SIEMENS

SIMATIC NET

Industrial Ethernet security SCALANCE SC-600

Operating Instructions

10/2023
C79000-G8976-C453-09

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-C453-09
Ⓟ 02/2024 Subject to change

Table of contents

Introduction 1

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

Purpose of the Operating Instructions

These operating instructions support you when installing and connecting up the SCALANCE SC-600 product line.

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

Validity of the Operating Instructions

These operating instructions apply to the following devices:

- SCALANCE SC622-2C
- SCALANCE SC626-2C
- SCALANCE SC632-2C
- SCALANCE SC636-2C
- SCALANCE SC642-2C
- SCALANCE SC646-2C

Designations used

Classification	Description	Terms used
Product line	If information applies to all product groups within the product line, the term SCALANCE SC-600 is used.	• SCALANCE SC-600
Product group	If information applies to all devices of a product group, a suitable term is used. • SCALANCE SC622-2C and SC626-2C • SCALANCE SC622-2C, SC632-2C and SCALANCE SC642-2C • SCALANCE SC626-2C, SCALANCE SC636-2C and SCALANCE SC646-2C • SCALANCE SC632-2C and SCALANCE SC636-2C • SCALANCE SC642-2C and SCALANCE SC646-2C	• SC62x-2C • SC6x2-2C • SC6x6-2C • SC63x-2C • SC64x-2C
Device	If information relates to a specific device, the device name is used.	• SCALANCE SC622-2C • SCALANCE SC626-2C • SCALANCE SC632-2C • SCALANCE SC636-2C • SCALANCE SC642-2C • SCALANCE SC646-2C

Documentation on configuration

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

- SCALANCE SC-600 Web Based Management (WBM)
- SCALANCE SC-600 Command Line Interface (CLI)

You will find the configuration manuals here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support:
  Link: (https://support.industry.siemens.com/cs/ww/en/ps/15327/man)

Further documentation

In the system manuals "Industrial Ethernet / PROFINET Industrial Ethernet" and "Industrial Ethernet / PROFINET passive network components", you will find information on other SIMATIC NET products that you can operate along with the devices of this product line in an Industrial Ethernet network.

There, you will find among other things optical performance data of the communications partner that you require for the installation.

You will find the system manuals here:

- On the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support:
  - Industrial Ethernet / PROFINET Industrial Ethernet System Manual
    Link: (https://support.industry.siemens.com/cs/ww/en/view/27069465)
  - Industrial Ethernet / PROFINET - Passive Network Components System Manual
    Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

SIMATIC NET manuals

You will find the SIMATIC NET manuals here:

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

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

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

License conditions

Note

Open source software

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

You will find the license conditions as a loadable file on the WBM pages of the device. You will find the description of opening and loading license conditions in section File list of the configuration manuals.

You can find the file with the license conditions for open source software under the following name:

- OSS_Readme.zip

Cybersecurity notes

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

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

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

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

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

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

Note on firmware/software support

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

Firmware

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

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.

Device defective

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

Decommissioning

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

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

Also restore the factory settings on the storage medium.

Recycling and disposal

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

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

Keep to the local regulations.

You will find information on returning the product on the Internet pages of Siemens Industry Online Support:
Link: (https://support.industry.siemens.com/cs/ww/en/view/109479891)

SIMATIC NET glossary

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

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

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

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 their product packaging or in a 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".

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.

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.

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

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.

⚠ **WARNING**

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

Batteries: Replacement, recycling and disposal

Handling batteries

⚠ **WARNING**

Risk of explosion and danger of release of harmful substances!

Do not throw batteries into a fire, do not solder the body of the cell, do not open batteries, do not short-circuit batteries, do not reverse the polarity of batteries, do not heat batteries above 100 °C.

Protect batteries from direct sunlight, dampness and condensation.

Dispose of batteries according to the regulations.

Replacing batteries

Note

Replacement not possible

It is not possible to replace the internal battery.

Recycling / disposal

Batteries and rechargeable batteries can be recycled. Their components can be used as raw materials for new batteries/rechargeable batteries or other products. Effective recycling procedures are only possible if batteries of the used batteries of the same type are collected together.

Note

Regulations for disposal of batteries

Keep to the local regulations for the recycling and disposal of batteries.

Security recommendations 3

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

General

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

Authentication

Note

Accessibility risk - Risk of data loss

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

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- 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 pre-installed Web server certificate (RSA, 2048 bit key length) and an SSH Private Key in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate in the WBM via "System > Load and Save".
- Use the certification authority including key revocation and management to sign the certificates.
- Use password-protected certificates in the format "PKCS #12".
- Use certificates with a key length of 4096 bits.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- SSH and SSL keys are available for admin users. Make sure that you take appropriate security measures when shipping the device outside of the trusted environment:
  - Replace the SSH and SSL keys with disposable keys prior to shipping.
  - Decommission the existing SSH and SSL keys. Create and program new keys when the device is returned.
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Physical/remote access

- If possible, operate the devices only within a protected network area. Attackers cannot access internal data from the outside when the internal and the external network are separate from each other.
- Limit physical access to the device exclusively to trusted personnel.
  The memory card or the PLUG (C-PLUG, KEY-PLUG, CLP) contains sensitive data such as certificates and keys that can be read out and modified. An attacker with control of the device's removable media could extract critical information such as certificates, keys, etc. or reprogram the media.
- Lock unused physical ports on the device. Unused ports can be used to gain forbidden access to the plant.
- We highly recommend that you keep the protection from brute force attacks (BFA) activated to prevent third parties from gaining access to the device. For more information, see the configuration manuals, section "Brute Force Prevention".
- If possible, use the VPN functionality to encrypt and authenticate communication for communication via non-secure networks.
- When you establish a secure connection to a server (for example for an upgrade), make sure that strong encryption methods and protocols are configured for the server.
- Terminate the management connections (e.g. HTTPS, SSH) properly.
- Make sure that the device has been powered down completely before you decommission it. For more information, refer to "Decommissioning (Page 5)".
- We recommend formatting a PLUG that is not being used.

Hardware / Software

- Use VLANs whenever possible as protection against denial-of-service (DoS) attacks and unauthorized access.
- Restrict access to the device using firewall rules.
- Selected services are enabled by default in the firmware. It is recommended to enable only the services that are absolutely necessary for your installation.
  For more information on available services, see "List of available services".
- To ensure you are using the most secure encryption methods available, use the latest web browser version compatible with the product. Also, the latest web browser versions of Mozilla Firefox, Google Chrome, and Microsoft Edge have 1/n-1 record splitting enabled, which reduces the risk of attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (for example, BEAST).
- Ensure that the latest firmware version is installed, including all security-related patches.
  You can find the latest information on security patches for Siemens products at the Industrial Security (https://www.siemens.com/industrialsecurity) or ProductCERT Security Advisories (https://www.siemens.com/cert/en/cert-security-advisories.htm) website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- Enable only those services that are used on the device, including physical ports. Free physical ports can potentially be used to gain access to the network behind the device.

- Use the authentication and encryption mechanisms of SNMPv3 if possible. Use strong passwords.
- Configuration files can be downloaded from the device. Ensure that configuration files are adequately protected.
  Configuration files can be password protected during download. You enter passwords on the WBM page "System > Load & Save > Passwords".
- When using SNMP (Simple Network Management Protocol):
  - Configure SNMP to generate a notification when authentication errors occur.
    For more information, see WBM "System > SNMP > Notifications".
  - Ensure that the default community strings are changed to unique values.
  - Use SNMPv3 whenever possible. SNMPv1 and SNMPv2c are considered non-secure and should only be used when absolutely necessary.
  - If possible, prevent write access.

Secure/ non-secure protocols

- Use secure protocols if access to the device is not prevented by physical protection measures.
- Restrict the use of non-secure protocols. While some protocols are secure (e.g. HTTPS, SSH, 802.1X, etc.), others were not designed for the purpose of securing applications (e.g. SNMPv1/v2c, RSTP, etc.).
  Therefore, take appropriate security measures against non-secure protocols to prevent unauthorized access to the device/network. Use non-secure protocols on the device using a secure connection (e.g. SINEMA RC).
- If non-secure protocols and services are required, ensure that the device is operated in a protected network area.
- Check whether use of the following protocols is necessary:
  - HTTP
  - Broadcast pings
  - Non authenticated and unencrypted interfaces
  - ICMP (redirect)
  - LLDP
  - DHCP Options 66/67
  - SNTP
  - NTP
  - TFTP
  - VRRPv3
  - DNS
  - SNMPv1/V2c

- If a secure alternative is available for a protocol, use it.
  The following protocols provide secure alternatives:
  - SNMPv1/v2 → SNMPv3
    Check whether use of SNMPv1 is necessary. SNMPv1 is classified as non-secure. Use the option of preventing write access. The product provides you with suitable setting options. If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
  - HTTP → HTTPS
  - NTP → Secure NTP
  - TFTP → SFTP
- Using a firewall, 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.
- For the DCP function, leave the "Read-Only" mode after commissioning.

Interfaces security

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

3.1 Ports

Notes on the ports

VLAN1 and VLAN2 on different ports

Depending on the device type, VLAN1 and VLAN2 are on different physical ports:

- SC632-2C, SC642-2C: VLAN1 = port 1, VLAN2 = port 2
- SC636-2C, SC646-2C: VLAN1 = port 1-4, VLAN2 = port 5-6

With SC62x-2C, only access via VLAN1 is possible:

- SC622: Port 1
- SC626: Port 1-5

No Layer2 bridge functionality

The following ports do not support Layer 2 bridge functionality and thus form a natural network boundary for PROFINET:

- SC622-2C: Port 2
- SC626-2C: Port 6

The SC622-2C and SC626-2C devices fulfil the properties of a 2-port router according to IEC 61784-3-3 (PROFIsafe), section 8.1.2.
They are therefore suitable for use as cell protection device in safety environments in which it cannot be guaranteed that PROFIsafe addresses are unique.

List of available services

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

The table includes the following columns:

- **Service/Protocol**
  The services/protocols that the device supports.
- **Protocol / Port number**
  Port number assigned to the protocol.
- **Default port status**
  The port status on delivery (factory setting) distinguishes between local and external access.
  - Local access: The port is accessed via a local connection (VLAN1).
  - External access: The port is accessed via an external connection (VLAN2).
    For SC622-2C: Port 2
    For SC626-2C: Port 6
- **Configurable port/service**
  Indicates whether the port number or the service can be configured via WBM / CLI.

- **Authentication**
  Specifies whether an authentication of the communication partner takes place or whether an authentication can be configured.
- **Encryption**
  Specifies whether the transfer is encrypted or whether the encryption can be configured.

Service/Protocol	Protocol/ Port number	Default status		Configurable		Authentication	Encryption [4]
		Local	External	Port	Service		
DHCPv4 Client	UDP/68	Closed	Open	--	✓	--	--
DHCPv4-Server	UDP/67	Closed	Closed	--	✓	--	--
DNS-Client	TCP/53 UDP/53	Outgoing only	Outgoing only	--	✓	--	--
DNS-Server	TCP/53 UDP/53	Closed	Closed	--	✓	--	--
DDNS	TCP/80 UDP/80 TCP/443 UDP/443	Outgoing only	Outgoing only	--	✓	✓	--
Firewall State Sync	UDP/3780	Closed	Closed	✓	✓	--	--
HTTP [1]	TCP/80	Open	Closed	✓	✓	✓	--
HTTP Proxy	TCP/3128 TCP/8080	Outgoing only	Outgoing only	✓	✓	Optional	--
HTTPS	TCP/443	Open	Closed	✓	✓	✓	✓
IPsec/IKE	UDP/500 UDP/4500	Closed	Closed	--	✓	✓	✓
IPv6 router-advertisement, neighbor-solicitation, neighbor-advertisement	ICMPv6	Open	Open	--	✓	--	--
NTP-Client	UDP/123	Outgoing only	Outgoing only	✓	✓	--	--
NTP-Server	UDP/123	Closed	Closed	✓	✓	--	--
NTP-Server (secure)	UDP/123	Closed	Closed	✓	✓	✓	--
OpenVPN-Client	UDP/1194 TCP/1194	Outgoing only	Outgoing only	✓	✓	✓	✓
OpenVPN-Server	UDP/1194 TCP/1194	Closed	Closed	✓	✓	✓	✓
OSPF	IP/89	Closed	Closed	--	✓	--	--
Ping	ICMP/ICMPv6	Open	Closed	--	✓	--	--
RADIUS	UDP/1812 UDP/1813	Outgoing only	Outgoing only	✓	✓	✓	--
SFTP	TCP/22	Outgoing only	Outgoing only	✓	✓	✓	✓
Siemens Remote Service (cRSP/SRS)	TCP/443	Outgoing only	Outgoing only	--	✓	Optional	✓

Service/Protocol	Protocol/ Port number	Default status		Configurable		Authentication	Encryption [4]
		Local	External	Port	Service		
SINEMA RC	HTTPS/443 and TCP/UDP depending on the server configuration	Outgoing only	Outgoing only	✓	✓	✓	✓
SMTP Client	TCP/25	Outgoing only	Outgoing only	✓	✓	Optional	--
SMTP (secure)	TCP/465 TCP/587	Outgoing only	Outgoing only	✓	✓	Optional	✓
SNMPv1/v2c [2]	UDP/161	Open	Closed	✓	✓	--	--
SNMPv3	UDP/161	Open	Closed	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outgoing only	Outgoing only	✓	✓	--	--
SNTP Client	UDP/123	Closed	Closed	✓	✓	--	--
SSH	TCP/22	Open	Closed	✓	✓	✓	✓
Syslog Client	UDP/514	Outgoing only	Outgoing only	✓	✓	--	--
Syslog Client TLS	TCP/6514	Outgoing only	Outgoing only	✓	✓	--	✓
TFTP	UDP/69	Outgoing only	Outgoing only	✓	✓	--	--
VRRP	IP/112	Closed	Closed	--	✓	--	--
VXLAN [3]	UDP/4789	Closed	Closed	✓	✓	--	--

[1] Is rerouted to HTTPS

[2] Read-only access

[3] Only SC63x-2C/SC64x-2C

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

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

The table includes the following columns:

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

Layer 2 service	Default status	Configurable
DCP	Open (when configured)	✓
LLDP	Open (when configured)	✓
SIMATIC NET TIME	Open (when configured)	✓
VLAN	Open (when configured)	✓

Description of the device

4

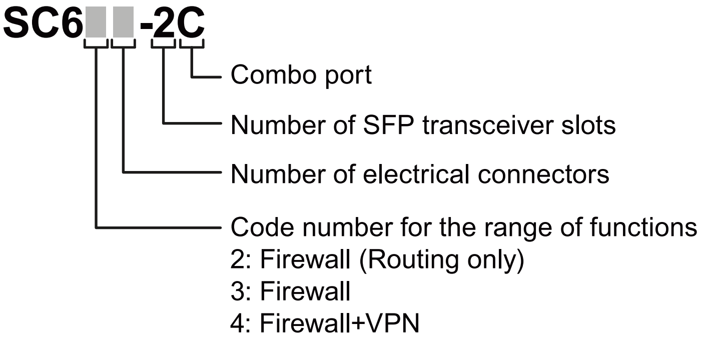
4.1 Product overview

Article numbers

Device	Description	Article number
SCALANCE SC622-2C	2 RJ45 ports, 2 SFP transceiver slots as combo ports	6GK5622-2GS00-2AC2
SCALANCE SC626-2C	6 RJ-45 ports, 2 SFP transceiver slots as combo ports	6GK5626-2GS00-2AC2
SCALANCE SC632-2C	2 RJ45 ports, 2 SFP transceiver slots as combo ports	6GK5632-2GS00-2AC2
SCALANCE SC636-2C	6 RJ-45 ports, 2 SFP transceiver slots as combo ports	6GK5636-2GS00-2AC2
SCALANCE SC642-2C	2 RJ45 ports, 2 SFP transceiver slots as combo ports	6GK5642-2GS00-2AC2
SCALANCE SC646-2C	6 RJ-45 ports, 2 SFP transceiver slots as combo ports	6GK5646-2GS00-2AC2

Type designation

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


SC6■■-2C
Combo port
Number of SFP transceiver slots
Number of electrical connectors
Code number for the range of functions
2: Firewall (Routing only)
3: Firewall
4: Firewall+VPN

Interfaces

Device	Total usable ports	SFP transceiver slots	Electrical connectors	Combo ports
SCALANCE SC622-2C	2 RJ45 ports	2	2	2
SCALANCE SC626-2C	6 RJ-45 ports	2	6	2
SCALANCE SC632-2C	2 RJ45 ports	2	2	2
SCALANCE SC636-2C	6 RJ-45 ports	2	6	2
SCALANCE SC642-2C	2 RJ45 ports	2	2	2
SCALANCE SC646-2C	6 RJ-45 ports	2	6	2

Components of the product

The following components are supplied with a SCALANCE SC-600:

- A SCALANCE SC-600 module
- A SIMATIC NET Manual Collection with documentation
- One securing screw for mounting on an S7 standard rail
- One 4-pin terminal block for the power supply (spring-loaded terminal)
- One 2-pin terminal block for the signaling contact (spring-loaded terminal)
- One 2-pin terminal block for the digital input (spring-loaded terminal)
- One connecting cable for the serial interface with RJ-11 plug and 9-pin D-sub female connector

4.2 Accessories

C-PLUG

Component	Description	Article number
C-PLUG	Removable data storage medium (32 MB) for the configuration data[1]	6GK1900-0AB00
	Exchangeable storage medium (256 MB) for the configuration data	6GK1900-0AB10

[1] From firmware version 2.2, use a C-PLUG with 256 MB, because otherwise there is not enough memory space for the function "Firmware on PLUG".

Cable

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

Pluggable transceiver

⚠ **WARNING**

Use only approved pluggable transceivers

If you use pluggable 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 pluggable transceivers, this can lead to the following problems:

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

Use only approved pluggable transceivers.

Note

Plugging and pulling during operation

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

SFP transceiver

Table 4-1 Pluggable transceiver SFP 100 Mbps (not for SCALANCE SC62x-2C)

Type	Properties	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
SFP991-1 (C)	1 x 100 Mbps, SC port optical, for glass FO cable (multimode), up to max. 5 km, varnished	6GK5 991-1AD00-8FA0
SFP991-1LD	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5 991-1AF00-8AA0
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

Table 4-2 Pluggable transceiver SFP 1000 Mbps

Type	Properties	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
SFP992-1 (C)	1 x 1000 Mbps, LC port optical, for glass FO cable (multimode), up to max. 750 m, varnished	6GK5 992-1AL00-8FA0
SFP992-1+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 2 km	6GK5 992-1AG00-8AA0
SFP992-1LD	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km	6GK5 992-1AM00-8AA0
SFP992-1LD (C)	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 10 km, varnished	6GK5 992-1AM00-8FA0
SFP992-1LD+	1 x 1000 Mbps, LC port optical for glass FO cable (multimode), up to max. 30 km	6GK5992-1AM30-8AA0
SFP992-1LH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 40 km	6GK5 992-1AN00-8AA0
SFP992-1LH+	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 70 km	6GK5 992-1AP00-8AA0
SFP992-1ELH	1 x 1000 Mbps LC port optical for glass FO cable (single mode) up to max. 120 km	6GK5 992-1AQ00-8AA0

Types appended with a (C) are provided with a UL-R/C-approved coating.

Active pluggable transceivers SFP (100 Mbps)

With active pluggable transceivers, Gigabit slots can be used as Fast Ethernet interfaces.

Type	Property	Article number
SFP991-1A	1 x 100 Mbps, LC port optical for glass FO cable (multimode), up to max. 5 km	6GK5 991-1AD00-8GA0
SFP991-1LD A	1 x 100 Mbps LC port optical for glass FO cable (single mode) up to max. 26 km	6GK5 991-1AF00-8GA0

Bidirectional plug-in transceiver SFP

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

Type	Properties	Article number
SFP992-1BXMT	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AL00-8TA0
SFP992-1BXMR	1 x 1000 Mbps LC port optical for glass FO (multimode) with max. 500 m, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AL00-8RA0
SFP992-1BX10T	1 x 1000 Mbps LC port optical for glass FO (single mode) with max. 10 km, transmits at 1550 nm, receives at 1310 nm	6GK5 992-1AM00-8TA0
SFP992-1BX10R	1 x 1000 Mbps LC port optical for glass FO (single mode) with max. 10 km, transmits at 1310 nm, receives at 1550 nm	6GK5 992-1AM00-8RA0

Note

Restriction for pluggable transceivers

The maximum ambient temperature changes if you use pluggable transceivers. You will find the permitted temperature ranges in the section Technical specifications (Page 71).

4.3 Spare parts

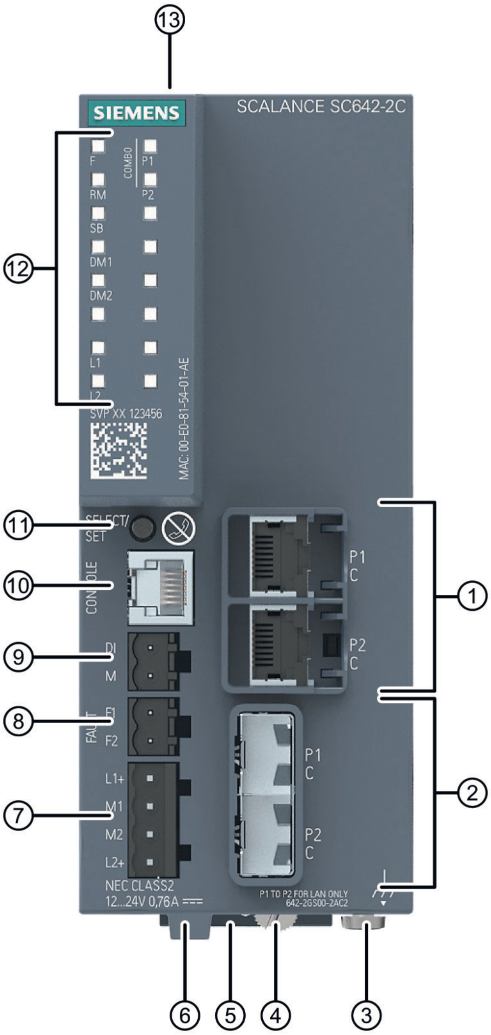
The following spare parts are available for SCALANCE SC-600:

Component	Description	Article number
Spring-loaded terminal block, 4 terminals	4-terminal spring-loaded terminal block to connect the power supply (24 VDC), for SCALANCE X/W/S/M, pack of 5	6GK5 980-1DB10-0AA5
Spring-loaded terminal block, 2 terminals	2-terminal spring-loaded terminal block to connect the signaling contact (24 VDC), for SCALANCE X/W/S/M, pack of 5	6GK5 980-0BB10-0AA5

4.4 Device views

4.4.1 Device view of a SCALANCE SC6x2-2C

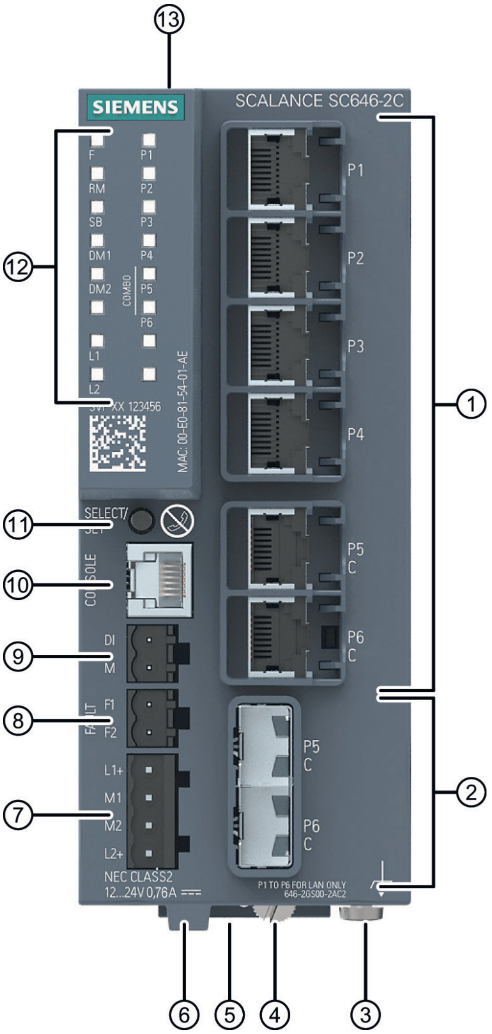
The following figure shows the design of the SC6x2-2C.



① Electrical ports
② SFP transceiver slots
③ Grounding screw
④ Knurled screw
⑤ Securing bar
⑥ Levering aid for moving the securing bar with a screwdriver
⑦ Power supply
⑧ Signaling contact
⑨ Digital input
⑩ Serial interface
⑪ "SELECT / SET" button
⑫ LED display
⑬ Slot for C-PLUG/KEY-PLUG

4.4.2 Device view of a SCALANCE SC6x6-2C

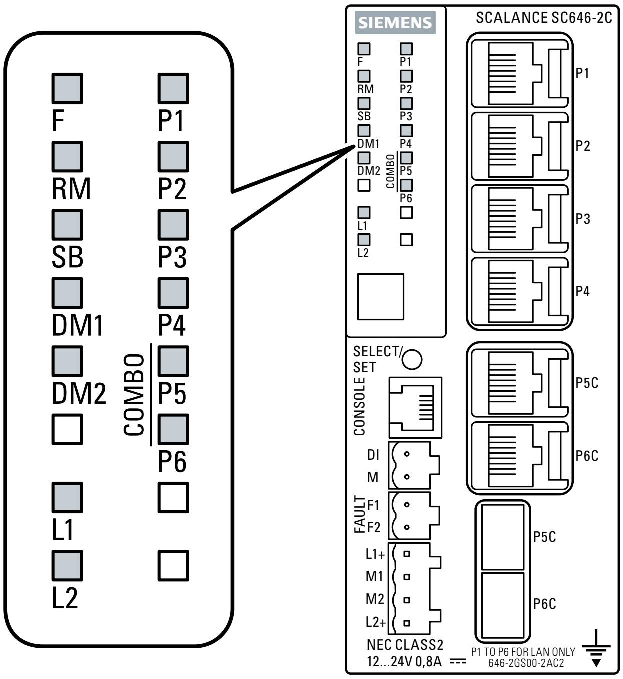
The following figure shows the design of the SC6x6-2C.



① Electrical ports
② SFP transceiver slots
③ Grounding screw
④ Knurled screw
⑤ Securing bar
⑥ Levering aid for moving the securing bar with a screwdriver
⑦ Power supply
⑧ Signaling contact
⑨ Digital input
⑩ Serial interface
⑪ "SELECT / SET" button
⑫ LED display
⑬ Slot for C-PLUG/KEY-PLUG

4.5 LED display

The following figure shows the arrangement of the LEDs based on the example of the SCALANCE SC646-2C.



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

4.5.1 "RM" LED / "SB" LED

This function/LED is not currently used.

4.5.2 "F" LED

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

Meaning during device startup

LED color	LED status	Meaning during device startup
-	Off	Device startup was completed successfully.
Red	On	Device startup is not yet completed or errors have occurred.
Red	Flashing	There are errors in the firmware.
Red	Flashes at interval 2000 ms on / 200 ms off	Firmware on PLUG The device is performing a firmware update or downgrade.

Meaning during operation

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

4.5.3 LEDs "DM1" and "DM2"

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

There are 4 display modes (A, B, C and D). Display mode A is the default mode.

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

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

Setting the display mode

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

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

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

4.5.4 LEDs "L1" and "L2"

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

The meaning of the "L1" and "L2" LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 30)".

Meaning in display modes A, B and C

In display modes A, B and C, from the "L1" and "L2" LEDs you can see whether the power supply is higher or lower than 9.3 V.

L1/L2 LED		L1/L2 connector
LED color	LED status	
-	Off	Power supply lower than 9.3 V
Green	On	Power supply higher than 9.3 V

Meaning in display mode D

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

L1/L2 LED		L1/L2 connector
LED color	LED status	
-	Off	Power supply is not monitored. If the power supply falls below 9.3 V, the signaling contact does not respond.
Green	On	Power supply is monitored. If the power supply falls below 9.3 V, the signaling contact responds.

4.5.5 Port LEDs

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

The meaning of the Port LEDs depends on the set display mode, see section "LEDs "DM1" and "DM2" (Page 30)".

Meaning in display mode A

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

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

* 1 period ≙ 2.5 seconds

Meaning in display mode B

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

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

If there is a connection problem and the type of transmission is fixed (autonegotiation off), the desired status, in other words the set transmission speed (1000 Mbps, 100 Mbps, 10 Mbps) continues to be displayed. If there is a connection problem and autonegotiation is active, the port LED goes off.

Meaning in display mode C

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

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

Meaning in display mode D

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

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

4.6 SELECT/SET button

Position

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

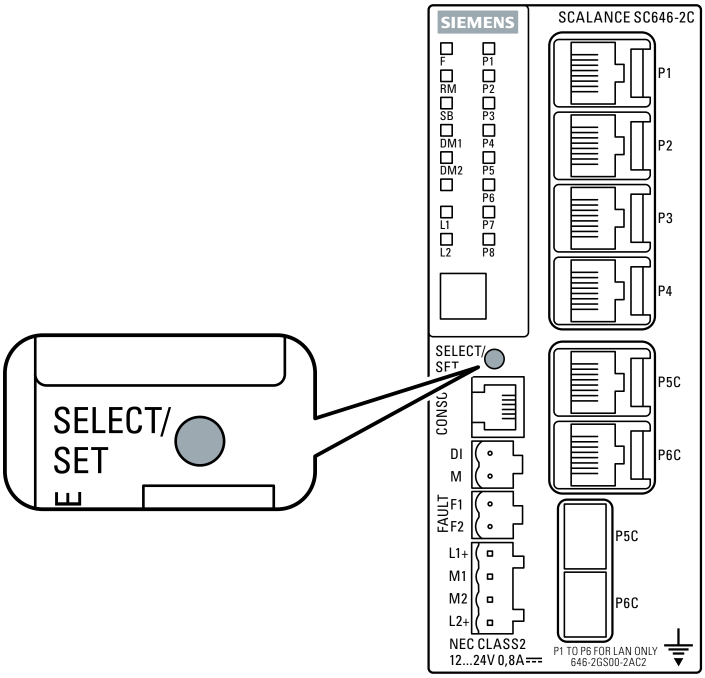


Figure 4-1 Position of the "SELECT/SET" button, for example on the SCALANCE SC646-2C

Setting the display mode

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

For more detailed information on the display modes, refer to the section "LED display (Page 29)".

Resetting the device to factory defaults

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

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

Requirement

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

> **Note**
>
> **Reset despite disabled "SELECT/SET" button**
>
> If you have disabled the "Restore Factory Defaults" function for the "SELECT/SET" button in the configuration, this does not apply during the startup phase, see section "Restoring the factory settings (Page 69)".
>
> If the function has been disabled in the configuration, it is only disabled on completion of the startup phase.

Procedure

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

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

Enabling and disabling the button

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

Defining the fault mask

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

You configure newly plugged-in connections in the configuration.

To define the fault mask, follow the steps below:

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

4.7 C-PLUG/KEY-PLUG

4.7.1 Function of the C-PLUG/KEY-PLUG

NOTICE

Do not remove or insert a C-PLUG/KEY-PLUG during operation

A C-PLUG/KEY-PLUG may only be removed or inserted when the device is turned off.

Saving the configuration data

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

A C-PLUG stores the current information about the configuration of a device.

Note

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

How it works

Operating mode

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

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

Operation with C-PLUG/KEY-PLUG

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

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

Response to errors

Inserting a C-PLUG/KEY-PLUG that does not contain the configuration of a compatible device type, accidentally removing the C-PLUG/KEY-PLUG or general malfunctions of the C-PLUG/KEY-PLUG are signaled by the diagnostics mechanisms of the device:

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

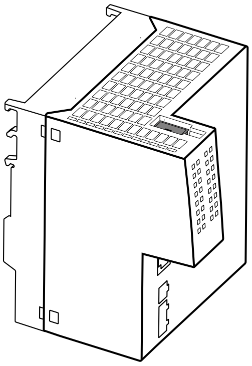
The user then has the choice of either removing the C-PLUG/KEY-PLUG again or selecting the option to reformat the C-PLUG/KEY-PLUG.

4.7.2 Replacing the C-PLUG/KEY-PLUG

Position of the C-PLUG/KEY-PLUG

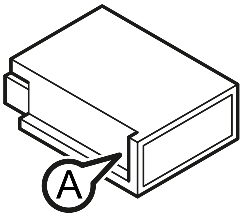
NOTICE
Do not remove or insert a C-PLUG/KEY-PLUG during operation
The C-PLUG may only be removed or inserted when the device is turned off.

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



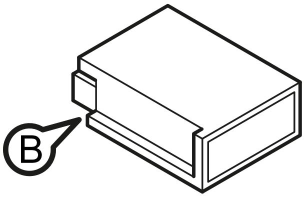
Replacing a C-PLUG/KEY-PLUG

Removing a C-PLUG/KEY-PLUG



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

Inserting a C-PLUG/KEY-PLUG



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

4.8 Combo ports

Characteristics

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

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

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

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

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

Setting the mode

The following modes can be configured for a combo port:

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

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

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

Installation 5

5.1 Safety notices for installation

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

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

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 equipment shall only be used in an area with pollution degree 1 or 2 (see also EN/IEC 60664-1, GB/T 16935.1).

⚠ WARNING
Suitable cables at high ambient temperatures in hazardous area
At an ambient temperature of ≥ 60 °C, use heat-resistant cables designed for an ambient temperature at least 20 °C higher. The cable entries used on the housing must comply with the IP degree of protection required by EN IEC / IEC 60079-0, GB/T 3836.1.

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

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

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

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

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

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 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.

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 Types of installation

Types of installation

The following types of installation are permitted for the device:

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

Permitted mounting positions

Note

Installation location - Dependency of the temperature range

Note the dependency of the permitted temperature range of the installation location:

- Horizontal installation of the rack (DIN rail) means a vertical position of the devices.
- Vertical installation of the rack (DIN rail) means a horizontal position of the devices.

You will find the permitted temperature ranges in the section Technical specifications (Page 71).

Minimum clearances

The module must be installed so that its upper and lower ventilation slits are not covered, allowing adequate ventilation.

Keep to the following minimum clearances for the circulation of air when the rack is installed horizontally:

- Above the device: Minimum 10 cm
- Below the device: Minimum 10 cm

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

5.2.1 Mounting on DIN rails

Installation

Note

Note the position of the securing bar, see also section “Dimension drawings (Page 77)“.

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 49)“.

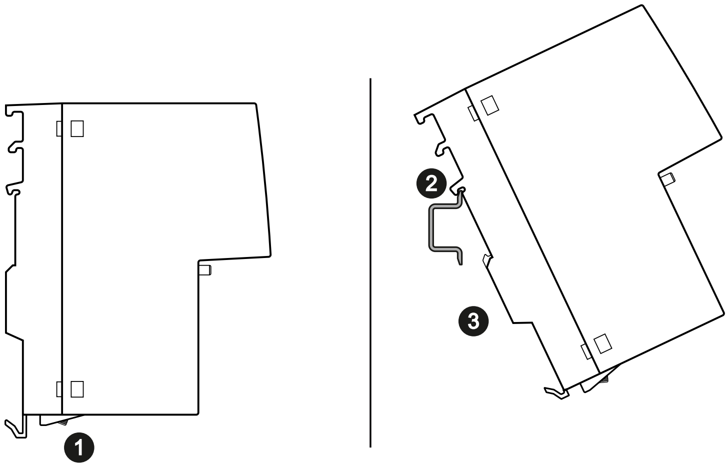


Figure 5-1 DIN rail mounting with securing bar in the wall mounting position.

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 the steps below:

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 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 (Page 51)".

Removal

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

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.

5.2.2 Installation on a standard S7-300 rail

Installing on an S7-300 standard rail

Note

Note the position of the securing bar, see also section “Dimension drawings (Page 77)“.

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 49)“.

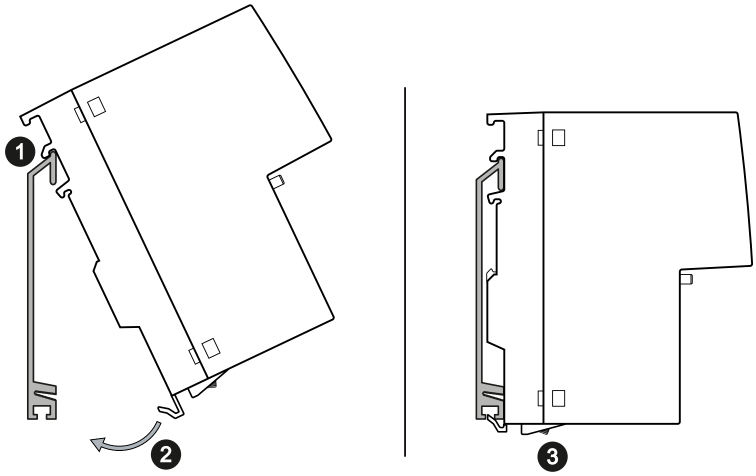


Figure 5-2 S7-300 mounting rail installation with the securing bar in the wall mounting position.

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

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

1. Place the second housing guide of the device on the top edge of the standard 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 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 (Page 51)".

Removal

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

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.

5.2.3 Installation on a standard S7-1500 rail

Installing on an S7-1500 standard rail

Note

Note the position of the securing bar, see also section “Dimension drawings (Page 77)“.

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 49)“.

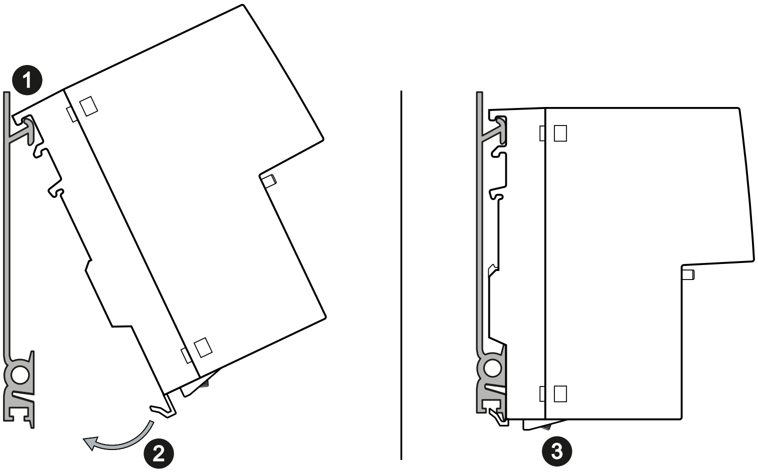


Figure 5-3 S7-1500 mounting rail installation with the securing bar in the wall mounting position.

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

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

1. Place the first housing guide of the device on the top edge of the standard 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 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 (Page 51)".

Removal

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

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.

5.2.4 Wall mounting

Preparation

Note the position of the securing bar, see also section “Dimension drawings (Page 77)“.

When supplied, the securing bar is in the wall mounting position. You do not need to prepare the device any further.

If the securing bar is in the rail mounting position, note the section “Changing the position of the securing bar (Page 49)“.

Tools

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

- 2 wall plugs
- 2 fillister head screws

Note

Depending on the mounting surface, use suitable fittings.

Installation

Note

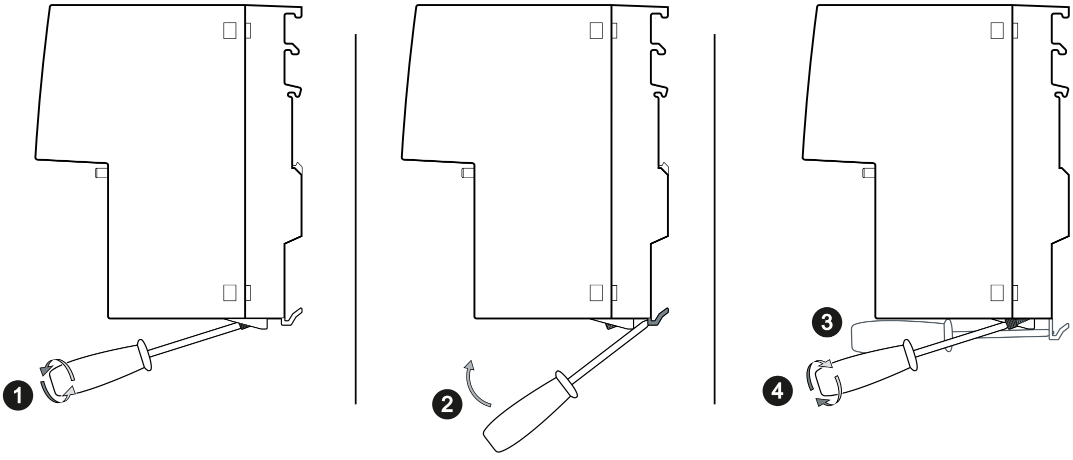
The wall mounting must be capable of supporting at least four times the weight of the device.

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 "Dimension drawings (Page 77)".
2. Turn the upper screw in to the wall so that 10 mm remains jutting out.
3. Hang the device with the keyhole hanging mechanism on the rear on the screw.
4. Fix the device to the wall with the lower screw.
5. Connect the electrical connecting cables, refer to the section "Connecting (Page 51)".

5.2.5 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.

5.3 Disassembly

⚠ **WARNING**

Improper disassembly

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

For proper disassembly, observe the following:

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

Connecting 6

6.1 Safety when connecting up

Safety notices

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

⚠ **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**

Power supply

The device is designed for operation with a directly connectable safety extra low voltage (SELV) from a limited power source (LPS).

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

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

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

NOTICE

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

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

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

> ⚠ **WARNING**
>
> **EXPLOSION HAZARD**
>
> Do not connect or disconnect cables to or from the device when a flammable or combustible atmosphere is present.

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

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

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

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

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

> ⚠ **WARNING**
>
> **Transient overvoltages**
>
> Take measures to prevent transient overvoltages of more than 40% of the rated voltage (or more than 119 V). This is the case if you only operate devices with SELV (safety extra-low voltage).

> ⚠ **WARNING**
>
> **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).

⚠ **WARNING**
EXPLOSION HAZARD Do not press the SELECT/SET button when there is an explosive atmosphere.

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
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 Power supply

Notes on the power supply

⚠ WARNING

Incorrect power supply

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

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

⚠ CAUTION

Damage to the device due to overvoltage

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

One of the tests used to attest the immunity of the device 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 is, for example, the Dehn Blitzductor BVT AVD 24, article number 918 422 or a comparable protective element.

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

Operate the device with suitable overvoltage protection.

Note

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

Information on the power supply

- The "L1" and "L2" LEDs indicate the current range of the power supply, see the section "LED display (Page 29)".
- The power supply is connected using a 4-pin plug-in terminal block (spring-loaded terminal). The terminal block ships with the device and can also be ordered as a spare part.
- The power supply can be connected redundantly. Both inputs are isolated. There is no distribution of load. When a redundant power supply is used, the power supply unit with the higher output voltage supplies the device alone.
- The power supply is connected over a high resistance with the enclosure to allow an ungrounded set up. The two power inputs are non-floating.
- Note the wiring rules.

Position and assignment

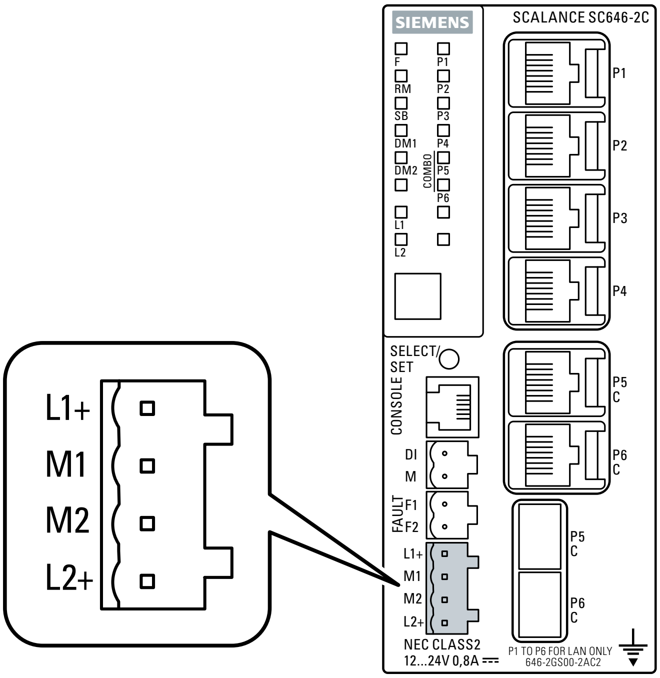


Figure 6-1 Position of the power supply based on the example of the SCALANCE SC646-2C and the assignment of the terminal block

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

6.4 Signaling contact

Information on the signaling contact

- The signaling contact is a floating switch that signals error states by interrupting the contact.
- The signaling contact must be operated within the range of the operating voltage.
- If an error occurs, the signaling contact opens. In normal operation, the signaling contact is closed.
- When you switch on the device, the signaling contact is closed for about 30 ms and is then opened again.
- The signaling contact is connected using a 2-pin plug-in terminal block (spring-loaded terminal). The terminal block ships with the device and can also be ordered as a spare part.
- Note the wiring rules.

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

Configuring signaling contact as digital output

The signaling contact can be configured as digital output via the WBM/CLI. In this case, the signaling contact is closed.

The digital output is opened as soon as you enable one of the following events for the digital output in the WBM under "Events > Configuration":

- Fault State Change
- Digital Input
- VPN Tunnel

To open the signaling contact again, you must disable all events.

You will find information on configuration in the WBM or CLI configuration manual.

Position and assignment

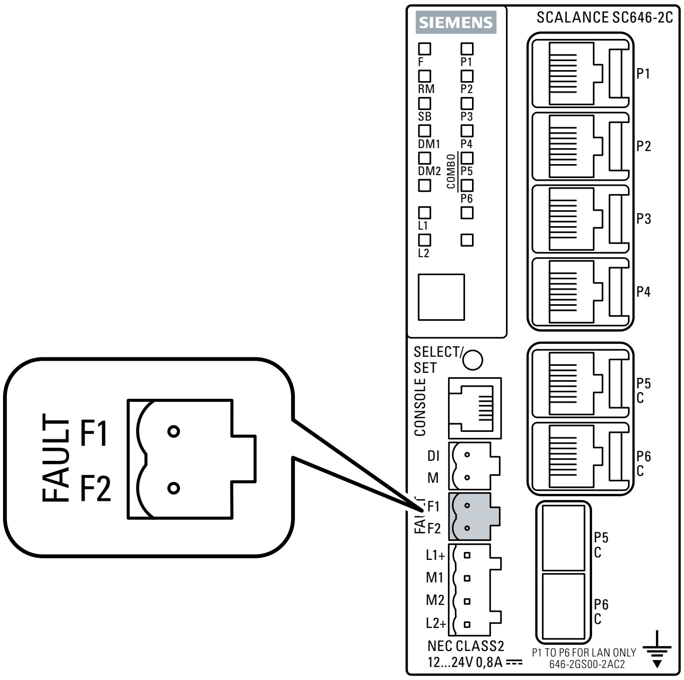


Figure 6-2 Position and assignment of the signaling contact based on the example of the SCALANCE SC646-2C.

Contact	Assignment
F1	Fault contact 1
F2	Fault contact 2

Signaling of errors at the signaling contact

- The signaling of errors by the signaling contact is synchronized with the fault LED "F", see section "LED display (Page 29)".
  All errors that the fault LED "F" indicates (freely configurable) are also signaled by the signaling contact.
- If an internal fault occurs, the fault LED "F" lights up and the signaling contact opens.
- If you connect a communications node to an unmonitored port or disconnect it, this does not cause an error message.
- The signaling contact remains open until one of the following events occurs:
  - The problem is eliminated.
  - The current status is entered in the fault mask as the new desired status.

Signaling of errors at the digital output

- If the signaling contact is configured as digital output, by default the signaling of errors does not run parallel to the fault LED "F".
- For an error to also be signaled by the fault LED "F", you must enable the event "Fault State Change" for the "Digital output" in the WBM under "Events > Configuration". In this case, the fault LED "F" lights up when an internal error occurs and the signaling contact is closed.

6.5 Digital input

Information on the digital input

- The digital input can be used to allow authorized access to the device with a key switch function.
- The digital input is connected using a 2-pin plug-in terminal block (spring-loaded terminal). The terminal block ships with the device and can also be ordered as a spare part.
- The voltage applied to the "DI" contact is converted to a digital status by the device as follows.

Voltage	Status
-30 to +3 VDC	0
+13 to +30 VDC	1

- The maximum input current is 8 mA
- The digital input is isolated from the electronics.

Position and assignment

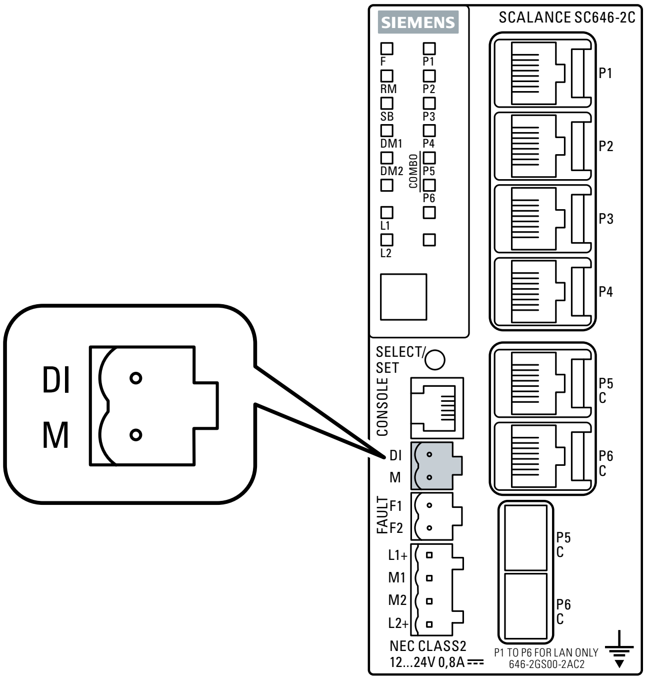


Figure 6-3 Position and assignment of the digital input based on the example of the SCALANCE SC646-2C.

Contact	Assignment
DI	-30 to +30 VDC
M	Ground

6.6 Serial interface

Information on the serial interface

- Via the serial interface on the device (RJ-11 jack), you can access the Command Line Interface of the device directly via an RS-232 (115200 8N1) connection without assigning an IP address.
- Access to the device is possible independent of the Ethernet ports.
- To connect the serial interface to a PC, you require a cable with an RJ-11 plug and 9-pin D-sub female connector. The connecting cable for the serial interface ships with the device.

Position and assignment

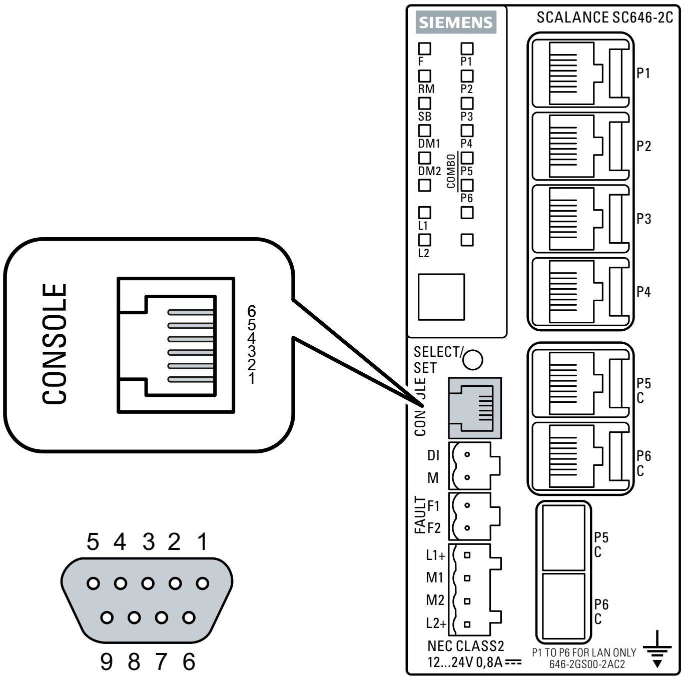


Figure 6-4 Position and pin assignment of the serial interface (RJ-11 jack), for example on the SCALANCE SC646-2C as well as the pin assignment of the D-sub socket.

Assignment of the terminal block

The connecting cable has the following assignment:

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

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

Note

Pin assignment of the RJ-11 jack on the device

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

6.7 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 SCALANCE SC-600 has a grounding screw (fillister head screw with clamping washer und disk) for functional ground, refer to the section "Device views (Page 27)".

The grounding screw is identified by the following symbol for the functional ground.

⏚

1. Loosen the grounding screw).
2. Put 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 ground system is normally in the cabinet close to the power feed-in. This ground conducts fault currents to ground safely and according DIN/VDE 0100 is a protective ground to protect people, animals and property from too high contact voltages.

Apart from the protective ground, there is functional grounding 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.

7 Upkeep and maintenance

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.

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.

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.

WARNING

Cleaning the housing

- **In hazardous areas**
  Only clean the outer parts of the housing with a damp, but not wet, cloth.
- **In non-hazardous areas**
  Only clean the outer parts of the housing with a dry cloth.

Do not use any liquids or solvents.

7.1 Loading new firmware using WBM

Requirement

- The device has an IP address.
- The user is logged in with administrator rights.

Firmware update via HTTP

1. Click "System > Load&Save" in the navigation area. Click the "HTTP" tab.
2. For "Firmware", click the "Load" button.
3. Go to the storage location of the firmware file.
4. Click the "Open" button in the dialog. The file is uploaded.

Firmware update via TFTP

1. Click "System > Load&Save" in the navigation area. Click the "TFTP" tab.
2. Enter the IP address of the TFTP server in the "TFTP Server Address" input box.
3. Enter the port of the TFTP server in the "TFTP Server Port" input box.
4. Click the "Load file" button in the "Firmware" table row.
5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

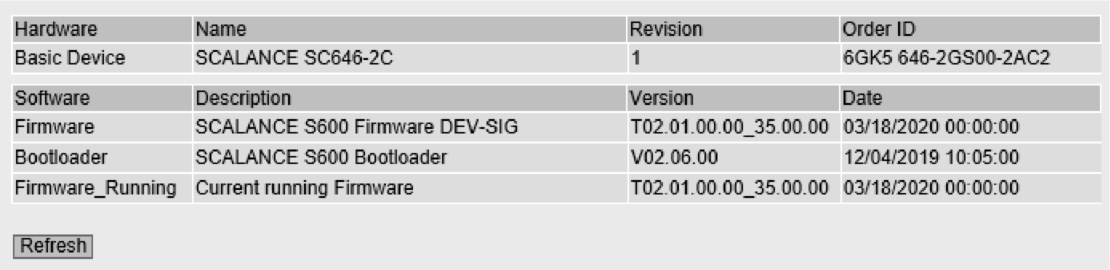
Firmware update via SFTP

1. Click "System > Load&Save" in the navigation area. Click the "SFTP" tab.
2. Enter the IP address of the SFTP server in the "SFTP Server Address" input box.
3. Enter the server port in the "SFTP Server Port" input box.
4. Click the "Load file" button in the "Firmware" table row.
5. Go to the storage location of the firmware file.
6. Click the "Open" button in the dialog. The file is uploaded.

Result

When the firmware is successfully loaded, a dialog is displayed. Confirm the dialog with "OK". The device is restarted.

In "Information > Versions" there is the additional entry "Firmware_Running". Firmware_Running shows the version of the current firmware. For "Firmware", the firmware version stored after loading the firmware is displayed.



Hardware	Name	Revision	Order ID
Basic Device	SCALANCE SC646-2C	1	6GK5 646-2GS00-2AC2

Software	Description	Version	Date
Firmware	SCALANCE S600 Firmware DEV-SIG	T02.01.00.00_35.00.00	03/18/2020 00:00:00
Bootloader	SCALANCE S600 Bootloader	V02.06.00	12/04/2019 10:05:00
Firmware_Running	Current running Firmware	T02.01.00.00_35.00.00	03/18/2020 00:00:00

Cause

If there is a power failure during the firmware update, it can occur that the device is no longer accessible using WBM and CLI.

Requirement

- The PC is connected to the device via the interfaces (P1 - P4).
- A TFTP client is installed on the PC and the firmware file is available.

Solution

You can then also transfer firmware to the device using TFTP.
Follow the steps below to load new firmware using TFTP:

1. Now press the SET button.
2. Hold down the button until the red fault LED (F) starts to flash after approximately 3 seconds.

   Note

   If you hold down the SET button for approximately 10 seconds, the device is reset to its factory settings and can be reached with the IP address 192.168.1.1.

3. Now release the button. The bootloader waits in this state for a new firmware file that you can download by TFTP.

   Note

   If you want to exit the bootloader without making changes, press the SET button briefly. The device restarts with the loaded configuration.

4. Connect a PC to the device over the Ethernet interface (P1 - P4).
5. Open a DOS box, change to the directory where the new firmware file is located and then execute the command "tftp -i <ip address> PUT <firmware>". As an alternative, you can use a different TFTP client.
   If you are not sure that the IP address is correct, you can check this, for example with SINEC PNI.

   Note

   Using TFTP

   If you want to access TFTP in Windows 7, make sure that the corresponding Windows function is enabled in the operating system.

Result

The firmware is transferred to the device.

Note

Please note that the transfer of the firmware can take several minutes. During the transmission, the red error LED (F) flashes.

Once the firmware has been transferred completely to the device, the device is restarted automatically.

7.2 Restoring the factory settings

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

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

Requirement

The device is in the startup phase.

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

Procedure

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

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

Restoring the factory defaults during operation

You can also reset the device to the factory defaults during operation, see section "SELECT/SET button (Page 33)".

Technical specifications 8

8.1 Technical specifications of the SCALANCE SC-600

Technical specifications						
Attachment to Industrial Ethernet						
Electrical connectors			SC6x2-2C		SC6x6-2C	
	Quantity		2		6	
	Connector		RJ-45 jack			
	Properties		Half/full duplex, MDI-X pinning			
	Transmission speed		10 / 100/ 1000 Mbps			
Slots for pluggable transceivers	Quantity		2			
	Connector		SFP transceiver			
	Transmission speed		100 / 1000 Mbps SC62x-2C: 100 Mbps via active SFPs			
Diagnostics interface						
Serial interface	Quantity		1			
	Connector		RJ-11 jack			
Electrical data						
Power supply [1)]	Rated voltage		12 to 24 VDC			
	Voltage range (incl. tolerance)		9.6 to 31.2 VDC Safe Extra Low Voltage (SELV)			
	Design		Terminal block, 4 terminals			
	Properties		Implemented redundantly			
Current consumption			SC622-2C	SC626-2C	SC632-2C/ SC642-2C	SC636-2C/ SC646-2C
	12 VDC	Without SFP	760 mA	1000 mA	660 mA	700 mA
		With SFP	780 mA	1100 mA	760 mA	800 mA
	24 VDC	Without SFP	380 mA	500 mA	330 mA	350 mA
		With SFP	390 mA	550 mA	380 mA	400 mA
Effective power loss		Without SFP	9.12 W	12 W	7.92 W	8.4 W
		With SFP	9.36 W	13.2 W	9.12 W	9.6 W
Fusing			2.5 A / 125 V			
Signaling contact [1)]	Quantity		1			
	Design		Terminal block, 2 terminals			
	Permitted voltage range		12 ... 24 VDC			
	Load capability		max. 100 mA			

Technical specifications		
Digital input	Quantity	1
	Design	Terminal block, 2 terminals
	Property	Isolated from electronics
	Rated voltage	24 VDC safety extra-low voltage (SELV)
	For state "0":	-30 to 3 VDC
	For state "1":	13 to 30 VDC
	Maximum input current	8 mA
	Maximum cable length	< 3 m
Permitted ambient conditions		
Ambient temperature	When operating with pluggable transceivers of the types: • SFP991-1/1 (C)/1LD/1LD (C) • SFP992-1/1 (C)/1LD/1LD (C) up to 2000 m	During operation with the rack installed horizontally: -40 °C to +65 °C During operation with the rack installed vertically: -40 °C to +60 °C
	When operating with pluggable transceivers of the types: • SFP991-1LH+/1ELH200 • SFP992-1+/1LD+/1LH/1LH+/1ELH • SFP992-1BXMT/1BXMR/1BX10T/1BX10R up to 2000 m	During operation with the rack installed horizontally: -40 °C to +60 °C During operation with the rack installed vertically: -40 °C to +50 °C
	During LAN operation with RJ45 connector up to 2000 m	During operation with the rack installed horizontally: -40 °C to +70 °C During operation with the rack installed vertically: -40 °C to +65 °C
	With operation between 2000 m and 3000 m	The maximum ambient temperature is reduced by 5 °C
	With operation between 3000 m and 4000 m	The maximum ambient temperature is reduced by 10°C
	Storage	-40 °C to +85 °C
	Transportation	-40 °C to +85 °C
Relative humidity	Operation at 25 ℃	≤ 95 % no condensation
Housing, dimensions and weight		
Design	compact	
Housing material	Basic housing	Die cast aluminum, powder coated
	Front cover	Polycarbonate (PC-GF10)
Degree of protection	IP20	
Dimensions (W x H x D)	60 x 145 x 125 mm	
Weight	580 g	

Technical specifications	
Installation options	• Wall mounting • Installation on a DIN rail • Mounting on an S7-300 standard rail • Mounting on an S7-1500 standard rail
Mean time between failure (MTBF)	
MTBF (EN/IEC 61709; 40 °C)	SC622-2C: 34.99 years SC626-2C: 29.63 years SC632-2C/SC642-2C: 37.83 years SC636-2C/SC646-2C: 31.64 years
Switching properties	
Aging time	Can be configured (default value: 30 seconds)
Response to LLDP frames	Blocking
CoS acc. to IEEE 802.1Q	Yes

[1)] Note the wiring rules (Page 55).

8.2 Mechanical stability (in operation)

Mechanical stability (in operation)

Device	**IEC 60068-2-27 shock**	**IEC 60068-2-6 vibration**
	15 g, 11 ms duration **6 shocks per axis**	**10 - 58 Hz: 0.075 mm** **85 - 150 Hz: 1 g** **1 octave/min, 20 sweeps**
SC6x2-2C	●	●
SC6x6-2C	●	●

8.3 Cable lengths

The following technical specifications apply to SCALANCE SC-600:

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

Dimension drawings

9

All dimensions specified in millimeters.

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

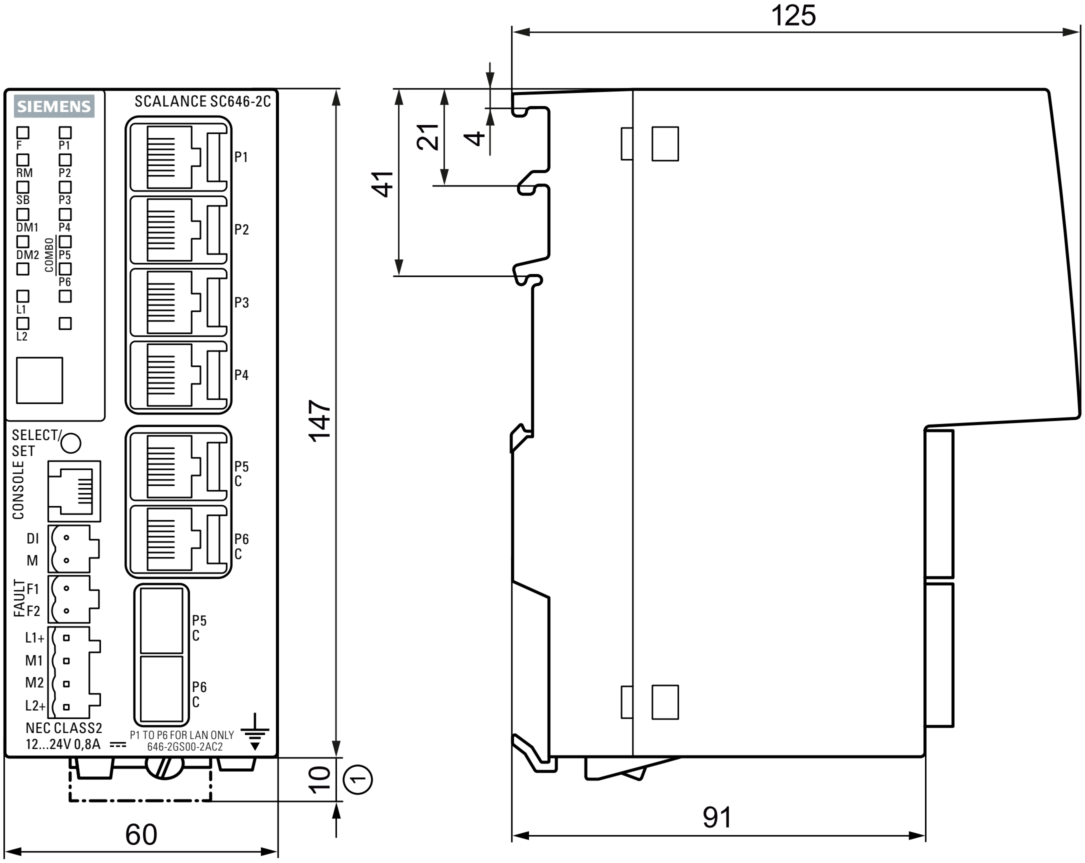


Figure 9-1 Front view and side view of the SCALANCE SC646-2C. All SCALANCE SC-600 modules have the same dimensions.

Approvals 10

Approvals issued

Note

Issued approvals on the type plate of the device

The specified approvals - with the exception of the certificates for shipbuilding - have only been obtained when there is a corresponding mark on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate. The approvals for shipbuilding are an exception to this.

Certificates for shipbuilding and national approvals

The device certificates for shipbuilding and special national approvals can be found in Siemens Industry Online Support on the Internet:
Link: (https://support.industry.siemens.com/cs/ww/en/ps/15326/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

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/15326/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

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/25661/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/ps/25661/cert).

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
DEKRA 21UKEX0001 X
IECEx DEK 18.0017X
Importer UK:
Siemens plc,
Manchester
M20 2UR
(Ex na IIC T4 Gc, not on the nameplate)
2020322310002626
2021322310003933
2020322310002987

The products meet the requirements of the following standards:

- EN/IEC 60079-7, GB 3836.8
- EN IEC/IEC 60079-0, GB 3836.1

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

EMC (electromagnetic compatibility)

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

Applied standards:

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

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

RoHS

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

Applied standard:

- EN IEC 63000

FM

The product meets the requirements of the standards:

- Factory Mutual Approval Standard Class Number 3611
- FM Hazardous (Classified) Location Electrical Equipment:
  Non Incendive / Class I / Division 2 / Groups A,B,C,D / T4 and
  Non Incendive / Class I / Zone 2 / Group IIC / T4

cULus approval for industrial control equipment

cULus Listed IND. CONT. EQ.

Underwriters Laboratories Inc. complying with

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

Report no. E115352

cULus Approval Hazardous Location

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

Underwriters Laboratories Inc. complying with

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

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

Report no. E240480

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

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

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

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)

⚠ 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