ... +50 °C
	During storage	-40 °C ... +85 °C If the storage period exceeds one year, the storage temperature can be max. 55 °C.
	During transportation	-40 °C ... +85 °C
Relative humidity	During operation, at 25 °C	≤ 95% without condensation
Housing, dimensions and weight		
Design	Compact	
Housing material	Basic housing	Die cast aluminum, powder coated
	Front cover	Polycarbonate (PC-GF10)
Degree of protection	IP 20	

Technical specifications	
Dimensions (W x H x D)	134 x 147 x 127 mm
Weight	1600 g
Installation options	• DIN rail mounting • Installation on an S7-300 mounting rail • Installation on an S7-1500 mounting rail • Wall mounting

[1] You will find the hardware release of your device on the type plate. On the type plate, the hardware release is printed as a placeholder "X". "X 2 3 4 5 6" designates a device with hardware release 1.

[2] Note the wiring rules.

[3] Depending on which plug-in transceiver you use, the maximum ambient temperature can change, see section "Accessories", "SFP plug-in transceiver (Page 24)".

9.2 Mechanical stability (in operation)

The device meets the following requirements relating to mechanical stability during operation:

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

9.3 RF radiation according to NAMUR NE21

The device meets the following requirement relating to RF radiation.

RF radiation according to IEC 61000-4-3/NAMUR NE21	
80 MHz - 2.0 GHz	2.0 GHz - 2.7 GHz
10 V/m	3 V/m
80% AM (1 kHz)	

9.4 Cable lengths

The following cable lengths apply to the device.

Cable	Permitted cable length
IE TP Torsion Cable with IE FC Outlet RJ45 + 10 m TP Cord	0 ... 45 m + 10 m TP Cord
IE TP Torsion Cable with IE FC RJ45 Plug 180	0 ... 55 m
IE FC TP Marine/Trailing/Flexible Cable with IE FC Outlet RJ45 + 10 m TP Cord	0 ... 75 m + 10 m TP Cord
IE FC TP Marine/Trailing/Flexible Cable with IE FC RJ45 Plug 180	0 ... 85 m
IE FC TP Standard Cable with IE FC Outlet RJ45 + 10 m TP Cord	0 ... 90 m + 10 m TP Cord
IE FC TP Standard Cable with IE FC RJ45 Plug 180	0 ... 100 m

Dimension drawings

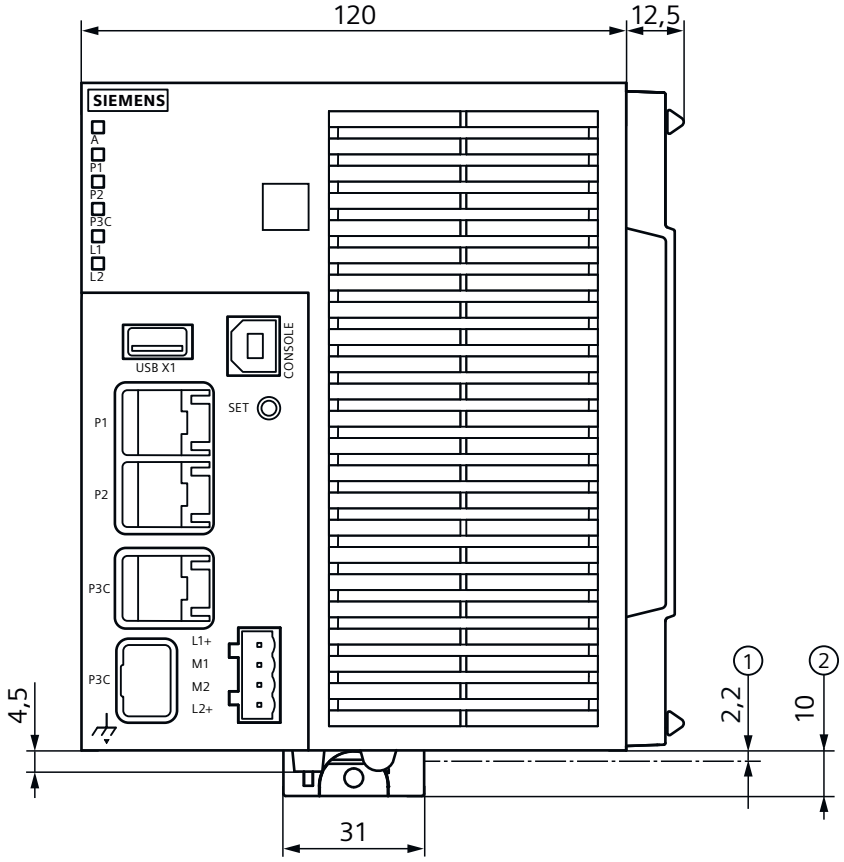
10

10.1 SCALANCE LPE9403 dimension drawings

Note

Dimensions are specified in mm.

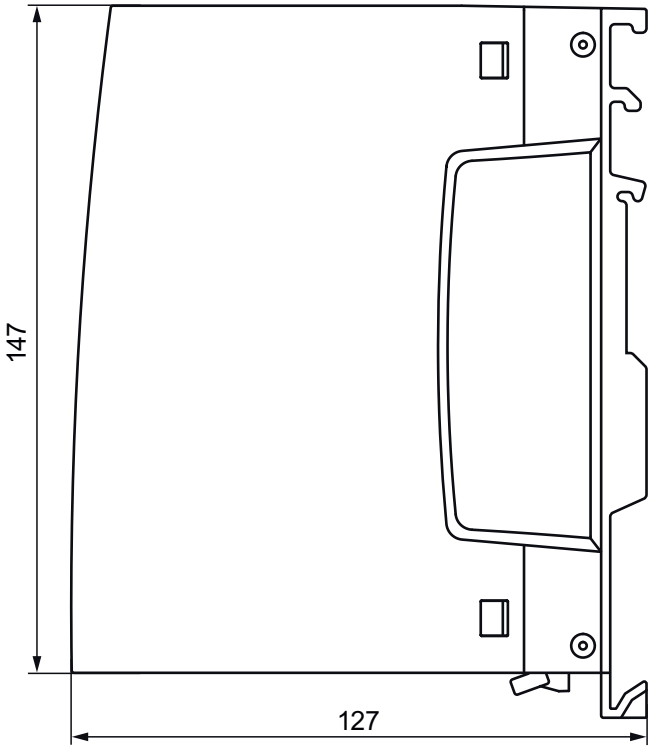
Front view



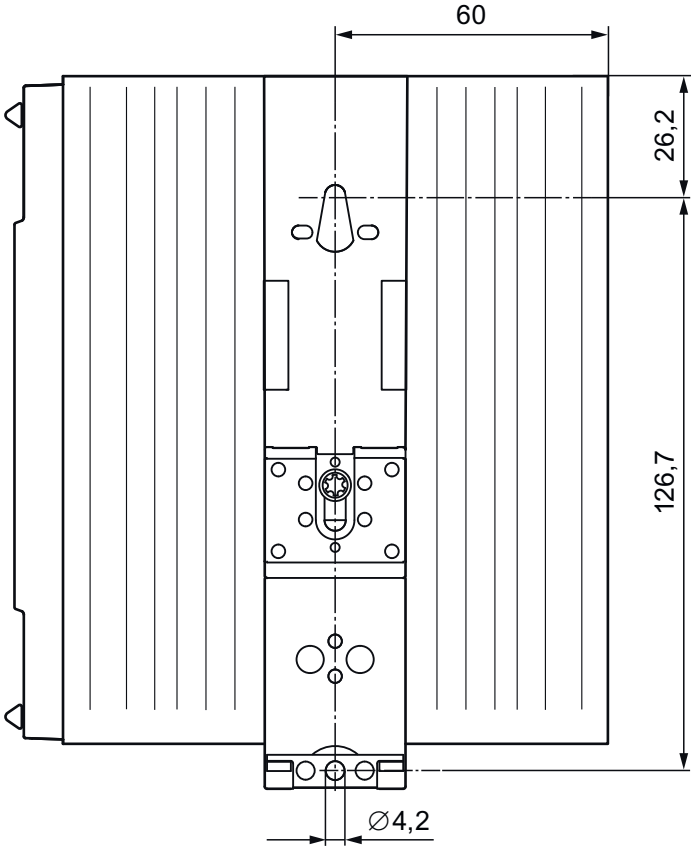
① Securing bar in the rail mounting position

② Securing bar in the wall mounting position (as supplied)

Side view



Drilling template for wall mounting

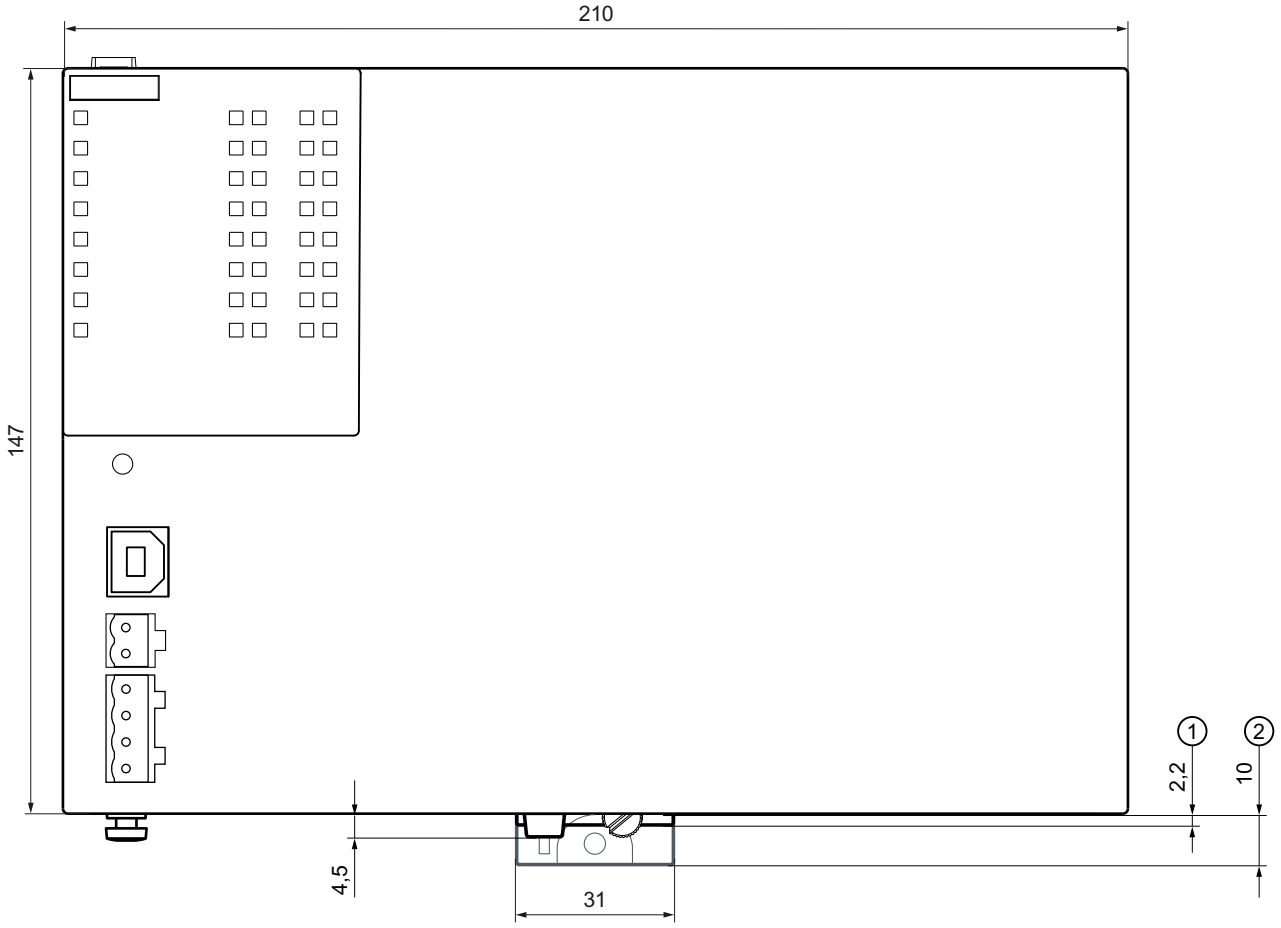


10.2 Dimension drawings SCALANCE XCM-300

Note

Dimensions are specified in mm.

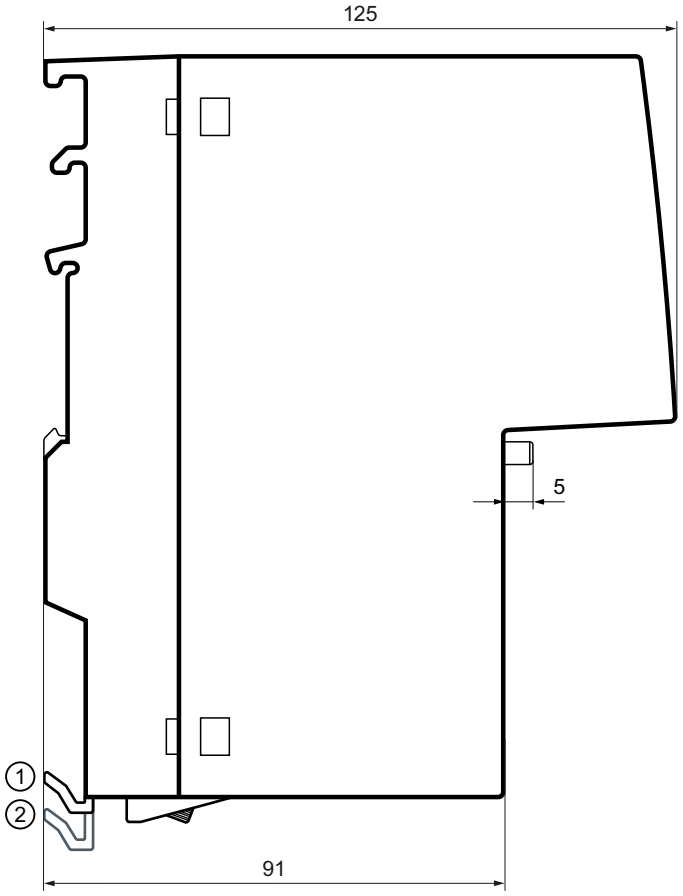
Front view



① Securing bar in the rail mounting position

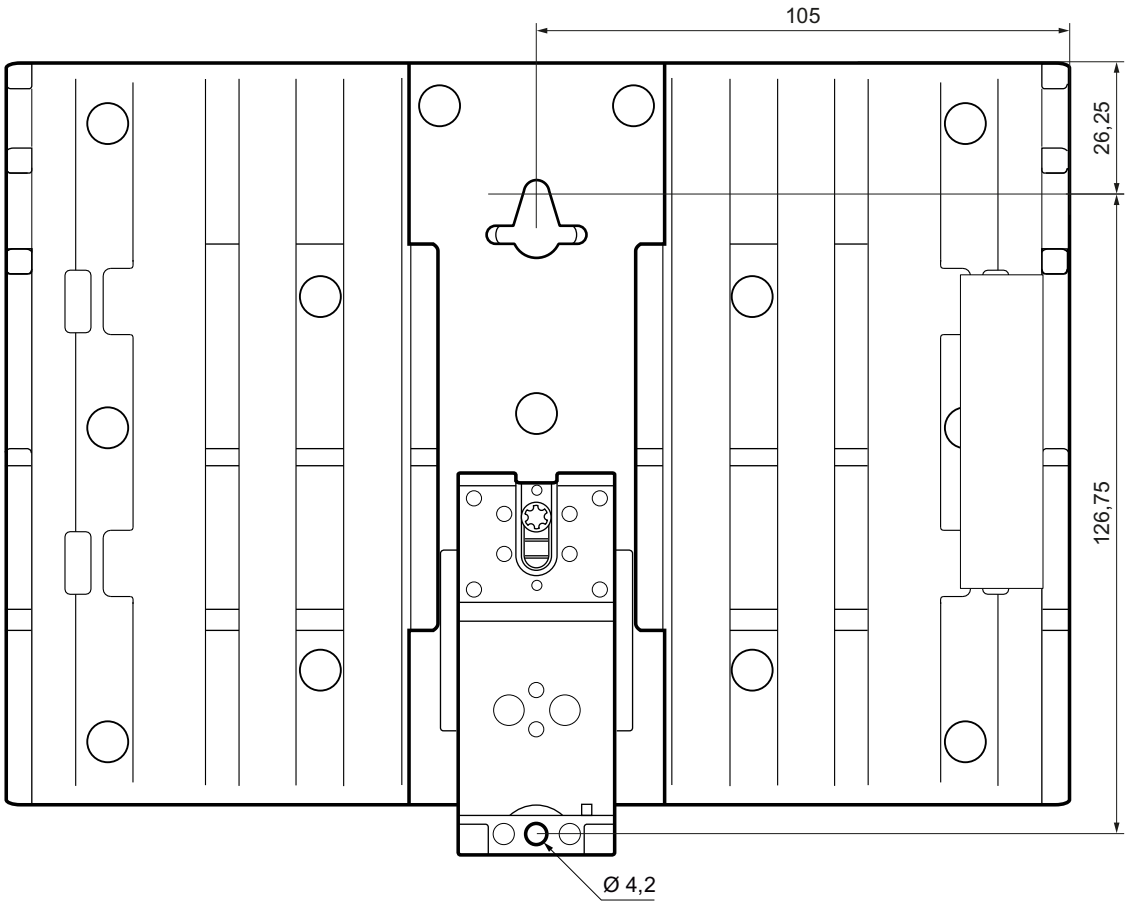
② Securing bar in the wall mounting position (as supplied).

Side view



① Securing bar in the rail mounting position
② Securing bar in the wall mounting position (as supplied).

Drilling template for wall mounting



Certifications and approvals

11

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/26683/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/26683/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.

Note for devices with CLASS 1 LASER

Important note on products certified according to Type Examination Certificate KEMA 07ATEX0145 X as of Issue 95 / DEKRA 18ATEX0025 X and IECEx Certificate of Conformity DEK 14.0025X as of Issue 43 / DEK 18.0017X and containing Class 1 optical radiation sources.

Note

CLASS 1 LASER

The device contains optical radiation sources which comply with the limits of Class 1 according to IEC 60825-1. Fiber-optic cables connected to these optical radiation sources may therefore be routed either to or through hazardous areas requiring Category 2G, 3G, 2D or 3D equipment.

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 61010-2-201
- CAN/CSA-IEC 61010-2-201

Report no. E85972

cULus Approval for Information Technology Equipment

cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

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

Report no. E115352

cULus Approval Hazardous Location

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

Underwriters Laboratories Inc. complying with

- UL121201
- ANSI/ISA 12.12.01
- CSA C22.2 No. 213

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

Report no. E240480

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

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

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

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

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

Marking for the customs union

EAC (Eurasian Conformity)

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

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

FDA and IEC marking

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

Device	CLASS 1 LASER PRODUCT
SCALANCE LPE	(*)

* In modular devices, you can find the marking on the plug-in transceiver used or in the relevant operating instructions.

Figure 11-1 FDA and IEC markings

CAUTION

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

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

"

"SET" button, 22, 27, 68, 71

A

Ambient conditions, 74
Approvals, 83
Article numbers, 21, 31
Autonegotiation, 59

C

Cable length, 76
CE mark, 83
Centering pin, 43
Certificate, 16
CLP, 23, 28
  Commissioning, 28
Combo port, 29
Connecting cable, 60
Connecting up
  Grounding, 56
Connection to Industrial Ethernet, 73

D

Dimensions, 74
DIN rail mounting, 38

E

Electrical data, 73
Environmental conditions, 25
ESD directives, 10

F

Fault status, 25
Firmware, 25, 67
  Update (error messages), 69
  Update via the Rescue system, 69
Firmware update
  TFTP, 67
Function extender interface, 43

G

Grounding, 56
Grounding screw, 22

H

Housing, 74

I

Installation, 74
  DIN rail mounting, 38
  Installation on a mounting rail, 39, 40
  Wall mounting, 41
Installation on a mounting rail, 39, 40

K

Key, 16
Knurled screw, 22, 38, 39, 40

L

LED display, 22, 25
Levering aid, 22, 42
Loading firmware, 67
Locking mechanism, 43

M

MDI / MDI-X autocrossover, 58
Mechanical stability, 75

P

Permitted ambient conditions, 25, 74
Pin assignment, 58
PKCS #12 format, 16
Pluggable transceiver
  SFP, 24, 25
Power supply, 22, 55

R

Rescue system
Function extender interface, 68
Resetting the configuration, 71
RF radiation, 75

S

S7-1500, 40
S7-300, 39
Safety notices
for installation, 33
general, 11
Use in hazardous areas, 11, 33, 47, 48
when connecting up, 47, 48
Scope of delivery, 22
Secure Boot, 19
Securing bar, 22, 38, 39, 40, 80
Serial cable, 24
Serial interface, 60
SFP transceiver, 24, 25
SFW format, 71
Signaling contact, 25
Spare parts, 23
Spring-loaded terminal, 22, 55
Startup phase, 25
SWU format, 71
System manual, 88

T

TFTP, 67

U

USB, 22
USB cable, 24
USB interface, 61

W

Weight, 74
Wiring rules, 55

X

X.509 TLS certificate, 16