

SIMATIC NET

Industrial Ethernet switches MM900 media modules for SCALANCE XR-500

Compact Operating Instructions

Introduction	1
Safety notes	2
Recommendations on network security	3
Device description	4
installing and removing	5
Connecting	6
Service and maintenance	7
Technical data	8
Dimension drawings	9
Approvals	10

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 AG. 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.

Table of contents

1	Introduction	5
1.1	Security information	6
2	Safety notes	9
3	Recommendations on network security	11
4	Device description	19
5	installing and removing	21
5.1	Safety notices for installation	21
5.2	Disassembly	27
6	Connecting	29
6.1	Safety when connecting up	29
6.2	Connecting a media module	31
7	Service and maintenance	33
8	Technical data	35
8.1	Mechanical and electrical data	35
8.2	Cable lengths of the MM900 media modules for SCALANCE XR-500M	37
8.3	Other properties	38
9	Dimension drawings	41
10	Approvals	43
	Index	51

Introduction

Purpose of the compact operating instructions

Based on the compact operating instructions, you will be able to install and connect up the MM900 media module correctly.

Validity of these compact operating instructions

These compact operating instructions apply to the MM900 product group of the SCALANCE X-500 product line as of product version 1:

- MM991-4
- MM991-4LD
- MM992-4
- MM992-4LD
- MM992-4SFP
- MM992-4CU
- MM992-4CUC
- MM992-4PoE
- MM992-4PoEC

Note

Additional literature

When working with media modules, you should also read the compact operating instructions of the SCALANCE XR-500M product group.

You will find the operating instructions of the SCALANCE XR-500M product group on the supplied CD.

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>)

Security information

1.1 Security information

Siemens provides products and solutions with industrial security 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 security 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 security measures that may be implemented, please visit

<https://www.siemens.com/industrialsecurity> (<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 Security RSS Feed under

<https://www.siemens.com/cert> (<https://www.siemens.com/cert>).

Device defective

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

Recycling and disposal



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

Do not dispose of the products at public disposal sites.

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

Note the different national regulations.

Trademarks

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

SCALANCE, C-PLUG, OLM

Safety notes

Read the safety notices

Note the following safety notices. These relate to the entire working life of the device.

You should also read the safety notices relating to handling in the individual sections, particularly in the sections "Installation" and "Connecting up".

**CAUTION**

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

**WARNING****EXPLOSION HAZARD**

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

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

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

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

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

Recommendations on network security

NOTICE

Information security

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

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

General

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

Physical access

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

Software (security functions)

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

Authentication

Note

Accessibility risk - Risk of data loss

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

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

Certificates and keys

- There is a preset SSL/TLS (RSA) certificate with 2048 bit key length in the device. Replace this certificate with a user-generated, high-quality certificate with key. Use a certificate signed by a reliable external or internal certification authority. You can install the certificate via the WBM ("System > Load and Save").
- Use certificates with a key length of 4096 bits.
- Use the certification authority including key revocation and management to sign the certificates.
- Make sure that user-defined private keys are protected and inaccessible to unauthorized persons.
- If there is a suspected security violation, change all certificates and keys immediately.
- Use password-protected certificates in the format "PKCS #12".
- Verify certificates based on the fingerprint on the server and client side to prevent "man in the middle" attacks. Use a second, secure transmission path for this.
- Before sending the device to Siemens for repair, replace the current certificates and keys with temporary disposable certificates and keys, which can be destroyed when the device is returned.

Secure/non-secure protocols and services

- Avoid or disable non-secure protocols and services, for example HTTP, Telnet and TFTP. For historical reasons, these protocols are available, however not intended for secure applications. Use non-secure protocols on the device with caution.
- Check whether use of the following protocols and services is necessary:
 - Non authenticated and unencrypted ports
 - MRP, HRP
 - IGMP snooping
 - LLDP
 - DCP
 - Syslog
 - RADIUS
 - 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.

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

The table includes the following columns:

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

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

Protocol	Protocol/ Port number	Default port status	Configurable		Authenti- cation	Encryption ⁶⁾
			Port	Service		
DHCPv4 Server	UDP/67	Closed	-	✓	-	-
DHCPv4 Client (IPv4)	UDP/68	Open	-	✓	-	-
DHCPv6 Client (IPv6)	UDP/546	Closed	-	✓	-	-
EtherNet/IP ²⁾	TCP/44818 UDP/2222 UDP/44818	Closed	-	✓	-	-
HTTP Server/Client ⁴⁾	TCP/80	Closed	✓	✓	✓	-
HTTPS WBM Server/Client	TCP/443	Open	✓	✓	✓	✓
MSDP	TCP/639	Closed	--	✓	-	-
NTP Client	UDP/123	Closed	✓	✓	-	-
NTP (secure)	UDP/123	Closed	✓	✓	✓	-
PROFINET	UDP/34964 UDP/49151 ... 49159 ¹⁾	Open	--	✓	-	-

Protocol	Protocol/ Port number	Default port status	Configurable		Authenti- cation	Encryption ⁶⁾
			Port	Service		
RADIUS Client	UDP/1812 ⁵⁾	Outbound only	✓	✓	-	-
	UDP/1813 ⁵⁾					
	UDP/3799	Open	✓	✓	-	-
RIP	UDP/520	Closed	-	✓	-	-
RIPng IPv6	UDP/521	Closed	-	✓	-	-
SFTP Server	UDP/22	Outbound only	✓	✓	✓	✓
SMTP Client	TCP/25	Closed	✓	✓	--	--
SMTP Client (secure)	TCP/465	Closed	✓	✓	✓	✓
SNMPv1/v2c ^{3) 4)}	UDP/161	Open	✓	✓	-	-
SNMPv3	UDP/161	Open	✓	✓	Optional	Optional
SNMP Traps	UDP/162	Outbound only	--	✓	-	-
SNTP Client	UDP/123	Closed	✓	✓	-	-
SSH CLI Server	TCP/22	Open	✓	✓	✓	✓
Syslog Client	UDP/514	Closed	✓	✓	-	-
Syslog (secure) Client	TCP/6514	Closed	✓	✓	-	-
Telnet ⁴⁾	TCP/23	Closed	✓	✓	✓	-
TFTP Client	UDP/69	Outbound only	✓	✓	-	-
VRRP	TCP/50000	Open, filtered	--	✓	-	-

1) Port number can be configured via the WBM.

2) Service disabled by default.

3) Read-only access only.

4) Protocol according to Security by Default.

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

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

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

The table includes the following columns:

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

Layer 2 service	Default status	Service configura- ble
DCP	Setup mode ¹⁾	✓
LLDP	Open	✓

Layer 2 service	Default status	Service configurable
RSTP	Closed	✓
MSTP	Open	✓

1) Setting according to Security by Default.

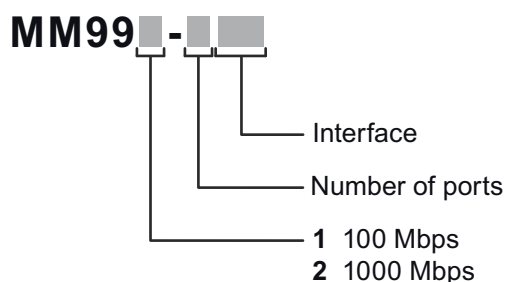
Device description

Article numbers

Type	Properties	Article number
MM991-4	4 x 100 Mbps, ST ports optical, multimode fiber-optic cable, up to max. 5 km.	6GK5 991-4AB00-8AA0
MM991-4LD	4 x 100 Mbps, ST ports optical, single mode fiber-optic cable, up to max. 26 km.	6GK5 991-4AC00-8AA0
MM992-4	4 x 1000 Mbps, SC ports optical, multimode FO cable, up to max. 750 m.	6GK5 992-4AL00-8AA0
MM992-4LD	4 x 1000 Mbps, SC ports optical, single mode FO cable, up to max. 10 km.	6GK5 992-4AM00-8AA0
MM992-4SFP	4 x 100 / 1000 Mbps, SFP media module	6GK5 992-4AS00-8AA0
MM992-4CU	4 x 10/100/1000 Mbps, RJ-45 ports electrical	6GK5 992-4SA00-8AA0
MM992-4CUC	4 x 10/100/1000 Mbps, RJ-45 ports electrical with securing collars	6GK5 992-4GA00-8AA0
MM992-4PoE	4 x 10/100/1000 Mbps, PoE ports electrical, max 60 W	6GK5 992-4QA00-8AA0
MM992-4PoEC	4 x 10/100/1000 Mbps, PoE ports electrical with securing collars, max 60 W	6GK5 992-4RA00-8AA0

Structure of the type designation

The type designation an MM900 media module for SCALANCE X-500 consists of several parts with the following meaning:



Interface	Property
CU	10/100/1000 Mbps RJ-45 port electrical.
CUC	10/100/1000 Mbps RJ-45 port electrical with securing collar.
SFP	100/1000 Mbps SFP media module.

Interface	Property
[-]	100 Mbps ST port optical, multimode fiber-optic cables, up to max. 3 km.
	1000 Mbps SC port optical, multimode fiber-optic cables, up to max. 750 m.
LD	100 Mbps ST port optical, single mode fiber-optic cables, up to max. 26 km.
	1000 Mbps SC port optical, single mode fiber-optic cable, up to max. 10 km.
PoE	10/100/1000 Mbps PoE port electrical, max. 60 W.
PoEC	10/100/1000 Mbps PoE port electrical, with securing collar, max. 60 W.



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.

If the consignment is incomplete or if there is damage to the exterior, contact your supplier or your local Siemens office.

Components of the product

The following components are supplied with an MM900 media module:

- MM900 media module
- Compact operating instructions

installing and removing

5.1 Safety notices for installation

Safety notices

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

**WARNING**

If a device is operated in an ambient temperature of more than 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.

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 3836.3.

 WARNING

Requirements for the cabinet/enclosure

The fiber-optic bus connections labeled SCALANCE MM400 (see type plate) may also be led through a hazardous area zone1 (see chapter Approvals (Page 43), section "ATEX").

 WARNING

If the temperature of the cable or housing socket exceeds 70 °C or the branching point of conductors exceeds 80 °C, special precautions must be taken. If the equipment is operated in an air ambient in excess of 50 °C to 60 °C, only use cables with a permissible operating temperature of at least 85 °C.

Additional notes



CAUTION

Use only approved components

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

Only use components approved for the SIMATIC NET devices.

NOTICE

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

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

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

Note

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

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

Connecting media modules and SFP transceivers



CAUTION

Remember the orientation of media modules

On modular devices, there are always two module slots arranged opposite each other. Remember the correct orientation when installing MM900 media modules.

Example:

- The first MM900 media module is installed in slot 3.
- The second MM900 media module installed in slot 4 must be turned through 180 degrees.

On modular devices for rack mounting, pairs of module slots are located one above the other in which modules can be inserted in a specific order:

Example of a rack device:

- The first MM900 media module is installed in slot 1.
- The second MM900 media module installed in slot 7 must be turned through 180 degrees.

Other modules are then inserted in slots 2 and 8 or 3 and 9 etc.

The permitted operating temperature is decided by the fully equipped device (switch + media module + SFP transceiver).

With modular devices, it is not only the switch that decides the permitted operating temperature of the overall device but also the temperature ranges of the MM900 media modules and the SFP transceivers. You will find details in the technical specifications of the relevant components.

The following aspects can restrict the maximum permitted operating temperature:

- The orientation of the carrier device.
- The use of SFP transceivers.
- The use of transceivers of the types LH, LH+ or ELH.

NOTICE

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

Optical sockets and plugs are sensitive to contamination of the end face. Contamination can lead to the failure of the optical transmission network.

Close unused optical sockets and plugs as well as pluggable transceivers and slots with the supplied protective caps.

Remove the protective caps only immediately before you use the plug-in connection.

NOTICE

Use only approved SFPs

If you use components not approved by Siemens AG, in particular SFPs, Siemens cannot accept any responsibility for the correct functioning of the "Ethernet switch system" according to the specification.

Moreover, if components are used that have not been Siemens approved, Siemens cannot vouch for their compatibility or for risk-free use of these components.

You can use media modules with the following devices:

- SCALANCE XR528-6M
- SCALANCE XR552-12M

Notes on plugging/pulling media modules

NOTICE

Use only approved media modules

In the module slots of the devices, use only approved media modules "MM900" of the SCALANCE XR-500 IE switches product line.

Note

Slots for PoE modules

You can only use PoE modules in slots 1, 2 and 3, refer to the following section "Identification of the media module slots and ports".

Note

Factory defaults of the media modules

When inserting a media module, the parameters of the ports are set to the factory defaults.

First plug a media module into the device, and then assign the parameters for the ports.

Note

The names and labeling of the media modules differ

Example: The media module is called MM992-4SFP [6GK5 992-4AS00-8AA0], the labeling on the media module is 9924AS.

Identification of the media module slots and ports

Below, you can see the arrangement of the slots and ports of a SCALANCE XR552-12M:

Slot	1				2				3			
Port	P1	P2	P3	P4	P1	P2	P3	P4	P1	P2	P3	P4
Slot	4				5				6			
Port	P1	P2	P3	P4	P1	P2	P3	P4	P1	P2	P3	P4
Slot					0							
Port (SFP+)					P1	P2	P3	P4				
Slot	7				8				9			
Port	P1	P2	P3	P4	P1	P2	P3	P4	P1	P2	P3	P4

Slot	10				11				12			
Port	P1	P2	P3	P4	P1	P2	P3	P4	P1	P2	P3	P4

A SCALANCE XR528-6M has a total of six slots and four SFP+ ports.

Note

Slot number

In modular devices, the MM900 media modules can be assigned a slot number. The labels for the slot numbers ship with the modular devices.

SFP+ ports in slot 0

The SFP+ ports in slot 0 are part of the basic device.

Plugging in media module

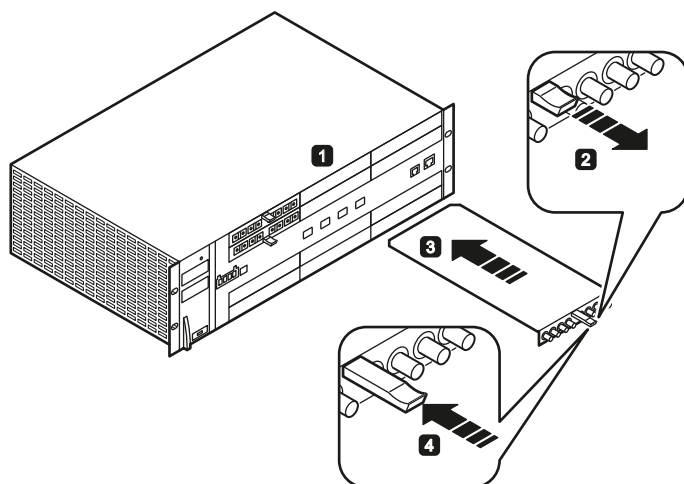


Figure 5-1 Plugging a media module into a SCALANCE XR552-12M. SCALANCE XR528-6M is used analogously.

To use MM900 media modules in a modular SCALANCE XR-500, follow the steps below:

1. Remove the dummy cover of the device slot into which you want to insert a media module ①.
2. Pull the handle out of the media module ②.
The media module cannot be installed unless the handle is pulled out.
3. Place the media module in the guide rails of the device slot ③.
The media module is correctly installed when it locks easily into the device and the front panel of the module is flush with the front of the device.
4. Push the handle back into the module ④.
The media module is then locked in place.

Pulling a media module

To pull a media module, follow the same steps as when plugging, but in the reverse order:

1. Pull out the handle of the media module.
2. Pull the media module out of the device slot.
3. Close the device slot with a dummy cover if you are not plugging in another module.

NOTICE

Operating the device only with closed module slots

The device meets degree of protection IP20, if all the module slots have either media modules inserted or are closed by dummy covers. Do not start up the device with open module slots since the ingress of objects can lead to damage.

If you operate the device with open module compartments, it is also not possible to guarantee the maximum ambient temperature.

Exchanging media modules - with change of medium

Exchanging a media module

If you replace an electrical media module with an optical media module (or vice versa), this can lead to malfunctions. The IE switch therefore reacts as follows:

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

Enabling a media module

To enable the replacement media module, restart the IE switch:

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

5.2 Disassembly

WARNING

Improper disassembly

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

For proper disassembly, observe the following:

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

Connecting

6.1 Safety when connecting up

Safety notices

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

Safety notices on use in hazardous areas

General safety notices relating to protection against explosion

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

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

 WARNING
Lack of equipotential bonding
If there is no equipotential bonding in hazardous areas, there is a risk of explosion due to equalizing current or ignition sparks.
• Ensure that equipotential bonding is available for the device.

 WARNING
Unprotected cable ends
There is a risk of explosion due to unprotected cable ends in hazardous areas.
• Protect unused cable ends according to IEC/EN 60079-14.

! WARNING**Improper installation of shielded cables**

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

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

! WARNING**Insufficient isolation of intrinsically safe and non-intrinsically safe circuits**

Risk of explosion in hazardous areas

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

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

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

! WARNING**EXPLOSION HAZARD**

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

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

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

! WARNING**Transient overvoltages**

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

**WARNING****Suitable cables at high ambient temperatures in hazardous area**

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

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

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

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

6.2 Connecting a media module

Power supply of the MM900 media modules

The MM900 media modules are supplied with power by the switch.

Service and maintenance



WARNING

Unauthorized repair of devices in explosion-proof design

Risk of explosion in hazardous areas

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



WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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



CAUTION

Hot surfaces

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

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

NOTICE

Cleaning the housing

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

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

Do not use solvents.

Technical data

8.1 Mechanical and electrical data

Device variants

The following technical specifications apply to the following device:

- MM900 media module for SCALANCE XR-500M

Note

Degree of protection of the media modules

Note that the media modules do not have a degree of protection. The degree of protection is only relevant for the basic devices.

Interfaces

Media module	Interfaces
MM992-4CU	4 x 10/100/1000 Mbps, RJ-45 ports electrical.
MM992-4CUC	4 x 10/100/1000 Mbps, RJ-45 ports electrical with securing collar.
MM992-4SFP	4 x 100/1000 Mbps, SFP media module.
MM992-4PoE	4 x 10/100/1000 Mbps, PoE ports electrical, max 60 W.
MM992-4PoEC	4 x 10/100/1000 Mbps, PoE ports electrical, with securing collar, max 60 W.
MM991-4	4 x 100 Mbps, ST ports optical, multimode fiber-optic cable, up to max. 5 km.
MM991-4LD	4 x 100 Mbps, ST ports optical, single mode fiber-optic cable, up to max. 26 km.
MM992-4	4 x 1000 Mbps, SC ports optical, multimode FO cable, up to max. 750 m.
MM992-4LD	4 x 1000 Mbps, SC ports optical, single mode FO cable, up to max. 10 km.

Construction

Media module	Dimensions and weight	Value
MM992-4CU	Dimensions	120 x 22 x 305 mm
MM992-4CUC	(W x H x D)	
MM992-4SFP	Weight	300 g
MM991-4		
MM991-4LD		
MM992-4		
MM992-4LD		

8.1 Mechanical and electrical data

Media module	Dimensions and weight	Value
MM992-4PoE	Dimensions (W x H x D)	120 x 22 x 305 mm
MM992-4PoEC		
	Weight	387 g

Permitted ambient conditions

Environmental conditions	
Transportation/storage temperature	-40 to +70 °C
Operating temperature	0 to +60 °C
Maximum relative humidity in operation at 25 °C	< 95 % no condensation
Operating altitude above sea level depending on ambient temperature	• 2000 m at max. 56 °C • 3000 m at max. 50 °C

Electrical data

Media module	Current consumption*	Maximum power consumption*
MM992-4CU MM992-4CUC	0.14 A	3.36 W
MM992-4SFP	0.02 A	0.48 W
MM992-4PoE MM992-4PoEC	2.89 A (at 60 W PoE load)	69.36 W (at 60 W PoE load)
MM991-4	0.20 A	4.8 W
MM991-4LD	0.16 A	3.84 W
MM992-4	0.13 A	3.12 W
MM992-4LD	0.15 A	3.6 W

* At 24 VDC rated voltage of the basic device

Note

Fusing and signal contacts with media modules

The MM900 media modules do not have their own fuses and have no signaling contacts. The fuses and the signaling contacts exist in the SCALANCE device.

Electrical data: Transmitter output (optical) and receiver input

Media module	Transmitter output (optical)		Receiver input	
	min. [dBm]	max. [dBm]	Sensitivity min. [dBm]	Input power max. [dBm]
MM992-4CU	-	-	-	-
MM992-4CUC	-	-	-	-

8.2 Cable lengths of the MM900 media modules for SCALANCE XR-500M

Media module	Transmitter output (optical)		Receiver input	
	min. [dBm]	max. [dBm]	Sensitivity min. [dBm]	Input power max. [dBm]
MM992-4SFP	-	-	-	-
MM992-4PoE	-	-	-	-
MM992-4PoEC	-	-	-	-
MM991-4	-19	-14	-32	-3
MM991-4LD	-15	-8	-34	-3
MM992-4	-9.5	-4	-17	-3
MM992-4LD	-9.5	-3	-21	-3

Electrical data: Galvanic isolation with PoE modules

Media module	Electrical isolation	
MM992-4PoE	Between ports P1 to P4	No
MM992-4PoEC	Between ports and ground	Yes
	Between ports and power input	Yes

8.2 Cable lengths of the MM900 media modules for SCALANCE XR-500M

Permitted cable lengths (copper cable)

Media module	Property	Lead	Permitted cable length
MM992-4CU	4 x 10/100/1000 Mbps, RJ-45 ports electrical with and without securing collar	IE TP torsion cable with	0 ... 45 m
MM992-4CUC		IE FC Outlet RJ-45 + 10 m TP cord	+ 10 m TP cord
MM992-4PoE		IE TP torsion cable	0 ... 55 m
MM992-4PoEC		with IE FC RJ-45 Plug 180	
		IE FC TP marine/trailing/flexible cable	0 ... 75 m + 10 m TP cord
		with IE FC Outlet RJ-45 + 10 m TP cord	
		IE FC TP marine/trailing/flexible cable	0 ... 85 m
		with IE FC RJ-45 Plug 180	
	IE FC TP standard cable with	0 ... 90 m	
	IE FC Outlet RJ-45 + 10 m TP cord	+ 10 m TP cord	
		IE FC TP standard cable	0 ... 100 m
		with IE FC RJ-45 plug 180	

8.3 Other properties

Permitted cable lengths (fiber-optic cable) for the SFP media module

Media module	Property	Max. permitted cable length
MM992-4SFP	4 x 100/1000 Mbps, SFP media module	Depending on the SFP transceiver used

Permitted cable lengths (fiber-optic cable - Fast Ethernet)

Media module	Property	Fiber	FO cable lengths
MM991-4	4 x 100 Mbps, BFOC ports optical, multimode glass, up to max. 5 km	50/125 µm multimode fiber	0-5 km (1 dB/km at 1310 nm; 1200 MHz*km)
MM991-4LD	4 x 100 Mbps, BFOC ports optical, single mode glass, up to max. 26 km	9/125 µm single mode fiber	0-26 km (0.5 dB/km at 1310 nm)

Permitted cable lengths (fiber-optic cable - gigabit Ethernet)

Media module	Property	Fiber	FO cable lengths
MM992-4	4 x 1000 Mbps, SC ports optical, multimode glass, up to max. 750 m	62.5/125 µm multimode fiber	0-350 m (3.1 dB/km at 850 nm; 1200 MHz*km)
		50/125 µm multimode fiber	0-750 m (2.5 dB/km at 850 nm; 1200 MHz*km)
MM992-4LD	4 x 1000 Mbps, SC ports optical, single mode glass, up to max. 10 km	9/125 µm single mode fiber	0-10 km (0.5 dB/km at 1310 nm)

8.3 Other properties

Table 8-1 Mean time between failure (MTBF)

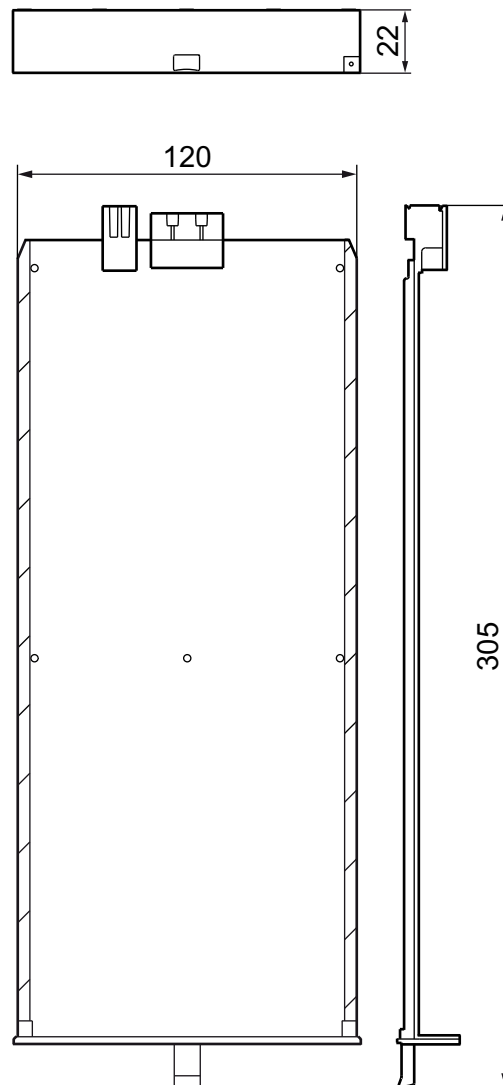
Device version (power supply)	MTBF
MM992-4CU MM992-4CUC	> 200 years
MM991-4,	> 90 years
MM991-4LD	> 70 years
MM992-4LD	> 75 years
MM992-4	> 85 years

Device version (power supply)	MTBF
MM992-4SFP	> 170 years ¹⁾
MM992-4PoE MM992-4PoEC	> 75 years

¹⁾ empty

Dimension drawings

View from the front, top, and side (right)



Dimensions are specified in mm.

Approvals

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.

Note

Note that the media modules meet the requirements of the approvals only in combination with the devices.

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/15318/cert>).

Notes for the manufacturers of machines

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

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

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

Machinery directive

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

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

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

EC declaration of conformity



The SIMATIC NET products described in these operating instructions meet the requirements and safety objectives of the following EC directives and comply with the harmonized European standards (EN) which are published in the official documentation of the European Union and here.

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

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



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.

Note for devices with CLASS 1 LASER

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

Note

CLASS 1 LASER

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

EMC (electromagnetic compatibility)

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

Applied standards:

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

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

RoHS

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

Applied standard:

- EN IEC 63000

FM

The product meets the requirements of the standards:

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

cULus Approval for Information Technology Equipment



cULus Listed I. T. E.

Underwriters Laboratories Inc. complying with

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

Report no. E115352

cULus Approval Hazardous Location



HAZ. LOC.

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

Underwriters Laboratories Inc. complying with

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

Approved for use in

Cl. 1, Div. 2, GP A, B, C, D T4

Cl. 1, Zone 2, GP IIC T4

Report no. E240480

Note for Australia - RCM

The product meets the requirements of the RCM standard.

Applied standards:

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

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

Marking for the customs union



EAC (Eurasian Conformity)

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

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

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 사용하는 것을 목적으로 합니다.

FDA and IEC markings

The following MM900 media modules meet the FDA and IEC requirements listed below:

Media module	CLASS 1 LASER PRODUCT
MM992-4CUC	-
MM992-4CU	-
MM992-4SFP	-
MM992-4PoE	-
MM992-4PoEC	-
MM991-4	●
MM991-4LD	●
MM992-4	●
MM992-4LD	●



Figure 10-1 FDA and IEC markings

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

Installation guidelines

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

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

**WARNING****Personal injury and property damage can occur**

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

Only use expansions that are approved for the system.

Note

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

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

Index

Slot number, 26
System manual, 23, 48

A

Approvals, 43
Article numbers, 19

C

CE mark, 43

D

Dummy cover, 26

F

Factory settings, 25

G

Glossary, 5

H

Handle, 26

M

Media module, 25
Modular device, 25
Module slot, 25

P

Power supply
Media modules, 31

S

Safety notices
for installation, 21
general, 9
Use in hazardous areas, 9, 21, 29
when connecting up, 29
SIMATIC NET glossary, 5

