SIEMENS

SIMATIC NET

Industrial Ethernet switches SCALANCE XP-200G PP

Operating Instructions

Introduction 1

Safety notices 2

Security recommendations 3

Description of the device 4

Installing and removing 5

Connecting up 6

Upkeep and maintenance 7

Technical specifications 8

Dimension drawings 9

Approvals A

12/2023
C79000-G8976-C722-01

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-C722-01
Ⓟ 12/2023 Subject to change

Copyright © Siemens 2023.
All rights reserved

Table of contents

1 Introduction 5

2 Safety notices 9

3 Security recommendations 11

4 Description of the device 19

4.1 Product overview 19

4.2 Device view 21

4.3 Accessories 21

4.4 Spare parts 22

4.5 LED display 23
4.5.1 "F" LED 23
4.5.2 "RM" LED 24
4.5.3 "SB" LED 24
4.5.4 "L1" LED 24
4.5.5 Port LEDs 24

4.6 RESET button 26

4.7 C-PLUG 28
4.7.1 Function of the C-PLUG 28
4.7.2 Replacing the C-PLUG 29

5 Installing and removing 33

5.1 Safety when mounting 33

5.2 Types of installation 36

5.3 Wall mounting 36

5.4 Disassembly 37

6 Connecting up 39

6.1 Safety when connecting 39

6.2 Industrial Ethernet 42

6.3 Power supply 43

6.4 Functional ground 46

7 Upkeep and maintenance 49

7.1 Downloading new firmware using TFTP without WBM and CLI 49

7.2 Restoring the factory settings 50

8 Technical specifications 53

8.1 Technical specifications of SCALANCE XP208G PP 53

8.2 Permitted cable lengths 54
8.3 Switching properties 54
9 Dimension drawings 57
A Approvals 59
Index 65

Introduction

1

Purpose of the Operating Instructions

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

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 XP208G PP

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

Designations used

Classification	Description	Terms used
Product line	The product line includes all devices and variants of all product groups. If information applies to all product groups within the product line, the term SCALANCE X-200 is used.	SCALANCE X-200
Product group	If information applies to all devices and variants of a product group, the term SCALANCE XP-200G PP is used.	SCALANCE XP-200G PP
Device	If information relates to a specific device, the device name is used.	e.g. SCALANCE XP208G PP

Documentation on configuration

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

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

You will find the configuration manuals here:

- on the data medium that ships with some products:
  - Product CD / product DVD
  - SIMATIC NET Manual Collection
- On the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/21869/man).

Further documentation

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

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

You will find the system manuals here:

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

SIMATIC NET manuals

You will find the SIMATIC NET manuals here:

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

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

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

Cybersecurity notes

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

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

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

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

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

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

Note on firmware/software support

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

Catalogs

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

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

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

Device defective

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

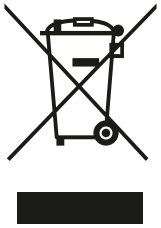
Decommissioning

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

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

Also restore the factory settings on the storage medium.

Recycling and disposal



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

Do not dispose of the products at public disposal sites.

For environmentally friendly recycling and the disposal of your old device contact a certified disposal company for electronic scrap or your Siemens contact (Product return (https://support.industry.siemens.com/cs/ww/en/view/109479891)).

Note the different national regulations.

Trademarks

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

SCALANCE, C-PLUG, OLM

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".

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

NOTICE
Loss of water and dust protection If you open the device, it loses its water and dust protection. • Do not open the device. If the is not adhered to, the manufacturer's guarantee is lost.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING
EXPLOSION HAZARD Do not open the device. There are no serviceable parts inside of the device.

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

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

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

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

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

Security recommendations

3

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

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

General

- Check the device regularly to ensure that these recommendations and/or other internal security policies are complied with.
- Evaluate the security of your location and use a cell protection concept with suitable products (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx).
- When the internal and external network are disconnected, an attacker cannot access internal data from the outside. Therefore operate the device only within a protected network area.
- No product liability will be accepted for operation in a non-secure infrastructure.
- Use VPN to encrypt and authenticate communication from and to the devices.
- For data transmission via a non-secure network, use an encrypted VPN tunnel (IPsec, OpenVPN).
- Separate connections correctly (WBM, SSH etc.).
- Check the user documentation of other Siemens products that are used together with the device for additional security recommendations.
- Using remote logging, ensure that the system protocols are forwarded to a central logging server. Make sure that the server is within the protected network and check the protocols regularly for potential security violations or vulnerabilities.

Physical access

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

Software (security functions)

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

Authentication

Note

Accessibility risk - Risk of data loss

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

- Replace the default passwords for all user accounts, access modes and applications (if applicable) before you use the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. password1, 123456789, abcdefgh) or recurring characters (e.g. abcabc).
  This recommendation also applies to symmetrical passwords/keys configured on the device.
- Make sure that passwords are protected and only disclosed to authorized personnel.
- Do not use the same passwords for multiple user names and systems.
- Store the passwords in a safe location (not online) to have them available if they are lost.
- Regularly change your passwords to increase security.
- A password must be changed if it is known or suspected to be known by unauthorized persons.
- When user authentication is performed via RADIUS, make sure that all communication takes place within the security environment or is protected by a secure channel.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP or IPv4. An attacker could use vulnerabilities in these protocols to attack hosts, switches and routers connected to your layer 2 network, for example, through manipulation (poisoning) of the ARP caches of systems in the subnet and subsequent interception of the data traffic. Appropriate security measures must be taken for non-secure layer 2 protocols to prevent unauthorized access to the network. Physical access to the local network can be secured or secure, higher layer protocols can be used, among other things.

Certificates and keys

- The devices SCALANCE XF204G, SCALANCE XB206-2 as of firmware version V4.4 or SCALANCE XP-200G, SCALANCE XP-200G PP as of firmware version V4.5 use certificates for elliptic curve cryptography ("ECDSA certificates"). Only use ECDSA certificates in PEM format that were generated with the following curves:
  - secp256r1 (NIST P-256)
  - secp384r1 (NIST P-384)
  - secp521r1 (NIST P-521)

  On the device there is a preset SSL certificate with the key length 256 bits for the elliptic-curves cryptography. Replace this certificate with a self-made certificate with key. We recommend that you use a certificate signed either by a reliable external or by an internal certification authority.
- There is a preset SSL/TLS (RSA) certificate with 2048 bit key length in other devices. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use a certification authority including key revocation and management to sign certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- Verify certificates and fingerprints on the server and client to prevent "man in the middle" attacks.
- Change certificates and keys immediately if there is a suspicion of compromise.

Secure/non-secure protocols and services

- Avoid or disable non-secure protocols and services, for example HTTP, Telnet and TFTP. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Check whether use of the following protocols and services is necessary:
  - Non authenticated and unencrypted ports
  - HTTP
  - Telnet
  - SNMPv1/v2c
  - NTP
  - MRP, HRP, STP, RSTP and MSTP
  - IGMP snooping
  - LLDP
  - DCP
  - Syslog
  - DHCP Options 66/67
  - TFTP
  - GMRP and GVRP
- The following protocols provide secure alternatives:
  - HTTP → HTTPS
  - Telnet → SSH
  - SNMPv1/v2c → SNMPv3
    Check whether use of SNMPv1/v2c. is necessary. SNMPv1/v2c is classified as non-secure. Use the option of preventing write access. The device provides you with suitable setting options.
    If SNMP is enabled, change the community names. If no unrestricted access is necessary, restrict access with SNMP.
    Use the authentication and encryption mechanisms of SNMPv3.
  - TFTP → SFTP
  - NTP → NTPsecure
- Use secure protocols when access to the device is not prevented by physical protection measures.
- If you require non-secure protocols and services, operate the device only within a protected network area.
- Restrict the services and protocols available to the outside to a minimum.
- If you use RADIUS for management access to the device, activate secure protocols and services.

Interfaces security

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

Available protocols

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

The table includes the following columns:

- **Protocol**
- **Port**
- **Default port status**
  - Open
    The factory setting of the port is "Open".
  - Closed
    The factory setting of the port is "Closed".
- **Configurable port**
  - ✓
    The port status can be changed.
  - --
    The port status cannot be changed.
- **Authentication**
  Specifies whether the communication partner is authenticated.
- **Encryption**
  Specifies whether or not the transfer is encrypted.

List of available services

Note

Packet filtering

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

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

The table includes the following columns:

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

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

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [5]
			Port	Service		
DHCPv4 Server	UDP/67	Closed	-	✓	-	-
DHCPv4 Client	UDP/68	Open	-	✓	-	-
EtherNet/IP	TCP/44818 UDP/2222 UDP/44818	Closed (Open with EtherNetIP variants)	-	✓	-	-
HTTP Server/Client [3]	TCP/80	Closed	✓	✓	✓	-
HTTPS WBM Server/ Client	TCP/443	Open	✓	✓	✓	✓
NTP Client	UDP/123	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Closed	✓	✓	✓	-
PROFINET	UDP/34964 UDP/49151 ... 49159 [1]	Open	-	✓	-	-
RADIUS Client	UPD/1812 [4] UPD/1813 [4]	Outbound only	✓	✓	-	-
	UDP/3799	Open	✓	✓	-	-
SFTP Server	UDP/22	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	-	-
SMTP Client (secure)	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c [2] [3]	UDP/161	Open	✓	✓	-	-
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outbound only	-	✓	-	-
SNTP Client	UDP/123	Closed	✓	✓	-	-
SSH CLI Server	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	-	-

Service	Protocol / Port number	Default port status	Configurable		Authentication	Encryption [5]
			Port	Service		
Syslog (secure) Client	TCP/6514	Closed	✓	✓	-	✓
Telnet [3]	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outbound only	✓	✓	-	-

1) Port number can be configured via the WBM.

2) Read-only access only.

3) Protocol according to Security by Default.

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

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

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

The table includes the following columns:

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

Layer 2 service	Default port status	Service configurable
DCP	Setup mode [1]	✓
LLDP	Open	✓
RSTP	Closed	✓
MSTP	Open	✓

1) Setting according to Security by Default.

Description of the device

4

4.1 Product overview

Article numbers

Device	Description	Article number
SCALANCE XP208G PP	8 x 10/100/1000 Mbps push-pull connector technology electrical	6GK5208-0JA00-2AS6

Factory settings

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

Ring ports

The factory setting defines the following ring ports:

- Ports P0.1 and P0.2

Unpacking and checking

⚠ WARNING

Do not use any parts that show evidence of damage

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

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

- Injury to persons
- Loss of the approvals
- Violation of the EMC regulations
- Damage to the device and other components

Use only undamaged parts.

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

Components of the product

The following components are supplied with a SCALANCE XP-200G PP:

- One device
- One product DVD with documentation and software
- Protective caps for all connectors
- Grounding screw

4.2 Device view

The following figure shows an overview of the components of the SCALANCE XP208G PP.



① Keyhole hang-up mechanism
② Ethernet ports for Gigabit Ethernet
③ Connector for power supply of the device
④ Grounding point
⑤ Connector for switched and unswitched power supply
⑥ Cover (captively connected to the housing) for:
- C-PLUG slot
- "RESET" button

⑦ Mounting for the cover
⑧ LED display

4.3 Accessories

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

C-PLUG

Component	Description	Article number
C-PLUG	Configuration plug, exchangeable storage medium for configuration data, 32 MB	6GK1 900-0AB00
	Configuration plug, exchangeable storage medium for configuration data, 32 MB, varnished (conformal coating)	6GK1 900-0AQ00

Plug Power Plug PRO

Component	Description	Article number
Power Plug PRO	5-pin push-pull plug with metal enclosure for on-site mounting 1 plug per package	6GK1907-0AB11-6AA0

RJ45 data plug-in connector PRO 2x2

Component	Description	Article number
IE FastConnect RJ45 Plug PRO (push pull)	RJ-45 data plug-in connector for IE FC TP cables 2x2, IP65 1 connector per package	6GK1 901-1BB20-6AA0
IE RJ45 Plug PRO (push pull)	RJ-45 data plug-in connector for IE TP cables 2x2, IP65 1 connector per package	6GK1 901-1BB10-6AA0

RJ45 data plug-in connector PRO 4x2

Component	Description	Article number
IE FastConnect RJ45 Plug PRO (push pull)	RJ45 data plug-in connector for IE FC TP cables 2x2 and 4x2, IP65 1 connector per package	6GK1 901-1BB21-6AA0

4.4 Spare parts

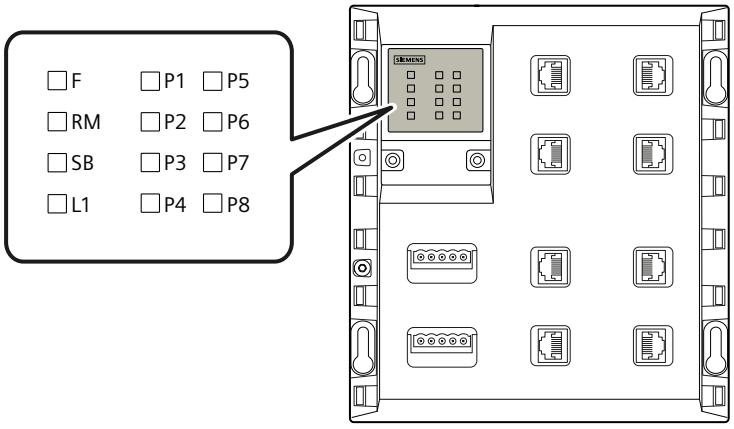
The following spare parts are available for the devices mentioned in the scope of validity:

Protective caps for push-pull sockets

Component	Description	Article number
Protective caps for push-pull sockets (1L +; 2L+)	Protective caps to protect unused connectors for the power supply Pack of 5	6ES7 194-4JA50-0AA0
Protective caps for push-pull sockets (SC RJ)	Protective caps to protect unused RJ45 connectors Pack of 5	6ES7 194-4JD50-0AA0

4.5 LED display

The following figure shows the arrangement of the LEDs.



F LED for displaying the fault/error status
RM LED for displaying the "redundancy manager" function
SB LED for displaying the "standby" function
L1 LEDs for displaying the power supply
P LEDs for displaying the port status

4.5.1 "F" LED

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

Meaning during device startup

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

Meaning during operation

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

4.5.2 "RM" LED

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

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

4.5.3 "SB" LED

The "SB" LED shows the status of the standby function.

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

4.5.4 "L1" LED

The "L1" LED shows whether the power supply L1+/M1 is connected to the X01 IN plug.

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

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 "AUTOHOTSPOT".

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 station turned off or cable not connected).
Green	On	Link exists and port in normal status. In this status, the port can receive and send data.
	Flashes once per period*	Link exists and port in "blocking" status. In this status, the port only receives management data (no user data).
	Flashes three times per period*	Link exists and port turned off by management. In this status, no data is sent or received via the port.
	Flashes four times per period*	Link exists and is in the "monitor port" status. In this status, the data traffic of another port is mirrored to this port.
Yellow	Flashing / lit	Receiving data at port

* 1 period ≙ 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.

Meaning in display mode E

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

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

4.6 RESET button

Position

NOTICE
Loss of water and dust protection
If the cover is not mounted correctly, the device is not water and dust proof.

The "RESET" button is located beneath the cover under the LED display.

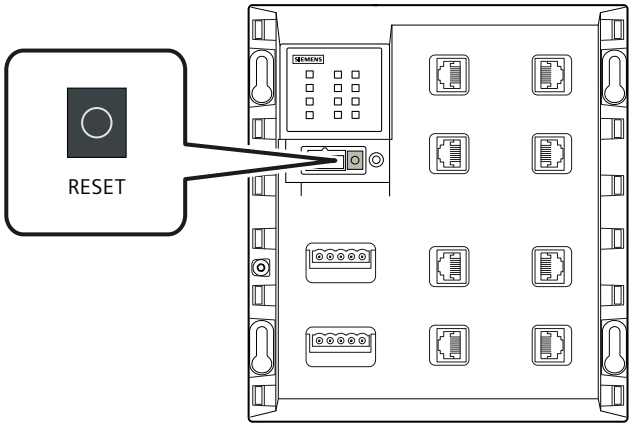


Figure 4-1 Position of the "RESET" button

Resetting the device to factory defaults

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

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

Requirement

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

Note

Reset despite disabled "RESET button"

If you have disabled the "Restore Factory Defaults" function for the "RESET" button in the configuration, this does not apply during the startup phase, see section "Restoring the factory settings
(Page 50)".

If the function has been disabled with 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. Loosen the screws of the cover.
2. Remove the cover.
3. Hold down the "RESET" button for 12 seconds.
   After 9 seconds, the port LEDs go on one after the other.
   After you have held down the button for 12 seconds, the factory defaults are restored.
   If you release the button before the 12 seconds have elapsed, the reset is canceled.
4. Close the cover (tightening torque 0.8 Nm), to ensure that the device is closed and water- and dust-proof.

Enabling and disabling the button

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

4.7 C-PLUG

4.7.1 Function of the C-PLUG

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

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

A C-PLUG can be used to save the firmware. You will find more information under "System > PLUG (Page 5)".

Note

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

How it works

Operating mode

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

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

Operation with C-PLUG

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

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

Response to errors

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

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

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

4.7.2 Replacing the C-PLUG

Position of the C-PLUG

NOTICE
Loss of water and dust protection If the cover is not mounted correctly, the device is not water and dust proof.

NOTICE
Do not remove or insert a C-PLUG during operation The C-PLUG may only be removed or inserted when the device is turned off. The device checks whether or not a C-PLUG is inserted at one second intervals. If it is detected that the PLUG was inserted or removed, there is a restart.

The C-PLUG slot is beneath a cover under the LED display.

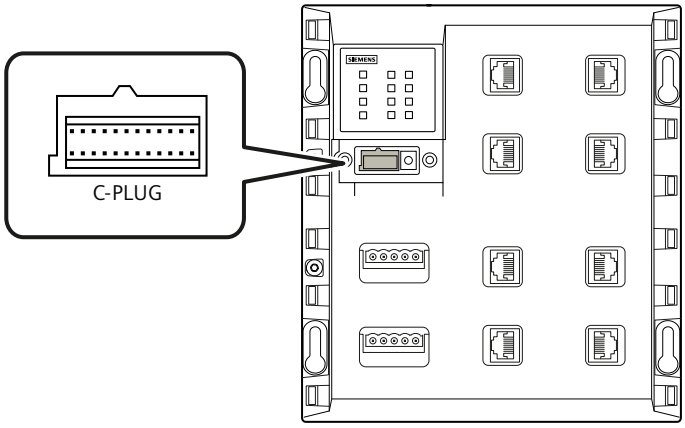
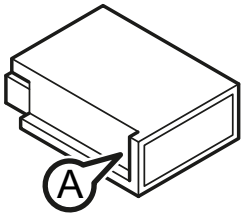


Figure 4-2 Position of the slot

Replacing a C-PLUG

Removing a C-PLUG



1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Insert a screwdriver between the front edge of the C-PLUG (A) and the slot and release the C-PLUG.
5. Remove the C-PLUG.
6. Close the cover (tightening torque 0.8 Nm), to ensure that the device is closed and water- and dust-proof.

Note

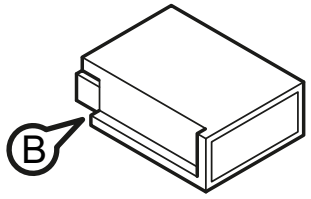
Loss of the configuration

The "RESET (Page 26)" button is located directly beside the slot for the C-PLUG. The button cannot be used to remove the C-PLUG.

If you hold down the "RESET" button, you reset all settings of the device to the factory defaults.

Remove the C-PLUG with a screwdriver.

Inserting a C-PLUG



1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. The housing of the C-PLUG has a protruding ridge on the long side (B). The slot has a groove at this position. Insert the C-PLUG correctly oriented into the slot.
5. Close the cover (tightening torque 0.8 Nm), to ensure that the device is closed and water- and dust-proof.

Installing and removing

5

5.1 Safety when mounting

Safety notices

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

⚠ WARNING

If a device is operated in an ambient temperature of more than 40 °C, the temperature of the device housing may be higher than 70 °C. The device must therefore be installed so that it is only accessible to service personnel or users that are aware of the reason for restricted access and the required safety measures at an ambient temperature higher than 40 °C.

⚠ WARNING

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

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING

EXPLOSION HAZARD

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

⚠ WARNING

The device is intended for indoor use only.

WARNING

The device may only be operated in an environment of contamination class 1 or 2 (see EN/IEC 60664-1, GB/T 16935.1).

WARNING

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

WARNING

EXPLOSION HAZARD

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

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

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

WARNING

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

WARNING

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

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

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

⚠ WARNING

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

Note

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

Additional notes

⚠ CAUTION

Use only approved components

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

NOTICE

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

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

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

Note

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

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

5.2 Types of installation

The SCALANCE XP-200G PP can be installed in the following ways:

- Wall mounting

Installation position

To use of the maximum ambient temperature of the devices, the following mounting position is recommended:

- Horizontal
  The SIEMENS logo and the LED display of the devices are at the top left with horizontal installation position. The device is upright and the labeling is in the reading direction.

Other installation positions are associated with deviating temperature values, see "Technical specifications of SCALANCE XP208G PP (Page 53)".

Observe the information on the installation position with loop-through of the power supply, see "Power supply (Page 43)".

5.3 Wall mounting

Note

Depending on the mounting surface, use suitable fittings.

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 drill holes for wall mounting.
   For the precise dimensions, refer to the section "Dimension drawings (Page 57)".
2. Screw the device to the wall using the keyhole hang-up mechanisms.
3. Fit the connectors for the power supply, see the section "Power supply (Page 43)".

5.4 Disassembly

⚠ WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

Connecting up

6

6.1 Safety when connecting

Safety notices

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

Note

Maximum current 16 A

The current through the Power Plug PRO must not exceed 16 A. This value also contains the power consumption of the device itself. For information on the power consumption of the device, see "Technical specifications (Page 53)".

Include a fuse that trips at a current higher than 16 A.

In areas subject to the NEC or CEC, the fuse must meet the following requirements:

- Suitable for DC (min. 60 V / max. 16 A)
- Breaking current at least 10 kA
- UL / CSA listed (UL 248-1 / CSA 22.2 No. 248.1)
- Classes R, J, L, T or CC

Otherwise the following requirements must be met:

- Suitable for DC (min. 60 V / max. 16 A)
- Breaking current at least 10 kA
- Approved according to IEC/EN 60127-1
- Breaking characteristics
  - With circuit breakers: B or C
  - With fuses: slow blow

Note

Close unused ports

Close all unused ports with protective caps, see "Spare parts (Page 22)".

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

WARNING

EXPLOSION HAZARD

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

WARNING

EXPLOSION HAZARD

Do not press the SELECT/SET button when there is an explosive atmosphere.

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

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

WARNING

Unprotected cable ends

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

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

WARNING

Improper installation of shielded cables

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

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

WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

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

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

WARNING

Transient overvoltages

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

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.

WARNING

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

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

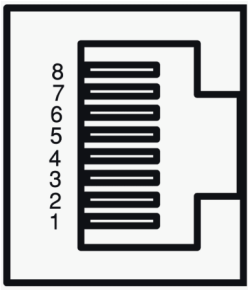
Do not connect any electrical connectors directly to the telephone network (telephone network voltage) or a WAN (Wide Area Network).

6.2 Industrial Ethernet

Connection to Industrial Ethernet takes place via the PROFINET-compliant push-pull connector technology.

Due to their high degree of protection (IP65), the push-pull connectors are suitable for installation outside cabinets. The plugs do not ship with the product, see the section "Accessories (Page 21)".

The following table shows the pin assignment of the connectors:

Pin no.:	Assignment	
8	D4-	
7	D4+	
6	D2-	
5	D3-	
4	D3+	
3	D2+	
2	D1-	
1	D1+	

MDI / MDI-X autocrossover

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

Note

Formation of loops

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

Autonegotiation

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

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

Note

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

6.3 Power supply

Notes on the power supply

Note

No redundant power supply

Since the devices do not have a redundant power supply, connect the power supply to X01 IN.

Information on the power supply

- The device is supplied with power via the X01 IN connector.
- The device is only supplied with power via the L1+/M1 connector.
- The device only monitors the L1+/M1 connector.
- Loop-through of the power supply takes place via the X02 OUT connector.
- Power: 24 V DC
- The power supply is connected over a high resistance with the housing to allow an ungrounded setup.
- The power supply is non-floating.
- The signal cables of the electrical Ethernet interfaces are floating.

Position and assignment

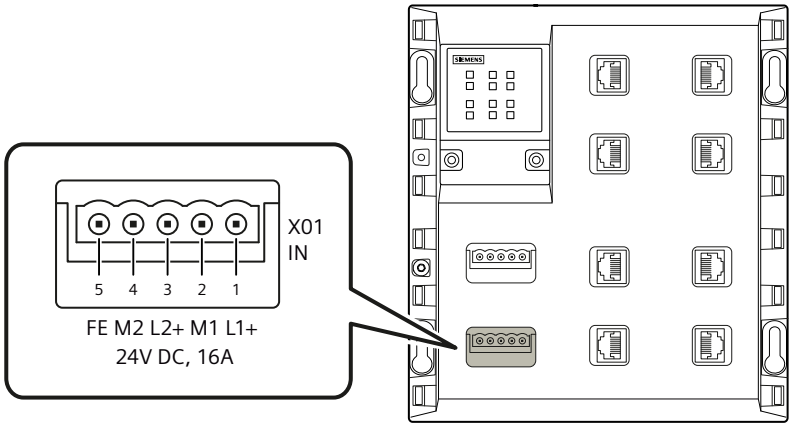


Figure 6-1 Position of the power supply for the device

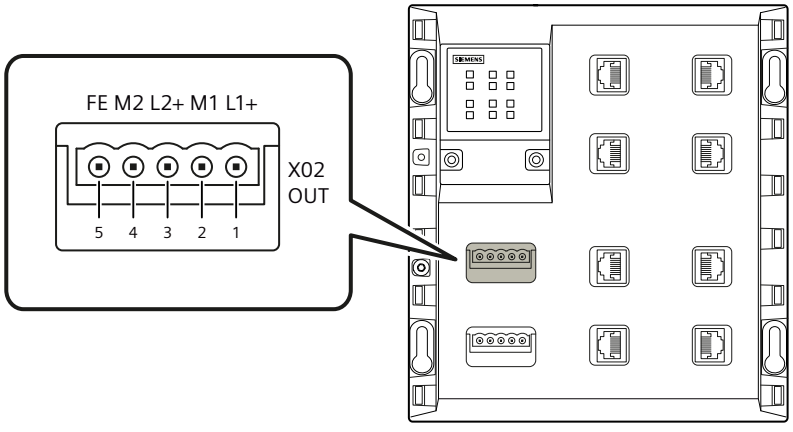


Figure 6-2 Position of the power supply for loop-through

The following table shows the pin assignment of the two power supply connectors:

Pin no.:	Assignment
1	L1+: 24 V DC (device supply)
2	M1 (device supply)
3	L2+: 24 V DC
4	M2
5	FE (Functional Earth)

Connector

Plastic version (standard)

The power supply is connected by default via the push-pull Power Plug PRO. This plug has a high degree of protection (IP65) and is suitable for use outside cabinets and complies with PROFINET connector technology.

The Power Plug PRO does not ship with the device, see the section "Accessories (Page 21)".

Metal version

In areas subject to the EU directives ATEX and IECEX of the National Electric Code (NEC), the Canadian Electric Code (CEC) and UL, metal connectors must be used.

Further information and technical advice on this subject is available from:
Jürgen Hertlein, juergen.hertlein@siemens.com.

Power supply looped through

The devices also have a connector for the switched and unswitched power supply of other devices with 24 V DC. Via this interface X02 OUT (L1+, M1 and L2+, M2), it is possible to loop the power through with connector technology compliant with PROFINET.

Refer also to the manual "SIMATIC Distributed IO System ET 200pro (https://support.industry.siemens.com/cs/ww/en/view/21210852)".

When looping through the power supply, you must take limit values into account; in other words, the maximum permitted current depending on the ambient temperature and the installation position:

Table 6-1 Operation under marginal conditions

Ambient temperature	Max Power 1 (L1+, M1)	Max Power 2 (L2+, M2)	Installation position
+60°C	16 A	16 A	Any
+70°C	8 A	8 A	Only horizontal

For the installation position, see also "Types of installation (Page 36)".

6.4 Functional ground

EMC disturbances are diverted to ground via the functional ground. This ensures the immunity of the data transmission.

The functional grounding must be connected with low impedance. The connection of the functional ground must be established directly on the mounting plate or the DIN rail terminal.

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

Protective earth/functional ground

The connection of the reference potential surface with the protective circuit is normally in the cabinet close to the power feed-in. This ground conducts fault currents to ground safely and according to 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) operational 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.

Position

The functional ground is established via a grounding screw.

The connector for the grounding cable is on the front of the housing.

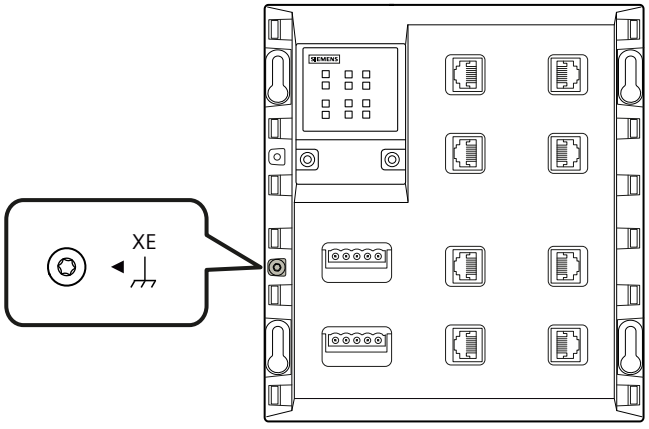
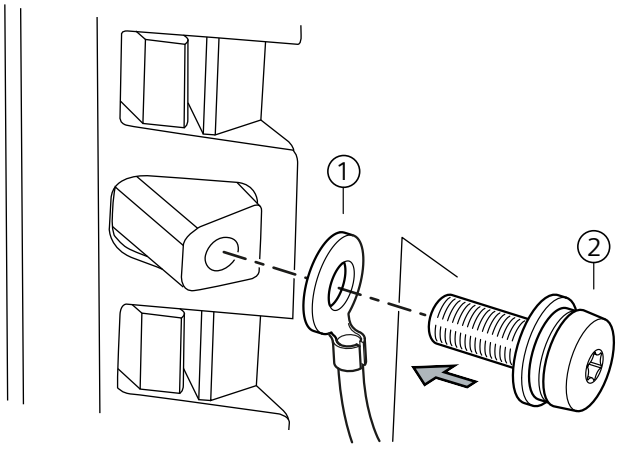


Figure 6-3 Position of the grounding screw

Connecting up functional ground



① Grounding terminal with cable
② Screw (M4 thread) with spring washer and washer

Follow the steps below to connect the functional ground:

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

Upkeep and maintenance

7

⚠ WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.

⚠ WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories (Page 21) and original spare parts (Page 22).
- Observe all relevant installation and safety instructions described in the manuals for the device or supplied with the accessories or spare parts.



⚠ CAUTION

Hot surfaces

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

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

NOTICE

Cleaning the housing

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

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

Do not use solvents.

7.1 Downloading new firmware using TFTP without WBM and CLI

Firmware

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

Pressing the "RESET" button

To load new firmware, you require the "RESET" button. When pressing the button, remember the information in the section "RESET button (Page 26)".

Procedure with Microsoft Windows

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

When pressing the button, observe the information in the section "RESET button (Page 26)".

Follow the steps below to load new firmware using TFTP:

1. Turn off the power to the device.
2. Press the SELECT/SET button and reconnect the device to the power supply with the button pressed.
3. Hold down the button until the red fault LED "F" starts to flash.
4. Release the button as long as the red error LED is still flashing..
   This time only lasts a few seconds.
   The bootloader of the device waits in this status for a new firmware file that you can download by TFTP.
5. Connect a PC to an Ethernet port of the device with an Ethernet cable.
6. Assign an IP address to the device using DHCP or SINEC PNI.
7. In a Windows command prompt, go to the directory where the file with the new firmware is located and use the following command:
   `tftp -i <IP address> put <firmware file>.`

Note

You can enable TFTP in Microsoft Windows as follows:

"Control Panel" > "Programs and Features" > "Turn Windows features on or off" > "TFTP Client".

Once the firmware has been transferred completely to the device and validated, the device restarts. This may take a few minutes.

7.2 Restoring the factory settings

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

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

With the "RESET" button

Restoring the factory settings during the startup phase

NOTICE
Reset despite disabled "RESET button" Using the "RESET" button, you can always reset the device parameters to the factory settings during the startup phase of the device. This also applies 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 with the configuration, it is only disabled on completion of the startup phase.

When pressing the button, observe the information in the section "RESET button (Page 26)".

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

1. Turn off the power to the device.
2. Loosen the screws of the cover.
3. Remove the cover.
4. Press the "RESET" button and reconnect the power supply to the device while holding down the button.
5. Hold down the button until the red error LED "F" stops flashing after approximately 20 seconds and is permanently lit.
6. Release the button and wait until the fault LED "F" goes off.
   The device starts automatically with the factory settings.
7. Close the cover (tightening torque 0.8 Nm), to ensure that the device is closed and water and dust proof.

Restoring the factory defaults during operation

You can reset the device to the factory defaults during operation, see section "RESET button (Page 26)".

With SINEC PNI

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

1. Select the device whose parameters you want to reset.
2. Click "Reset device".
   A dialog opens in which you can select one of the following options:
   - Reset to PROFINET default settings
     Resets the selected device to the respective default settings of the PROFINET IO profile. The settings that are reset depend on the functional scope of the device. This function is only available for devices that support the current PROFINET standard.

     Note

     Loss of the IP address

     When the settings are reset to the default settings of a PROFINET IO profile, the IP address is also lost. The device can then only be addressed via the serial interface, SINEC PNI or via DHCP.

   - Restore Factory Defaults
     Resets the selected device to factory settings.
3. Confirm the selection with "OK".

During configuration

You will find detailed information on resetting the device parameters using the WBM and CLI in the configuration manuals see also section "Introduction (Page 5)":

- SCALANCE XB-200/XP 200 Web Based Management, section "Restart"
- SCALANCE XB-200/XP-200 Command Line Interface, section "Reset and Defaults"

Technical specifications

8

8.1 Technical specifications of SCALANCE XP208G PP

Technical specifications		
Attachment to Industrial Ethernet		
	Quantity	8
	Connector	RJ45, push-pull
	Transmission speed	10 / 100 / 1000 Mbps
Electrical data		
Power supply	Rated voltage	24 V DC
	Voltage range	19.2 to 31.2 V DC safety extra low voltage
	Connector	Power Plug PRO, 5-pin
	Cable cross-section	≥ 0.25 mm^2 (24 AWG) ≥ 2.5 mm^2 (13 AWG) with loop-through of power supply
	Property	Not implemented redundantly
Current consumption	at 24 VDC	320 mA
Effective power loss	at 24 VDC	7.7 W
Fusing		1.5 A (non-replaceable fuse F)
Permitted ambient conditions		
Ambient temperature	During operation up to 2000 m above sea level	Horizontal installation position: -40 °C to +70 °C All other installation positions: -40 °C to +60 °C
	With operation between 2000 m and 3000 m above sea level	The maximum ambient temperature is reduced by 5 °C [1)]
	With operation between 3000 m and 4000 m above sea level	The maximum ambient temperature is reduced by 10 °C [1)]
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation at 25 ℃	≤ 95 % no condensation
Housing, dimensions and weight		
Design	compact	
Housing material	Aluminum	
Degree of protection	IP 65	
Dimensions (W x H x D)	184 x 200 x 63 mm (depth without protective caps)	
Weight	1050 g	
Installation options	Wall mounting	

Technical specifications	
Mean time between failure (MTBF)	
MTBF (EN/IEC 61709; 40 °C)	> 55 years

[1] The derating values depend on the maximum ambient temperatures during operation up to 2000 m.

8.2 Permitted cable lengths

The following cables are permitted in the specified lengths:

- **0 to 55 m:**
  IE TP torsion cable with IE FastConnect RJ45 Plug PRO (push-pull)
- **0 to 85 m:**
  IE FC TP marine/trailing/flexible/FRNC/festoon/food cable with IE FastConnect RJ45 Plug PRO (push-pull)
- **0 to 100 m:**
  IE FC TP standard cable with IE FastConnect RJ45 Plug PRO (push-pull)

8.3 Switching properties

The switching characteristics listed below apply to the devices named in the scope of validity.

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

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

Full wire speed switching		
1280	9615	96153
1518	8127	81274

Note

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

Dimension drawings

9

Note

Dimensions are specified in mm.

Front view of the SCALANCE XP208G

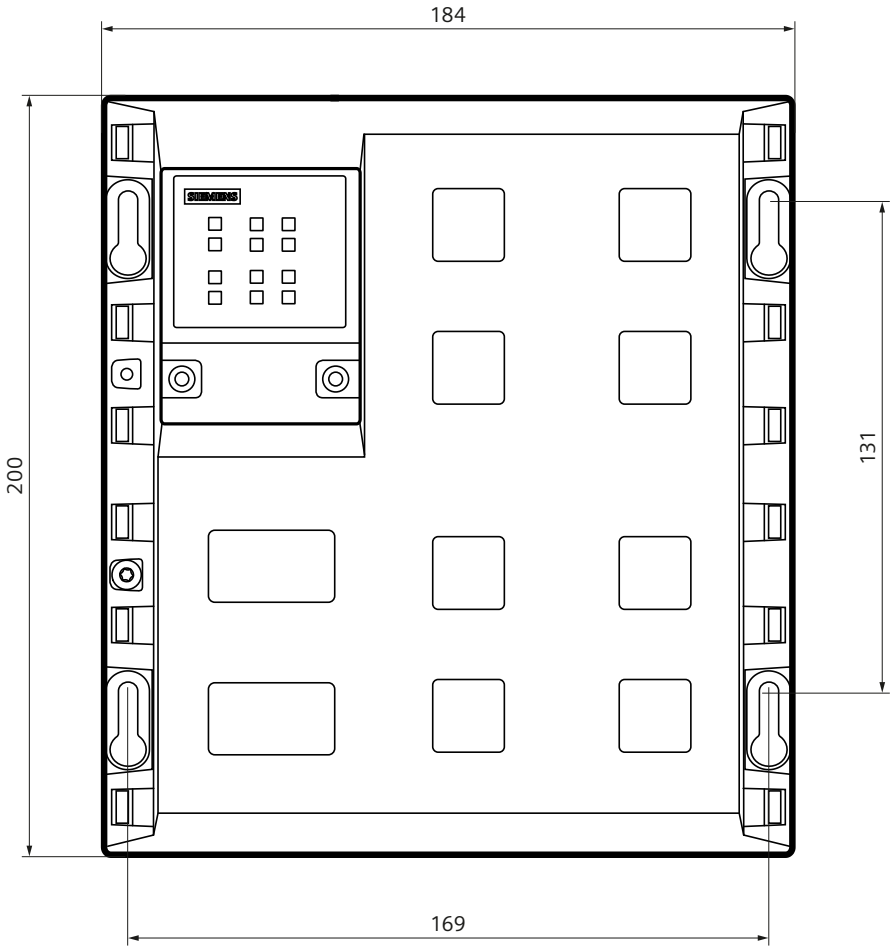


Figure 9-1 Width, height and dimensions for wall mounting

Side view SCALANCE XP-200G

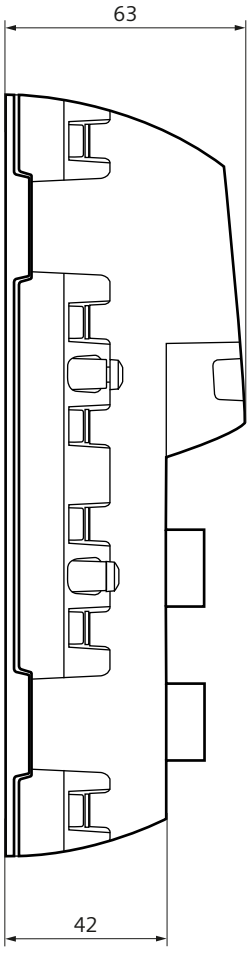


Figure 9-2 Depth

Approvals

A

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

Note

Issued approvals on the type plate of the device

The specified approvals apply only when the corresponding mark is printed on the product. You can check which of the following approvals have been granted for your product by the markings on the type plate.

Current approvals on the Internet

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

Notes for the manufacturers of machines

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

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

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

Machinery directive

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

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

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

EC declaration of conformity

CE

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

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

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

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

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

Siemens Aktiengesellschaft

Digital Industries
DE-76181 Karlsruhe
Germany

UK Declaration of Conformity

UK CA

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

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76181 Karlsruhe
Germany

Importer UK:

Siemens plc,
Manchester M20 2UR

You can find the current UK Declaration of Conformity for these products on the Internet pages under Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/15273/cert).

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

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

ATEX, IECEx, UKEX and CCC Ex certification

⚠ WARNING

Risk of explosion in hazardous areas

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

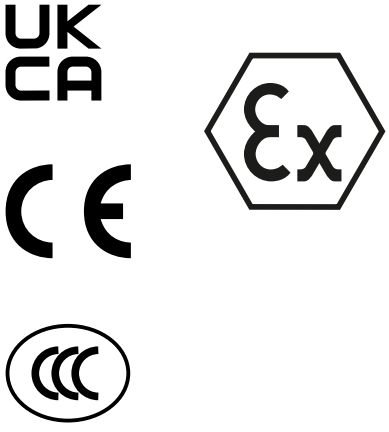
"SIMATIC NET Product Information Use of subassemblies/modules in a Zone 2 Hazardous Area".

You will find this document

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

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

The markings of the electrical devices are:



II 3 G Ex ec IIC T4 Gc
DEKRA 18ATEX0025 X
DEKRA 21UKEX0001 X
IECEx DEK 18.0017X
Importer UK:
Siemens plc,
Manchester
M20 2UR
(Ex ec IIC T4 Gc, not on the nameplate)

The products meet the requirements of the following standards:

- EN/IEC 60079-7, GB 3836.3
- 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 Information Technology Equipment

cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

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

Report no. E115352

cULus Approval Hazardous Location

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

Underwriters Laboratories Inc. complying with

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

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

Report no. E240480

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

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

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

MSIP 요구사항 - For Korea only

A급 기기(업무용 방송통신기자재)

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

Marking for the customs union

EAC (Eurasian Conformity)

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

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

Mechanical stability (in operation)

Device	IEC 60068-2-27 shock	IEC 60068-2-6 vibration
	15 g, 11 ms duration 6 shocks per axis	**10 - 58 Hz: 0.075 mm 85 - 150 Hz: 1 g 1 octave/min, 20 sweeps**
SCALANCE XP208G PP	●	●

Installation guidelines

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

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

WARNING

Personal injury and property damage can occur

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

Only use expansions that are approved for the system.

Note

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

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

Index

A

Accessories, 21
Ambient temperature, 53
Approvals, 59
Article number
    Power Plug PRO, 45
    RJ-45 data plug-in connector, 22
Article numbers, 19
Attachment to Industrial Ethernet, 53
Autonegotiation, 43

B

Button
    Cover, 21
    Function, 26
    RESET, 26

C

CE mark, 59
Command Line Interface (CLI), 29, 50
Components of the product, 20
Configuration, 27
Configuration manuals, 52
Connecting up
    Grounding, 46
C-PLUG
    Configuration, 28
    Cover, 21, 29
    Overview, 21
    Replacing, 29

D

Dimensions, 53

E

Electrical data, 53
Environmental conditions, 53
ESD directives, 8

F

Factory defaults, 26, 27, 50
Factory setting, 26, 50
Fault/error status, 23
Firmware, 23
Functional ground
    Connecting up, 46

G

Gigabit Ethernet
    Overview, 21
Glossary, 6
Grounding, 46
    Connecting up, 46
    Overview, 21
Grounding point, 21, 46

H

Housing, 53

I

Installation, 53

K

Keyhole hang-up mechanism
    Overview, 21

L

LED, 23
    Display, 23
    Overview, 21, 23

M

MDI / MDI-X autocrossover, 43
MTBF, 54

P

Permitted ambient conditions, 53
PLUG, 28
Power Plug PRO
    Article number, 45
Protective cap, 22
Protective caps, 20

R

Reset device, 26, 27, 50
Reset to Factory Defaults, 27, 50

S

Safety notices
    for installation, 33
    general, 9
    Use in hazardous areas, 9, 33, 39
    when connecting up, 39
SELECT/SET button, 50
Signaling contact, 23
SIMATIC NET glossary, 6
SIMATIC NET manual, 6
Spare parts, 22
Startup phase, 23, 27, 51
System manual, 6, 35, 64

W

Web Based Management (WBM), 29, 50
Weight, 53