

SIMATIC NET

S7-1500 - PROFINET SIMATIC CM 1542-1

Operating Instructions

Preface

Properties and functions

1

LEDs, connections, QR code

2

Installation, connecting up, commissioning, operation

3

Configuration, program blocks

4

Diagnostics and upkeep

5

Technical specifications

6

Approvals

7

Dimension drawings

8

Documentation references

A

CM 1542-1, firmware V3.0 (6GK7542-1AX00-0XE0)
CM 1542-1, firmware V4.2 (6GK7542-1AX10-0XE0)

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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

WARNING

Siemens products may only be used for the application described in the catalog and the associated usage information. 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.

Preface



CAUTION

Risk of injury

To prevent injury, read the manual before use.

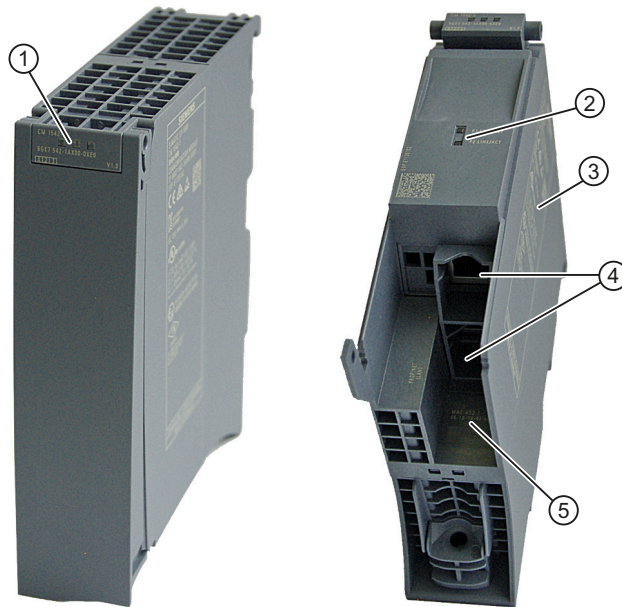
Validity of this manual

This document contains information on the following products:

- Communications module CM 1542-1
Article number 6GK7 542-1AX00-0XE0
Hardware product version 1
Firmware version V3.0
- Communications module CM 1542-1
Article number 6GK7 542-1AX10-0XE0
Hardware product version 1
Firmware version V4.2

Communications modules for connecting S7-1500 to PROFINET

View of the CM



- ① LEDs for status and error displays
- ② LED display of the Ethernet ports X1 P1 and X1 P2
- ③ Type plate
- ④ PROFINET interface: 2 x 8-pin RJ45 socket
- ⑤ Label with MAC address

Figure 1 View of the CM 1542-1 with closed (left) and open (right) front cover

Abbreviations and reference to the module version

- CM / module / device
These terms are used in the following instead of the complete product designation. In this case, the information applies equally to both firmware versions or hardware product versions of the module.
If the data of the two devices differs, the firmware version or the hardware product version of the respective device is explicitly stated.
- CM "AX00"
CM 1542-1 with article number 6GK7 542-1AX00-0XE0
- CM "AX10"
CM 1542-1 with article number 6GK7 542-1AX10-0XE0
- STEP 7
The name STEP 7 is used to mean the STEP 7 Professional configuration tool.

Address label: Unique MAC address preset for the CM

When supplied, the CM has a total of 3 default MAC addresses with the following assignment:

- PROFINET interface
The MAC address of the PROFINET interface is printed on the enclosure.
(Visible in STEP 7 for "Accessible devices")
- One MAC address for each of the 2 Ethernet ports of the PROFINET interface
The MAC addresses of the Ethernet ports are required only for detection and evaluation of neighborhood and topology relations (LLDP).

Purpose of the manual

This manual supplements the S7-1500 system manual.

With the information in this manual and the system manual, you will be able to commission the CM.

New in this edition

New firmware version V4.2 of the "AX10" module with the following new functions:

- Support of the virtual interface of the CPU, see section Virtual interface of the CPU (Page 46).

General revisions:

- For information on the cycle for data exchange with the CPU, see section Transmission and reaction times (Page 19).
- For information on the TTL value when routing via the backplane bus, see section IP routing (Page 45).
- "Security Recommendations" section renamed "Industrial Cybersecurity".
- Editorial revisions

Replaced edition**Edition 12/2024**

New in edition 12/2024:

Editorial revision:

- Correction to technical specifications (6GK7 542-1AX10-0XE0)
 - Transmission speed/direction dependency
 - Permissible temperature range
- New notes on Ethernet interface, QR code and FM approval

New functions:

- Reset to factory settings
- Expanded online diagnostics
- Integrated recording of data traffic

Edition 04/2023

New in edition 04/2023:

- New module with new article number, see above.
- New firmware versions, with the following functions among others:
 - Safety-related product improvements, see section Security information (Page 17).
 - CM 1542-1 (6GK7 542-1AX10-0XE0, firmware version V4.0):
Enabling/disabling SNMP via data record; see section Disabling SNMP via data record (Page 50).
- New approvals: CCC / UKEX
- Editorial revision

Manual on DVD

You will find the manual on the DVD supplied with the product. This DVD contains the product manuals valid at the time it is created.

Current manual edition on the Internet

You will also find the current version of this manual on the Internet pages of Siemens Automation Customer Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/man>)

Information can be accessed via QR code

There is a QR code on the device via which you can call up a web page relating to the device which provides a great deal of information. Refer to section QR code (Page 28) for more on this.

Cybersecurity information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary

and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

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

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://www.siemens.com/cert>.

License conditions

Note

Open source software

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

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

- OSS_CM15421_86.pdf
- OSS_CM15421_99.pdf

Firmware

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

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.

Documentation guide

The documentation of the SIMATIC products has a modular structure and covers topics relating to your automation system.

The complete documentation for the S7-1500 system consists of a system manual, function manuals and device manuals.

The STEP 7 information system (online help) also supports you in configuring and programming your automation system.

Overview of the documentation on communication with S7-1500

The following table lists additional documents, which supplement this description of the CM 1542-1. The documents are available on the Internet.

Table 1 Documentation for the S7-1500 system

Topic	Documentation	Important contents
System description	S7-1500 automation system (https://support.industry.siemens.com/cs/ww/en/view/59191792) system manual	• Application planning • Installation • Connecting • Commissioning
Module properties	Power supplies (https://support.industry.siemens.com/cs/ww/en/ps/13743/man) manual	• Connecting • Parameter assignment, addressing • Interrupts, error messages, diagnostics and system alarms • Technical specifications • Dimension drawing
	Signal modules (https://support.industry.siemens.com/cs/ww/en/ps/13721/man) manual	
System diagnostics	System diagnostics (https://support.industry.siemens.com/cs/ww/en/view/59192926) function manual	• Overview • Diagnostics evaluation for hardware/software
Communication	Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) function manual	• Overview
	Function manual PROFINET with STEP 7	• PROFINET basics • PROFINET functions • PROFINET diagnostics
	Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) function manual	• Function • Operation
Interference-free installation of control systems	Designing interference-free controllers (https://support.industry.siemens.com/cs/ww/en/view/59193566) function manual	• Basics • Electromagnetic compatibility • Lightning protection • Housing selection
Memory concept	Structure and Use of the CPU Memory (https://support.industry.siemens.com/cs/ww/en/view/49948856) function manual	• Design • Principle of operation • Use

Topic	Documentation	Important contents
Cycle and response times	Function manual: Cycle and Response Times (https://support.industry.siemens.com/cs/ww/en/view/59193558)	- Basics - Calculations
Analog value processing	Function manual: Analog value processing (https://support.industry.siemens.com/cs/ww/en/view/67989094)	- Wiring options - Tables of measured values

Table 2 Documentation on Industrial Ethernet / PROFINET

Topic	Documentation	Important contents
Industrial Ethernet / PROFINET	SIMATIC NET Industrial Ethernet / PROFINET System manual - Industrial Ethernet Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465) - Passive network components Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)	- Ethernet/PROFINET networks - Network configuration - Network components

You will find additional documents on the Siemens Industry Online Support pages in the appendix Documentation references (Page 77).

FAQs on the Internet

You will find detailed information (FAQs) on using the CM described here on the Internet at the following address (entry type "FAQ"):

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/faq>)

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:

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

Device defective

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

Decommissioning

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

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

Recycling and disposal

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.

Table of contents

	Preface	3
1	Properties and functions	15
1.1	Communication services	15
1.2	Further functions	15
1.3	Security information	17
1.4	Intended operating environment	18
1.5	Configuration limits and performance data	19
1.5.1	Transmission and reaction times	19
1.5.2	Connection resources	19
1.5.3	Characteristic data Open User Communication incl. e-mail	20
1.5.4	Characteristics of S7 communication	21
1.5.5	PROFINET IO characteristic data	21
1.5.6	Rack components	22
1.6	Requirements for use	22
1.6.1	Usable CPUs	22
1.6.2	Project engineering	23
1.6.3	Program blocks	24
2	LEDs, connections, QR code	25
2.1	LED display	25
2.2	Ethernet interface	27
2.3	QR code	28
3	Installation, connecting up, commissioning, operation	31
3.1	Important notes on using the device	31
3.1.1	Notices on use in hazardous areas	31
3.1.2	Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex	31
3.1.3	Notes on use in hazardous areas according to UL HazLoc and FM	32
3.2	Installation, removal and repairs in hazardous areas	33
3.3	Installation	35
3.4	Connecting	38
3.5	Mode of the CPU - effect on the CM	39
3.6	Disassembly	40
4	Configuration, program blocks	41
4.1	Industrial Cybersecurity	41
4.2	Network settings	44
4.2.1	Fast Ethernet	44

4.3	IP configuration	44
4.3.1	Restart after detection of a duplicate IP address in the network	44
4.3.2	Remove retentive storage of the IP address if there are duplicate addresses	44
4.3.3	IP routing.....	45
4.3.4	Virtual interface of the CPU	46
4.3.5	CM in multiple use IO systems (standard machines).....	48
4.4	Media redundancy	49
4.5	Time-of-day synchronization	50
4.6	Disabling SNMP via data record	50
4.7	Program blocks for OUC	51
5	Diagnostics and upkeep.....	55
5.1	Diagnostics	55
5.1.1	Diagnostics options.....	55
5.1.2	SNMP	55
5.2	Maintenance.....	57
5.2.1	Update firmware	58
5.2.2	Reset to factory settings	60
5.2.3	Module replacement.....	61
6	Technical specifications	63
6.1	Technical specifications of the CM (6GK7542-1AX00-0XE0)	63
6.2	Technical specifications of the CM (6GK7542-1AX10-0XE0)	64
6.3	Terminal assignment.....	65
6.4	Permitted cable lengths - Ethernet.....	66
6.5	Ambient temperature.....	66
6.6	Resistance to harmful gases according to ISA-71.04.....	67
7	Approvals	69
8	Dimension drawings	75
A	Documentation references	77
A.1	Introduction to the documentation	77
A.2	System manual S7-1500	77
A.2.1	/1/	77
A.3	Diagnostics	78
A.3.1	/2/	78
A.3.2	/3/	78
A.4	Communication	78
A.4.1	/4/	78
A.4.2	/5/	78
A.4.3	/6/	79
A.5	Interference-free installation of control systems	79
A.5.1	/7/	79

A.6	Memory concept.....	79
A.6.1	/8/	79
A.7	Cycle and response times	79
A.7.1	/9/	79
Index		81

Properties and functions

1.1 Communication services

The CM supports the following communications services:

- **PROFINET IO**
PROFINET IO allows direct access to IO devices over Industrial Ethernet.
 - Real-Time communication (RT)
 - Isochronous Real-Time communication (IRT)
 - Media redundancy MRP
 - Device replacement without exchangeable storage medium
 - IO controller
 - IO device (iDevice, Shared Device, Prioritized startup)
 - Isochronous real time
- **Open User Communication**
Open User Communication supports the following communications services via the CM using programmed or configured communications connections:
 - TCP (complying with RFC 793), ISO-on-TCP (complying with RFC 1006) and UDP (complying with RFC 768)
With the interface via TCP connections, the CM supports the socket interface to TCP/IP available on practically every end system.
 - Multicast with UDP
The multicast mode is made possible by selecting a suitable IP address when configuring connections. A maximum of six multicast groups are supported via UDP.
- **S7 communication**
 - PG communication
 - Operator control and monitoring functions (HMI communication)
 - Data exchange over S7 connections

1.2 Further functions

Time synchronization with NTP (Network Time Protocol)

The CP can synchronize its local time of day via NTP.

For details, see section Time-of-day synchronization (Page 50).

Media redundancy (MRP)

Within an Ethernet network with a ring topology, the CM supports the media redundancy protocol MRP. You can assign the role of "Client" or "Manager (Auto)" to the CM.

Addressable with the factoryset MAC address

To assign the IP address to a new CM (direct from the factory), it can be accessed using the preset MAC address on the interface being used. You perform online address assignment in STEP 7.

SNMP agent

The CM supports data queries using SNMP in version V1 (Simple Network Management Protocol).

For details, see section SNMP (Page 55).

IP configuration - IPv4

The essential features of IP configuration for the CM:

- The CM supports the use of IP addresses according to IPv4.
- You can configure how and with which method the CM is assigned the IP address, the subnet mask and the address of a gateway.
- The IP configuration and the connection configuration (IPv4) can also be assigned to the CM by the user program. For information on the program blocks, see section Program blocks (Page 24).

Note: Does not apply to S7 connections.

IP routing

The CM supports static IP routing (IPv4) to other CMs/CPs.

For details, see section IP routing (Page 45).

Access to the Web server of the CPU

Via the LAN interface of the CM, you have access to the Web server of the CPU. With the aid of the Web server of the CPU, you can read out module data from a station.

Note the special description of the Web server; refer to the section Documentation references (Page 77)

Note

Web server access using the HTTPS protocol

The Web server of a SIMATIC S7-1500 station is located in the CPU. For this reason, when there is secure access (HTTPS) to the Web server of the station using the IP address of the CM 1542-1, the SSL certificate of the CPU is displayed.

1.3 Security information

Note

Security

- Security recommendations
Refer to the information in the section Industrial Cybersecurity (Page 41).
 - Configuration with implementation of security measures
You can find a sample network configuration with the CM and the relevant data flows can be found in the section Intended operating environment (Page 18).
-

Security Advisories

If Siemens detects and resolves security incidents in the products, this is published in Security Advisories.

You can find the documents for CM on the following Siemens AG web page:

Link: (<https://new.siemens.com/global/en/products/services/cert.html?s=CM%201542-1#SecurityPublications>)

There, enter "CM 1542-1" in the "Search Security Advisories" search field.

Security Incidents and fixes

The following Security Incidents are open for the CM 1542-1 at the time of publication of this manual:

- None

The following Security Incidents have been fixed with the listed firmware versions:

- **V3.0**
 - **SSA-462066**
Vulnerability known as TCP SACK PANIC in Industrial Products
Affected versions: All versions < V3.0
Remediation: Update to V3.0 or later version
 - **SSA-599968**
Denial-of-Service Vulnerability in Profinet Devices
Affected versions: All versions < V3.0
Remediation: Update to V3.0 or later version
 - **SSA-936080**
Multiple Vulnerabilities in Third-Party Component libcurl
Affected versions: All versions < V3.0
Remediation: Update to V3.0 or later version
- **V2.0**
 - **SSA-293562**
Denial of Service Vulnerabilities in PROFINET DCP Implementation of Industrial Products
Affected versions: All versions < V2.0
Remediation: Update to V2.0 or later version

Further security-related information

You can configure the access to the CM or the station in the STEP 7 project.

For information about the ports used by the CM, refer to section Industrial Cybersecurity (Page 41).

1.4 Intended operating environment

The following figure shows a sample system configuration as intended operating environment for the CM.

- The CM is located in the field level.
- Communication partners are also in the field or control level and in the input level.

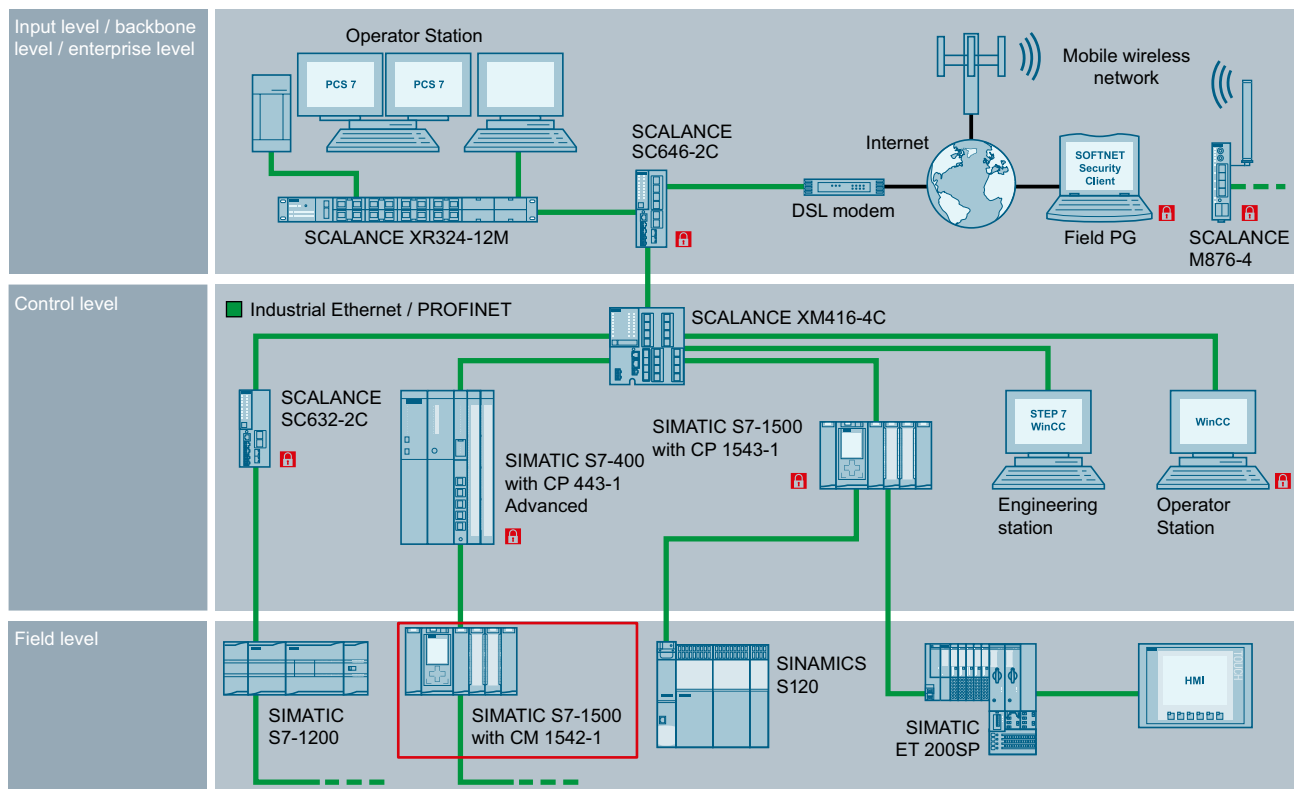


Figure 1-1 Example of a system configuration for the intended operating environment of the CM 1542-1

For protection of the company and plant network, the following security components are recommended:

- External firewalls with Intrusion Detection System (IDS) protect the company network against external attacks.
- DMZ firewalls in the backbone level protect the plant network.
- Security modules protect each individual automation cell.

Note**Security information**

To protect your system, refer to the information in the section Industrial Cybersecurity (Page 41).

1.5 Configuration limits and performance data

1.5.1 Transmission and reaction times

Note**Cycle for data exchange with the CPU**

The CPU exchanges data, including PROFINET IO data, via the backplane bus every 4 ms.

Note**Measured values on the Internet**

Measured values of transmission and reaction times in PROFINET networks for a series of configurations can be found on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/view/25209605>)

1.5.2 Connection resources

Characteristic	Explanation / values
Total number of freely usable connections on Industrial Ethernet	64 configurable connections, 1 PG connection The value applies to the total number of connections of the following types: • Connections for open communications services

Note**Connection resources CPU dependent**

Depending on the CPU type, different numbers of connection resources are available. The number of connection resources is the decisive factor for the number of configurable connections. This means that the values that can actually be achieved may be lower than specified in this section "Properties and functions" describing the CM.

1.5.3 Characteristic data Open User Communication incl. e-mail

Open User Communication (OUC) provides access to communication over TCP, ISO-on-TCP and UDP connections.

Characteristic	Explanation / values
Number of connections	Max. number of connections in total (configured and programmed): $(\text{ISO-on-TCP} + \text{TCP} + \text{UDP} + \text{e-mail}) \leq 64$ of which: • TCP connections: 0 ... 64 ¹⁾ • ISO-on-TCP connections: 0 ... 64 • Total number of UDP connections (specified and free) that can be configured: 0 ... 64 • Connection for e-mail: 0 to 1; only one e-mail can be processed at any one time.
Number of multicast address groups	Max. 6
Maximum data length for program blocks	Program blocks allow the transfer of user data in the following lengths: 1. ISO-on-TCP, TCP: 1 - 64 kbytes 2. UDP – CM with article number 6GK7542-1AX00-0XE0: 1 - 1452 bytes – CM with article number 6GK7542-1AX10-0XE0: 1 - 2048 bytes 3. E-mail (job header + user data): 1 - 256 bytes e-mail attachment: ≤ 64 kbytes
LAN interface max. data field length generated by the CM per protocol data unit (TPDU = transport protocol data unit)	For sending • ISO-on-TCP, TCP: 1452 bytes / TPDU For receiving • ISO-on-TCP: 512 bytes / TPDU • TCP: 1452 bytes / TPDU

¹⁾ Avoid overload at receiving end Make sure that the processing capabilities of a receiving CM are not permanently exceeded by the sender (approximately 150 ... 200 messages per second).

Note

Connection resources of the CPU

Depending on the CPU type, different numbers of connection resources are available. The number of connection resources is the decisive factor for the number of configurable connections. This means that the values that can actually be achieved may be lower than specified in this section describing the CM.

You will find detailed information on the topic of connection resources in the function manual /4/ (Page 78).

Restrictions for UDP

- Restrictions UDP broadcast / multicast
To avoid overloading the CM due to high broadcast/multicast frame traffic, the receipt of UDP broadcast/multicast on the CM is limited.

1.5.4 Characteristics of S7 communication

S7 communication provides data transfer via the ISO-on-TCP protocol.

Characteristic	Explanation / values
Total number of freely usable S7 connections on Industrial Ethernet	Max. 64
LAN interface - data field length generated by CM per protocol data unit (PDU = protocol data unit)	• for sending: 480 bytes / PDU • for receiving: 480 bytes / PDU

Note

Maximum values for an S7-1500 station

Depending on the CPU you are using, there are limit values for the S7-1500 station. Note the information in the relevant documentation.

1.5.5 PROFINET IO characteristic data

Configuration limits of the CM as an IO controller

The CM supports the following maximum configuration as a PROFINET IO controller:

Characteristic	Explanation / values
Number of operable PROFINET IO devices	128, of which: • Max. 64 IRT devices
Size of the input area over all PROFINET IO devices *)	Max. 8192 bytes
Size of the output area over all PROFINET IO devices	Max. 8192 bytes
Size of the IO data area per submodule of a module in an IO device	• Inputs: 256 bytes • Outputs: 256 bytes
Size of the consistency area for a submodule	256 bytes

*) The diagnostics addresses of the PROFINET IO devices cannot be used as an input on the IO controller. The data area of the inputs is reduced by the diagnostics addresses used.

1.5.6 Rack components

When using the CM type described here, the following limits apply:

- The number of CMs that can be operated in a rack depends on the CPU type being used. By operating several CMs, you can increase the configuration limits listed in the section Properties and functions (Page 15) for the station as the whole. The CPU does, however, have set limits for the entire configuration.
Note the information in the documentation of the CPU, refer to the section Documentation references (Page 77)

Note

Power supply via the CPU adequate or additional power supply modules required

You can operate a certain number of modules in the S7-1500 station without an additional power supply. Make sure that you keep to the specified power feed to the backplane bus for the particular CPU type. Depending on the configuration of the S7-1500 station you may need to provide additional power supply modules.

1.6 Requirements for use

1.6.1 Usable CPUs

The following CPUs can be used as local CPU of the communications module:

- Compatible CPUs
All CPUs that can be configured in STEP 7 as of firmware version V2.1 from the following series:
 - Standard CPUs (CPU 15xx)
 - Compact CPUs (CPU 15xxC)
 - Technology CPUs (CPU 15xxT / TF)
 - Fail-safe CPUs (CPU 15xxF)
- Non-compatible CPUs
 - H-CPU (CPU 1517H / HF)
 - R-CPU (CPU 151xR)

Note**Keep the firmware version of the CPUs and communications modules up to date**

To avoid possible problems when using newer CPUs together with older communications modules, you should keep the firmware of both your communications modules and your CPUs up to date.

Check regularly for security updates for the firmware and use them.

Information regarding product news and new firmware versions of the communications module is available at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/dl>)

1.6.2 Project engineering

Software for configuration and online functions

To configure the CM, the following configuration tool is required:

STEP 7 version	CM "AX00"	CM "AX10"
STEP 7 Professional V14	The functionality of the CM with firmware version V2.0 can be configured.	The CM is configurable, but with the functionality of the CM "AX00" with firmware version V2.0.
STEP 7 Professional V17	The full functionality of the CM with firmware version V3.0 can be configured.	The CM is configurable, but with the functionality of the CM "AX00" with firmware version V3.0.
STEP 7 Professional as of V18	The full functionality of the CM with firmware version V3.0 can be configured.	The full functionality of the CM with firmware version V4.0 can be configured.
STEP 7 Professional V20	The full functionality of the CM with firmware version V3.0 can be configured.	The full functionality of the CM with firmware version V4.1 can be configured.

Downloading the configuration data

When there is a download to the CPU, the CM is supplied with the relevant configuration data. The configuration data can be downloaded to the CPU via a memory card or any Ethernet/PROFINET interface of the S7-1500 station.

1.6.3 Program blocks

Program blocks

For communications services, there are preprogrammed program blocks (instructions) available as the interface in your STEP 7 user program.

Table 1-1 Instructions for communications services

Protocol	Program block (instruction)	System data type
TCP	Establish connection and send/ receive data via: • TSEND_C / TRCV_C or	• TCON_IP_v4 • TCON_Configured • TCON_QDN
ISO-on-TCP	• TCON, TSEND / TRCV (Termination of the connection possible using TDISCON)	• TCON_IP_RFC
UDP	• TCON, TUSEND/TURCV (Termination of the connection possible using TDISCON)	• TCON_IP_v4 • TCON_QDN
E-mail	• TMAIL_C	• TMail_V4

Table 1-2 Instructions for configuration tasks

Function	Program block (instruction)	System data type
Configuration of the Ethernet interface	• T_CONFIG	• CONF_DATA

For more detailed information, refer to section AUTOHOTSPOT.

Refer to the documentation of the program blocks in the online help of STEP 7.

See also

Program blocks for OUC (Page 51)

LEDs, connections, QR code

2.1 LED display

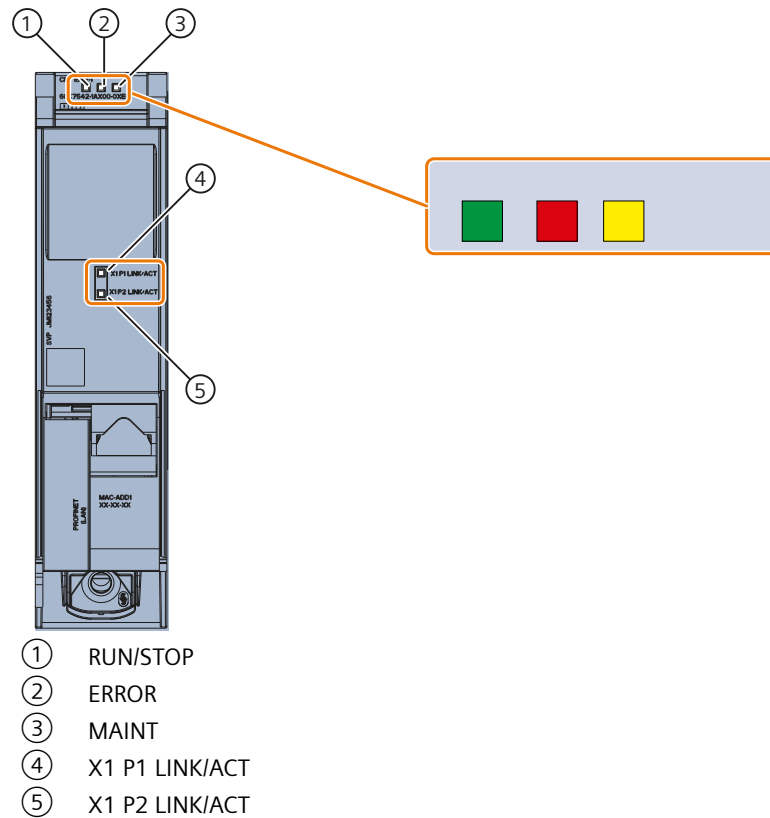


Figure 2-1 LED display of the CM 1542-1 (without front cover)

Meaning of the LED displays

The CM 1542-1 has 3 LEDs to display the current operating status and the diagnostics status and these have the following meanings:

- RUN/STOP (single color green)
- ERROR (single color red)
- MAINT (single color yellow)

2.1 LED display

The following table shows the meaning of the various combinations of colors of the RUN, ERROR and MAINT LEDs.

Table 2-1 Meaning of the LEDs

RUN/STOP	ERROR	MAINT	Meaning
 LED off	 LED off	 LED off	- No supply voltage on the CM or supply voltage too low - The CM was reset to factory settings
 LED lit green	 LED lit red	 LED lit yellow	LED test during startup
 LED lit green	 LED lit red	 LED off	CM startup
 LED lit green	 LED off	 LED off	CM is in RUN mode. No disruptions.
 LED lit green	 LED flashing red	 LED off	A diagnostics event has occurred.
 LED lit green	 LED off	 LED lit yellow	Maintenance is demanded.
 LED lit green	 LED off	 LED flashing yellow	- Maintenance is required - Downloading the user program
 LED lit green	 LED flashing red	-	Duplicate IP address detected. Ethernet interface unreachable.
 LED flashing green	 LED off	 LED off	- No CM configuration exists - Loading firmware
 LED flashing green	 LED flashing red	 LED flashing yellow	Module fault (LEDs flashing synchronized)

Meaning of the LED displays of the PROFINET ports: X1 P1 / X1 P2

To signal whether a connection exists and data is being transferred each port has a two-color LED (green/yellow):

- X1 P1 LINK/ACT
- X1 P2 LINK/ACT

The following table shows the meaning of the various color combinations of the LEDs X1 P1 and X1 P2.

Table 2-2 Meaning of the LEDs

X1 P1 LINK/ACT / X1 P2 LINK/ACT		Meaning
 green off	 yellow off	No connection to PROFINET There is no Ethernet connection between the Ethernet interface of the CM and the communications partner. At the current time, there is no data being received/sent via the Ethernet interface.
 flashing green	 yellow off	The "node flash test" is being performed.
 green on	 yellow off	Connection to PROFINET exists There is an Ethernet connection between the Ethernet interface of the CM and a communications partner.
 green on	 yellow flickers	At the current time, data is being received/sent via the Ethernet interface of the Ethernet device of a communications partner on Ethernet.

2.2 Ethernet interface

The CM has an Ethernet interface for connection to PROFINET.

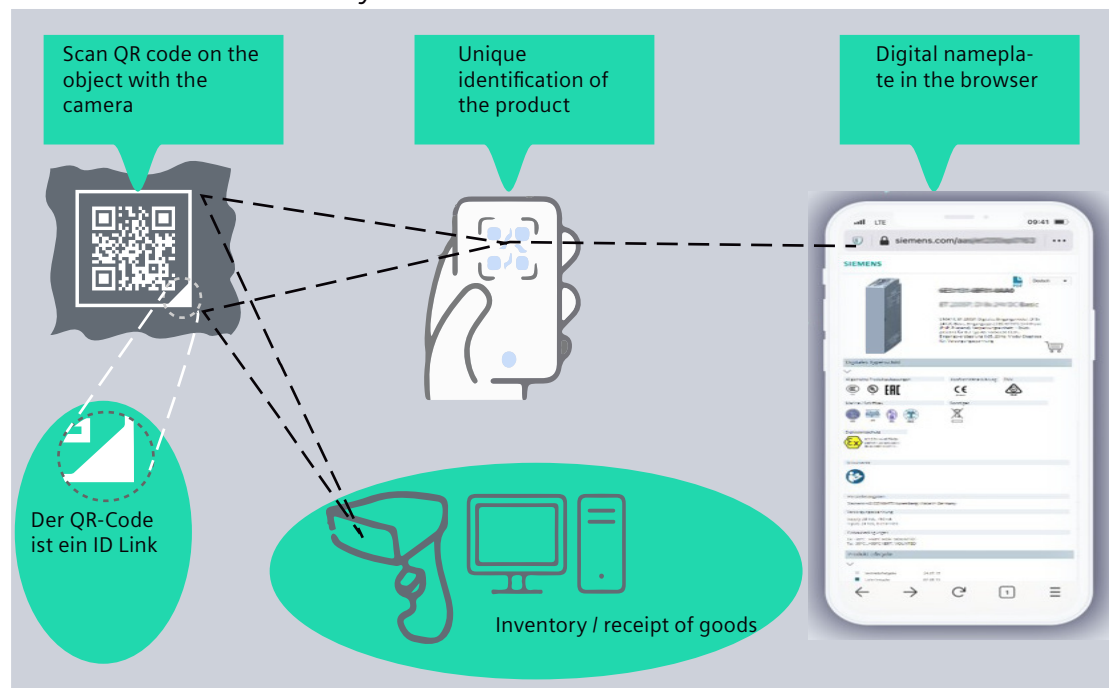
The interface is designed as 2-port switch with two RJ45 sockets.

Refer to section Fast Ethernet (Page 44) for information on the transmission speed and direction dependency.

For information on pin assignment, see section Terminal assignment (Page 65).

2.3 QR code

Identification link - Easy to use



QR code

The QR code on the front of this product and on the packaging uniquely identifies the product.

The QR code is an Identification Link in accordance with IEC 61406-1.

When you scan the QR code, e.g. with a smartphone, you directly open the Siemens web page of the digital nameplate. The web page of the digital nameplate is structured in line with responsive web design.

For your plant documentation, you have the option to connect the link with your data.

Digital nameplate

The digital nameplate is:

- A contribution by Siemens towards reducing the CO₂ footprint and conserving resources.
- An efficient way to access the product information available on the Internet. This information is kept up to date over the entire product life.

You can retrieve the following information about the product on the web page of the digital nameplate:

- Product identification
- User documentation
- Technical specifications

- Certificates, Declaration of Conformity, manufacturer information
- Current software/firmware versions
- Product news and more information

2.3 QR code

Installation, connecting up, commissioning, operation

3

3.1 Important notes on using the device

Safety notices on the use of the device

Note the following safety notices when setting up and operating the device and during all associated work such as installation, connecting up or replacing the device.

3.1.1 Notices on use in hazardous areas

WARNING
--

The device may only be operated in an environment with pollution degree 1 or 2 as described in EN/IEC 60664-1, GB/T 16935.1.
--

WARNING
--

EXPLOSION HAZARD

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

3.1.2 Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex

WARNING
--

Requirements for the cabinet

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 3836.8.

3.1 Important notes on using the device

 WARNING

Suitable cables at high ambient temperatures in hazardous area

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

 WARNING

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).

3.1.3 Notes on use in hazardous areas according to UL HazLoc and FM

 WARNING

The IP degree of protection marking on the nameplate is not associated with FM approval.

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

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

 WARNING

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

 WARNING

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

 WARNING

EXPLOSION HAZARD

The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 °C higher than maximum ambient temperature.

 WARNING

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

 WARNING

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

 WARNING

EXPLOSION HAZARD

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

3.2 Installation, removal and repairs in hazardous areas

 WARNING

Impermissible accessories and spare parts

Risk of explosion in hazardous areas

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

 WARNING

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

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

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

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

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.

3.3 Installation

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

Open equipment

The devices are "open equipment" acc. 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.

Installation

NOTICE

Install and remove the device only when the power is off

Turn off the power supply to the station before you install or remove the module. Installing and removing modules with the power supply on can lead to damage to the modules and to loss of data.

NOTICE

Installation location - Dependency of the temperature range

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

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

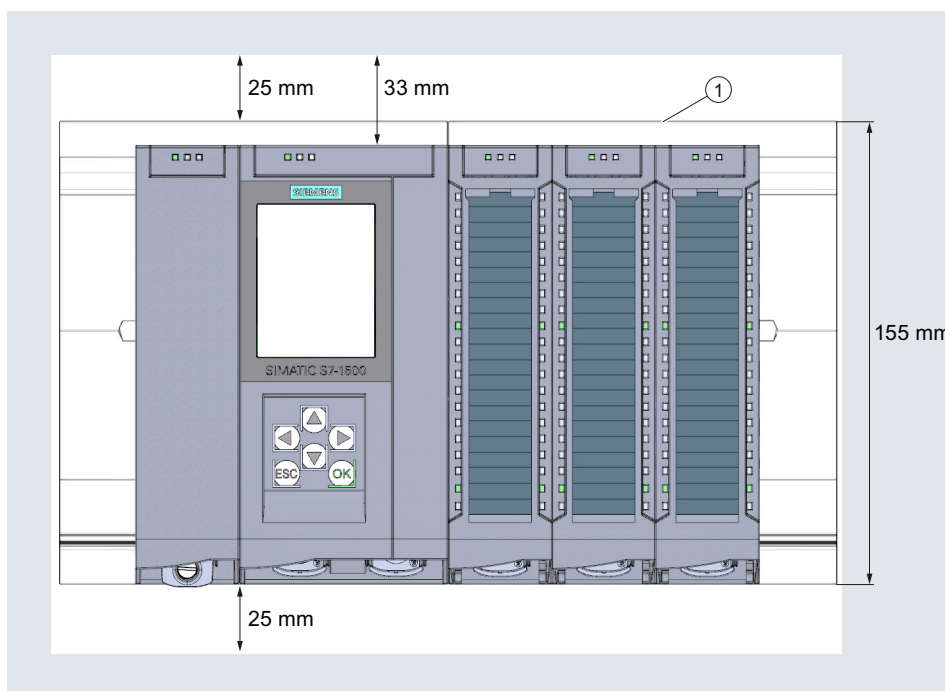
You will find the permitted temperature ranges in the section Technical specifications of the CM (6GK7542-1AX00-0XE0) (Page 63) or Technical specifications of the CM (6GK7542-1AX10-0XE0) (Page 64).

Minimum clearances

Install the module in such a way that its upper and lower ventilation slits are not covered, allowing adequate ventilation as protection from overheating.

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

- Above the module: At least 33 mm
- Below the module: At least 25 mm



Installation of the rack	Installation position of the modules
Horizontal installation of the rack	 A photograph showing a Siemens SIMATIC CM 1542-1 control unit installed horizontally in a rack. The unit is blue and features a small screen and several buttons on its front panel.
Vertical installation of the rack	 A photograph showing a Siemens SIMATIC CM 1542-1 control unit installed vertically in a rack. The unit is blue and features a small screen and several buttons on its front panel.

Installation and commissioning

WARNING

Read the system manual "S7-1500 Automation System"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System" (see section Documentation references (Page 77)).

Make sure that the power supply is turned off when installing/uninstalling the devices.

NOTICE

No plugging and pulling during operation

The CM must not be pulled or plugged during operation.

Configuration

One requirement for the commissioning of the CM is the completeness of the STEP 7 project data.

3.4 Connecting

Procedure for installation and commissioning

Step	Execution	Notes and explanations
1	When installing and connecting up, keep to the procedures described for installing I/O modules in the system manual "S7-1500 Automation System".	
2	Connect the CM to Industrial Ethernet via the RJ45 jack. Where necessary, connect another component to the remaining free RJ45 jack.	Underside of the CM
3	Turn on the power supply.	
4	Close the front covers of the module and keep them closed during operation.	
5	The remaining steps in commissioning involve downloading the STEP 7 project data.	The STEP 7 project data of the CM is transferred when you download to the station. To load the station, connect the engineering station on which the project data is located to the Ethernet interface of the CPU. You will find more detailed information on loading in the following sections of the STEP 7 online help: • "Compiling and loading project data" • "Using online and diagnostics functions"

3.4 Connecting

WARNING

Power supply

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

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

- Only safety extra low voltage (SELV) with limited power source (LPS) complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 or IEC 62368-1 / EN 62368-1 / VDE 62368-1 may be connected to the power supply terminals.

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

Terminal



WARNING

Read the system manual "S7-1500 Automation System"

Prior to installation, connecting up and commissioning, read the relevant sections in the system manual "S7-1500 Automation System", see Cybersecurity information (Page 6), Documentation guide.

Power supply off

Make sure that the power supply is turned off when connecting the devices.

Procedure

1. Connect the communications module to Industrial Ethernet via the RJ45 jack (lower side of the device).

Note

Connecting a switch

To connect a switch that does not support autocrossing, use a crossover cable.

For the pin assignment of the Ethernet interface, see section Terminal assignment (Page 65).

2. Switch on the power supply of the S7 station.
 3. Close the front covers of the modules.
- During operation, keep the hinged front panel closed.

3.5 Mode of the CPU - effect on the CM

Changing the CPU from RUN to STOP

You can switch the operating mode of the CPU between RUN and STOP via STEP 7.

Note

RUN/STOP LED of the CM

The green RUN/STOP LED of the CM continues to be lit green regardless of the STOP mode of the CPU.

When the CPU is in STOP mode, the CM remains in RUN mode.

3.6 Disassembly

The following behavior applies to the CM:

- This applies to established connections (S7, ISO Transport, ISO-on-TCP, TCP, UDP):
 - Programmed connections are terminated.
 - Configured connections are retained.
- The following functions remain enabled:
 - Configuration and diagnostics of the CM
System connections for configuration, diagnostics and PG channel routing are retained.
 - Web diagnostics
 - S7 routing function
 - Time-of-day synchronization

3.6 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.

Configuration, program blocks

4.1 Industrial Cybersecurity

Observe the following security recommendations to prevent unauthorized access to the system.

General

- You should make regular checks to make sure that the device meets these recommendations and other internal security guidelines if applicable.
- Evaluate your plant as a whole in terms of security. Use a cell protection concept with suitable products.
- Do not connect the device directly to the Internet. Operate the device within a protected network area.
- Check regularly for news on the Siemens Internet pages.
 - You can find information on Industrial Security here:
Link: (<http://www.siemens.com/industrialsecurity>)
 - You can find a selection of documentation on the topic of network security here:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/92651441>)
- Keep the firmware up to date. Check regularly for security updates of the firmware and use them.
Information regarding product news and new firmware versions is available at the following address:
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/pm>)

Physical access

Restrict physical access to the device to qualified personnel.

Network attachment

Do not connect the CM directly to the Internet. If a connection from the CM to the Internet is required, arrange for suitable protection before the CM, for example a SCALANCE S with firewall.

Security functions of the product

Use the options for security settings in the configuration of the station. These includes among others:

- Protection levels and security functions of the CPU
Configure access to the CPU under "Protection and Security".
Use the other security functions of the CPU to prevent unauthorized access to the station.
- Security function of the communication
 - Use the secure protocol variant HTTPS when accessing the Web server of the CPU.
 - If you do not require access to the Web server, leave access to the Web server of the CPU (CPU configuration) and to the Web server of the CM disabled.
- Protection of the passwords for access to program blocks
Protect the passwords stored in data blocks for the program blocks from being viewed. You will find information on the procedure in the STEP 7 information system under the keyword "Know-how protection".

Passwords

- Define rules for the use of devices and assignment of passwords.
- Regularly update the passwords to increase security.
- Only use passwords with a high password strength. Avoid weak passwords for example "password1", "123456789" or similar.
- Make sure that all passwords are protected and inaccessible to unauthorized personnel. See also the preceding section for information on this.
- Do not use one password for different users and systems.

Protocols

Secure and non-secure protocols

- Only enable protocols that you require to use the system.
- Use secure protocols when access to the device is not prevented by physical protection measures.

Note that, for example, the e-mail function uses a non-secure protocol via the "TMAIL_C" program block.

Table: Meaning of the column titles and entries

The following table provides you with an overview of the open ports on this device.

- **Protocol / function**
Protocols that the device supports.
- **Port number (protocol)**
Port number assigned to the protocol.

- **Default of the port**
 - Open
The port is open at the start of the configuration.
 - Closed
The port is closed at the start of the configuration.
- **Port status**
 - Open
The port is always open and cannot be closed.
 - Open after configuration
The port is open if it has been configured.
 - Open (login, when configured)
As default the port is open. After configuring the port, the communication partner needs to log in.
 - Open with block call
The port is only opened when a suitable program block is called.
- **Authentication**
Specifies whether or not the protocol authenticates the communication partner during access.

Protocol / function	Port number (protocol)	Default of the port	Port status	Authentication
S7 communication	102 (TCP)	Open	Open	No
HTTP	80 (TCP)	Closed	Open after configuration	No
SNMP	161 (UDP)	Open	Open	No
PROFINET	34964 (UDP)	Open	Open	No

Ports of communication partners and routers

Make sure that you enable the required client ports in the corresponding firewall on the communication partners and in intermediary routers.

These can be:

- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP) - in the CM open on block call (only outgoing)

4.2 Network settings

4.2.1 Fast Ethernet

Transmission speed/directionality of the interface

- CM 1542-1 (6GK7542-1AX00-0XE0)
Only "Automatic" for automatic detection (autosensing) and "100 Mbps full duplex" can be set for the transmission speed/directionality of the connection.
In normal situations, the basic setting ensures troublefree communication.
- CM 1542-1 (6GK7542-1AX10-0XE0)
In PROFINET operation, the CM only supports "100 Mbps full duplex".

Auto-crossover mechanism

With the integrated auto-crossover mechanism, it is possible to use a standard cable to connect the PC/PG. A crossover cable is not necessary.

To connect a switch that does not support auto-crossover, use a crossover cable.

4.3 IP configuration

4.3.1 Restart after detection of a duplicate IP address in the network

To save you timeconsuming troubleshooting in the network, during startup the CM detects double addressing in the network.

Behavior when the CM starts up

If double addressing is detected when the CM starts up, the CM changes to RUN and cannot be reached via the Ethernet interface. The ERROR LED flashes.

4.3.2 Remove retentive storage of the IP address if there are duplicate addresses

The IP address and the device name of the CM 1542-1 remain installed retentively:

If, for example during startup, the CM detects a duplicate address in another network, the CM is not connected to the network. The CM changes to RUN and cannot be reached via the Ethernet interface.

To be able to connect the CM to the network, you can remove the retentively stored IP address as follows:

1. Set the CPU to STOP.
2. Remove the memory card of the CPU.
3. With SINEC PNI via DCP, set the IP address of the CM to 0.0.0.0 without configuration. You have removed the retentively stored IP address of the CM. The CM can be integrated into the network.
4. Insert the memory card in the CPU again.

Note

If you reset the CM to factory settings, the retentively saved IP address is also removed.

4.3.3 IP routing

IP routing via the backplane bus

The function enables static IPv4 routing between communications modules in a rack via the backplane bus. This means that routing between two subnets that are connected via two communications modules of the station is enabled.

The function is supported by the following modules:

- CP 1545-1
- CM 1542-1
As of firmware version V2.0
- CP 1543-1
 - As of firmware version V2.0 with disabled security functions
 - As of firmware version V2.1 with enabled security functions

You can use IP routing, for example, for Web server access by lower-level modules.

With IP routing, the data throughput is limited to 1 Mbps. Remember this in terms of the number of modules involved and the expected data traffic via the backplane bus.

Restrictions

- IPv4 routing via the communications module into the CPU of the station is not possible.
- The TTL value is reduced by more than 1 when routing via the backplane bus.

Configuration

You reach the function in STEP 7 via:

"Ethernet interface > Ethernet addresses > IP routing between communications modules"

IP routing must be activated in at least 2 modules of a station.

4.3 IP configuration

IP routing runs via the configured default router.

Please note:

If you wish to use IP routing, you can only configure a router for one communications module in the station.

IP configuration with CM 1542-1 as PROFINET IO controller

If the CM with enabled IPv4 routing is used as PROFINET IO controller via the backplane bus, observe the following for IP configuration of the lower-level IO devices:

If the IP address of the lower-level IO devices was configured permanently (option "Set IP address in the project"), no IPv4 routing via the CM to the IO devices is possible.

To enable IPv4 routing via the CM to the lower-level IO devices, the following must be set in the IP configuration of the IO devices:

- First, enable the "Use router" option on the IO device.
Copy the IP address of the IO controller (CM) into the router address field.
- Then, enable the "IP address is set directly at the device" option on the IO device.

4.3.4 Virtual interface of the CPU

CM 1542-1 (6GK7542-1AX10-0XE0) as of V4.2 supports the virtual interface of the CPU.

Requirement

The following requirements must be met to use the virtual interface of the CPU:

- S7-1500 CPU firmware V2.8 or higher
- CM 1541-1
 - CM "AX10" as of firmware version V4.2
- Configurability
 - As of STEP 7 V21

Virtual interface of the CPU

As of firmware version V2.8, the S7-1500 CPU offers the option of reaching its IP-based applications, such as OPC UA client and server, not only via its local PROFINET interfaces, but also via the interface of a CM "AX10" in the same station.

The virtual interface is called W1.

Features of the virtual interface

The virtual interface is not a fully diagnosable interface with the familiar properties of conventional interfaces. The virtual interface is not displayed in the graphical views, because the internal connection via the backplane bus does not represent an S7 subnet and does not have any ports. A physical connection by means of a network cable therefore cannot be established.

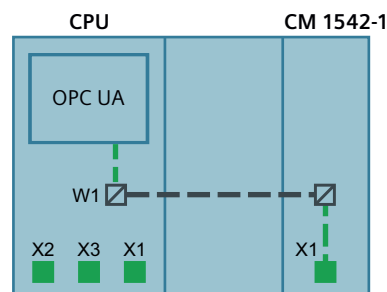
The following IP-based services can also be reached via the virtual interface:

- OPC UA (client and server)
- Programmed OUC connections
- S7 communication: ES/HMI access and instructions for S7 communication such as PUT/GET

The IP address of the virtual interface is displayed in STEP 7 and in the display of the CPU.

The activated interface can be used in the configuration of the communication partners.

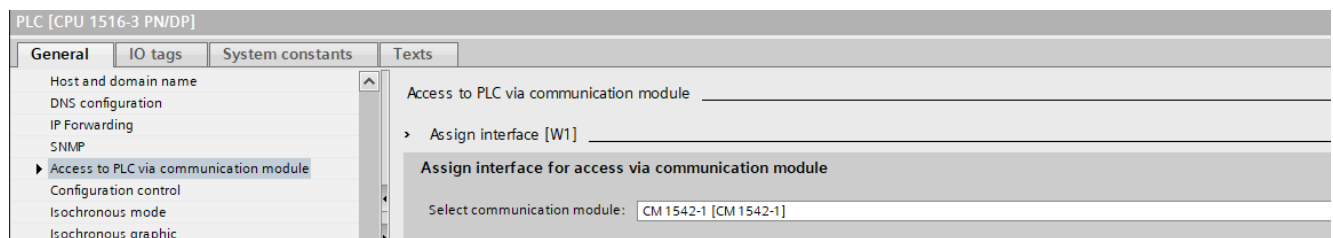
For information on the restrictions of the virtual interface as compared to physical interfaces, see the STEP 7 information system.



Configuration of the virtual interface W1

The virtual interface of the CPU is configured in STEP 7 in the parameter group "Advanced configuration > Access to PLC via communication module".

Here, the virtual interface is assigned to a CM of the station, via which external access to the CPU can take place. The configured CMs of the station can be selected in the drop-down list.



After selecting the CM, configure the IP and PROFINET parameters of the virtual interface.

Observe the following rules:

- The IP address of the virtual interface and the IP addresses of the PROFINET interfaces of the CPU must be in different subnets

After loading the configuration data, the CPU services such as the OPC UA server can be reached via the CM and the virtual interface.

The IP address of the virtual interface is shown in the list of server addresses in the properties dialog of the OPC UA server of the CPU. Created connections and S7 communication (e.g. HMI and BSEND, BRCV) run over this interface.

The IP address of the virtual interface W1 is not listed under the currently displayed local interfaces (Xn) in the device display, but under "Addresses" in the "Settings" section. The

4.3 IP configuration

virtual interface is also visible when no CM is plugged or when the virtual interface is deactivated. If there is no IP configuration, the IP address and subnet mask are shown with 0.0.0.0.

The virtual interface W1 is displayed in the diagnostics view under "Online & Diagnostics".

The hardware ID of the virtual interface is displayed in the system constants in the CPU properties.

Note

Address change during runtime and restart

When the IP parameters of the virtual interface are loaded, you can then change them via the display of the CPU, via T_CONFIG or online.

However, note that the originally loaded configuration will be active again after a restart of the CPU.

Configuration changes

A change of the assigned CM may have an effect on the configuration of the virtual interface:

- Changes in the configuration
 - Assignment of a different CM
The configuration is adopted for the new CM.
 - Deselect the assigned CM
The virtual interface W1 is deactivated and the configuration is lost.
When a CM is assigned again, you need to configure the virtual interface again.
- Changes to the station configuration
 - Move the CM
If the CM is only moved to another slot of the device, the configuration remains valid.
 - Remove the CM
If the CM is removed from the station, the configuration is retained in the CPU.
In the drop-down list of the parameter group of the CPU, the CM is displayed as missing and compiling the configuration indicates an error. To rectify this, the missing CM can be deselected or another CM can be assigned.

4.3.5 CM in multiple use IO systems (standard machines)

Multiple use IO system in standard machines

In PROFINET IO controller mode, the CM can be used in standard machines of the same type.

After configuration, the address parameters of the CM are adapted to the required settings. With suitable configuration of the CM, the lower-level IO devices adopt the address parameters from the CM.

Requirements in the configuration

In terms of configuration it is assumed that the standard machine is delivered with a configured PROFINET IO system and the CM is the IO controller to which several IO devices are assigned in the PROFINET IO system.

The following requirements must be met in the configuration:

- PROFINET IO system
In the configuration of the PROFINET IO system, the option "Multiple use IO system" was activated in the "General" tab. This makes the IO system a standard machine project in the STEP 7 project.
- IO controller (CM) > PROFINET interface
 - In the Ethernet addresses of the CM, the following option is activated under "PROFINET": "PROFINET device name is set directly at the device"
 - In the advanced options the following option is activated in the interface options: "Permit overwriting of device names of all assigned IO devices"
- IO devices > PROFINET interface
With the lower-level IO devices there are also some settings to be made that are described in the STEP 7 information system.

Help in the STEP 7 information system

You will find the required information in the STEP 7 information system with the following search term:

- Creating a standard machine project

Changing address parameters at runtime

After the standard machine has started up, you can adapt the preset address parameters using the following methods:

- Using the following STEP 7 commissioning tools:
 - SINEC PNI
 - PRONETA
- From the user program using the program block "IP_CONFIG"
- Using the program block "T_CONFIG"

4.4 Media redundancy

You can use the CM in a ring topology with media redundancy.

For more detailed information on configuration, refer to the STEP 7 online help of the "Media redundancy" parameter group.

4.5 Time-of-day synchronization

Note

Recommendation for setting the time

Synchronization with a external clock at intervals of approximately 10 seconds is recommended. This achieves as small a deviation as possible between the internal time and the absolute time.

Procedure

When the option is enabled the CM sends timeofday queries at regular intervals to an NTP server and synchronizes its local time of day.

The time is also be forwarded automatically to the CPU modules in the S7 station allowing the time to be synchronized in the entire S7 station.

The CM supports the following mode for time-of-day synchronization:

- NTP (NTP: Network Time Protocol)

Four NTP servers can be configured in STEP 7.

If you use the program block "T_CONFIG" together with the "SDT CONF_DATA" for assigning the parameters of NTP servers, you can use four additional NTP servers.

Configuration

For information on configuration, refer to the STEP 7 online help of the "Time-of-day synchronization" parameter group.

- **Accept time of day from non-synchronized NTP servers**

The parameter has the following effect:

- If the option is enabled, the CM also accepts the time-of-day from non-synchronized NTP servers with stratum 16.
- If the option is disabled, the response is as follows: If the CM receives a time-of-day frame from an unsynchronized NTP server with stratum 16, the time of day is not set according to the frame. In this case, none of the NTP servers is displayed as "NTP master" in the diagnostics; but rather only as being "reachable".

4.6 Disabling SNMP via data record

Disabling SNMP via user program

As of firmware version V4.0 of the CM, you can disable enabled SNMP functions in the CM via the user program.

To do this, use the block WRREC.

Disabling SNMP with WRREC

Create a data block with the following structure of the data record 0xB071 and transfer the data record to the CM using WRREC. In WRREC, you use the CM interface as the hardware identifier.

Static		
snmp_record	Struct	
• BlockID	UInt	16#F003
• BlockLength	UInt	8
• Version	USInt	1
• Subversion	USInt	0
• Reserved	UInt	0
• SNMPControl *	UDInt	0

* SNMPControl = TRUE: SNMP is enabled.
 SNMPControl = FALSE: SNMP is disabled.

More detailed information on enabling/disabling SNMP is available in the information system of STEP 7 and in the Communication Function Manual, see Cybersecurity information (Page 6), Documentation Guide.

For information on diagnostics via SNMP, see section SNMP (Page 55).

4.7 Program blocks for OUC

Programming Open User Communication (OUC)

The instructions (program blocks) listed below are required for the following communication services via Ethernet:

- TCP
- ISO-on-TCP
- UDP (Multicast)
- E-mail

For this, create suitable program blocks. The program block can be found in STEP 7 in the "Instructions > Communication > Open user communication" window.

You will find details on the program blocks in the information system of STEP 7.

Note

Different program block versions

Note that in STEP 7 you cannot use different versions of a program block in a station.

Supported program blocks for OUC

The following instructions in the specified minimum version are available for programming Open User Communication:

- **TSEND_C V3.1 / TRCV_C V3.1**

Compact blocks for connection establishment/termination and for sending and receiving data

As an alternative:

- **TCON V4.0 / TDISCON V2.1**

Connection establishment / connection termination

- **TUSEND V4.0 / TURCV V4.0**

Sending and receiving data via UDP

- **TSEND V4.0 / TRCV V4.0**

Sending and receiving data via TCP or ISOonTCP

- **TMAIL_C V4.0**

Sending e-mails

Note the description of TMAIL_C as of version V4.0 in the STEP 7 information system.

Note

Personal data unencrypted in TMAIL_C

Note that TMAIL_C uses personal data, such as user name and password, in its parameters. This data is stored unencrypted in a data block.

- **T_CONFIG**

Program-controlled configuration of the PROFINET interfaces of a CPU or the Ethernet interface of a CP/CM

Connection establishment and termination

Connections are established using the program block TCON. Note that a separate program block TCON must be called for each connection.

A separate connection must be established for each communications partner even if identical blocks of data are being sent.

After a successful transfer of the data, a connection can be terminated. A connection is also terminated by calling "TDISCON".

Note

Connection abort

If an existing connection is aborted by the communications partner or due to disturbances on the network, the connection must also be terminated by calling TDISCON. Make sure that you take this into account in your programming.

Connection descriptions in system data types (SDTs)

For the connection description, the blocks listed above use the parameter CONNECT (or MAIL_ADDR_PARAM with TMAIL_C). The connection description is stored in a data block whose structure is specified by the system data type (SDT).

Creating an SDT for the data blocks

You create the SDT required for every connection description as a data block. You generate the SDT type in STEP 7 by entering the name (e.g. "TCON_IP_V4") in the "Data type" box manually in the declaration table of block instead of selecting an entry from the "Data type" drop-down list. The corresponding SDT is then created with its parameters.

The following SDTs can be used.

- **Configured connections:**
 - **TCON_Configured**
For transferring frames via TCP
- **Programmed connections:**
 - **TCON_IP_V4**
For transferring frames via TCP or UDP
 - **TCON_QDN**
For transferring frames via TCP or UDP
 - **TCON_IP_RFC**
For transferring frames via ISO-on-TCP
 - **TMail_V4**
For transferring e-mails addressing the e-mail server using an IPv4 address
 - **IF_CONF_V4**
Block "T_CONFIG", parameter "CONF_DATA": Program-controlled configuration of the parameters of the CM/CP
 - **IF_CONF_NOS**
Block "T_CONFIG", parameter "CONF_DATA": Program controlled configuration of the PROFINET device name of the CM
 - **IF_CONF_NTP**
Block "T_CONFIG", parameter "CONF_DATA": Programmatic configuration of up to 4 NTP servers
 - **IF_CONF_MAC**
Block "T_CONFIG", parameter "CONF_DATA": Program-controlled configuration of the MAC address of the CM/CP

Note:

The address parameters can only be configured with temporary validity in the CP. In the respective "IF_CONF_..." SDT, the "Mode" = 2 parameter must be set.

You will find the description of the SDTs with their parameters in the STEP 7 information system under the relevant name of the SDT.

Diagnostics and upkeep

5.1 Diagnostics

5.1.1 Diagnostics options

Diagnostics options

You have the following diagnostics options available for the module:

- The LEDs of the module
For information on the LED displays, refer to the section LEDs, connections, QR code (Page 25).
- STEP 7: The "Diagnostics" tab in the Inspector window
Here, you can obtain the following information on the selected module:
 - Information on the online status of the module
- STEP 7: Diagnostics functions in the "Online > Online and diagnostics" menu
Here, you can obtain static information on the selected module:
 - General information on the module
 - Diagnostics status
 - Extended diagnostic functions
 - Information on the PROFINET interface

You will find further information on the diagnostics functions of STEP 7 in the STEP 7 online help.

- Web diagnostics
With the aid of Web diagnostics of the CPU, you read the diagnostics data from an S7 station via the Web browser on the PG/PC.
- Display of the CPU
Using the CPU display, read out diagnostics data from an S7 station on the PG/PC.
You can only use diagnostics via the CPU display if the S7 station is suitably configured.

5.1.2 SNMP

SNMP (Simple Network Management Protocol)

SNMP is a protocol for diagnostics and managing networks and nodes in the network. To transmit data, SNMP uses the connectionless UDP protocol.

The information on the properties of SNMP-compliant devices is entered in MIB files (MIB = Management Information Base).

You will find detailed information on SNMP and the Siemens Automation MIB in the "Diagnostics and Configuration with SNMP" manual, see /3/ (Page 78).

For information on disabling SNMP, see section Disabling SNMP via data record (Page 50).

Range of performance of the CM

The CM supports the following SNMP versions:

- **SNMPv1**

Traps are not supported by the CM.

The CM supports the following MIBs:

- **MIB II (acc. to RFC1213)**
The CM supports the following groups of MIB objects:
 - System
 - Interfaces
 - IP
 - ICMP
 - TCP
 - UDP
 - SNMP
- **LLDP MIB**
- **MRP Monitoring**
- **Siemens Automation MIB**

Write permissions

Write access is permitted only for the following MIBs and MIB objects:

- Siemens Automation MIB, group "System"
The group returns status information about the CM interfaces.
Write access is permitted only for the following MIB objects:
 - sysContact
 - sysLocation
 - sysName
- MRP Monitoring, object "mrpDomainResetRoundTripDelays"
A write command "resetDelays(1)" to the object sets the values of "mrpDomainRoundTripDelayMax" and "mrpDomainRoundTripDelayMin" to zero.

For all other MIB groups and objects, only read access is possible for security reasons.

Access permissions using community names

The CM uses the following community strings to control the rights for authentication of the access to its SNMP agent via SNMPv1:

Table 5-1 Access rights and authentication in the SNMP agent

Type of access	Community string for authentication *)
Read access	public
Read and write access	private

*) Note the use of lowercase letters!

Note

Security of the access

For security reasons, change the generally known strings "public" and "private".

Disable SNMP

If you do not want your CM to respond to SNMP requests, then you can disable the SNMP agent of the CM via the data record B071_H.

5.2 Maintenance



! CAUTION

Hot surfaces

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

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

! WARNING

Cleaning the housing

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

Do not use any liquids or solvents.



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.

5.2.1 Update firmware

New firmware versions of the module

If a new firmware version is available for the module, you will find this on the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/dl>)

Firmware files have the file format *.upd.

Save the firmware file on your PC.

There are different ways of loading a new firmware file into the module:

- Online functions of STEP 7 via Ethernet
- Loading the firmware file into the CPU from an SD card

Note

SD card only for firmware file

For the firmware file, you need a SIMATIC SD memory card, for example (article numbers):

- 6AV6671-8XB10-0AX1
- 6AV2181-8XP00-0AX0
- 6AV2181-8AQ10-0AX0

The firmware update card may not contain any other files. An SD card with configuration data cannot be used.

Note

Duration of the firmware update

Downloading a new firmware file can take several minutes.

Always wait until the completion of the firmware update can be recognized from the LEDs (see below).

Loading the firmware with the online functions of STEP 7 via Ethernet

Requirements:

- The CPU of the station is accessible via Ethernet.
- The engineering station and the CPU are located in the same subnet.
- The new firmware file is stored on your engineering station.
- The engineering station is connected to the network.
- The relevant STEP 7 project is open on the engineering station.

Procedure:

1. Select the station that you want to update with a new firmware.
2. Enable the online functions using the "Connect online" icon.
3. In the "Connect online" dialog, select the Ethernet interface in the "Type of PG/PC interface" list box.
4. Select the CPU of the station.
5. Click on "Start search" to search for the module in the network and to specify the connection path.
When the module is found it is displayed in the table.
6. Connect using the "Connect" button.
The "Connect online" wizard guides you through the remaining steps in installation.
7. Select the CPU in the network view and select the "Online & Diagnostics" shortcut menu (right-click).
8. In the navigation panel of the Online & Diagnostics view, select the entry "Functions > Firmware update".
9. Using the "Browse" button (parameter group "Firmware loader") search for the new firmware file in the file system of the engineering station.
10. Start to download the firmware with the "Start update" button when the correct version of the signed firmware is displayed in the "Status" output box.

You will find further information on the online functions in the STEP 7 information system.

Loading the firmware via the SD card

You can find detailed information on using an SD card in the S7-1500 System Manual, see Cybersecurity information (Page 6), Documentation guide.

Requirements:

- You have copied the new firmware file from your PC to the SD card using a suitable card reader.
- Optional: You have saved a backup file of the currently used firmware file.

Procedure:

1. Set the operating mode switch of the CPU to STOP.
Ensure that no write functions (e.g. online or test functions) are active in the STOP state.
2. Remove the SIMATIC Memory Card with the configuration data from the slot of the CPU.
3. Insert the SD card with the firmware file in the card slot of the CPU.
The firmware update starts shortly after the card has been inserted. The display shows the following: "STOP - FW UPDATE"
If errors occur, appropriate messages are displayed.
After completing the firmware update, the display shows a result page.
A successful firmware update can be recognized by the following LED pattern from the CPU:
 - RUN lights up yellow.
 - MAINT flashing yellow.
4. Remove the SD card and insert the SIMATIC Memory Card again.
5. Set the operating mode switch of the CPU to RUN.
The module uses the new firmware during startup.

For the LED pattern of the module during startup, refer to section LEDs, connections, QR code (Page 25).

5.2.2 Reset to factory settings

Requirement

- If you initiate the reset to factory settings from the project context, there must be an online connection to the affected CM.
- The relevant CPU is in STOP mode.

Note

If the CPU is still in RUN mode and you start the reset operation, you can place it in STOP mode after acknowledging a confirmation prompt.

Procedure

To reset a CM to factory settings, follow the steps below:

1. Open the Online and Diagnostics view of the CM (either from the project context or via "Accessible devices").
2. In the "Functions" folder, select the "Reset to factory settings" group.
3. Click the "Reset" button.
4. Respond to the confirmation prompt with "Yes".
Result: After successful reset, the CM restarts and is then no longer reachable for the CPU. The status of the status LED is "Off".
5. To remove the CM from the station, disconnect the station from the power.

Result

The module is reset to the factory settings. This means:

- All parameters are reset to their defaults.
- The I&M data are deleted except for I&M0 data.
- The IP address is deleted.

5.2.3 Module replacement

General procedure

The configuration data of the module is stored on the CPU. This makes it possible to replace this module with a module of the same type (identical article number) without a programming device.

If you want to exchange a module with the article number of the predecessor module for a newer module with the current article number (same module name), the data of the older module is adopted when the newer module starts.

Note**Note the power loss**

When replacing an older module with a new module, note the power loss of the new module, see section Technical specifications (Page 63).

Check whether the power supply of the station is still ensured with the new module.

Technical specifications

6.1 Technical specifications of the CM (6GK7542-1AX00-0XE0)

You will find the product functions in the section Properties and functions (Page 15).

Observe the information in the System Manual S7-1500 automation system /1/ (Page 77).

In addition to the information in the system description, the following technical specifications apply to the module.

Technical specifications - 6GK7542-1AX00-0XE0	
Product name	CM 1542-1
Article number	6GK7542-1AX00-0XE0
Attachment to Industrial Ethernet	
Quantity	1 x PROFINET interface with 2-port switch
Design	2 x RJ45 socket, galvanically isolated
Properties	• Standard • Transmission speeds • Other properties
	• 100BASE-TX, IEEE 802.3-2005 • 10 / 100 Mbps • Half duplex/full duplex, auto-crossover, auto-negotiation
Aging time	5 minutes
Special features of the ports X1 P1 and X1 P2	Integration in ring topology / MRP possible
Power supply	
Design	Via S7-1500 backplane bus (15 V)
Further electrical data	
Current consumption (typical)	220 mA from S7-1500 backplane bus
Active power loss (typical)	3.3 W
Overvoltage category according to IEC / EN 60664-1	Category II
Permissible ambient conditions	
Ambient temperature *	During operation with the rack installed horizontally
	0 °C ... +60 °C
	During operation with the rack installed vertically
	0 °C ... +40 °C
	During storage
	-40 °C ... +70 °C
	During transportation
	-40 °C ... +70 °C
Relative humidity	During operation
	≤ 95 % at 30 °C, no condensation
Permitted contaminant concentration	Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3
Design, dimensions and weight	
Module format	Compact module S7-1500, single width
Degree of protection	IP20

6.2 Technical specifications of the CM (6GK7542-1AX10-0XE0)

Technical specifications - 6GK7542-1AX00-0XE0	
Weight	400 g
Dimensions (W x H x D)	35 x 147 x 129 mm
Mounting type	Mounting in S7-1500 rack, S7-1500 mounting bar installation

* Also read the information in the Ambient temperature (Page 66) section.

6.2 Technical specifications of the CM (6GK7542-1AX10-0XE0)

You will find the product functions in the section Properties and functions (Page 15).

Observe the information in the System Manual S7-1500 automation system /1/ (Page 77).

In addition to the information in the system description, the following technical specifications apply to the module.

Technical specifications - 6GK7542-1AX10-0XE0	
Product name	CM 1542-1
Article number	6GK7542-1AX10-0XE0
Attachment to Industrial Ethernet	
Quantity	1 x PROFINET interface with 2-port switch
Design	2 x RJ45 socket, galvanically isolated
Properties	• Standard • Transmission speeds • Other properties
	• 100BASE-TX, IEEE 802.3-2005 • 100 Mbps • Full duplex, auto-crossover • In PROFINET operation, only 100 Mbps full duplex
Aging time	5 minutes
Special features of the ports X1 P1 and X1 P2	Integration in ring topology / MRP possible
Power supply	
Design	Via S7-1500 backplane bus (15 V)
Further electrical data	
Current consumption (typical)	200 mA from S7-1500 backplane bus
Active power loss (typical)	3 W
Overvoltage category according to IEC / EN 60664-1	Category II
Permissible ambient conditions	
Ambient temperature *	During operation with the rack installed horizontally
	-30 °C ... +60 °C, without condensation or ice
	During operation with the rack installed vertically
	-30 °C ... +40 °C, without condensation or ice
	During storage
	-40 °C ... +70 °C
	During transportation
	-40 °C ... +70 °C
Relative humidity	During operation
	≤ 95 % at 30 °C, no condensation

Technical specifications - 6GK7542-1AX10-0XE0

Permitted contaminant concentration Corrosive gas test according to ISA-S71.04 severity level G1, G2, G3

Design, dimensions and weight

Module format Compact module S7-1500, single width

Degree of protection IP20

Weight 260 g

Dimensions (W x H x D) 35 x 147 x 129 mm

Mounting type Mounting in S7-1500 rack, S7-1500 mounting bar installation

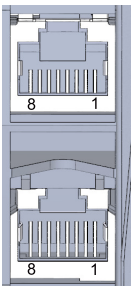
* Also read the information in the Ambient temperature (Page 66) section.

6.3 Terminal assignment

PROFINET interface X1 with 2-port switch

The table below shows the pin assignment of the ports of the PROFINET interface (RJ-45 jack). The assignment corresponds to the Ethernet standard IEEE 802.3.

Table 6-1 Pin assignment of the PROFINET interface with 2-port switch

View	No.	Terminal	Designation
	1	TD	Transmit Data +
	2	TD_N	Transmit Data -
	3	RD	Receive Data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive Data -
	7	GND	Ground
	8	GND	Ground

6.4 Permitted cable lengths - Ethernet

Permitted cable lengths - Ethernet	Alternative combinations per length range
0 ... 55 m	- Max. 55 m IE TP Torsion Cable with IE FC RJ45 Plug 180 - Max. 45 m IE TP Torsion Cable with IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet
0 ... 85 m	- Max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable with IE FC RJ45 Plug 180 - Max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet
0 ... 100 m	- Max. 100 m IE FC TP Standard Cable with IE FC RJ45 Plug 180 - Max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet

See also Siemens Mall: (<https://mall.industry.siemens.com>)

6.5 Ambient temperature

Restrictions of the maximum specified ambient temperature

The maximum permissible temperatures of the module for altitudes up to 2000 m can be found above in the technical specifications.

When using the module at higher altitudes, the decrease in the cooling effect due to convection as a result of the lower air pressure must be taken into account. According to IEC 61010-2-201 CD2 2015, the temperature at altitudes > 2000 m must be reduced.

The following derating factors and maximum ambient temperatures apply.

Table 6-2 Restrictions of the maximum permissible ambient temperature in relation to the installation altitude

Installation altitude (Height above mean sea level)	Derating factor ¹⁾	Maximum ambient temperature when the rack is mounted horizontally
-1000 m to 2000 m	1.00	60 °C
2000 m to 3000 m	0.93	56 °C
3000 m to 4000 m	0.86	52 °C
4000 m to 5000 m	0.78	47 °C

¹⁾ Basic value for applying the derating factor is the maximum permissible ambient temperature in °C for 2000 m.

Note

- The derating factors compensate for the decreasing cooling effect of air at higher altitudes due to lower density.
- Linear interpolation between altitudes is permissible.

6.6 Resistance to harmful gases according to ISA-71.04

The devices listed in the scope of validity meet the following requirements regarding resistance to harmful gases:

Corrosive gases as airborne contaminants Reactive species H ₂ S and SO ₂	ISA-71.04 severity level	G1, G2, G3 RH ≤ 75%, no condensation
	Test according to	IEC 60068-2-42 (SO ₂ 10ppm)
		IEC 60068-2-43 (H ₂ S 1ppm)

Approvals

Approvals issued

Note

Issued approvals on the type plate of the device

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

Certificates for shipbuilding and national approvals

The device certificates for shipbuilding and special national approvals can be found in Siemens Industry Online Support on the Internet:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/cert>)

Documents on the Internet

You will find the declarations of conformity listed below and certificates of the product on the Internet at the following address:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/cert>)

You can see the current versions of the standards in the relevant certificate, which you will find on the Internet at the address specified above.

Address for declarations of conformity

The EU and the UK declarations of conformity are available to all responsible authorities at:

Siemens Aktiengesellschaft
Digital Industries
P.O. Box 48 48
90026 Nuremberg
Germany

EU declaration of conformity



The device meets the requirements and safety objectives of the following EC directives and it complies with the harmonized European standards (EN) for programmable logic controllers which are published in the official documentation of the European Union.

- **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 26 February 2014 on the approximation of the laws of the member states relating to electromagnetic compatibility; official journal of the EU L96, 29/03/2014, p. 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

UK Declaration of Conformity



Importer UK:

Siemens plc
Sir William Siemens House
Princess Road
Manchester
M20 2UR

The product meets the requirements of the following directives:

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

ATEX / IECEx / UKEX / CCC-Ex

Observe the information in the "Use of subassemblies/modules in a Zone 2 Hazardous Area" document, which you will find here:

- On the documentation DVD supplied with the product, under:
"All documents" > "Use of subassemblies/modules in a Zone 2 Hazardous Area"
- On the Internet at the following address:
Link: (<https://support.industry.siemens.com/cs/ww/en/view/78381013>)

The conditions must be met for safe usage of the product according to the section Notes on use in hazardous areas according to ATEX / UKEX / IECEx / CCC-Ex (Page 31).

The product meets the explosion protection requirements outlined below.

IECEx

Classification: Ex ec IIC T4 Gc, Certificate no.: IECEx DEK 18.0019X

The product meets the requirements of the standards:

- IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- IEC 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

ATEX

Classification: II 3 G Ex ec IIC T4 Gc, Certificate no.:DEKRA 18ATEX0027 X

The product meets the requirements of the standards:

- EN IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

UKEX

Classification: II 3 G Ex ec IIC T4 Gc, Certificate no.:DEKRA 21UKEX0003 X

The product meets the requirements of the standards:

- EN IEC 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements
- EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

Importer UK: Siemens plc (see above)

CCC-Ex

Classification: Ex ec IIC T4 Gc

The product meets the requirements of the following standards:

- GB/T 3836.1
Hazardous areas - Part 0: Equipment - General requirements
- GB/T 3836.3
Explosive atmospheres - Part 3: Equipment protection by increased safety 'e'

EMC

The device meets the requirements of the following guidelines:

- EU directive 2014/30/EU "Electromagnetic Compatibility" (EMC directive)
- EMC Regulations SI 2016/1091 The Electromagnetic Compatibility Regulations 2016, and related 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

RoHS

The device meets the requirements of the following guidelines:

- EU directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment.
- SI 2012/3032 The Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012, and related amendments.

Applied standard: EN IEC 63000

c(UL)us



Applied standards:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E 85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations



Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

Applied standards:

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta: Refer to the temperature class on the type plate of the module

Report / UL file: E223122 (NRAG, NRAG7)

Note the conditions for the safe deployment of the product according to the section Notes on use in hazardous areas according to UL HazLoc and FM (Page 32).

Note

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

CSA



CSA Certification Mark Canadian Standard Association (CSA) nach Standard C 22.2 No. 142:

- Certification Record 063533–C-000

FM



Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

You will find the temperature class on the type plate on the module.

For the permissible temperature range of the module, refer to the section Technical specifications (Page 63).

Australia - RCM



The product meets the requirements of the AS/NZS 2064 standards (Class A).

Canada

This class A digital device meets the requirements of the Canadian standard ICES-003.

AVIS CANADIEN

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

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.

Note that in terms of the emission of interference, this device corresponds to limit class A. This device can be used in all areas except for residential environments.

Current approvals

SIMATIC NET products are regularly submitted to the relevant authorities and approval centers for approvals relating to specific markets and applications.

If you require a list of the current approvals for individual devices, consult your Siemens contact or check the Internet pages of Siemens Industry Online Support:

Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15341/cert>)

Dimension drawings

All dimensions in the dimension drawings are in millimeters.

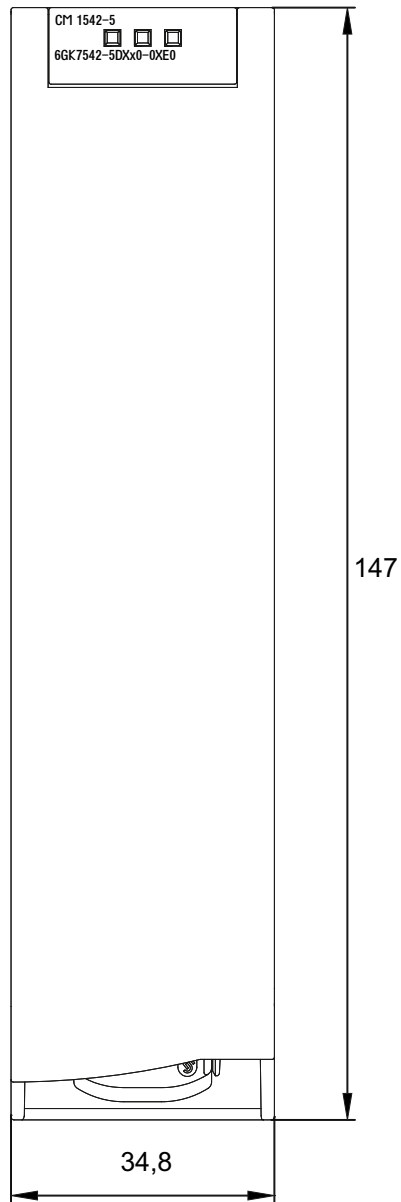


Figure 8-1 Front view

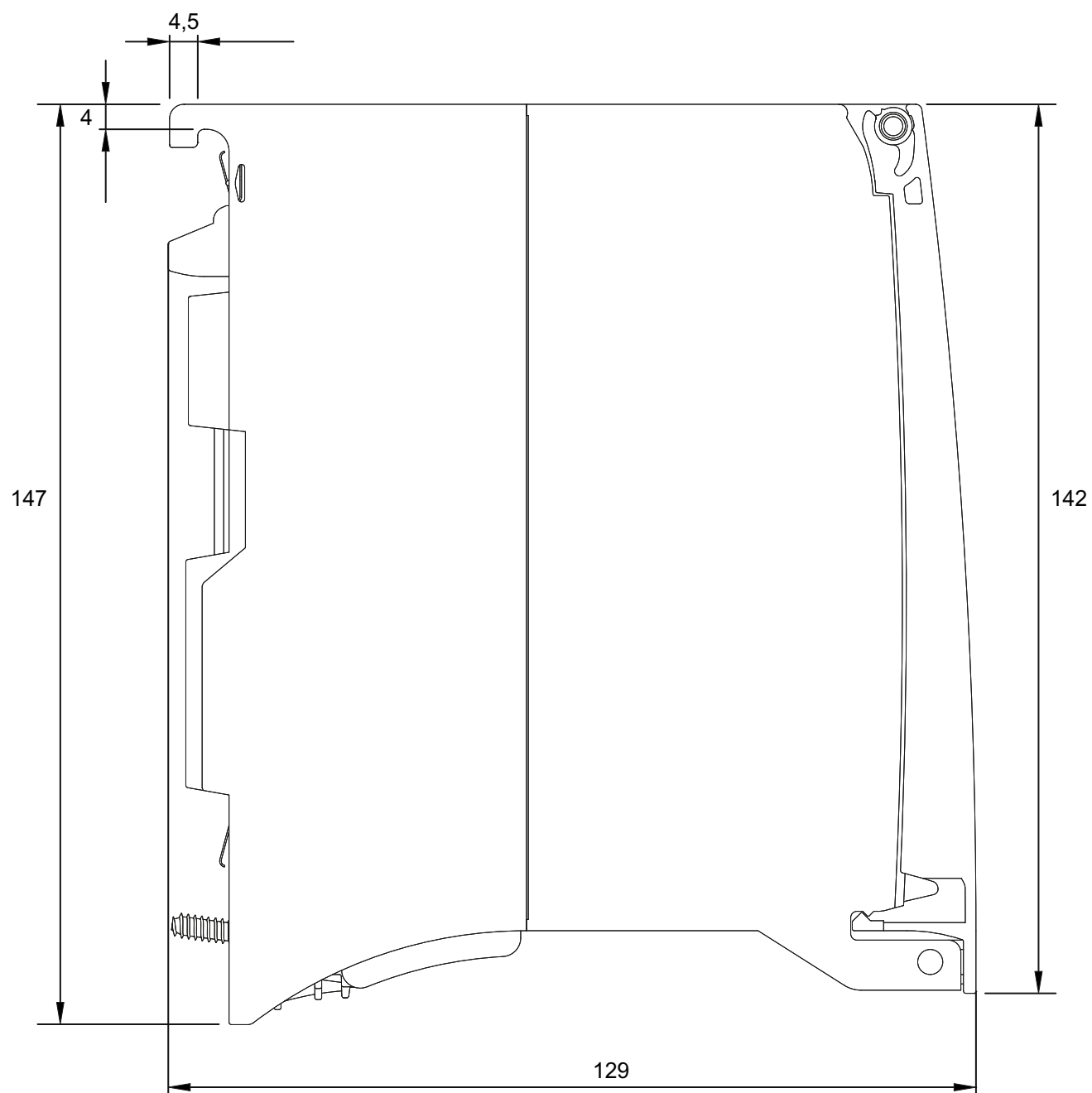


Figure 8-2 Side view

Documentation references

A.1 Introduction to the documentation

Where to find Siemens documentation

- Article numbers
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 70You can request the catalogs and additional information from your Siemens representative. You will also find the product information in the Siemens Industry Mall at the following address:
Link: (<https://mall.industry.siemens.com>)
- Manuals on the Internet
You will find SIMATIC NET manuals on the Internet pages of Siemens Industry Online Support:
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15247/man>)
Go to the required product in the product tree and make the following settings:
Entry type "Manuals"
- Manuals on the data medium
You will find manuals of SIMATIC NET products on the data medium that ships with many of the SIMATIC NET products.

A.2 System manual S7-1500

A.2.1 /1/

SIMATIC
S7-1500 Automation System
System Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/59191792>)

A.3 Diagnostics

A.3.1 /2/

SIMATIC
SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro
Diagnostics
Function Manual Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/59192926>)

A.3.2 /3/

SIMATIC NET
Diagnostics and configuration with SNMP
Diagnostics manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/ps/15392/man>)

A.4 Communication

A.4.1 /4/

SIMATIC
SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL, ET 200pro
Communication
Function Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/59192925>)

A.4.2 /5/

SIMATIC
SIMATIC PROFINET with STEP 7 V14
Function Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/49948856>)

A.4.3 /6/

SIMATIC
SIMATIC S7-1500, ET 200SP, ET 200pro
Web Server
Function Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/59193560>)

A.5 Interference-free installation of control systems

A.5.1 /7/

SIMATIC
SIMATIC S7-1500, ET 200MP, ET 200SP, ET 200AL
Interference-free Installation of Control Systems
Function Manual
Siemens AG
Interference-free installation of control systems (<https://support.industry.siemens.com/cs/ww/en/view/59193566>)

A.6 Memory concept

A.6.1 /8/

SIMATIC S7-1500, ET 200SP, ET 200pro
Structure and Use of the CPU Memory
Function Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/59193101>)

A.7 Cycle and response times

A.7.1 /9/

SIMATIC
SIMATIC S7-1500, ET 200SP, ET 200pro
Cycle and Response Times
Function Manual
Siemens AG
Link: (<https://support.industry.siemens.com/cs/ww/en/view/59193558>)

Index

C

- Changing mode (RUN / STOP), 39
- CONF_DATA, 24
- Configuration of the Ethernet interface, 24
- Connection resources, 19

D

- Data storage of the configuration data of the module, 61
- Diagnostics options, 55
- Disposal, 10
- Documentation, 7
- Double addressing in the network, 44
- Downloading project data, 38

E

- E-mail connections, 20, 24
- Ethernet interface, 4
 - Configuration, 24

F

- Factory settings
 - Resetting to, 60

H

- HMI communication, 15

I

- iDevice, 15
- Installation and commissioning, 37
 - Procedure, 38
- Instructions, 24
- IP configuration IPv4, 16
- IP routing, 45
- IRT, 15
- ISO-on-TCP (RFC 1006), 15
- ISO-on-TCP connections, 20, 24

L

- LEDs, 25

M

- MAC address, 4, 16
- Maximum data length for program blocks, 20
- Media redundancy, 15, 16
- MIB, 55
- Multicast
 - via UDP, 15

N

- NTP, 50
- Number
 - of operable CMs, 22
- Number of connections, 20

O

- Open User Communication, 15
- OUC (Open User Communication), 51
- Overall configuration limits, 22

P

- PG communication, 15
- Plugging in, 37
- Power supply modules
 - Additional, 22
- PROFINET interface, 4
- Program blocks, 24
- Pulling, 37

R

- Recycling, 10
- Reset
 - To factory settings, 60

S

- S7 communication, 15

- S7 connections
 - Number of freely usable, 21
- Safety notices, 31
- Security Advisories, 17
- Security fixes:, 17
- Security Incidents, 17
- Shared Device, 15
- SNMP, 55
- SNMP agent, 16
- STEP 7 (version), 23
- System data types, 24
- System data types (SDTs), 53

T

- T_CONFIG, 24
- TCON, 24
- TCON_..., 24
- TCP (RFC 793), 15
- TCP connections, 20, 24
- Time synchronization, 15
- Time-of-day synchronization, 50
- TMail_..., 24
- TMAIL_C, 24
- TSEND/TRCV, 24

U

- UDP
 - Restrictions, 21
- UDP (RFC 768), 15
- UDP connections, 20
- UDP frame buffering, 21

V

- Virtual interface, 46

W

- Web server, 16