

SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet CP 1543-1

Manual

Preface

Guide to the documentation

1

Product overview

2

Functional characteristics

3

Requirements for use

4

Connecting up /
commissioning

5

Interrupts, diagnostics
messages, error and system
alarms

6

Notes on operation

7

Technical specifications

8




Approvals

9

Legal information

Warning notice system

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

 DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
 WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
 CAUTION
indicates that minor personal injury can result if proper precautions are not taken.
NOTICE
indicates that property damage can result if proper precautions are not taken.


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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Preface

Purpose of the documentation

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 CP.

See also Guide to the documentation (Page 7)

Conventions

Make sure you read the special notices below:

Note

A notice contains important information on the product described in the documentation, handling the product or about parts of the documentation you should pay particular attention to.

Names

- In this document, the term "CP" is also used instead of the full product name.
- The name STEP 7 is used to mean the STEP 7 Professional configuration tool.

SIMATIC NET glossary

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

You will find the SIMATIC NET glossary here:

- SIMATIC NET Manual Collection
The DVD ships with certain SIMATIC NET products.
- On the Internet under the following entry ID:
50305045 (<http://support.automation.siemens.com/WW/view/en/50305045>)

License conditions

Note

Open source software

Read the license conditions for open source software carefully before using the product. The acceptance of the disclaimers of liability and warranty it contains is a clear precondition of the use of open source software.

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

- DOC_OSS-Siemens_74.pdf
 - DOC_OSS-CP1243-1DNP3_76.pdf
-

Security information

Siemens provides automation and drive products with industrial security functions that support the secure operation of plants or machines. They are an important component in a holistic industrial security concept. With this in mind, our products undergo continuous development. We therefore recommend that you keep yourself informed with respect to our product updates. Please find further information and newsletters on this subject at: <http://support.automation.siemens.com>.

To ensure the secure operation of a plant or machine it is also necessary to take suitable preventive action (e.g. cell protection concept) and to integrate the automation and drive components into a state-of-the-art holistic industrial security concept for the entire plant or machine. Any third-party products that may be in use must also be taken into account. Please find further information at: <http://www.siemens.com/industrialsecurity>

Table of contents

	Preface	3
1	Guide to the documentation	7
2	Product overview	9
	2.1 Further functions	11
	2.2 Industrial Ethernet Security	13
3	Functional characteristics	15
	3.1 General characteristic data	15
	3.2 Characteristics of open communication	16
	3.3 Characteristics of S7 communication	18
	3.4 Characteristic data for FTP / FTPS mode	18
	3.5 Characteristics of VPN tunnel communication	19
4	Requirements for use	21
	4.1 Configuration limits	21
	4.2 Project engineering	21
	4.3 Programming	22
5	Connecting up / commissioning	23
	5.1 Important notes on using the device	23
	5.2 Installing and commissioning the CP 1543-1	25
	5.3 Replacing a module without a programming device	27
	5.4 Mode of the CPU - effect on the CP	28
6	Interrupts, diagnostics messages, error and system alarms	29
	6.1 Status and error display of the CP	29
	6.2 Diagnostics options	31
7	Notes on operation	33
	7.1 Network settings	33
	7.1.1 Fast Ethernet	33
	7.2 IP configuration	34
	7.2.1 Points to note about IP configuration	34
	7.2.2 Restart after detection of a duplicate IP address in the network	34
	7.3 Security	34
	7.3.1 Filtering of the system events	34
	7.3.2 VPN tunnel communication between the CP 1543-1 and CP x43-1 for configured connection (advanced firewall mode)	35

7.3.3	Firewall	35
7.3.3.1	Firewall sequence when checking incoming and outgoing frames	35
7.3.3.2	Online diagnostics and download with the firewall activated	35
7.3.3.3	Bandwidth limitation < 1 Mbps has no effect (advanced firewall mode)	36
7.3.3.4	Maximum number of firewall rules (advanced firewall mode)	36
7.3.3.5	Correct notation for the source IP address/address range (advanced firewall mode)	36
7.3.3.6	HTTP and HTTPS not possible with IPv6	36
7.3.4	VPN	37
7.3.4.1	Creating VPN tunnel communication between S7-1500 stations	38
7.3.4.2	Successfully establishing VPN tunnel communication between the CP 1543-1 and SCALANCE M	41
7.3.4.3	VPN tunnel communication with SOFTNET Security Client	41
7.4	FTP	42
7.5	Time-of-day synchronization	43
7.6	SNMP agent	44
7.7	Interface in the user program	45
7.7.1	IP access protection with programmed communications connections	45
8	Technical specifications	47
9	Approvals	49
9.1	Approvals - note	49
	Index	53

Guide to the documentation

Introduction

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 CP 1543-1 and are available in the Internet.

Table 1- 1 Configuration tools for the CP 1543-1

Topic	Documentation	Most important contents
System description	System manual: S7-1500 Automation System (http://support.automation.siemens.com/WW/view/en/59191792)	<ul style="list-style-type: none"> • Application planning • Installation • Connecting • Commissioning
System diagnostics	Function manual: System diagnostics (http://support.automation.siemens.com/WW/view/en/59192926)	<ul style="list-style-type: none"> • Overview • Diagnostics evaluation for hardware/software
Communication	Function manual: Communication (http://support.automation.siemens.com/WW/view/en/59192925)	<ul style="list-style-type: none"> • Overview
	Function manual: Web Server (http://support.automation.siemens.com/WW/view/en/59193560)	<ul style="list-style-type: none"> • Function • Operation
	Manual Industrial Ethernet Security (http://support.automation.siemens.com/WW/view/en/56577508)	<ul style="list-style-type: none"> • Overview and description of the security functions in Industrial Ethernet
	Manual SIMATIC NET: Twisted Pair and Fiber Optic Networks (http://support.automation.siemens.com/WW/view/en/8763736)	<ul style="list-style-type: none"> • Ethernet networks • Network configuration • Network components

Topic	Documentation	Most important contents
Interference-free installation of control systems	Function Manual: Interference-free installation of control systems (http://support.automation.siemens.com/WW/view/en/59193566)	<ul style="list-style-type: none">• Basics• Electromagnetic compatibility• Lightning protection• Housing selection
Cycle and response times	Function manual: Cycle and Response Times (http://support.automation.siemens.com/WW/view/en/59193566)	<ul style="list-style-type: none">• Basics• Calculations

SIMATIC manuals

All current manuals for SIMATIC products are available for download free of charge from the Internet (<http://www.siemens.com/automation/service&support>).

CP documentation in the Manual Collection (article number A5E00069051)

The "SIMATIC NET Manual Collection" DVD contains the device manuals and descriptions of all SIMATIC NET products current at the time it was created. It is updated at regular intervals.

Version History / Current Downloads for the SIMATIC NET S7 CPs

The "Version History/Current Downloads for SIMATIC NET S7 CPs (Ind. Ethernet)" provides information on all CPs available up to now for SIMATIC S7 (Ind. Ethernet).

An up-to-date version of this document can be found on the Internet (<http://support.automation.siemens.com/WW/view/en/9836605>)

Product overview

Article number, validity and product names

This description contains information on the following product

CP 1543-1

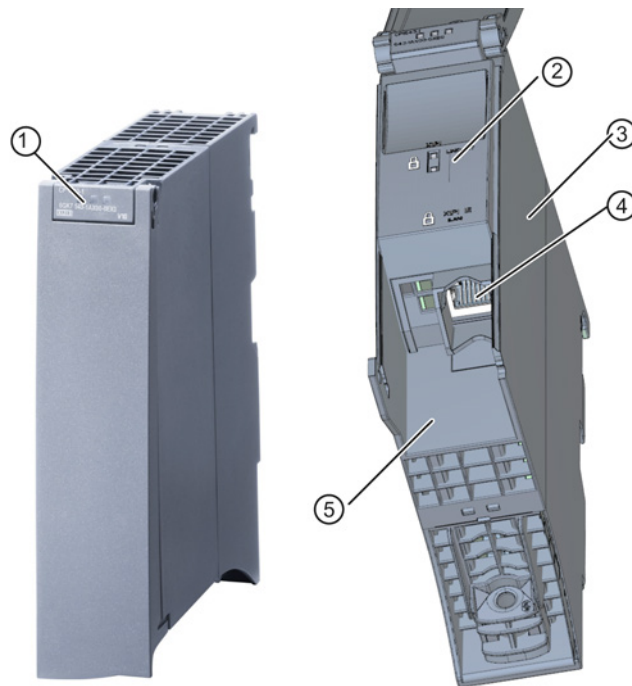
Article number: 6GK7 543-1AX00-0XE0

Hardware product version 2

Firmware version V1.1

Communications processor for SIMATIC S7-1500

View of the CP 1543-1



- ① LEDs for status and error displays
- ② LED displays of the Ethernet interface for LINK and ACTIVITY
- ③ Type plate
- ④ Ethernet port: 1 x 8-pin RJ-45 jack
The padlock icon symbolizes the interface to the external, non-secure subnet.
- ⑤ Label with MAC address

Figure 2-1 View of the CP 1543-1 with closed (left) and open (right) front cover

Address label: Unique MAC address preset for the CP

The CP ships with a default MAC address:

The MAC address is printed on the housing.

If you configure a MAC address (ISO transport connections), we recommend that you use the MAC address printed on the module for module configuration!

- This ensures that you assign a unique MAC address in the subnet!

Application

The CP is intended for operation in an S7-1500 automation system. It allows the S7-1500 to be connected to Industrial Ethernet.

With a combination of different security measures such as firewall and protocols for data encryption, the CP protects individual S7-1500 stations or even entire automation cells from unauthorized access.

Ethernet interface with gigabit specification and security access

The CP has an Ethernet interface according to the gigabit standards IEEE 802.3. The Ethernet interface supports autocrossing, autonegotiation and autosensing.

Note

Term "Ethernet interface"

The interface of the CP with the gigabit specification described earlier is known in the rest of this manual as "Ethernet interface".

The Ethernet interface allows a secure connection to external networks via a firewall. The CP provides the following protective function:

- Protection of the S7-1500 station in which the CP is operated;
- Protection of the underlying company networks connected to the other interfaces of the S7-1500 station.

The CP supports the following communication services:

- **Open communication**

Open communication supports the following communications services via the CP using programmed or configured communications connections:

- ISO transport (complying with ISO/IEC 8073)
- 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 CP supports the socket interface to TCP/IP available on practically every end system.

- Multicast over UDP connection

The multicast mode is made possible by selecting a suitable IP address when configuring connections.

- FETCH/WRITE services (server services; corresponding to S5 protocol) via ISO transport connections, ISOonTCP connections and TCP connections;

Here, the SIMATIC S71500 with the CP is always the server (passive connection establishment) while the fetch or write access (client function with active connection establishment) is always initiated by a SIMATIC S5 or a third-party device / PC.

- **S7 communication**

- PG communication
- Operator control and monitoring functions (HMI communication)
- Data exchange over S7 connections

- **IT functions**

- FTP functions (File Transfer Protocol FTP/FTPS) for file management and access to data blocks on the CPU (client and server functions).
- Sending email via SMTP or ESMTP with "SMTPAuth" for authentication on an email server.

2.1 Further functions

Timeofday synchronization over Industrial Ethernet using the NTP mode (NTP: Network Time Protocol)

The CP 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.

Security function: The CP supports the NTP (secure) protocol for secure time-of-day synchronization and transfer of the time of day.

Addressable with the factoryset MAC address

To assign the IP address to a new CP (direct from the factory), it can be accessed using the preset MAC address on the interface being used. Online address assignment is made in STEP 7.

SNMP agent

The CP supports data queries over SNMP in version V1 (Simple Network Management Protocol). It delivers the content of certain MIB objects according to the MIB II standard and Automation System MIB.

If security is enabled, the CP supports SNMPv3 for transfer of network analytical information protected from eavesdropping.

IP configuration - IPv4 and IPv6

The essential features of IP configuration for the CP:

- The CP supports the use of IP addresses according to IPv4 and IPv6.
- You can configure how and with which method the CP 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 CP by the user program (for program blocks refer to the section Programming (Page 22)).

Note: Does not apply to S7 connections.

IP address according to the IPv6 format - range of use on the CP

An IP address according to IPv6 can be used for the following communications services:

- FTP server mode
- FETCH/WRITE access (CP is server)
- FTP client mode with addressing via a program block
- E-mail transfer with addressing via a program block

Access to the Web server of the CPU

Via the LAN interface of the CP, 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 Guide to the documentation (Page 7)

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 CP 1543-1, the SSL certificate of the CPU is displayed.

S5/S7 addressing mode for FETCH/WRITE

The addressing mode can be configured for FETCH/WRITE access as S7 or S5 addressing mode. The addressing mode specifies how the position of the start address is identified during data access (S7 addressing mode applies only to data blocks / DBs).

Read the additional information in the online help of STEP 7.

2.2 Industrial Ethernet Security

All-round protection - the task of Industrial Ethernet Security

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected. The data transfer from the external network connected to the CP 1543-1 can be protected by a combination of different security measures:

- Data espionage (FTPS, HTTPS)
- Data manipulation
- Unauthorized access

Secure underlying networks can be operated via additional Ethernet/PROFINET interfaces implemented by the CPU or additional CPs.

Security functions of the CP for the S7-1500 station

As result of using the CP, the following security functions are accessible to the S7-1500 station on the interface to the external network:

- Firewall
 - IP firewall with stateful packet inspection (layer 3 and 4)
 - Firewall also for Ethernet "non-IP" frames according to IEEE 802.3 (layer 2)
 - Bandwidth limitation
 - Global firewall rules

- Logging

To allow monitoring, events can be stored in log files that can be read out using the configuration tool or can be sent automatically to a syslog server.

- FTPS (explicit mode)

For encrypted transfer of files.
- Secure NTP

For secure time-of-day synchronization and transmission.

- **SNMPv3**

For secure transmission of network analysis information safe from eavesdropping.

- **Protection for devices and network segments**

The firewall protective function can be applied to the operation of single devices, several devices, or entire network segments.

NOTICE

Plants with security requirements - recommendation

Use the following options:

- If you have systems with high security requirements, use the secure protocols NTP (secure), FTPS, HTTPS and SNMPv3.
- If you connect to public networks, you should use the firewall. Think about the services you want to access via public networks. By using the bandwidth limitation of the firewall, you can restrict the possibility of flooding and DoS attacks.

The FETCH/WRITE functionality allows you to access any data of your PLC. In conjunction with public networks, the FETCH/WRITE functionality should not be used.

Functional characteristics

3.1 General characteristic data

Characteristic	Explanation / values
Total number of freely usable connections on Industrial Ethernet	118 The value applies to the total number of connections of the following types: <ul style="list-style-type: none">• S7 connections• Connections for open communications services• FTP (FTP client)

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 CP.

3.2 Characteristics of open communication

Open communication provides access to communication via TCP, ISOonTCP, ISO transport and UDP connections.

The following characteristics are important:

Characteristic	Explanation / values
Number of connections	<ul style="list-style-type: none"> • Max. number of connections in total (configured and programmed: (ISO transport and ISOonTCP + TCP + UDP + FETCH/WRITE + e-mail) <= 118 <p>of which:</p> <ul style="list-style-type: none"> – TCP connections: 1...118 ¹⁾ – ISO-on-TCP connections: 1...118 – ISO transport connections: 1...118 – Total number of UDP connections (specified and free) that can be configured: 1...118 – Connections for FETCH/WRITE: 1...16 – Connection for e.mail: 1 <p>Notes:</p> <ul style="list-style-type: none"> • ¹⁾ Avoid overload at receiving end <p>The flow control on TCP connections cannot control permanent overload of the recipient. You should therefore make sure that the processing capabilities of a receiving CP are not permanently exceeded by the sender (approximately 150200 messages per second).</p>
Maximum data length for program blocks	<p>Program blocks allow the transfer of user data in the following lengths:</p> <ol style="list-style-type: none"> 1. ISO-on-TCP, TCP, ISO transport: 1 to 64 kB 2. UDP: 1 to 1452 bytes 3. E-mail (job header + user data): 1 to 256 bytes <p>E-mail attachment: up to 64 kbytes</p>
LAN interface max. data field length generated by CP per protocol data unit(TPDU = transport protocol data unit)	<ul style="list-style-type: none"> • sending <ul style="list-style-type: none"> ISO transport, ISOonTCP, TCP: <ul style="list-style-type: none"> – 1452 bytes / TPDU • receiving <ul style="list-style-type: none"> ISO transport: 512 bytes / TPDU ISO-on-TCP: 1452 bytes / TPDU TCP: 1452 bytes / TPDU

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 CP.

You will find detailed information on the topic of connection resources in the "Communication" function manual, refer to the section Guide to the documentation (Page 7)

Restrictions for UDP

- Transfer is not confirmed

The transfer of UDP frames is unconfirmed, in other words the loss of messages is not detected or displayed by the send program block.

- UDP frame buffering

Length of the frame buffer:

at least 7360 bytes

Note:

Following a buffer overflow, newly arriving frames are discarded.

3.3 Characteristics of S7 communication

S7 communication provides data transfer via the ISO Transport or ISO-on-TCP protocols.

Feature	Explanation / values
Total number of freely usable S7 connections on Industrial Ethernet	Max. 118
LAN interface - data field length generated by CP per protocol data unit (PDU = protocol data unit)	<ul style="list-style-type: none"> • for sending: 480 bytes / PDU • for receiving: 480 bytes / PDU
Number of reserved OP connections	4
Number of reserved PG connections	4
Number of reserved connections for Web	2

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.

3.4 Characteristic data for FTP / FTPS mode

TCP connections for FTP

FTP actions are transferred from the CP over TCP connections. Depending on the mode, the following characteristic data applies:

- FTP in client mode:

You can use a maximum of 32 FTP sessions. Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).

- FTP in server mode:

You can operate a maximum of 16 FTP sessions at the same time. Up to 2 TCP connections are occupied per activated FTP session (1 control connection and 1 data connection).

Program block FTP_CMD (FB40) for FTP client mode

For communication, use the FTP program block FTP_CMD.

The block execution time in FTP depends on the reaction times of the partner and the length of the user data. A generally valid statement is therefore not possible.

3.5 Characteristics of VPN tunnel communication

VPN tunnel communication allows the establishment of secure IPsec tunnel communication with one or more security modules.

Configuration limits	Value
Number of IPsec tunnels	16 maximum

Requirements for use

4.1 Configuration limits

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

- The number of CPs that can be operated in a rack depends on the CPU type being used.

By operating several CPs, you can increase the configuration limits listed below for the station as the whole. The CPU does, however, have set limits for the entire configuration. The size of the configuration made available by a CP can be increased by using more than one CP within the framework of the system limits.

Note the information in the documentation of the CPU, refer to the section Guide to the documentation (Page 7)

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.

4.2 Project engineering

Configuration and downloading the configuration data

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

The following version of STEP 7 is required:

STEP 7 version	Functions of the CP
STEP 7 Professional V12 SP1 or higher	The full functionality of the CP 1543-1 (6GK7 543-1AX00-0XE0) can be configured.

4.3 Programming

Program blocks

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

Table 4- 1 Instructions for communications services

Protocol	Program block (instruction)	System data type
TCP	Establish connection and send/receive data via: <ul style="list-style-type: none"> • TSEND_C/TRCV_C or • TCON, TSEND/TRCV (termination of the connection using TDISCON possible) 	<ul style="list-style-type: none"> • TCON_IP_v4 • TCON_Configured
ISO-on-TCP		<ul style="list-style-type: none"> • TCON_IP_RFC
ISO		<ul style="list-style-type: none"> • TCON_ISOnative
UDP	<ul style="list-style-type: none"> • TCON, TUSEND/TURCV (termination of the connection using TDISCON possible) 	<ul style="list-style-type: none"> • TCON_IP_v4
E-mail	<ul style="list-style-type: none"> • TMAIL_C 	<ul style="list-style-type: none"> • TMail_v4* • TMail_v6* • TMAIL_FQDN*
FTP	<ul style="list-style-type: none"> • FTP_CMD 	<ul style="list-style-type: none"> • FTP_CONNECT_IPV4* • FTP_CONNECT_IPV6* • FTP_CONNECT_NAME* • FTP_FILENAME* • FTP_FILENAME_PART*

*User-defined data type

Table 4- 2 Instructions for configuration tasks

Function	Program block (instruction)	System data type
Configuration of the Ethernet interface	<ul style="list-style-type: none"> • T_CONFIG 	<ul style="list-style-type: none"> • CONF_DATA

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


Connecting up / commissioning

5.1 Important notes on using the device


Safety notices on the use of the device


The following safety notices must be adhered to when setting up and operating the device and during all associated work such as installation, connecting up, replacing devices or opening the device.


General notices


 WARNING
<p>Safety extra low voltage</p> <p>The equipment is designed for operation with Safety Extra-Low Voltage (SELV) by a Limited Power Source (LPS). (This does not apply to 100 V...240 V devices.)</p> <p>This means that only SELV / LPS complying with IEC 60950-1 / EN 60950-1 / VDE 0805-1 must be connected to the power supply terminals. The power supply unit for the equipment power supply must comply with NEC Class 2, as described by the National Electrical Code (r) (ANSI / NFPA 70).</p> <p>There is an additional requirement if devices are operated with a redundant power supply:</p> <p>If the equipment is connected to a redundant power supply (two separate power supplies), both must meet these requirements.</p>


General notices on use in hazardous areas


 WARNING
<p>Risk of explosion when connecting or disconnecting the device</p> <p>EXPLOSION HAZARD</p> <p>DO NOT CONNECT OR DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT.</p>

 WARNING
Replacing components EXPLOSION HAZARD SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2 OR ZONE 2.


 WARNING
Requirements for the cabinet/enclosure 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
Restricted area of application This equipment is suitable for use in Class I, Division 2, Groups A, B, C and D or non-hazardous locations only.

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

 WARNING
LAN attachment A LAN or LAN segment with the attachments belonging to it should be within a single low-voltage supply system and within a single building. Make sure that the LAN is in an of type A environment according to IEEE 802.3 or in a type 0 environment according to IEC TR 62101. Never establish a direct electrical connection to TNV networks (telephone network) or WANs (Wide Area Network).

General notices on use in hazardous areas according to ATEX

 WARNING
Requirements for the cabinet/enclosure To comply with EU Directive 94/9 (ATEX95), this enclosure must meet the requirements of at least IP54 in compliance with EN 60529.

 WARNING**Suitable cables for temperatures in excess of 70 °C**

If the cable or conduit entry point exceeds 70°C or the branching point of conductors exceeds 80°C, special precautions must be taken. If the device is operated at ambient temperatures above 50°C, the permitted temperature range of the selected cable must be suitable for the temperatures actually measured.

 WARNING**Protection against transient voltage surges**

Provisions shall be made to prevent the rated voltage from being exceeded by transient voltage surges of more than 40%. This criterion is fulfilled, if supplies are derived from SELV (Safety Extra-Low Voltage) only.

5.2 Installing and commissioning the CP 1543-1

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" (references to documentation, refer to the section Guide to the documentation (Page 7)).

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

Configuration

Commissioning the CP fully is only possible if the STEP 7 project data is complete.

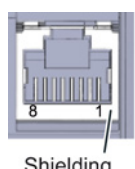
Procedure for installation and commissioning

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".	
3	Connect the CP to Industrial Ethernet via the RJ45 jack.	Underside of the CP
4	Turn on the power supply.	
5	Close the front covers of the module and keep them closed during operation.	
6	The remaining steps in commissioning involve downloading the STEP 7 project data.	<p>The STEP 7 project data of the CP 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.</p> <p>You will find more detailed information on loading in the following sections of the STEP 7 online help:</p> <ul style="list-style-type: none"> • "Compiling and loading project data" • "Using online and diagnostics functions"

Ethernet interface

The table below shows the pin assignment of the Ethernet interface. The assignment corresponds to the Ethernet standard for a RJ45 plug.

Table 5- 1 Pin assignment of the Ethernet interface

View	Pin	10/100 Mbps operation		10/100 Mbps or gigabit operation	
		Signal name	Pin assignment	Signal name	Pin assignment
	1	TD	Transmit data +	D1+	D1 bidirectional +
	2	TD_N	Transmit data -	D1-	D1 bidirectional -
	3	RD	Receive data +	D2+	D2 bidirectional +
	4	GND	Ground	D3+	D3 bidirectional +
	5	GND	Ground	D3-	D3 bidirectional -
	6	RD_N	Receive data -	D2-	D2 bidirectional -
	7	GND	Ground	D4+	D4 bidirectional +
	8	GND	Ground	D4-	D4 bidirectional -

Reference

You will find additional information on the topics of "Connecting up" and "Accessories (RJ-45 plug)" in the system manual S7-1500 Automation System (<http://support.automation.siemens.com/WW/view/en/59191792>).

5.3 Replacing a module without a programming device

General procedure

The configuration data of the CP 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 PG.

Note

Configured MAC address is adopted

When setting the ISO protocol, remember that MAC address set previously during configuration is transferred by the CPU to the new CP module.

Module replacement: Special feature of IP address assignment from a DHCP server (IPv4)

During configuration of the CP you can specify the IP configuration in the properties dialog; one option is to obtain the IP address from a DHCP server.

Note

Recommendation: Configuring a client ID

When replacing modules, remember that the factoryset MAC address of the new module is different from the previous module. When the factoryset MAC address of the new module is sent to the DHCP server, this will return either a different or no IP address.

Ideally, you should therefore configure IP as follows:

- Always configure a client ID and configure your DHCP server accordingly. This makes sure that after replacing the module, you always obtain the same IP address from the DHCP server.

If, in exceptional situations, you have configured a new MAC address instead of the MAC address set in the factory, the configured MAC address will always be transferred to the DHCP server. In this case, the new CP also has the same IP address as the previous module.

5.4 Mode of the CPU - effect on the CP

You can change the mode of the CPU between RUN and STOP using the STEP 7 configuration software.

Depending on the operating status of the CPU, the CP behaves as described below.

Changing the CPU from RUN to STOP:

When the CPU is in STOP mode, the CP remains in RUN and behaves as follows:

- For established connections (ISO transport, ISOonTCP, TCP, UDP connections), the following applies depending on the configuration:
 - Programmed connections are retained.
 - Configured connections are terminated.
- The following functions remain enabled:
 - The configuration and diagnostics of the CP (system connections for configuration, diagnostics, and PG channel routing are retained);
 - Web diagnostics
 - S7 routing function
 - Time-of-day synchronization

Note

RUN/STOP LED of the CP

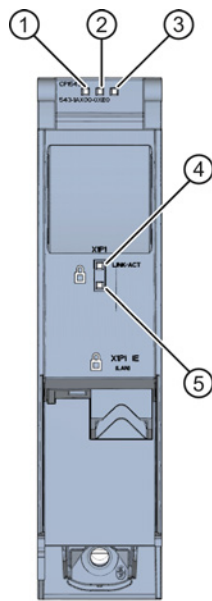
The green RUN/STOP LED of the CP continues to be lit green regardless of the STOP mode of the CPU.

Interrupts, diagnostics messages, error and system alarms

6

6.1 Status and error display of the CP

LED display



- ① RUN LED
- ② ERROR LED
- ③ MAINT LED
- ④ LINK/ACT LED
- ⑤ Reserve LED

Figure 6-1 LED display of the CP 1543-1 (without front cover)

Meaning of the LED displays




























The CP 1543-1 has 3 LEDs to display the current operating status and the diagnostics status and these have the following meanings:

- RUN LED (one-color LED: green)
- ERROR LED (one-color LED: red)
- MAINT LED (one-color LED: yellow)

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

6.1 Status and error display of the CP

Table 6- 1 Meaning of the LEDs

RUN LED	ERROR LED	MAINT LED	Meaning
 LED off	 LED off	 LED off	No supply voltage on the CP or supply voltage too low.
 LED lit green	 LED lit red	 LED lit yellow	LED test during startup
 LED lit green	 LED lit red	 LED off	Startup (booting the CP)
 LED lit green	 LED off	 LED off	CP 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, maintenance is demanded.
 LED lit green	 LED off	 LED flashing yellow	Maintenance is required.
			Downloading the user program
 LED flashing green	 LED off	 LED off	No CP 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 Ethernet interface: X1 P1

The port has an LED that indicates the following meaning:

- LINK/ACT Connection exists / data is being transferred (two-color LED: green/yellow)

The following table shows the various LED combinations of the Ethernet interface of the CP 1543-1.

Table 6- 2 Meaning of the LED

LINK/ACT LED		Meaning
 green off	 yellow off	No link There is no Ethernet connection between the Ethernet interface of the CP 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	link exists There is an Ethernet connection between the Ethernet interface of your CP 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.

6.2 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 Status and error display of the CP (Page 29).
- 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
 - Information on the Ethernet interface
 - Security (with security enabled)

You can obtain further information on the diagnostics functions of STEP 7 in the STEP 7 online help.

Notes on operation

7.1 Network settings

7.1.1 Fast Ethernet

Automatic setting

The Ethernet interface of the CPU is set permanently to autosensing.

Note

In normal situations, the basic setting ensures troublefree communication.

Autocrossing mechanism

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

Note**Connecting a switch**

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

7.2 IP configuration

7.2.1 Points to note about IP configuration

Configured S7 and OUC connections cannot be operated if the IP address is assigned using DHCP

Note

If you obtain the IP address using DHCP, any S7 and OUC connections you may have configured will not work. Reason: The configured IP address is replaced by the address obtained via DHCP during operation.

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

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

Behavior when the CP starts up

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

7.3 Security

7.3.1 Filtering of the system events

Avoiding problems in productive communication due to high output of system events

If the value for filtering the system events is set too high, you may not be able to use the maximum number of communications connections. The high number of output error messages can delay or prevent the processing of the communications connections.

To ensure the reliable establishment of the communications connections: In the local security settings of the CP 1543-1 ("Security > Log settings > Filtering of system events"), we recommend that you set the level value "3 (Error)".

7.3.2 VPN tunnel communication between the CP 1543-1 and CP x43-1 for configured connection (advanced firewall mode)

If you set up VPN tunnel communication for configured connections between a CP 1543-1 and CP x43-1, you will need to adapt the local firewall settings of the CP 1543-1:

- For both communications directions of the VPN tunnel, select the action "Allow" in the advanced firewall mode ("Security > Firewall > IP rules").

If you do not select this setting, the VPN tunnel connection will be terminated and re-established.

7.3.3 Firewall

7.3.3.1 Firewall sequence when checking incoming and outgoing frames

Each incoming or outgoing frame initially runs through the MAC firewall (layer 2). If the frame is discarded at this level, it is not checked by the IP firewall (layer 3). This means that with suitable MAC firewall rules, IP communication can be restricted or blocked.

7.3.3.2 Online diagnostics and download with the firewall activated

Characteristics with STEP 7 and Windows XP

Due to a feature of the Windows XP firewall, when online access to an S7-1500 station by STEP 7 is required, a ping is sent to the module prior to the connection establishment attempt. The ping packet checks whether or not the partner is available. This feature exists only if STEP 7 is installed on a PG with Windows XP. If you use STEP 7 with Windows 7, no ping packet is sent.

To allow STEP 7 to establish an online connection via the Ethernet interface of the CP for diagnostics or downloading when the CP firewall is activated, special settings are required in the firewall. The ping command is only acknowledged successfully if such access is allowed in the firewall.

Setting the firewall - steps involved

With security enabled, follow the steps outlined below:

1. In the global security settings, select the entry "Firewall > Services > Define services for IP rules".
2. Select the "ICMP" tab.
3. Insert a new entry of the type "Echo reply" and another of the type "Echo request".
4. Now select the CP in the S7-1500 station.
5. In the local security settings of the CP, open the parameter group "Properties > General > Security > Firewall" and enable the advanced firewall mode.
6. Open the "IP rules" parameter group.

7. In the table, insert a new IP rule for the previously created global services as follows:
 - Action: Allow; "From external -> to station" with the globally created "Echo request" service
 - Action: Allow; "From station -> to external" with the globally created "Echo reply" service
8. For the IP rule for the Echo Request, enter the IP address of the PG/PC in "Source IP address". This ensures that only PING packets from your PG/PC can pass through the firewall.

7.3.3.3 Bandwidth limitation < 1 Mbps has no effect (advanced firewall mode)

Bandwidth limitation with values < 1 Mbps is not possible.

This means that the available options for bandwidth limitation are restricted to the following range of values: 1 to 100 Mbps.

7.3.3.4 Maximum number of firewall rules (advanced firewall mode)

The maximum number of firewall rules in advanced firewall mode is limited to 256.

The firewall rules are divided up as follows:

- 226 rules with individual addresses
- 30 rules with address ranges or network addresses (e.g. 140.90.120.1-140.90.120.20 or 14.90.120.0/16)
- The number of rules with entered bandwidth limitation is limited to 128.

7.3.3.5 Correct notation for the source IP address/address range (advanced firewall mode)

If you specify an address range for the source IP address in the advanced firewall settings of the CP 1543-1, make sure that the notation is correct:

- Separate the two IP addresses only using a hyphen.
Correct: 192.168.10.0-192.168.10.255
- Do not enter any other characters between the two IP addresses.
Incorrect: 192.168.10.0 - 192.168.10.255

If you enter the range incorrectly, the firewall rule will not be used.

7.3.3.6 HTTP and HTTPS not possible with IPv6

It is not possible to use HTTP and HTTPS communication on the Web server of the station using the IPv6 protocol.

If the firewall is enabled in the local security settings in the entry "Firewall > Predefined IPv6 rules": The selected check boxes "Allow HTTP" and "Allow HTTPS" have no function.

7.3.4 VPN

What is VPN?

Virtual Private Network (VPN) is a technology for secure transportation of confidential data in public IP networks, for example the Internet. With VPN, a secure connection (= tunnel) is set up and operated between two secure IT systems or networks via a non-secure network.

One of the main characteristics of the VPN tunnel is that it forwards all network packets regardless of higher protocols (HTTP, FTP).

The data traffic between two network components is transported practically unrestricted through another network. This allows entire networks to be connected together via a neighboring network.

Properties

- VPN forms a logical subnet that is embedded in a neighboring (assigned) network. VPN uses the usual addressing mechanisms of the assigned network, however in terms of the data, it transports its own network packets and therefore operates independent of the rest of this network.
- VPN allows communication of the VPN partners with the assigned network.
- VPN is based on tunnel technology, can be individually configured, is customer-specific and is self-contained.
- Communication between the VPN partners is protected from eavesdropping or manipulation by using passwords, public keys or a digital certificate (= authentication).

Areas of application

- Local area networks can be connected together securely via the Internet ("site-to-site" connection).
- Secure access to a company network ("end-to-site" connection).
- Secure access to a server ("end-to-end" connection).
- Communication between two servers is possible without being accessible to third parties ("end-to-end" or "host-to-host" connection).
- Ensuring information security in networked automation systems.
- Securing the computer systems including the associated data communication within an automation network or secure remote access via the Internet.
- Secure remote access from a PC/programming device to automation devices or networks protected by security modules is possible via public networks.

Cell protection concept

With Industrial Ethernet Security, individual devices, automation cells or network segments of an Ethernet network can be protected:

- The access to individual devices or even to entire automation cells protected by security modules is allowed.
- Secure connections via non-secure network structures becomes possible.

Due to the combination of different security measures such as firewall, NAT/NAPT routers and VPN via IPsec tunnels, security modules protect against the following:

- Data espionage
- Data manipulation
- Unwanted access

7.3.4.1 Creating VPN tunnel communication between S7-1500 stations

Requirements

To create a VPN tunnel between two S7-1500 stations, the following requirements must be met:

- Two S7-1500 stations have been configured.
- Both CPs must be configured in firmware version V1.1.
- The Ethernet interfaces of the two stations are located in the same subnet.

Note

Communication also possible via an IP router

Communication between the two S7-1500 stations is also possible via an IP router. To use this communications path, however, you need to make further settings.

Procedure

To create a VPN tunnel, you need to work through the following steps:

1. Create a security user.
If the security user has already been created: Log on as a user.
2. Select the "Activate security features" check box.
3. Create the VPN group and assign security modules.
4. Configure properties of the VPN group.
Configure local VPN properties of the two CPs.

You will find a detailed description of the individual steps in the following paragraphs of this section.

Creating a security user

To create a VPN tunnel, you require appropriate configuration rights. To activate the security functions, you need to create at least one security user.

1. In the local security settings of the CP, click the "User logon" button.

Result: A new window opens.

2. Enter the user name, password and confirmation of the password.

3. Click the "User login" button.

You have created a new security user. The security functions are now available to you.

With all further logons, log on as user.

Selecting the "Activate security features" check box

- After logging on, select the "Activate security features" check box for both CPs.
You now have the security functions available for both CPs.

Creating the VPN group and assigning security modules

Note

Current date and current time of day on the security modules

When using secure communication (for example HTTPS, VPN...), make sure that the security modules involved have the current time of day and the current date. Otherwise the certificates used will not be evaluated as valid and the secure communication will not work.

1. In the global security settings, select the entry "Firewall" > "VPN groups" > "Add new VPN group".
2. Double-click on the entry "Add new VPN group", to create a VPN group.
Result: A new VPN group is displayed below the selected entry.
3. In the global security settings, double-click on the entry "VPN groups" > "Assign module to a VPN group".
4. Assign the security modules between which VPN tunnels will be established to the VPN group.

Configuring properties of the VPN group

1. Double-click on the newly created VPN group.
Result: The properties of the VPN group are displayed under "Authentication".
2. Enter a name for the VPN group. Configure the settings of the VPN group in the properties.
These properties define the default settings of the VPN group that you can change at any time.

Note

Specifying the VPN properties of the CP

You specify the VPN properties of the required CP in the local properties of the module ("Security" > "Firewall" > "VPN")

Result

You have created a VPN tunnel. The firewalls of the CPs are activated automatically: The "Activate firewall" check box is selected as default when you create a VPN group. You cannot deselect the check box.

- Download the configuration to all modules that belong to the VPN group.

7.3.4.2 **Successfully establishing VPN tunnel communication between the CP 1543-1 and SCALANCE M**

Creating VPN tunnel communication between the CP 1543-1 and SCALANCE M is the same as described in Procedure for S7-1500 stations (Page 38).

VPN tunnel communication will only be established if you have selected the check box "Perfect Forward Secrecy" in the global security settings of the created VPN group ("VPN groups > Authentication").

If the check box is not selected, the CP 1543-1 rejects establishment of the tunnel.

7.3.4.3 **VPN tunnel communication with SOFTNET Security Client**

Creating VPN tunnel communication between the CP SOFTNET Security Client and CP 1543-1 is the same as described in Procedure for S7-1500 stations (Page 38).

VPN tunnel communication works only if the internal node is disabled

Under certain circumstances the establishment of VPN tunnel communication between SOFTNET Security Client and the CP 1543-1 fails.

SOFTNET Security Client also attempts to establish VPN tunnel communication to a lower-level internal node. This communication establishment to a non-existing node prevents the required communication establishment to the CP 1543-1.

To establish successful VPN tunnel communication to the CP 1543-1, you need to disable the internal node.

Use the procedure for disabling the node as explained below only if the described problem occurs.

Disable the node in the SOFTNET Security Client tunnel overview:

1. Remove the checkmark in the "Enable active learning" check box.
The lower-level node initially disappears from the tunnel list.
2. In the tunnel list, select the required connection to the CP 1543-1.
3. With the right mouse button, select "Enable all members" in the shortcut menu.
The lower-level node appears again temporarily in the tunnel list.
4. Select the lower-level node in the tunnel list.
5. With the right mouse button, select "Delete entry" in the shortcut menu.

Result: The lower-level node is now fully disabled. VPN tunnel communication to the CP 1543-1 can be established.

7.4 FTP

FTP access only with security enabled

FTP access to the S7-1500 station as an FTP server is only possible if a user with suitable rights has been created in the STEP 7 project. This means that the "Security" property must be enabled on the CP. This makes global security settings available with the global user management.

FTP access using the FTP_CMD instruction - parameters for command types NOOP and QUIT

In contrast to the information in the online help of STEP 7 regarding the FTP_CMD instruction, note the following:

Supply the FTP_CMD with a reference to a job block with the following command types as well:

CMD = 0 (NOOP)

CMD = 5 (QUIT)

The content of the job block is not evaluated when these command types execute, the type (UDT) of the specified job block is therefore unimportant.

NOTICE
Response if the reference to the FTP job block is missing
If this reference is not supplied, the command is not executed. The instruction remains blocked in an apparent execution status without any feedback to the user program on the interface.

Evaluating the "LOCKED" and "NEW" status bits from the FTP_CMD program block

- In version 1.2 of the "FTP_CMD" program block, the status bits "LOCKED" and "NEW" of the FILE_DB_HEADER are not evaluated.

With the functions of the FTP server or when using the same file DB, the possibility of multiple simultaneous access to the same data area cannot be excluded. This can lead to data inconsistency.

- As of version 1.5 of the "FTP_CMD" program block, the status bits "LOCKED" and "NEW" of the FILE_DB_HEADER are set correctly. The two status bits are evaluated. Version 1.5 is available as of STEP 7 Professional V12 SP1.

NOTICE
Avoiding data inconsistency
Make sure that you do not access the same file DB more than once at the same time.

7.5 Time-of-day synchronization

General rules

The CP supports the following mode for timeofday synchronization:

- NTP mode (NTP: Network Time Protocol)

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.

Note**Special feature of time-of-day synchronization in NTP mode**

If the option "Accept time of the non-synchronized NTP server" is not selected, the response is as follows

If an NTP frame is detected by the CP as "not exact" (example: NTP server is not synchronized externally), there is no forwarding. If this problem occurs, none of the NTP servers is displayed as "NTP master" in the diagnostics; but rather all NTP servers are displayed only as being "accessible".

Security

In the extended NTP configuration, you can create and manage additional NTP servers including those of the type NTP (secure).

Note**Ensuring a valid time of day**

If you use security, a valid time of day is extremely important. If you do not obtain the time-of-day from the station (CPU), we therefore recommend that you use an NTP server of the type NTP (secure).

Configuration

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

7.6 SNMP agent

SNMP (Simple Network Management Protocol)

SNMP is a protocol for 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).

The CP supports data queries over SNMP in versions V1 (standard) and 3 (security). It delivers the content of certain MIB objects according to the MIB II standard and Automation System MIB.

Further information

For more detailed information on using MIB files, refer to the documentation of the SNMP client you are using (example of an SNMP client: SNMP OPC server from SIMATIC NET).

You will find more information on MIBs on the Internet (<http://support.automation.siemens.com/WW/view/en/15177711>)

MIB files are available using the following entry ID: 67637278 (<http://support.automation.siemens.com/WW/view/en/67637278>)

Supported MIBs

The CP supports the following groups of MIB objects of the standard MIB II according to RFC1213:

- System
- Interfaces
- IP (IPv4 and IPv6)
- ICMP
- TCP
- UDP
- SNMP
- Address Translation (AT)

The other groups of the MIB II standard are not supported:

- EGP
- Transmission

The CP continues to support the Automation System MIB.

Exceptions / restrictions:

- Write access is permitted only for the following MIB objects of the system group:

- sysContact
- sysLocation
- sysName

A set sysName is sent as the host name using DHCP option 12 to the DHCP server to register with a DNS server.

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

- Traps are not supported by the CP.

"Interfaces" MIB group

The "Interfaces" MIB object provides status information about the CP interfaces.

Access permissions using community name

The CP uses the following community names to control the access rights in the SNMP agent:

Table 7- 1 Access rights in the SNMP agent

Type of access	Community name *)
Read access	public
Read and write access	private

*) Note the use of lowercase letters!

7.7 Interface in the user program

7.7.1 IP access protection with programmed communications connections

In principle, it is possible to set up communications connections program-controlled using the program block TCON and at the same time by configuring the firewall.

When configuring specified connections (active endpoints) in STEP 7, the IP addresses of the partners are **not** entered automatically in the firewall configuration.

The configuration of IP access protection and the aspects of activated security are described in the online help of STEP 7.

Technical specifications

Note the information in the System description of SIMATIC S7-1500 (Page 7).

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

6GK7 543-1AX00-0XE0	
Product type name	CP 1543-1
Attachment to Industrial Ethernet	
• Number	1 x Ethernet (gigabit) interface
Design of the Ethernet interface	
• Connector	1 x RJ-45 jack
• Transmission speed	10 / 100/ 1000 Mbps
Electrical data	
Power supply	
• via S7-1500 backplane bus	15 V
Current consumption	
• From backplane bus	350 mA
• Power dissipation	5.3 W
Insulation	
Insulation tested with	707 VDC (type test)
Design, dimensions and weight	
Module format	Compact module S7-1500, single width
Degree of protection	IP20
Weight	Approx. 350 g
Dimensions (W x H x D)	35 x 142 x 129 mm
Installation options	Mounting in an S7-1500 rack
Permitted cable lengths	(Alternative combinations per length range) *
0 ... 55 m	<ul style="list-style-type: none"> • 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

6GK7 543-1AX00-0XE0

0 ... 85 m	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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

Product functions **

* For details, refer to the IK PI catalog, cabling technology

** You will find the product functions in the section Functional characteristics (Page 15).

Approvals

9.1 Approvals - note

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 on the pages of Siemens Automation Customer Support on the Internet (<http://support.automation.siemens.com/WW/news/en/10805878>)

Under this entry, go to the required product and select the following settings: "Entry list" tab > entry type "Certificates".

Standards and test specifications

The device meets the following standards and test specifications. The test criteria for the module are based on these standards and test specifications.

IEC 61131-2

The SIMATIC NET S7 CPs described in this manual fulfill the requirements and criteria of the IEC 61131-2 standard (Programmable Logic Controllers, Part 2: equipment requirements and verifications).

CE mark



The SIMATIC NET S7-CPs described in this manual fulfill the requirements and protection goals of the following EC directives and meet the harmonized European standards (EN) that have been published for the programmable logic controllers in the official journals of the European communities:

- 2004/108/EEC "Electromagnetic Compatibility" (EMC Directive)
- 94/9/EC "Equipment and protective systems intended for use in potentially explosive atmospheres" (Explosion Protection Directive)

The EC Declarations of Conformity are available for the responsible authorities according to the above-mentioned EC Directive at the following address:

- Siemens Aktiengesellschaft
Industry Automation
Industrielle Kommunikation SIMATIC NET
Postfach 4848
D-90327 Nürnberg

You will find the EC Declaration of Conformity at the following address / under the following entry ID on the Internet (<http://support.automation.siemens.com/WW/view/en/50302933>)

EMC directive

The SIMATIC NET S7 CPs listed above are designed for use in an industrial environment.

Field of application	Requirements	
	Emission	Immunity to interference
Industry	EN 61000-6-4	EN 61000-6-2

Explosion Protection Directives



Complying with EN 60079 (electrical apparatus for potentially explosive atmospheres; Type of protection "n")
 EN 60079-15, EN 60079-0
 II 3 G Ex nA IIC T4 Gc
 DEKRA 12 ATEX 0240X

Note

When using (installing) SIMATIC NET products in hazardous area zone 2, make absolutely sure that the associated conditions are adhered to!

You will find these conditions here:

- In the SIMATIC NET Manual Collection under "All Documents" > "Use of subassemblies/modules in a Zone 2 Hazardous Area"

Notice for Australia - C-TICK



The above listed SIMATIC NET S7 CPs meet the requirements of the standard AS/NZS 2064 (Class A).

Notices for 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.

UL and CSA approval

Note

You will recognize the approval, UL/CSA or cULus, assigned to your product from the mark on the rating plate.

UL approval



UL Recognition Mark Underwriters Laboratories (UL) nach Standard UL 508:

- Report E 85972

CSA approval



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

- Certification Record 063533-C-000

cULus Approval, Hazardous Location



CULUS Listed 7RA9 IND. CONT. EQ. FOR HAZ. LOC.


Underwriters Laboratories Inc. complying with

- UL 508 (Industrial Control Equipment)
- CSA C22.2 No. 142 (Process Control Equipment)
- ANSI ISA 12.12.01, CSA C22.2 No. 213-M1987 (Hazardous Location)
- CSA-213 (Hazardous Location)

APPROVED for Use in

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

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

 WARNING
Explosion Hazard - Do not disconnect while circuit is live unless area is known to be non hazardous. Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2.

Note

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

Note

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

Note

This plant has to be mounted according to the NEC (National Electrical Code) stipulations.

When used in environments according to class I, division 2 (see above) , the SIMATIC NET S7 CPs must be mounted in an enclosure.

FM approval




Factory Mutual Approval Standard Class Number 3611,

Class I, Division 2, Group A, B, C, D, T3...T6 or

Class I, Zone 2, Group IIC, T3...T6.

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

 WARNING
Personal injury and damage to property may occur. In hazardous areas, personal injury or property damage can result if you create or break an electrical circuit during operation of a SIMATIC NET S7 CP (for example, by means of plug-in connections, fuses, switches). WARNING - EXPLOSION HAZARD: DO NOT DISCONNECT EQUIPMENT WHEN A FLAMMABLE OR COMBUSTIBLE ATMOSPHERE IS PRESENT. When used in hazardous locations (division 2 or zone 2), the device must be installed in an enclosure.

Index

"

"Interfaces" MIB group, 45

A

ATEX, 24

Autocrossing mechanism, 33

Autocrossover, 10

Autonegotiation, 10

Autosensing, 10, 33

B

Bandwidth limitation, 13

Block execution time, 18

C

Cabinet, 24

Cables for temperatures in excess of 70 °C, 25

CE mark, 49

Cell protection concept

VPN, 38

Changing CPU mode

From RUN to STOP, 28

Commissioning

Completeness of the STEP 7 project data, 25

Configuration, 25

Configuration and downloading the configuration data, 21

Configuration of the Ethernet interface, 22

Instruction, 22

Connecting a switch, 33

Connection resources of the CPU, 15

Connections for Web

Number, 18

Crossover cable, 33

CSA

Approval, 51

C-Tick

Approval, 50

D

Data storage of the configuration data of the CP, 27

DHCP server, 27

Diagnostics, 35

Diagnostics options, 31

Double addressing in the network, 34

Downloading, 35

Downloading project data, 26

Downloads, 8

E

E-mail, 11, 16, 22

EMC - electromagnetic compatibility, 50

ERROR LED, 29

Ethernet interface, 9, 10

Pin assignment, 26

F

FETCH/WRITE, 11, 16

S5/S7 addressing mode, 13

Firewall, 13

Firewall configuration, 45

Firmware version, 9

FM

Approval, 52

FTP, 22

FTP (FTP client), 15

FTP access only with security enabled, 42

FTP access using the FTP_CMD instruction - parameters for command types NOOP and QUIT, 42

FTP in client mode

Configuration limits, 18

FTP in server mode

Configuration limits, 18

FTPS (explicit mode), 13

G

Gigabit specification, 10

Global firewall rules, 13

Glossary, 3

- H**
 - Hardware product version, 9
 - Hazardous area, 23
 - Hazardous areas according to ATEX, 24
 - HMI communication, 11

- I**
 - IEC 61131-2, 49
 - Installation and commissioning, 25
 - Procedure, 26
 - Instruction
 - FTP_CMD, 18, 22
 - T_CONFIG, 22
 - TCON, 45
 - TCON, TSEND/TRCV, 22
 - TDISCON, 22
 - TMAIL_C, 22
 - TSEND_C/TRCV_C, 22
 - TUSEND/TURCV, 22
 - IP access protection, 45
 - IP address
 - IPv6, 12
 - Via DHCP, 34
 - IP configuration
 - IPv4 and IPv6, 12
 - IPsec tunnel
 - Number, 19
 - ISO, 22
 - ISO transport (complying with RFC 8073), 11
 - ISO transport connections, 16
 - ISO-on-TCP, 22
 - ISO-on-TCP (acc. to RFC 1006), 11
 - ISO-on-TCP connections, 16
 - IT functions, 11

- L**
 - LED display, 29
 - Logging, 13

- M**
 - MAC address, 9, 12, 27
 - MAINT LED, 29
 - Manual Collection, 8
 - Maximum data length for program blocks, 16
 - MIB
 - Supported, 44
 - MIB file and SNMP profile file, 44

- N**
 - Module replacement
 - Special feature of IP address assignment from a DHCP server (IPv4), 27
 - Multicast
 - via UDP connection, 11

- N**
 - NTP
 - (secure), 13, 43
 - NTP mode, 11, 43
 - NTP server, 43
 - Number
 - Operable CPs, 21
 - Number of connections, 16

- O**
 - Online help of STEP 7, 26
 - OP connections
 - Number, 18
 - Open communication, 11
 - Overall configuration limits, 21

- P**
 - PG communication, 11
 - PG connections
 - Number, 18
 - Ping, 35
 - Power supply modules
 - Additional, 21
 - PROFINET interface
 - LEDs, 30
 - Program block, (Instruction)
 - Programmed communications connections, 45
 - Protection against transient voltage surges, 25

- R**
 - Replacing components, 24
 - RUN/STOP LED, 29

- S**
 - S5/S7 addressing mode, 13
 - S7 communication, 11
 - S7 connections, 11, 15
 - Number of freely usable, 18
 - S7 routing function, 28

Safety extra low voltage, 23
 Safety notices, 23
 Security, 13
 Security access, 10
 Security functions, 13
 Setting the firewall, 35
 SIMATIC NET glossary, 3
 SIMATIC NET Manual Collection, 8
 SNMP (Simple Network Management Protocol), 44
 SNMP agent, 12
 SNMPv3, 14
 Special notes

- Connecting a switch, 33
- Ensuring a valid time of day, 43
- Recommendation for setting the time, 43
- Response if the reference to the FTP job block is missing, 42
- Special feature of time-of-day synchronization in NTP mode, 43

 Stateful packet inspection (layer 3 and 4), 13
 STEP 7, 3, 21
 System data type

- CONF_DATA, 22
- FTP_CONNECT_IPV4, 22
- FTP_CONNECT_IPV6, 22
- FTP_CONNECT_NAME, 22
- FTP_FILENAME, 22
- FTP_FILENAME_PART, 22
- TCON_Configured, 22
- TCON_IP_v4, 22
- TCON_ISOnative, 22
- TMAIL_FQDN, 22
- TMail_v4, 22
- TMail_v6, 22

T

TCP, 22
 TCP (acc. to RFC 793), 11
 TCP connections, 16
 TCP connections for FTP, 18
 Time synchronization, 11
 Time-of-day synchronization, 28, 43

U

UDP

- Restrictions, 17

 UDP (acc. to RFC 768), 11
 UDP connections, 16
 UDP frame buffering, 17

UL

- Approval, 51

V

Version history, 8
 Virtual Private Network

- Definition, 37

 VPN, (Virtual Private Network)

- Areas of application,
- Cell protection concept,

W

Web diagnostics, 28
 Web server, 12
 Windows XP firewall, 35

