SIEMENS

SIMATIC NET

Industrial Remote Communication Remote Networks SCALANCE M804PB

Operating Instructions

Preface

Safety notices 1

Security recommendations 2

Description of the device 3

Installation and removal 4

Connecting up 5

Maintenance and cleaning 6

Technical specifications 7

Dimension drawing 8

Approvals 9

10/2024
C79000-G8976-C496-06

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER

indicates that death or severe personal injury **will** result if proper precautions are not taken.

⚠ WARNING

indicates that death or severe personal injury **may** result if proper precautions are not taken.

⚠ CAUTION

indicates that minor personal injury can result if proper precautions are not taken.

NOTICE

indicates that property damage can result if proper precautions are not taken.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING

Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens Aktiengesellschaft. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

C79000-G8976-C496-06
Ⓟ 10/2024 Subject to change

Copyright © Siemens 2018 - 2024.
All rights reserved

Preface

Scope of validity of the operating instructions

These operating instructions are valid for SCALANCE M804PB.

Purpose of the operating instructions

Using the operating instructions, you will be able to install and connect the SCALANCE M804PB correctly. The configuration and the integration of the device in a network are not described in these instructions.

Naming of the devices

Classification	Description	Terms used
Product line	For all devices and variants of all product groups within the SCALANCE M-800 product line, the term **M-800** is used.	M-800
Device	For a device, only the device name is used.	M804PB

Article number

Product	Description	Article number
SCALANCE M804PB	IE router, 2x RJ45 ports, 1x PROFIBUS / MPI	6GK5804-0AP00-2AA2

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)

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

Identification Link

There are multiple scannable codes, including a QR code, on the product. The QR code is an Identification Link (ID-Link), a globally unique product identifier according to IEC 61406-1. You can recognize the ID-Link from the frame, which has a black corner at the bottom right.

Disconnect the device from the power and scan the QR code with a smartphone camera, a bar code scanner or a read app. Open the ID-Link. The Siemens web page corresponding to the product opens with the digital nameplate.

In the digital nameplate, you will find product data, manuals, declarations of conformity, certificates, and other helpful information about your product.

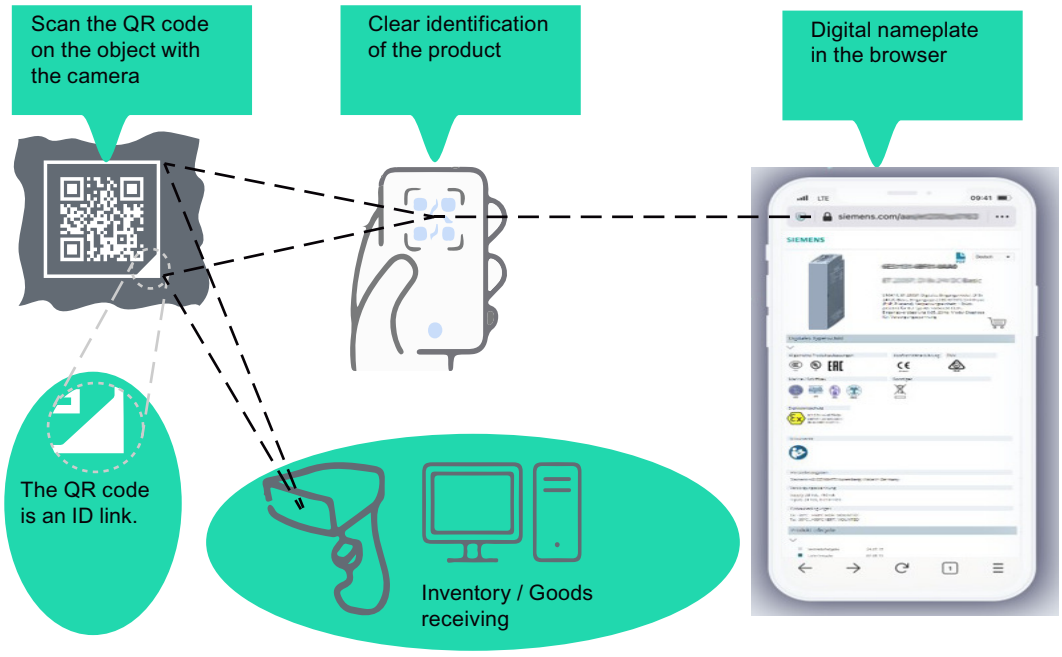


Figure 1 Application & functions of the Identification Link

Documentation on the Internet

You can find the current version of the document on the Internet at. (https://support.industry.siemens.com/cs/ww/en/ps/25380/man)

Enter the name or article number of the product in the search filter.

Documentation on configuration

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

- SCALANCE M-800 Web Based Management
- SCALANCE M-800 Command Line Interface

Note

Make sure that you read the explanations and instructions in the readme.htm file.

Further documentation

- System manual "Industrial Ethernet"
  The system manual contains 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.
  The "SIMATIC NET Industrial Ethernet" system manual can be found on the Internet pages of Siemens Industry Online Support under the following entry ID: 27069465 (https://support.industry.siemens.com/cs/ww/en/view/27069465)
- "Passive network components" system manual
  This system manual contains installation instructions for several of the most common components and guidelines for setting up networked automation plants in buildings.
  The "Passive network components" system manual can be found on the Internet pages of Siemens Industry Online Support under the following entry ID: 84922825 (https://support.industry.siemens.com/cs/ww/en/view/84922825)

SIMATIC NET manuals

You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:

- using the search function:
  Link to Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/)
  Enter the entry ID of the relevant manual as the search item.
- In the navigation panel on the left hand side in the area "Industrial Communication":
  Link to the area "Industrial Communication" (https://support.industry.siemens.com/cs/ww/en/ps/15982/man)
  Go to the required product group and make the following settings:
  tab "Entry list", Entry type "Manuals"

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/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

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://new.siemens.com/global/en/products/services/cert.html).

Firmware

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

The firmware is available on the Internet pages of the Siemens Industry Online Support: (https://support.industry.siemens.com/cs/ww/en/ps/15982/dl)

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.

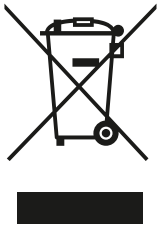
Decommissioning

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.

Device defective

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

Trademarks

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

SCALANCE, SINEMA, KEY-PLUG, C-PLUG

License conditions

Note

Open source software

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

You will find license conditions in the following documents on the supplied data medium:

- OSS_Scalance-M-800-S615-RM1224_86.pdf

SIMATIC NET glossary

The SIMATIC NET glossary describes terms that may be used in this document.

You will find the SIMATIC NET glossary in the Siemens Industry Online Support at the following address:

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

Table of contents

Preface **3**

1 Safety notices **11**

2 Security recommendations **13**

2.1 Passwords 13

3 Description of the device **23**

3.1 Product characteristics 23

3.2 Device view 24

3.3 Scope of delivery 24

3.4 Accessories 25

3.4.1 Installation 25

3.4.2 PLUG 26

3.5 Terminals 26

3.6 LED display 28

3.7 SET button 31

3.8 PLUG 32

4 Installation and removal **35**

4.1 Safety notices for installation 35

4.2 Securing the housing 38

4.3 Wall mounting 39

4.4 Installing on the DIN rail 40

4.5 Installing on the S7-300 standard rail 41

4.6 Installing on the S7-1500 standard rail 42

4.7 Mounting on a pedestal 43

5 Connecting up **45**

5.1 Safety when connecting up 45

5.2 Power supply 49

5.3 Grounding 50

5.4 Digital input/output 51

5.5 Ethernet 54

5.6 MPI/DP interface 55

5.7 Replacing the PLUG 56

6 Maintenance and cleaning 59

7 Technical specifications 61

8 Dimension drawing 65

9 Approvals 69

9.1 EC declaration of conformity 70
9.1.1 ATEX 71
9.1.2 EMC 71
9.1.3 RoHS 72

9.2 UK Declaration of Conformity 72
9.2.1 UK Declaration of Conformity for SCALANCE M 72
9.2.2 The Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016 73
9.2.3 The Electromagnetic Compatibility Regulations 2016 73
9.2.4 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 74

9.3 General approvals 74

Index 77

Safety notices

1

⚠ CAUTION

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

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".



⚠ WARNING

Hot surfaces

Electric devices have hot surfaces. Do not touch these surfaces. They could cause severe burns.

- Allow the device to cool down before starting any work on it.

⚠ WARNING

EXPLOSION HAZARD

Do not open the device when the supply voltage is turned on.

Security recommendations

2

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

Note

Note that GNSS signals can be obfuscated or blocked by malicious third-party devices.

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.

2.1 Passwords

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. Create a separate user account for each user that will receive access to the device.
- Define rules for the assignment of passwords.
- Use passwords with a high password strength. Avoid weak passwords, (e.g. Passwort1, 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 user account details in a safe location to have them available if they are lost. You can use password managers or encrypted files/drives for this purpose.
- 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. Use a RADIUS connection with changing passwords, expiry time, etc.
- Watch out for link layer protocols that do not offer their own authentication between endpoints, such as ARP. 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.
- Use TOTP-based two-factor authentication of the user. You can find more information on this under "Security > Passwords > Two-Factor Authentication".

Certificates and keys

- There is a pre-installed Web server certificate 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 & 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:
  - Reset the device to the factory settings. Replace the SSH and SSL keys with disposable keys prior to shipping to Siemens.
  - 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, reset it to factory settings and replace the current certificates and keys with temporary throwaway certificates and keys that 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 3)".
- 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 or ProductCERT Security Advisories website.
  For updates on Siemens product security advisories, subscribe to the RSS feed on the ProductCERT Security Advisories website or follow @ProductCert on Twitter.
- 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:
  - Telnet
  - HTTP
  - Broadcast pings
  - Non authenticated and unencrypted interfaces
  - ICMP (redirect)
  - LLDP
  - DHCP Options 66/67
  - SNTP
  - NTP
  - TFTP
  - TIA Portal Cloud Connector (not available with SCALANCE MUx85x)
  - 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
  - Telnet → SSH
  - NTP → Secure NTP
  - TFTP → SFTP
  - TIA Portal Cloud Connector using a secure connection (not available with SCALANCE MUx85x). Use the "TIA Portal Cloud Connector" integrated in the product over a VPN solution (e.g. SINEMA RC).
    Configure the firewall settings of the SCALANCE M800/S615 (e.g. predefined IPv4 rules "Cloud Connector" to prevent unauthorized access of network devices to the "TIA Portal Cloud Connector Server").
  - DNS > DNSSec
- Using a firewall, restrict the services and protocols available to the outside to a minimum.
- Select a trusted DNS provider.
  Enable the DNSSec option on the WBM page "System > DNS client" or with the CLI command `dnssec`.

- SCALANCE MUM85x, SCALANCE M87x and RUGGEDCOM RM1224:
  For command SMS, use the identifier to secure your SMS messages. You can set a configurable value for a SCALANCE M device that, in addition to the phone number, must match the received identifier of the SMS. You configure the identifier on the WBM page "System > SMS > SMS Command" or with the CLI commands `sms-cmd idx identifier` and `sms-cmd sender`.
- The TCP Diagnostics Stream is considered non-secure without encryption. As of V8.1, encryption that enables secure use in productive operation is supported. Enable encryption of the function to use it securely.
- Only use the TCP Event function in secured networks or VPN. The firewall must be activated beforehand.
- With authentication on the RADIUS server and RADIUS client, use the Message Authenticator attribute to check packets.

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**
  The services 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).
- **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/ Port number	Default port status		Configurable		Authentication	Encryption [2]
		Local access	External access [1]	Port	Service		
DHCPv4 Client	UDP/68	Closed [3]	Closed	--	✓	--	--
DHCPv6 Client	TCP/546 UDP/546	Open	Open	--	--	--	--
DHCPv4-Server	UDP/67	Closed	Closed [4]	--	✓	--	--
DNS Client	TCP/53 UDP/53	Outgoing only	Outgoing only	--	✓	--	--

Service	Protocol/ Port number	Default port status		Configurable		Authentication	Encryption [2]
		Local access	External access [1]	Port	Service		
DNS Server	TCP/53 UDP/53 UDP/49000 ... UDP/65535	Open [5]	Closed	--	✓	--	--
DynDNS	TCP/80 UDP/80 TCP/443 UDP/443	Outgoing only	Outgoing only	--	✓	✓	--
HTTP	TCP/80	Open	Closed	✓	✓	✓	--
HTTP Proxy	TCP/3128 TCP/8080	Outgoing only	Outgoing only	✓	✓	Optional	--
HTTPS WBM Server/Client	TCP/443	Open	Closed	✓	✓	✓	✓
IPsec/IKE	UDP/500 UDP/4500	Closed	Closed	--	✓	✓	✓
iperf3 [8]	TCP/5201	Closed	Closed	✓	✓	--	--
NTP Client	UDP/123	Outgoing only	Outgoing only	✓	✓	--	--
NTP Client (secure)	UDP/123	Outgoing only	Outgoing only	✓	✓	✓	--
NTP Server	UDP/123	Closed	Closed	✓	✓	--	--
NTP Server (secure)	UDP/123	Closed	Closed	✓	✓	✓	--
OpenVPN [10]	UDP/1194 TCP/1194	Outgoing only	Outgoing only	✓	✓	✓	✓
Packet Capture [11]	TCP/2002	Disabled	Disabled	✓	✓	--	--
Ping	ICMP	Open	Closed	--	✓	--	--
RADIUS Client	UDP/1812	Closed	Closed	✓	✓	✓	Optional
	UDP/1813						--
SFTP Server	TCP/22	Outgoing only	Outgoing only	✓	✓	✓	✓
Siemens Remote Service (cRSP/SRS) [10]	TCP/443	Outgoing only	Outgoing only	--	✓	Optional	✓
SINEMA RC	HTTPS/443 and TCP/UDP depending on the server configuration	Outgoing only	Outgoing only	✓	✓	✓	✓
SMS Relay [7]	TCP/26864	Closed	Closed	✓	✓	--	--
SMTP Client	TCP/25	Outgoing only	Outgoing only	✓	✓	--	--
SMTP (secure)	TCP/465 TCP/587	Outgoing only	Outgoing only	✓	✓	Optional	✓
SNMPv1/v2c [12]	UDP/161	Open	Closed	✓	✓	--	--
SNMPv3 Server	UDP/161	Open	Closed	✓	✓	Optional	Optional
SNMP Trap	UDP/161	Open	Closed	✓	✓	Optional	Optional

Service	Protocol/ Port number	Default port status		Configurable		Authentica-tion	Encryption [2]
		Local access	External access [1]	Port	Service		
SNTP Client	UDP/123	Closed	Closed	✓	✓	--	--
SSH CLI	TCP/22	Open	Closed	✓	✓	✓	✓
Syslog Client	UDP/514	Outgoing only	Outgoing only	✓	✓	--	--
Syslog Client TLS	TCP/6514	Outgoing only	Outgoing only	✓	✓	--	✓
Telnet	TCP/23	Closed	Closed	✓	✓	✓	--
TFTP	UDP/69	Outgoing only	Outgoing only	✓	✓	--	--
TIA Portal Cloud Connector [6]	TCP/9023	Closed	Closed	✓	✓	--	--
TCP Diagnostic Stream [11]	TCP/5510 TCP/5511	Closed	Closed	✓	✓	--	✓
TCP Event	TCP/26864	Closed	Closed	✓	✓	--	--
VXLAN [9]	UDP/4789	Closed	Closed	✓	✓	--	--

[1] With SCALANCE M826 and M804PB, only access via vlan1 is possible in the delivery state (factory setting).

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

[3] Only open with SCALANCE M826

[4] Only open with SCALANCE S615

[5] Only closed with SCALANCE S615

[6] Not available with SCALANCE MUx85x

[7] Only available with SCALANCE M87x, MUM85x and RUGGEDCOM RM1224

[8] Only available with SCALANCE MUM85x

[9] Only available with SCALANCE M87x, MUx85x, S615 and RUGGEDCOM RM1224

[10] Not available with SCALANCE MUB852

[11] Only available with SCALANCE MUx85x

[12] Read Only

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	Configurable
DCP	Open (when configured)	✓
LLDP	Open (when configured)	✓
SIMATIC NET TIME	Open (when configured)	✓
VLAN	Open (when configured)	✓
VXLAN [1)]	Open (when configured)	✓

[1)] Only available with SCALANCE M87x, MUx85x, S615 and RUGGEDCOM RM1224

Description of the device

3

3.1 Product characteristics

Interfaces

Functionality	SCALANCE M804PB
MPI/DP interface	RS 485 (up to max. 12 Mbps)
Ethernet interface	2 x RJ45 10 / 100 Mbps
Digital input/output	1/1

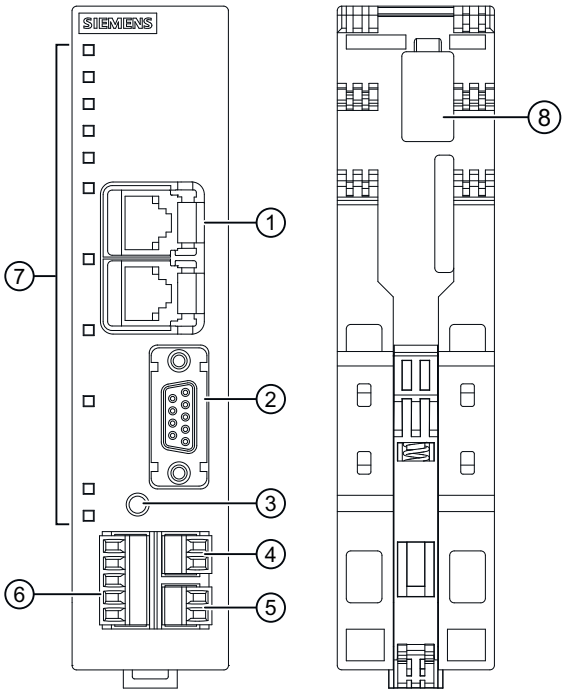
Using the device in a PROFINET environment

Note

When using the device in a PROFINET environment, follow the configuration instructions in the configuration manuals:

- Web Based Management: Description > Requirements for operation > Use in a PROFINET environment
- Command Line Interface: General > Use in a PROFINET environment

3.2 Device view



On the device front:

① Ethernet connectors (P1, P2)
② MPI/DP interface
③ SET button
④ Digital input (DI)
⑤ Digital output (DO)
⑥ Power supply connection
⑦ LED display

On the device rear:

⑧ PLUG slot

3.3 Scope of delivery

The following components are supplied with the product:

- One SCALANCE M device
- A 5-pin terminal block for the power supply
- A 2-pin terminal block for the digital output
- A 2-pin terminal block for the digital input
- A product DVD

Please check that the consignment you have received is complete. If the consignment is incomplete, contact your supplier or your local Siemens office.

Note

Not included with the product

The following components do not ship with the product:

- PLUG
  You will find more detailed information in "PLUG (Page 26)".

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

Use only undamaged parts.

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

3.4 Accessories

Technical data subject to change.

You will find further information on the range of accessories in the Industry Mall (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10022025)

Use the TIA Selection Tool (https://mall.industry.siemens.com/tst/) for configuring the device.

3.4.1 Installation

Type	Properties	Article number
Desktop pedestal	SCALANCE M-800 desktop pedestal for table mounting for SCALANCE M812 / M816 / M874-X / M876-X / S615 / M804PB	6GK5898-8MD00

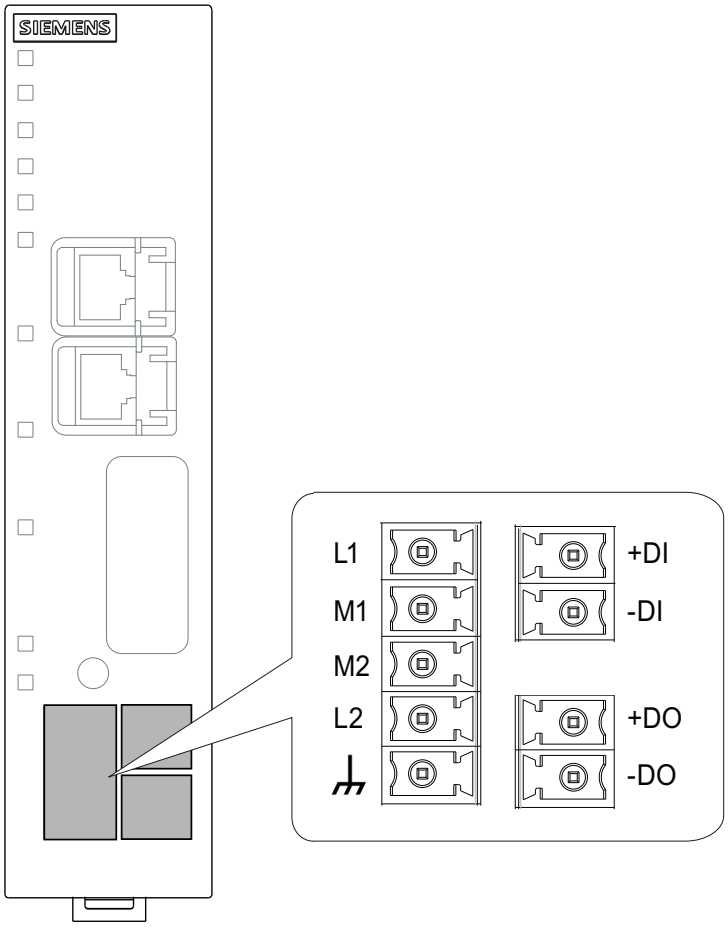
3.4.2 PLUG

Type	Properties	Article number
C-PLUG	Removable data storage medium (256 MB) for the configuration data	6GK1900-0AB10
KEY-PLUG SINEMA RC	Removable data storage medium (256 MB) to enable the connection functionality to SINEMA Remote Connect and for storing configuration data	6GK5908-0PB00

3.5 Terminals

Position

The device has a 5-pin plug-in terminal block for the power supply and two 2-pin plug-in terminal blocks for the digital input and output.



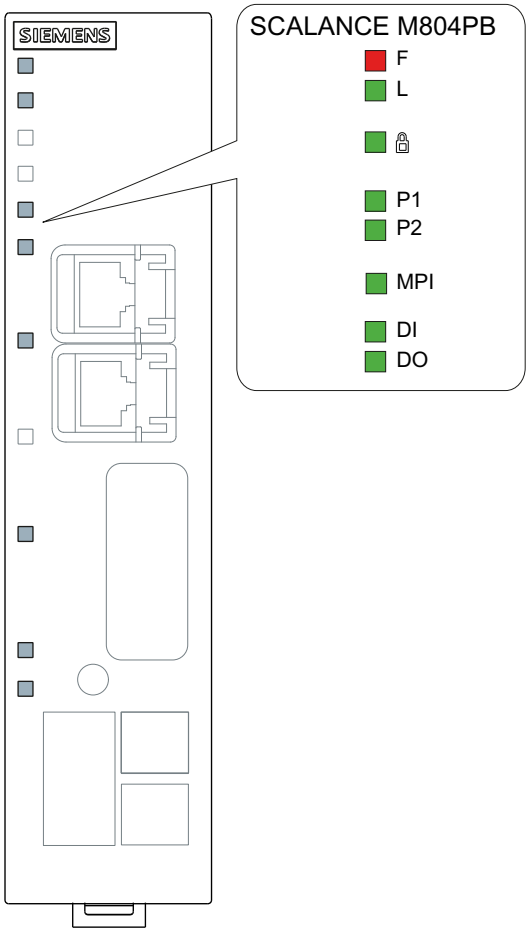
Connectors and terminal markings

L1, M1, L2, M2	Input for the power supply	Terminal block with five terminal connectors
	Functional grounding	
+DI, -DI	Digital input	Terminal block with two terminal connectors
+DO, -DO	Digital output	Terminal block with two terminal connectors

Terminals and wiring

Connectors	+DI, -DI /+D0, -DO	L1, M1, L2, M2
AWG	28 AWG	16 AWG
Wire end ferrule without plastic collar to DIN 46228/1	0.2 mm^2	1.5 mm^2
Wire end ferrule with plastic collar to DIN 46228/4	0.2 mm^2	1.5 mm^2
Stripped length	7 mm	7 mm

3.6 LED display



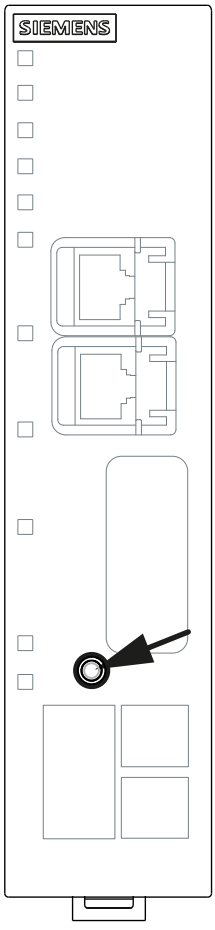
LED	Status	Meaning
F	OFF 	No fault/error.
	ON 	The device is starting up or an error has occurred. For example, the inserted PLUG has an invalid or incompatible configuration.
	Flashing 	The bootloader waits in this state for a new firmware file that you can download using TFTP.
	Flashing  at the interval: 1 s on/ 1 s off	The device is starting up for the first time or has been reset to factory settings. The password of the default user "admin" has not yet been changed.
	Flashing  at the interval: 2000 ms on / 200 ms off	Firmware on PLUG The device is performing a firmware update or downgrade.
L	OFF 	The device is turned off, no operating voltage.
	ON 	The device is turned on, operating voltage is present.
🔒	OFF 	No VPN connection is established.
	ON 	All configured VPN connections are established.
	Flashing 	Only some of the configured VPN connections are established.
P1/P2	OFF 	There is no Ethernet connection to the local computer or LAN.
	ON 	The Ethernet connection to the local computer or LAN has been established.
	ON 	The device is receiving / sending data.

LED	Status	Meaning
MPI	OFF ☐	There is no MPI/PROFIBUS connection.
	ON ■	The MPI/PROFIBUS connection has been established.
DI	OFF ☐	The digital input is inactive.
	ON ■	The digital input is active.
DO	OFF ☐	The digital output is inactive.
	ON ■	The digital output is active.

3.7 SET button

Position

The SET button is on the front of the device beside the LED display.



Function

The SET button has the following functions:

- **Restarting the device**
  To restart the device, press the SET button briefly.

  Note

  If you make changes to the configuration and restart immediately afterwards with the SET button, the changes may be lost. If you restart the device using the WBM (menu command "System > Restart") or using the CLI (command "restart" in the Privileged EXEC Modus), the configuration changes are always retained.

- **Loading a firmware file via TFTP**
  If the normal procedure with the "Load & Save" menu of Web Based Management is unsuccessful, the SET button can be used to load new firmware. This situation can occur if there is a power outage during the normal firmware update.
  - Hold down the button until the red fault LED (F) starts to flash after approximately 3 seconds.
  - Now release the button. The bootloader waits in this state for a new firmware file that you can download using TFTP.

  You will find more information in the section "Service and Maintenance" in the Web Based Management Configuration Manual.
- **Resetting the device to factory settings**
  If you reset, all the settings you have made will be overwritten by factory defaults. If a PLUG is inserted in the device, the PLUG is also reset to default settings.
  - Hold down the button until the red fault LED (F) stops flashing after approximately 10 seconds and is permanently lit.
  - Now release the button and wait until the fault LED (F) goes off again. The device then starts automatically with the factory settings and can be reached via the IP address 192.168.1.1.

  You will find more information in the section "Service and Maintenance" in the Web Based Management Configuration Manual.

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

3.8 PLUG

The PLUG is a removable medium and is used to transfer the configuration of the old device to the new device when a device is replaced.

The following PLUG types are available:

- C-PLUG: The removable data storage medium only saves the configuration data of the device.
- KEY-PLUG: In addition to the configuration data, the removable data storage medium contains a license with which specific functions can be enabled, e.g. SINEMA RC.
- CLP (Configuration License PLUG)
  The SCALANCE CLP is a removable data storage medium for the storage and securing of configuration data that can be used in all SCALANCE devices with CLP slot, e.g. SCALANCE MUM85x. The SCALANCE CLP is used to transfer the configuration of the old device to the new device when a device is replaced. The CLP is a successor to the previously described PLUGs. The CLP is also referred to as PLUG in the description. The PLUG is available in the following variants:
  - PLUG Configuration
  - PLUG License

Position

The PLUG slot is located on the back of the device, see the Device views (Page 24) section in the Operating Instructions of the device.

Function

Devices with a PLUG slot support the following operating modes:

- **Without PLUG**
  The device saves the configuration data in the internal memory. This mode is active when no PLUG is inserted.
- **With PLUG**
  In the startup phase:
  - If an **empty** PLUG (as supplied) is inserted in the device, the device automatically backs up the configuration data on the PLUG during startup. After that, it behaves like a PLUG with data.
  - When a PLUG **with data** is plugged into a device, the device automatically adopts the configuration of the PLUG during the startup phase. The prerequisite for this is that the configuration data was written by a compatible device type.
    One exception to this can be the IP configuration if it is set using DHCP and the DHCP server has not been reconfigured accordingly. Reconfiguration is necessary if you use functions based on MAC addresses.
  - If the PLUG contains a license, additional functions are also enabled.

    Note

    If the device was configured at some time with a KEY-PLUG or PLUG license, the device can no longer be used without this PLUG. To be able to use the device again, reset the device to the factory settings.

  During operation:
  - During operation, changes to the configuration are saved on the PLUG and in the internal memory.
  - The configuration data of the device is stored in a secured memory area of the PLUG. This secured memory area can only be accessed via the authentication of the Siemens device.
  - The device checks whether or not a PLUG is inserted at one second intervals. If the device detects that the PLUG has been removed, it restarts automatically.

NOTICE
Operating risk - Danger of data loss Only pull and plug the PLUG when the device is de-energized.

  - The device signals deviations from normal operation of the PLUG (e.g., incompatible data, incorrect operation or malfunctions) via the existing diagnostic mechanisms (e.g., LEDs or user interfaces). The user then has the choice of either removing the PLUG again or selecting the option to reformat the PLUG.

The procedure for pulling and plugging the PLUG can be found in the section "Replacing the PLUG (Page 56)" in the operating instructions for the device.

Installation and removal

4

4.1 Safety notices for installation

Safety notices

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

Note

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

⚠ WARNING

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

NOTICE

Improper mounting

Improper mounting may damage the device or impair its operation.

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

⚠ WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

WARNING

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

WARNING

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

WARNING

The device is intended for indoor use only.

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

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

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

WARNING

The device shall only be used in an area with pollution degree 1 or 2 (according to EN/IEC 60664-1, GB/T 16935.1).

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

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

WARNING

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

Safety notices when using according to FM

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

WARNING

EXPLOSION HAZARD

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 installation wiring connections with admitted maximum operating temperature of at least 10 °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.

WARNING

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

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

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

⚠ WARNING

Open equipment

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

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

4.2 Securing the housing

Types of installation

For the device, you have the following options:

- Wall mounting (no ceiling mounting)
- Installation on a DIN rail
- Installation on the S7-300 standard rail
- Installation on the S7-1500 standard rail
- Mounting on a pedestal

Strain relief for the cables

Regardless of the type of installation, make sure that there is suitable strain relief for the connecting cable.

Shielding of cables

If cables are installed permanently, it is advisable to remove the insulation of the shielded cable and to establish contact on the shield/PE conductor bar.

Permitted mounting position

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

You can find information about the ambient temperature under Permitted ambient conditions. (Page 61)

Keep to the minimum clearances to other components or to walls of a housing so that the convection ventilation of the device is not blocked.

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

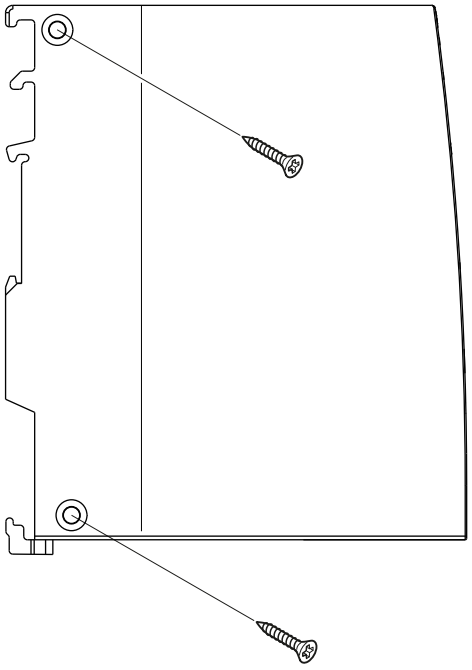
4.3 Wall mounting

Note

The wall mounting must be capable of supporting four times the weight of the device, but at least 50 N. For information on the weight, refer to the section "Technical specifications (Page 61)".

Installation

1. Prepare the drill holes for wall mounting. For the precise dimensions, refer to the section "Dimension drawing (Page 65)".
2. Secure the device to the wall with two screws. When mounting on a wall, use mounting fittings suitable for the type of wall.

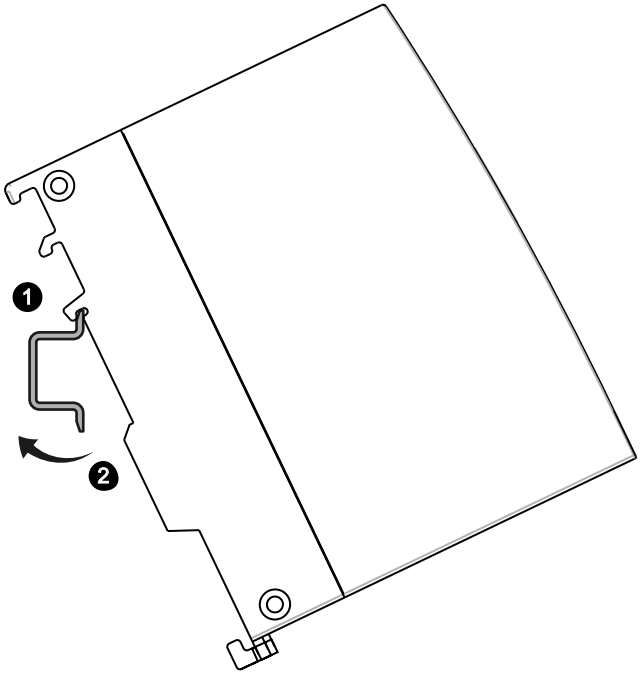


3. Connect the power supply, refer to the section "Power supply (Page 49)".
4. Fit the connectors for the digital input and digital output, refer to the section "Digital input/ output (Page 51)".
5. Connect the device to the local network, refer to the section "Ethernet (Page 54)".
6. Connect the device to the automation system, refer to the section "MPI/DP interface (Page 55)".
7. Connect the terminal with as short a cable as possible ≤ 150 mm and a large cross-sectional area of 1.5 mm^2 to the functional ground of the system, see section "Terminals (Page 26)" and section "Grounding (Page 50)".

4.4 Installing on the DIN rail

Installation

1. Place the third housing guide of the device on the top edge of the DIN rail ①.



2. Press the device down against the DIN rail until the spring catch locks in place ②.
3. Connect the power supply, refer to the section "Power supply (Page 49)".
4. Fit the connectors for the digital input and digital output, refer to the section "Digital input/ output (Page 51)".
5. Connect the device to the local network, refer to the section "Ethernet (Page 54)".
6. Connect the device to the automation system, refer to the section "MPI/DP interface (Page 55)".
7. Connect the terminal with as short a cable as possible ≤ 150 mm and a large cross-sectional area of 1.5 mm^2 to the functional ground of the system, see section "Terminals (Page 26)" and section "Grounding (Page 50)".
8. Also connect the DIN rails of a system with functional ground.

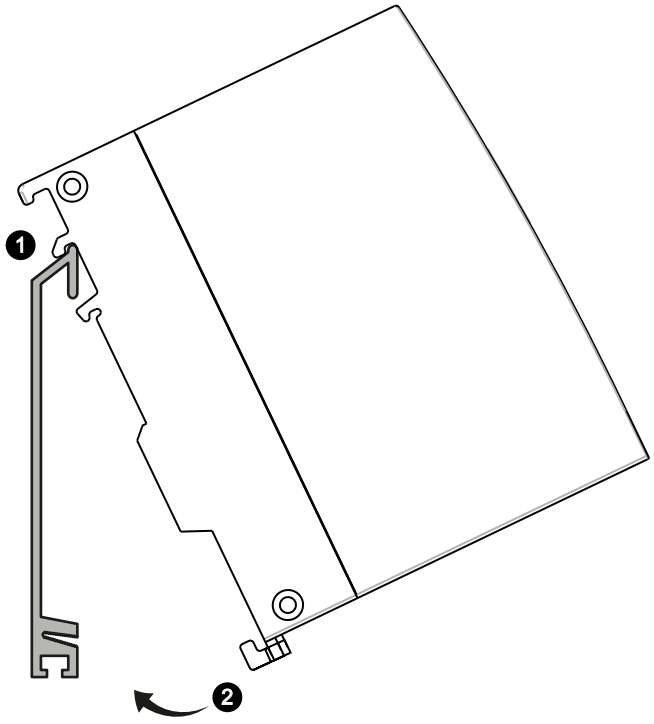
Dismantling

1. Disconnect all connected cables.
2. Using a screwdriver, pull down the catch on the rear of the device.
3. Pull lower part of the device away from the DIN rail.

4.5 Installing on the S7-300 standard rail

Installation

1. Place the second housing guide of the device on the top edge of the standard rail ①.



2. Press the device down against the standard rail until the spring catch locks in place ②.
3. Connect the power supply, refer to the section "Power supply (Page 49)".
4. Fit the connectors for the digital input and digital output, refer to the section "Digital input/ output (Page 51)".
5. Connect the device to the local network, refer to the section "Ethernet (Page 54)".
6. Connect the device to the automation system, refer to the section "MPI/DP interface (Page 55)".
7. Connect the terminal with as short a cable as possible ≤ 150 mm and a large cross-sectional area of 1.5 mm^2 to the functional ground of the system, see section "Terminals (Page 26)" and section "Grounding (Page 50)".

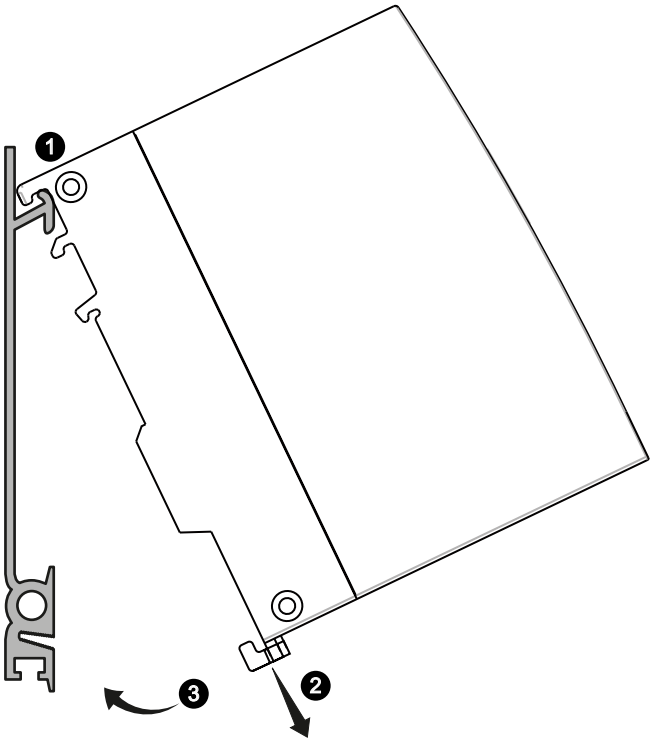
Dismantling

1. Disconnect all connected cables.
2. Using a screwdriver, pull down the catch on the rear of the device.
3. Remove the device from the standard rail.

4.6 Installing on the S7-1500 standard rail

Installation

1. Place the first housing guide of the device on the top edge of the standard rail ①.



2. Using a screwdriver, pull down the catch ② on the rear of the device.
3. Swing the device down while pulling down the catch ③. After it is released, the spring catch locks in place.
4. Connect the power supply, refer to the section "Power supply (Page 49)".
5. Fit the connectors for the digital input and digital output, refer to the section "Digital input/ output (Page 51)".
6. Connect the device to the local network, refer to the section "Ethernet (Page 54)".
7. Connect the device to the automation system, refer to the section "MPI/DP interface (Page 55)".
8. Connect the terminal with as short a cable as possible ≤ 150 mm and a large cross-sectional area of 1.5 mm^2 to the functional ground of the system, see section "Terminals (Page 26)" and section "Grounding (Page 50)".

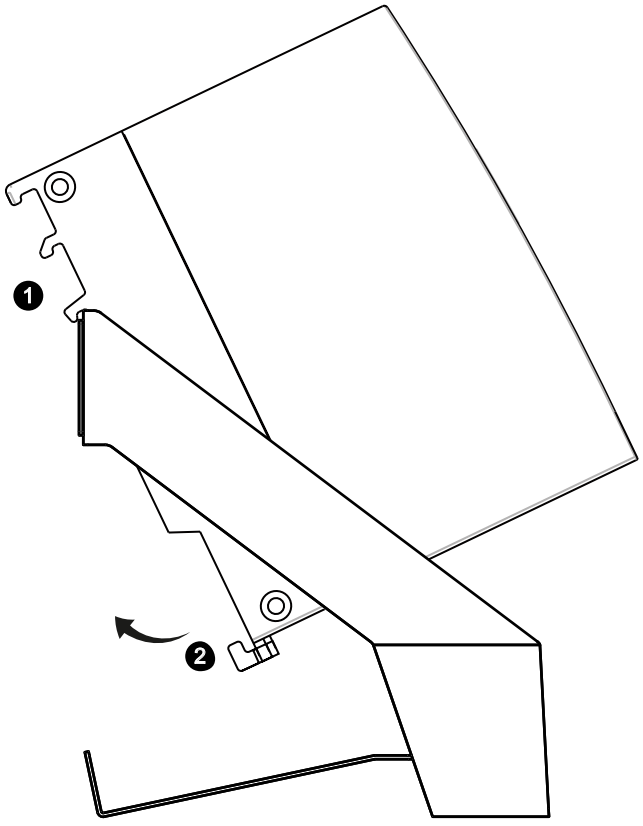
Dismantling

1. Disconnect all connected cables.
2. Using a screwdriver, pull down the catch on the rear of the device.
3. Remove the device from the standard rail.

4.7 Mounting on a pedestal

Installation

1. Place the third housing guide of the device on the top edge of the pedestal ①.



2. Press the device down against the pedestal until the spring catch locks in place ②.
3. Connect the power supply, refer to the section "Power supply (Page 49)".
4. Fit the connectors for the digital input and digital output, refer to the section "Digital input/ output (Page 51)".
5. Connect the device to the local network, refer to the section "Ethernet (Page 54)".
6. Connect the device to the automation system, refer to the section "MPI/DP interface (Page 55)".
7. Connect the terminal with as short a cable as possible ≤ 150 mm and a large cross-sectional area ≥ 1.5 mm² to the functional ground of the system, see section "Grounding (Page 50) " and section “Terminals (Page 26)”.

Dismantling

1. Disconnect all connected cables.
2. Using a screwdriver, pull down the catch on the rear of the device.
3. Remove the device from the pedestal.

Connecting up

5

5.1 Safety when connecting up

Safety notices

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

Note

Strain relief for the Ethernet cables

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

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

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

⚠ WARNING

Power supply

The device is designed for operation with Safety Extra-Low Voltage (SELV) that can be connected directly by 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 62368-1 / EN 62368-1 / VDE 62368-1 can 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 device is connected to a redundant power supply (two separate power supplies), both must meet these requirements.

⚠ WARNING

Insulation of external power supplies

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

Note

Protective ground

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

Note

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

⚠ WARNING

EXPLOSION HAZARD

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

⚠ WARNING

EXPLOSION HAZARD

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

⚠ WARNING

Unsuitable cables or connectors

Risk of explosion in hazardous areas

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

⚠ WARNING

Lack of equipotential bonding

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

- Ensure that equipotential bonding is available for the device.

⚠ WARNING

Unprotected cable ends

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

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

⚠ WARNING

Improper installation of shielded cables

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

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

⚠ WARNING

Insufficient isolation of intrinsically safe and non-intrinsically safe circuits

Risk of explosion in hazardous areas

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

⚠ WARNING

EXPLOSION HAZARD

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

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 surges of more than 40% of the rated voltage. Under no circumstances may transient surges exceed 119 V. This is the case if you only operate devices with SELV (safety extra low voltage).

WARNING

Suitable cables at high ambient temperatures in hazardous area

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

General notes on use in hazardous areas according to UL-HazLoc

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

WARNING

WARNING - EXPLOSION HAZARD -

DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS AREA IS KNOWN TO BE NON-HAZARDOUS.

WARNING

Restricted area of application

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

WARNING

Restricted area of application

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

Further notes

WARNING

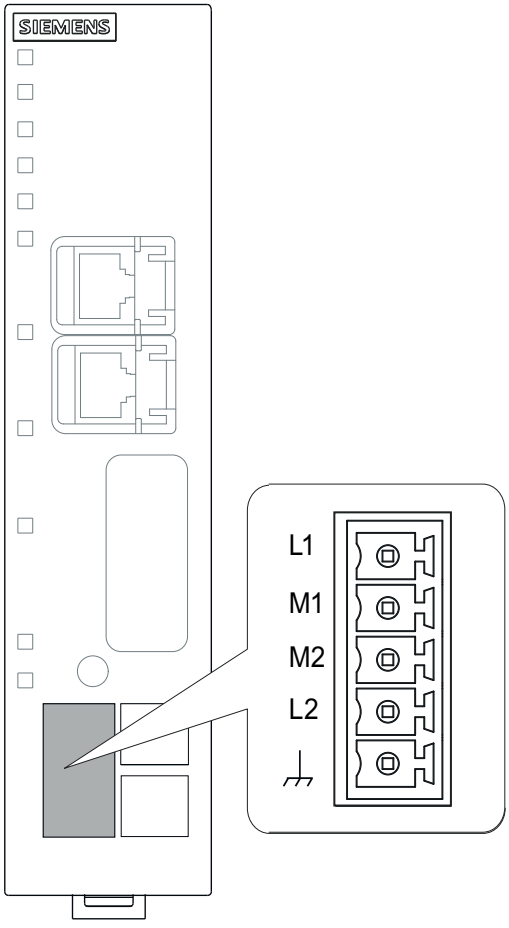
LAN connection (Local Area Network)

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

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

5.2 Power supply

The power supply is connected using a 5-pin terminal block. The power supply is non-floating.



PIN	Signal	Description
1	L1+	24 VDC
2	M1	Ground

PIN	Signal	Description
3	M2	Ground
4	L2+	24 VDC
5	⏚	Functional ground, refer to the section "Grounding (Page 50)"

You can find information on wiring in the section "Terminals (Page 26)".

External power supply

Note

Permitted external power supplies

The power supply unit to supply the SCALANCE M804PB must comply with the requirements for a limited power source according to IEC/EN 60950-1, section 2.5.

The external power supply for the SCALANCE M804PB must meet the requirements for NEC class 2 circuits as specified in the National Electrical Code ® (ANSI/NFPA 70).

Refer to the section Connecting up (Page 45) and the installation instructions and instructions for use of the manufacturer of the power supply, the battery or the accumulator.

Note

The requirements of EN61000-4-5, "Surge Immunity Test" on power supply lines with 24 VDC are met only when a Blitzductor is used:

24 VDC: BVT AVD 24 type no. 918 422

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

Note

External power supply for operation in China

The device may only be used with an external power supply that has a CCC approval.

5.3 Grounding

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

It is crucial for the correct operation of ground that the connection to the reference potential surface always has low impedance. Such a connection of the functional ground of the device does not go first through the cable channel and then to the mounting plate or DIN rail terminal, but goes directly to the mounting plate or DIN rail terminal.

The device has a terminal for grounding, refer to section "Terminals (Page 26)" or section "Power supply (Page 49)".

The terminal is identified by the following symbol for the grounding.



1. Connect the terminal of the device with as short a cable as possible ≤ 150 mm and a large cross-sectional area ≥ 2.5 mm² to the functional ground of the system. In many cases, the entire metallic construction of the system serves as ground.
2. Also connect the standard rails of a system with ground.

Protective earth/functional ground

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

Apart from the protective earth, there is functional 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.

In terms of the large-area and low impedance implementation, a functional ground set up for this purpose generally also meets the requirements of protective earth. On the other hand, protective earth does not always meet the requirements of functional ground. In general while the connection for protective earth is always low resistance, it is not necessarily low impedance.

The resistance of a connection for protective earth must always be as small as possible to divert fault currents safely to ground. The length of a protective earth cable can therefore be several meters (m) long, without seriously impairing this effect. For a functional ground for diverting HF disturbances, this cable does however have impedance and is therefore not suitable.

5.4 Digital input/output

The digital input and output are connected using a 2-pin plug-in terminal block in each case. Two terminal blocks ship with the device.

The digital output (relay contact) is a floating switch with which error/fault states can be signaled by breaking the contact.

⚠ CAUTION

Damage due to voltage being too high or too low

The voltage at the digital input/output must not exceed 30 VDC and not fall below -30 VDC, otherwise the digital input/output will be destroyed.

Note

Interference pulse

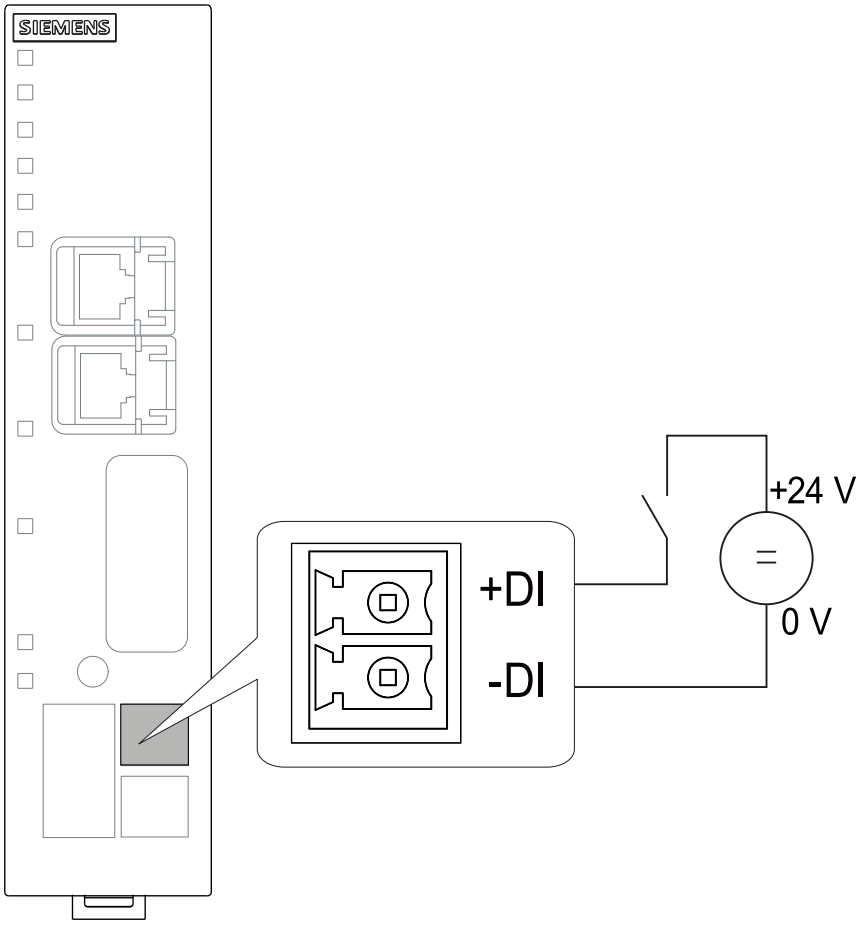
To avoid evaluating an interference pulse, the pulse for the signal 1 (TRUE / HIGH) must be at least 200 ms.

Rules for wiring

- To wire the digital input/output, use a copper cable of category AWG18-16 or a cable with a cross-section of 0.75 to 1.5 mm^2.
- Always wire the digital input/output in pairs.
- The maximum permitted cable length is 30 m.

Digital input

The 2-pin terminal block has the following assignment:



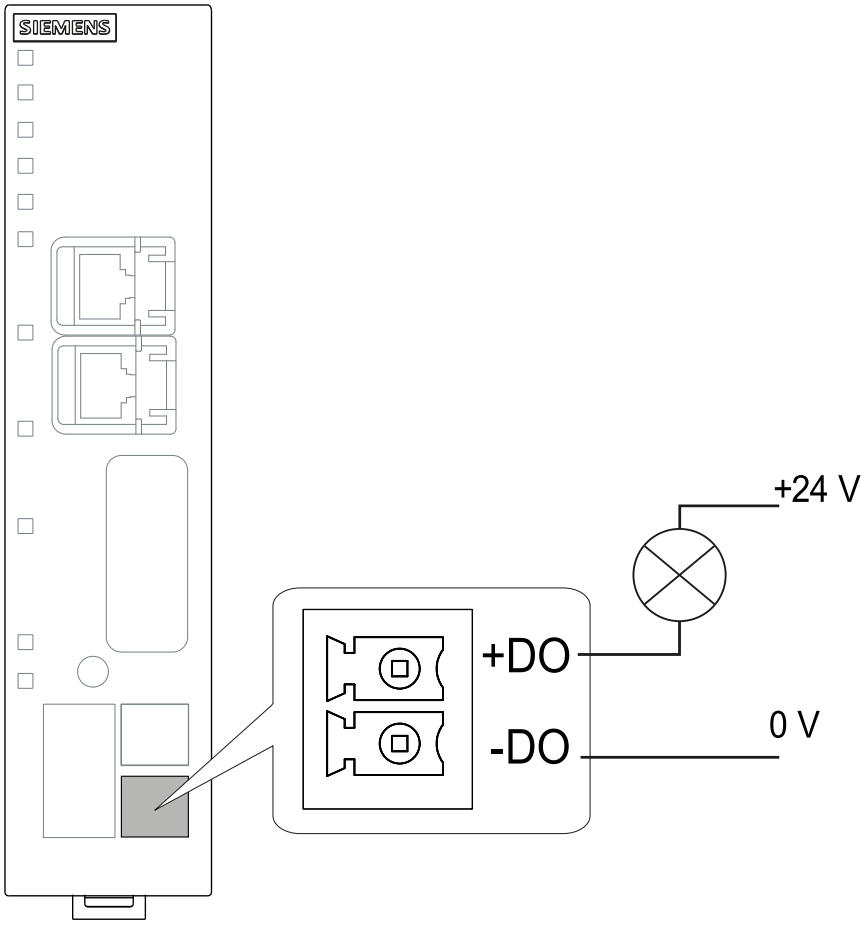
Contact	Assignment
+DI	Input
-DI	Ground

The voltage applied to the "DI" contact is converted to a digital status by the device as follows:

Voltage	Status
-30 to +3 V DC	0
+10 to +30 V DC	1

Digital output

The 2-pin terminal block has the following assignment:



Contact	Assignment
+DO	Switching signal Relay 24 V DC / 1 A
-DO	Ground

The output is a switch that switches the signal at +DO to -DO.

5.5 Ethernet

Connect the local network with the local applications to the Ethernet port, for example a programmable logic controller, a machine with an Ethernet interface for remote monitoring or a PC.

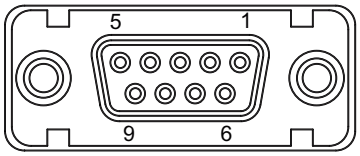
To set up the device, connect a PC with a Web browser to one of the Ethernet ports.

For the connection, use a path cable with an RJ-45 plug. You will find the properties of the Ethernet interface in the technical specifications.

5.6 MPI/DP interface

Pin assignment

The MPI/DP socket has the following pin assignment:



Signal description

Pin no.	Short name	Meaning	Input/output
1	NC	not connected	-
2	NC	not connected	-
3	LTG_B	Data line B	Input and output
4	RTS_AS	RTSAS, control signal for received data stream. The signal is '1' active when the directly connected S7 automation system sends.	Input
5	M5V	Reference potential of the MPI/DP interface for the signals RTS_AS and RTS_PG	Output
6	P5V	+5 V (only for bus termination)	Output
7	NC	not connected	-
8	LTG_A	Data line A	Input and output
9	RTS_PG	RTS output signal of the SCALANCE M804PB. The signal is '1' active when the SCALANCE M804PB sends. The signal is not included in the 0.3 m MPI cable.	Output
Shield	-	on connector housing For more on this, refer to the information on the grounding concept in the system manual "SIMATIC NET PROFIBUS Network Manual (https://support.industry.siemens.com/cs/ww/en/view/35222591)".	-

Connecting to the automation system

1. Connect the supplied MPI cable to the SCALANCE M804PB and screw it tight.
2. Connect the other end of the MPI cable to the MPI/PG interface of your CPU and screw it tight.

Note

The SCALANCE M804PB and the S7/M7/C7 system each represent a network device.

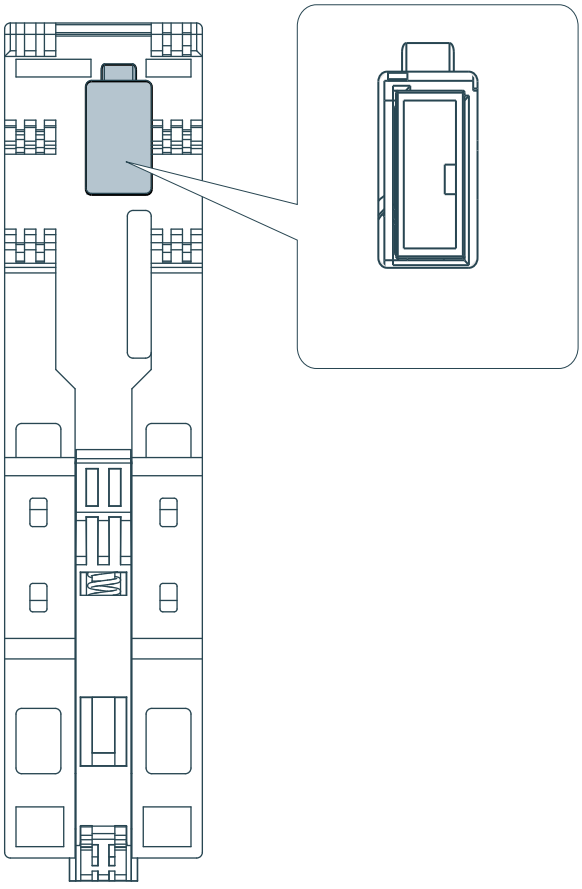
- In networks made up of 2 devices (SCALANCE M804PB and S7/M7/C7 system), the SCALANCE M804PB is operated directly on the socket of the S7/M7/C7 system.
- In networks made up of more than 2 devices, the SCALANCE M804PB is connected to the "PG socket" of a PROFIBUS connector (SINEC L2 bus connector). This does not require any change to the setting of the terminating resistors.

5.7 Replacing the PLUG

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

Inserting the PLUG

1. Turn off the power to the device.
2. Insert the PLUG correctly oriented into the slot.
   To ensure this, the housing of the PLUG has a protruding ridge on the long side. The slot has a groove at this position.



Removing the PLUG

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

Maintenance and cleaning

6

WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

- Repair work may only be performed by personnel authorized by Siemens.
- For function checks, maintenance and servicing work, you need to observe the requirements on checking and maintaining plants in hazardous areas according to the standards EN / IEC 60079-17.

WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

- Only use original accessories (Page 26) and original spare parts.
- Observe all relevant installation and safety instructions described in the manuals for the device or supplied with the accessories or spare parts.



CAUTION

Hot surfaces

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

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

NOTICE

Cleaning the housing

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

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

Do not use solvents.

Technical specifications

7

		SCALANCE M804PB
Article number		6GK5804-0AP00-2AA2
Ethernet interface		
Connection to Industrial Ethernet	Quantity	2
	Design	RJ-45 jack Properties: • 10/100BASE-T • Ethernet IEEE 802 • 10/100 Mbps
MPI/DP interface		
Connection to S7/M7/C7	Quantity	1
	Design	RS 485 socket Properties: • up to a maximum of 12 Mbps
Electrical data		
Power supply	Input voltage	12 to 24 VDC min. 10.8 V DC, max. 28.8 V
	Maximum power consumption	3 W
Digital input	Quantity	1
	Design	Terminal block, 2 terminals
	Properties:	Rated voltage 24 VDC Safety Extra Low Voltage (SELV)
		For state "1": 13 to 30 V DC For state "0": -30 to 3 VDC Maximum input current 8 mA Cables should be routed in pairs Maximum cable length < 30 m Inputs isolated from electronics.
Digital output	Quantity	1
	Design	Terminal block, 2 terminals
	Properties	Rated voltage 24 VDC Safety Extra Low Voltage (SELV)
		internal, not current limited Maximum current carrying capacity 1 A Cables should be routed in pairs Maximum cable length < 30 m Output isolated from electronics

		SCALANCE M804PB
Permitted ambient conditions		
Ambient temperature	During operation	-20 °C to +60 °C (vertical installation)
	During storage	-40 °C to +85 °C
	During transportation	-40 °C to +85 °C
Relative humidity	During operation	≤ 95% at 25 °C, no condensation
Design, dimensions and weight		
Module format		Compact module S7-1500
Degree of protection		IP20
Weight		352 g
Dimensions (W x H x D)		34.8 x 147 x 126.8 mm
Installation options		• Wall mounting • Mounting on a DIN rail • Mounting on an S7-300 standard rail • Mounting on an S7-1500 standard rail • Mounting on a pedestal
Installation direction		Vertical (ventilation openings at the top and bottom)
Product functions		
Configuration / management		• Web Based Management (WBM) via HTTP and HTTPS. • Command Line Interface (CLI) via Telnet and SSH
Security		• Router with NAT function – IP masquerading – NAPT – SourceNAT – NETMAP • Password protection • Firewall function – Port forwarding – IP firewall with stateful packet inspection (layer 3 and 4) – Global and user-defined firewall rules VPN functions – To establish a VPN (Virtual Private Network), the following functions are available – Up to 20 connections – IPsec VPN, OpenVPN (as client) • SINEMA RC client • Proxy server • Siemens Remote Service (SRS)

	SCALANCE M804PB
Monitoring / diagnostics / maintenance	• LEDs Display of operating statuses via the LED display. You will find further information on this in the operating instructions of the device. • Logging For monitoring have the events logged. • SNMPv1/v2/v3 For monitoring and controlling network components such as routers or switches from a central station.
Other functions	• Time-of-day synchronization – NTP client and NTP server – Secure NTP server – SIMATIC Time Client – SNTP Client • DHCP – DHCP server (local network) • Virtual networks (VLAN) To structure Industrial Ethernet networks with a fast growing number of devices, a physical network can be divided into several virtual subnets • Digital input/digital output • Dynamic DNS client • DNS client / DNS proxy • SMTP client • TIA Portal Cloud Connector

Dimension drawing

8

Note

CAx data

You can find the CAx data on the Internet at (https://www.automation.siemens.com/bilddb/index.aspx?lang=en)

1. Click on the "CAx data" link in the "Direct Links" area.
   The Industry Image Database page is loaded.
2. Enter the name or article number of the product in the search filter.
   You can refine your search using the "Motif type" selection list.

Dimensions are specified in mm.

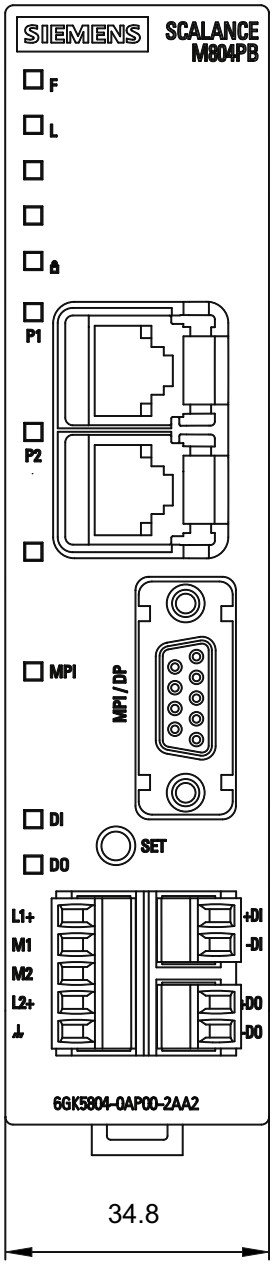


Figure 8-1 Front view

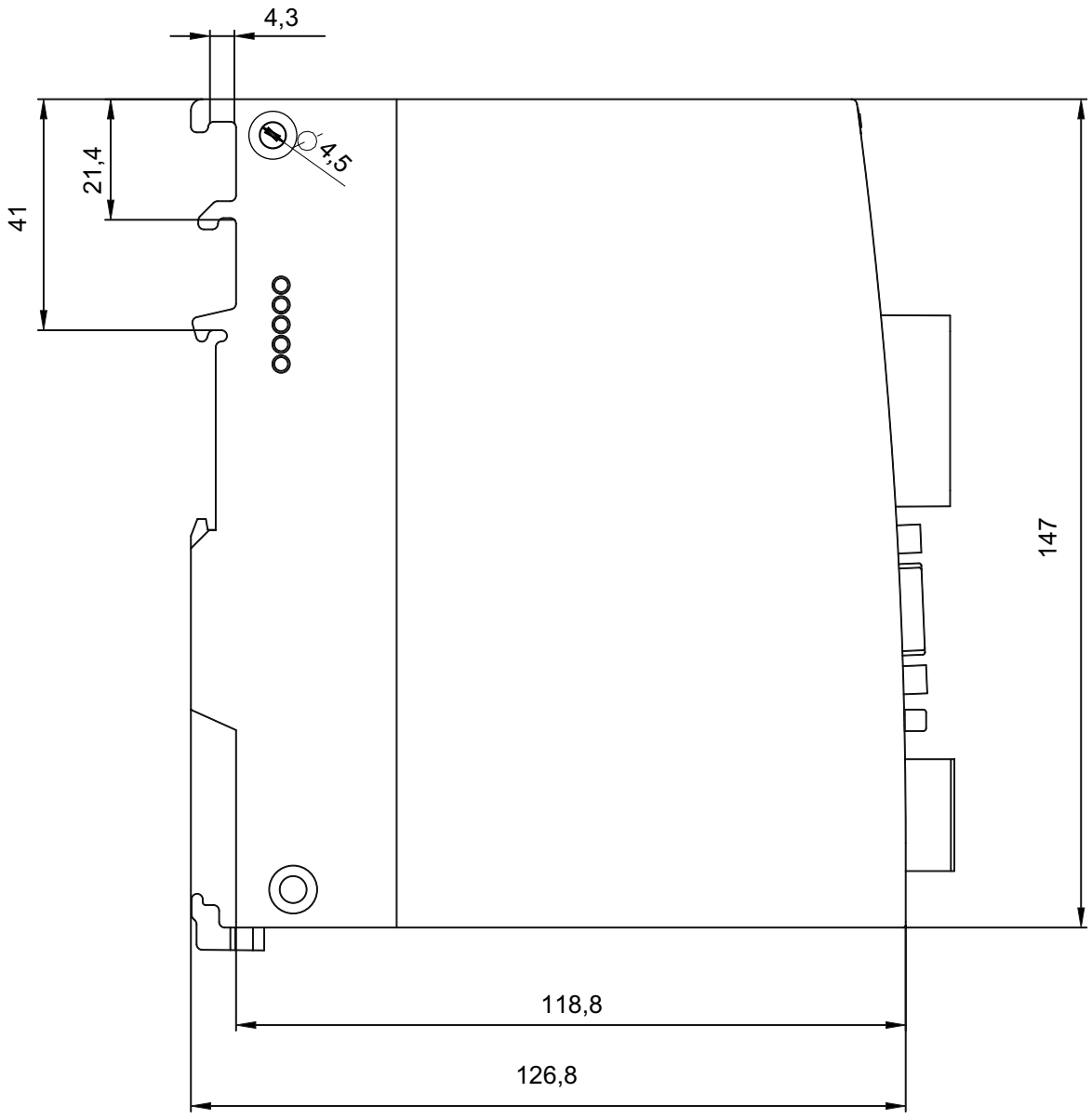


Figure 8-2 Side view

Approvals

9

Approvals issued

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.

Approvals for shipbuilding are not printed on the device 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 at the following link: (https://support.industry.siemens.com/cs/ww/en/ps/6GK5804-0AP00-2AA2/cert)

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)
- "SIMATIC NET PROFIBUS Network Manual" system manual (https://support.industry.siemens.com/cs/ww/en/view/35222591)
- "SIMATIC NET PROFIBUS Network Manual" system manual (https://support.industry.siemens.com/cs/ww/en/view/1971286)

⚠ WARNING

Personal injury and property damage can occur

The installation of expansions that are not approved for 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.

9.1 EC declaration of conformity

CE

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

Siemens Aktiengesellschaft
Digital Industries
Process Automation
DE-76187 Karlsruhe
Germany

You can find the current EU declaration of conformity for these products on the Internet pages of Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps/25380/cert).

The products described in these operating instructions meet the requirements of the following EC directives:

- ATEX directive 2014/34/EU
  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.
- EMC directive 2014/30/EU
  Directive of the European Parliament and of the Council of 26 February 2014 on the harmonization of the laws of the member states relating to electromagnetic compatibility.
- RoHS directive 2011/65/EU
  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.

9.1.1 ATEX

ATEX directive (correct usage in potentially explosive atmospheres)

The SIMATIC NET products described in these operating instructions meet the requirements of the EU directive 2014/34/EU "Equipment and Protective Devices for Use in Potentially Explosive Atmospheres".

Applied standards:

1. EN / EN IEC 60079-0
   Hazardous areas - Part 0: Equipment - General requirements
2. EN 60079-7
   Explosive atmospheres - Part 7: Equipment protection by increased safety "e"
3. EN / EN IEC 60079-15
   Explosive atmospheres - Part 15: Equipment protection by type of protection "n"

9.1.2 EMC

EMC directive (electromagnetic compatibility)

The SIMATIC NET products described in these operating instructions meet the requirements of EU directive 2014/30/EU "Electromagnetic Compatibility" for the following areas of application:

Applied standards:

- EN 61000-6-1
  Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments
- EN 61000-6-2
  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN 61000-6-3
  Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments
- EN 61000-6-4
  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

9.1.3 RoHS

RoHS directive (restriction of the use of certain hazardous substances)

The SIMATIC NET products described in these operating instructions meet the requirements of the EC directive 2011/65/EC for the restriction of the use of certain hazardous substances in electrical and electronic equipment.

Applied standard:

6 EN IEC 63000
Technical documentation for the assessment of electrical and electronic products with respect to restriction of hazardous substances

9.2 UK Declaration of Conformity

9.2.1 UK Declaration of Conformity for SCALANCE M

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/25380/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

9.2.2 The Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016

Correct usage in potentially explosive atmospheres

The SIMATIC NET products described in these operating instructions meet the requirements of "The Equipment and Protective Systems Intended for use in Potentially Explosive Atmospheres Regulations 2016".

Applied standard:

1. EN / EN IEC 60079-0
   Hazardous areas - Part 0: Equipment - General requirements
2. EN 60079-7
   Explosive atmospheres - Part 7: Equipment protection by increased safety "e"
3. EN / EN IEC 60079-15
   Explosive atmospheres - Part 15: Equipment protection by type of protection "n"

9.2.3 The Electromagnetic Compatibility Regulations 2016

Electromagnetic compatibility

The SIMATIC NET products described in these operating instructions meet the requirements of "The Electromagnetic Compatibility Regulations 2016".

Applied standards:

- EN 61000-6-1
  Electromagnetic compatibility (EMC) - Part 6-1: Generic standards - Immunity for residential, commercial and light-industrial environments
- EN 61000-6-2
  Electromagnetic compatibility (EMC) - Part 6-2: Generic standards - Immunity for industrial environments
- EN 61000-6-3
  Electromagnetic compatibility (EMC) - Part 6-3: Generic standards - Emission standard for residential, commercial and light-industrial environments
- EN 61000-6-4
  Electromagnetic compatibility (EMC) - Part 6-4: Generic standards - Emission standard for industrial environments

9.2.4 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012

Restriction of the use of certain hazardous substances

The SIMATIC NET products described in these operating instructions meet the requirements of "The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012".

Applied standard:

6 EN IEC 63000

Technical documentation for the assessment of electrical and electronic products with respect to restriction of hazardous substances

9.3 General approvals

ATEX, IECEx, UKEX and CCC Ex certification

⚠ WARNING

Risk of explosion in hazardous areas

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

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

You will find this document

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

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

The markings of the electrical devices are:



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



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

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



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

The products meet the requirements of the following standards:

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

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

FM



The product meets the requirements of the standards:

- FM Class 3600, FM Class 3611, FM Class 3810
- ANSI/UL 121201, ANSI/UL 61010-1
- 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
- CSA C22.2 No. 62368-1

Report no. E115352

cULus approval for industrial control equipment



cULus Listed PROG-CNTLR.

Underwriters Laboratories Inc. complying with

- UL 61010-1
- UL 61010-2-201

- CSA C22.2 NO 61010-1
- CSA C22.2 NO 61010-2-201

Report no. E115352

cULus Approval Hazardous Location

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

Underwriters Laboratories Inc. complying with

- UL 121201 (Non Incendive electrical equipment) approved for use in Class I, Division 2, Groups A, B, C, D, T4.
- UL CSA C22.2 NO 213 (Non Incendive electrical equipment) approved for use in Class I, Zone 2, Group IIC, T4.

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

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

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

Marking for the customs union

EAC (Eurasian Conformity)

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

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

Index

A

Accessories, 25
Article number, 3

B

Button, 31

C

CAx data, 65
Configuration manuals, 4
Connecting
  Digital input, 53
  Digital output, 54
  Power supply, 26, 49
Connecting up
  Ethernet interface, 54
  Grounding, 51

D

Device view, 24
Digital input, 53
Digital output, 54
Dimension drawing
  SCALANCE M804PB, 66
DIN rail, 40
Documentation on the Internet, 4

E

Ethernet interface, 54
External power supply
  China, 50

F

Factory default, 32

G

Glossary, 7
Grounding, 51

I

Installation
  DIN rail, 40
  Pedestal, 43
  S7-1500 standard rail, 42
  S7-300 standard rail, 41
  Wall, 39
Interfaces, 23

L

LED display, 29, 30
Loading firmware via TFTP, 32

P

PLUG, 32
Power supply, 26, 49
Product property, 23

R

Resetting the device, 32
Restart of the device, 32

S

S7-1500 standard rail, 42
S7-300 standard rail, 41
Safety notices
  for installation, 35
  general, 11
  Use in hazardous areas, 11, 35, 45
  when connecting up, 45
Scope of delivery, 24
SET button, 31
SIMATIC NET glossary, 7
System manual, 69

T

Terminals, 26

W

Wall mounting, 39
Wiring, 27