SIEMENS

SIMATIC

S7-1500, ET 200MP, ET 200SP, ET 200AL Communication

Function Manual

Preface

Documentation guide 1

Product overview 2

Communications services 3

PG communication 4

HMI communication 5

Open communication 6

S7 communication 7

Point-to-point link 8

Routing 9

Connection resources 10

Connection diagnostics 11

Industrial Ethernet Security 12

Service & Support A

12/2014

A5E03735815-AD

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.

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E03735815-AD
Ⓟ 12/2014 Subject to change

Copyright © Siemens AG 2013 - 2014.
All rights reserved

Preface

Purpose of the documentation

This function manual provides you with an overview of the communication options, the CPUs, communication modules and processors of the SIMATIC S7-1500, ET 200MP, ET 200SP and ET 200AL systems. This function manual describes the connection-oriented, asynchronous communication.

The documentation covers the following:

- Overview of the communication services
- Properties of the communication services
- Overview of the user activities for setting up the communication services

Basic knowledge required

The following knowledge is required in order to understand the Function manual:

- General knowledge of automation technology
- Knowledge of the industrial automation system SIMATIC
- Knowledge about how to use STEP 7 (TIA Portal)

Scope of the documentation

This documentation is the basic documentation for all products of the SIMATIC S7-1500, ET 200MP, ET 200SP and ET 200AL systems. The product documentation is based on this documentation.

Changes compared to previous version

The following changes / additions are described in this manual, compared to the previous version (version 06/2014):

- Addition to the communication protocols and port numbers used for SIMATIC S7-1500 software controller
- Addition to the maximum connection resources used for HMI devices
- Addition to the data record routing functionality

Conventions

STEP 7: We refer to "STEP 7" in this documentation as a synonym for the configuration and programming software "STEP 7 as of V12 (TIA Portal)".

This documentation contains pictures of the devices described. The figures may differ slightly from the device supplied.

You should also pay particular attention to notes such as the one shown below:

Note

A note contains important information on the product, on handling of the product and on the section of the documentation to which you should pay particular attention.

Additional support

Information about Technical Support is available in the appendix Service & Support (Page 84).

The range of technical documentation for the individual SIMATIC products and systems can be found on the Internet (http://www.siemens.com/simatic-tech-doku-portal).

The online catalog and the ordering system are available on the Internet (http://mall.industry.siemens.com).

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. You can find more information about industrial security on the Internet (http://www.siemens.com/industrialsecurity).

To stay informed about product updates as they occur, sign up for a product-specific newsletter. You can find more information on the Internet (http://support.automation.siemens.com).

Table of contents

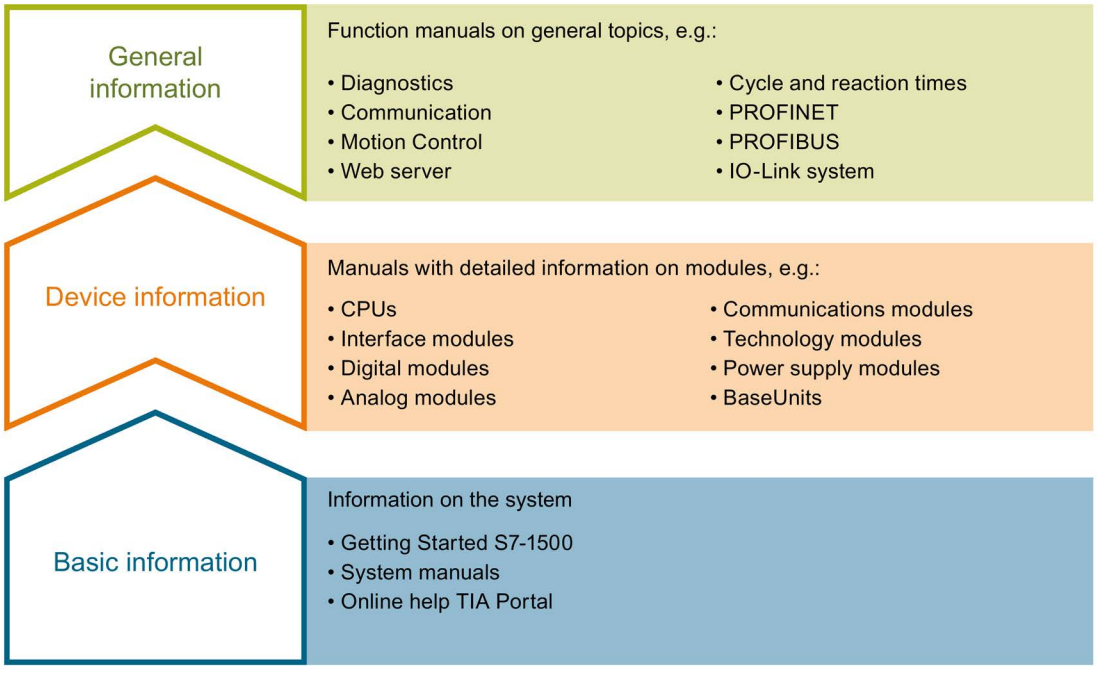
Preface 3
1 Documentation guide 7
2 Product overview 10
3 Communications services 15
3.1 Overview of communication options 15
3.2 Overview of connection resources 17
3.3 Setting up a connection 18
3.4 Data consistency 20
3.5 Communications protocols and used port numbers 22
4 PG communication 26
5 HMI communication 29
6 Open communication 31
6.1 Overview of open communication 31
6.2 Protocols for open communication 32
6.3 Instructions for open communication 33
6.4 Setting up open communication with TCP, ISO-on-TCP, UDP and ISO 36
6.5 Setting up communication with Modbus TCP 42
6.6 Setting up communication via e-mail 44
6.7 Setting up communication via FTP 45
6.8 Establishment and termination of communications relations 48
7 S7 communication 49
8 Point-to-point link 58
9 Routing 64
9.1 S7 routing 64
9.2 Data record routing 69
10 Connection resources 71
10.1 Allocation of connection resources 71
11 Connection diagnostics 77

12 Industrial Ethernet Security 81
12.1 Firewall 82
12.2 Logging 82
12.3 NTP client 83
12.4 SNMP 83
A Service & Support 84
Glossary 87
Index 97

Documentation guide

1

The documentation for the SIMATIC S7-1500 automation system and the SIMATIC ET 200MP, ET 200SP and ET 200AL distributed I/O systems is divided into three areas. This division allows you easier access to the specific information you require.



Basic information

System manuals and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500, ET 200MP, ET 200SP and ET 200AL systems. The STEP 7 online help supports you in the configuration and programming.

Device information

Product manuals contain a compact description of the module-specific information, such as properties, terminal diagrams, characteristics and technical specifications.

General information

The function manuals contain detailed descriptions on general topics such as diagnostics, communication, Motion Control, Web server.

You can download the documentation free of charge from the Internet (http://w3.siemens.com/mcms/industrial-automation-systems-simatic/en/manual-overview/Pages/Default.aspx).

Changes and additions to the manuals are documented in product information sheets.

Manual Collections

The Manual Collections contain the complete documentation of the systems put together in one file.

You will find the Manual Collections on the Internet:

- S7-1500/ET 200MP (http://support.automation.siemens.com/WW/view/en/86140384)
- ET 200SP (http://support.automation.siemens.com/WW/view/en/84133942)
- ET 200AL (http://support.automation.siemens.com/WW/view/en/95242965)

My Documentation Manager

The My Documentation Manager is used to combine entire manuals or only parts of these to your own manual.
You can export the manual as PDF file or in a format that can be edited later.

You can find the My Documentation Manager on the Internet (http://support.automation.siemens.com/WW/view/en/38715968).

Applications & Tools

Applications & Tools supports you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus in individual products.

You can find Applications & Tools on the Internet (http://support.automation.siemens.com/WW/view/en/20208582).

CAx Download Manager

The CAx Download Manager is used to access the current product data for your CAx or CAe systems.

You configure your own download package with a few clicks.

In doing so you can select:

- Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files
- Manuals, characteristics, operating manuals, certificates
- Product master data

You can find the CAx Download Manager on the Internet (http://support.automation.siemens.com/WW/view/en/42455541).

TIA Selection Tool

With the TIA Selection Tool, you can select, configure and order devices for Totally Integrated Automation (TIA).
This tool is the successor of the SIMATIC Selection Tool and combines the known configurators for automation technology into one tool.
With the TIA Selection Tool, you can generate a complete order list from your product selection or product configuration.

You can find the TIA Selection Tool on the Internet (http://w3.siemens.com/mcms/topics/en/simatic/tia-selection-tool).

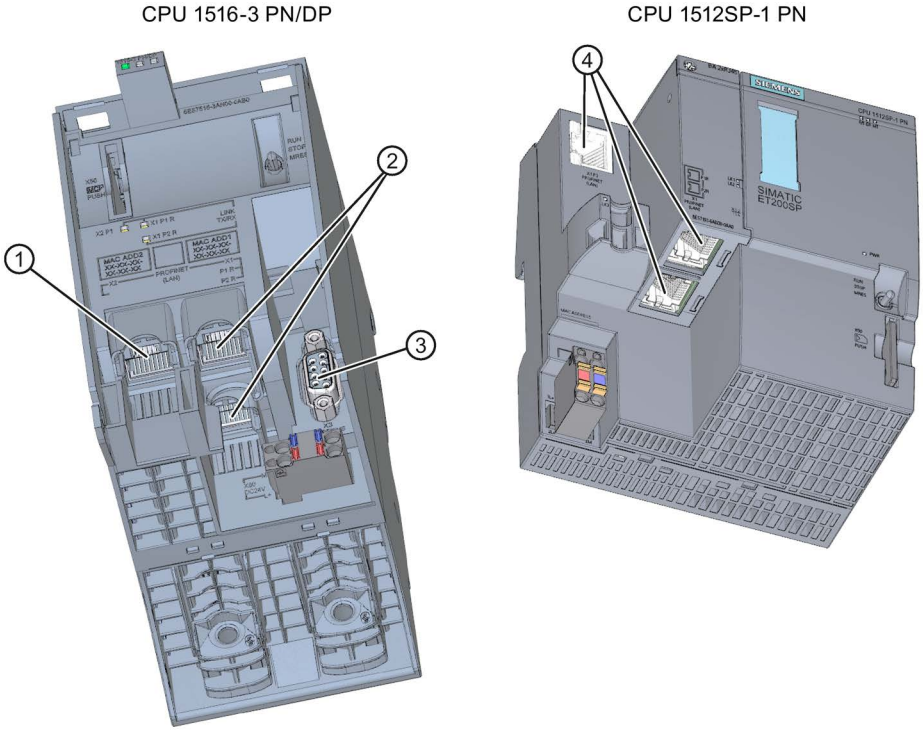
Product overview

2

CPUs, communications modules and processors, and PC systems of the S7-1500, ET 200MP, ET 200SP and ET 200AL systems provide you with interfaces for communication via PROFINET, PROFIBUS and point-to-point connections.

CPUs, communications modules and communications processors

PROFINET and PROFIBUS DP interfaces are integrated in the S7-1500 CPUs. The CPU 1516-3 PN/DP for example has two PROFINET interfaces and one PROFIBUS DP interface. Other PROFINET and PROFIBUS DP interfaces are available by using communications modules (CM) and communications processors (CP).

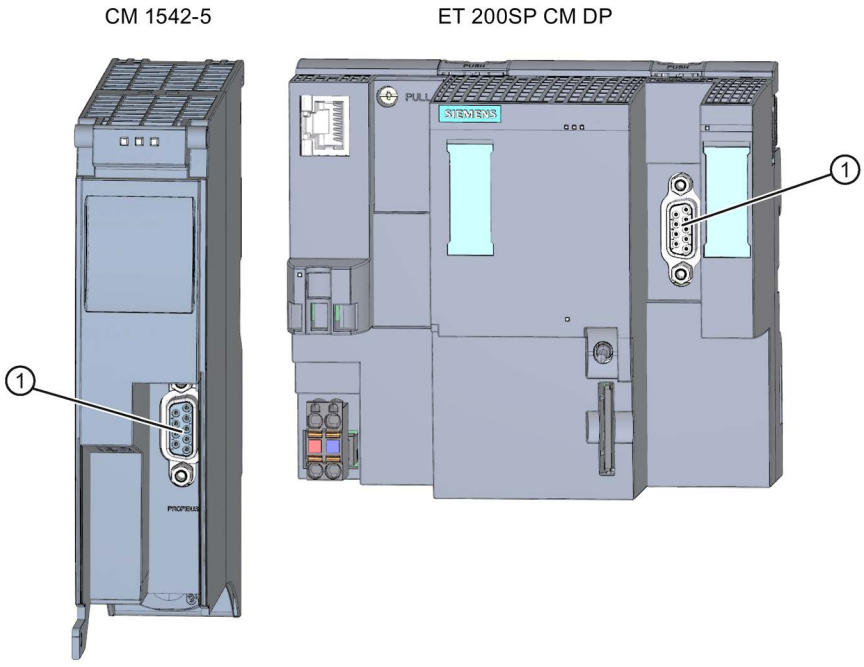


① PROFINET interface (X1) with 1 port
② PROFINET interface (X2) with 2-port switch
③ PROFIBUS DP interface (X3)
④ PROFINET interface (X1) with 3-port switch

Figure 2-1 Interfaces of the CPU 1516-3 PN/DP and CPU 1512SP-1 PN

Interfaces of communications modules

Interfaces of communications modules (CM) behave in exactly the same way as integrated interfaces of S7-1500 CPUs of the same interface type (for example PROFIBUS DP). They serve to extend the system with the corresponding interfaces (for example, they add a PROFIBUS interface to the communication module CM 1542 5 of the S7-1500 automation system).

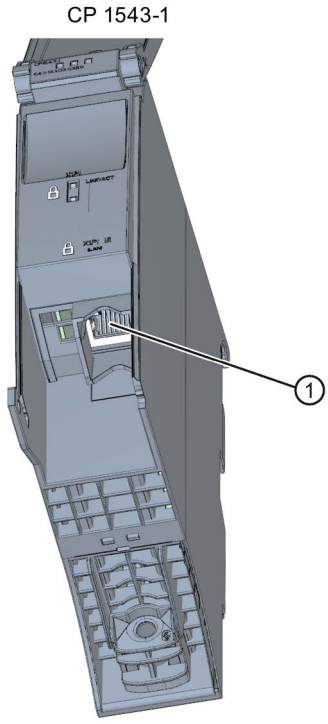


① PROFIBUS DP interface

Figure 2-2 PROFIBUS DP interface of the CM 1542-5 and CM DP

Interfaces of communications processors

Interfaces of communications processors (CP) provide different functionalities compared with the integrated interfaces of the CPUs. CPs allow special applications, for example the CP 1543-1 provides Industrial Ethernet security functions for protecting Industrial Ethernet networks via its Industrial Ethernet interface.



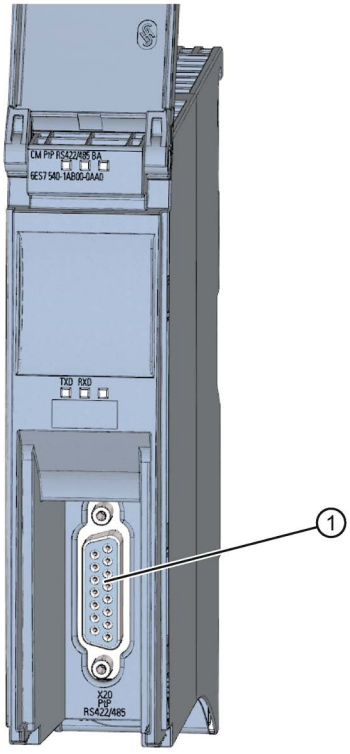
① Industrial Ethernet interface

Figure 2-3 Industrial Ethernet interface of the CP 1543-1

Interfaces of communications modules for point-to-point connections

The communication modules for point-to-point connections provide communication via their RS 232-, RS 422- and RS 485 interfaces, for example, Freeport or Modbus communication.

CM PtP RS422/485 BA

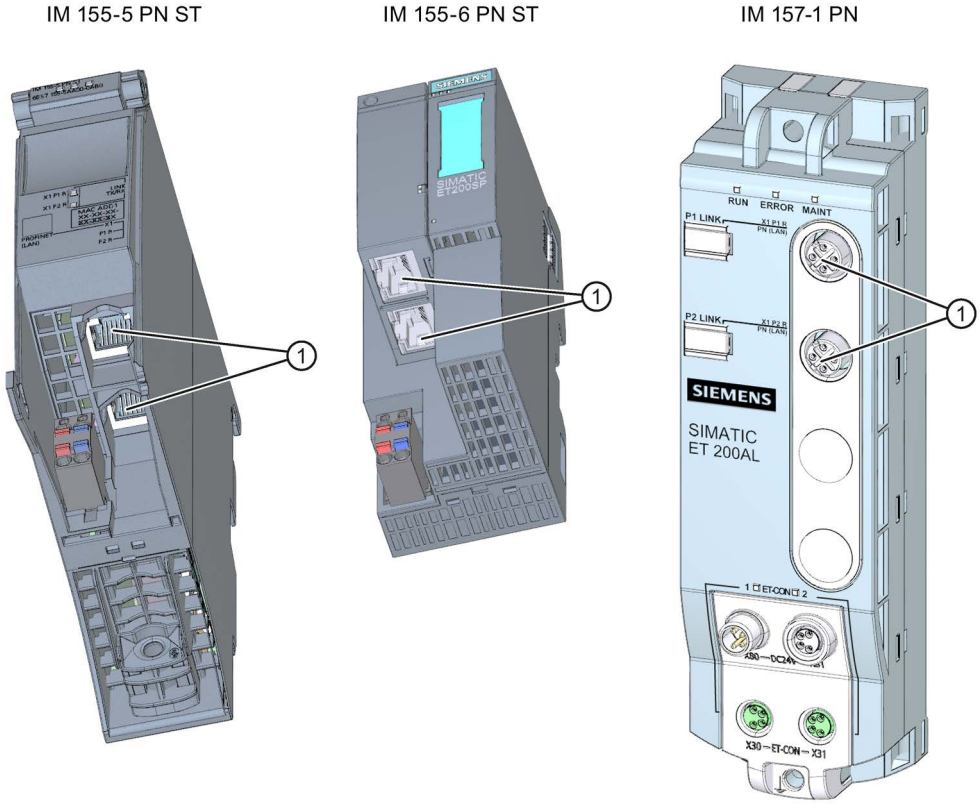


① Interface for point-to-point connections

Figure 2-4 Interface for point-to-point connection of the CM PtP RS422/485 BA

Interfaces of interface modules

PROFINET and PROFIBUS DP interfaces of the interface modules (IM) in ET 200MP, ET 200SP and ET 200AL are used to connect the distributed I/O ET 200MP, ET 200SP and ET 200AL to PROFINET or PROFIBUS of the higher-level IO controller or DP master.



① PROFINET interface with 2-port switch

Figure 2-5 PROFINET interfaces IM 155-5 PN ST (ET 200MP), IM 155-6 PN ST (ET 200SP), and IM 157-1 PN (ET 200AL)

Communications services

The communications services described below use the interfaces and communication mechanisms provided by the system via CPUs, communication modules and processors.

Communications services 3

3.1 Overview of communication options

Overview of communications options

The following communications options are available for your automation task.

Table 3- 1 Communications options

Communications options	Functionality	Via interface:		
		PN/IE*	DP	serial
PG communication	On commissioning, testing, diagnostics	X	X	-
HMI communication	On operator control and monitoring	X	X	-
Open communication using TCP/IP	Data exchange via PROFINET/Industrial Ethernet with TCP/IP Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Open communication using ISO-on-TCP	Data exchange via PROFINET/Industrial Ethernet with ISO-on-TCP Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Open communication with UDP	Data exchange via PROFINET/Industrial Ethernet with UDP Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-

Communications options	Functionality	Via interface:		
		PN/IE*	DP	serial
Open communication via ISO (only CPs with PROFINET/Industrial Ethernet interface)	Data exchange via PROFINET/Industrial Ethernet with the ISO protocol Instructions: • TSEND_C/TRCV_C • TSEND/TRCV • TCON • T_DISCON	X	-	-
Communication via Modbus TCP	Data exchange via PROFINET with Modbus TCP protocol Instructions: • MB_CLIENT • MB_SERVER	X	-	-
E-mail	Sending process alarms via e-mail Instruction: • TMAIL_C	X	-	-
FTP (only CPs with PROFINET/Industrial Ethernet interface)	File management and file access via FTP (File Transfer Protocol); CP can be FTP client and FTP server Instruction: • FTP_CMD	X	-	-
Fetch/Write (only CPs with PROFINET/Industrial Ethernet interface)	Server services via TCP/IP, ISO-on-TCP and ISO Via special instructions for Fetch/Write	X	-	-
S7 communication	Data exchange client/server or client/client Instructions: • PUT/GET • BSEND/BRCV • USEND/URCV	X	X	-
Serial point-to-point connection	Data exchange via point-to-point with Freeport, 3964(R), USS or Modbus protocol Via special instructions for PtP, USS or Modbus/RTU	-	-	X
Web server	Data exchange via HTTP(S), for example for diagnostics	X	-	-
SNMP (Simple Network Management Protocol)	Diagnostics for "network health" of IP networks, possibly parameterization of the IP network components via standard SNMP protocol	X	-	-
Time-of-day synchronization	Via PN/IE interface: CPU is NTP client (Network Time Protocol)	X	-	-
	Via DP interface: CPU/CM/CP is time-of-day master or time slave	-	X	-

* IE - Industrial Ethernet

Additional information

- You will find information about the Fetch/Write services in the STEP 7 online help.
- You can find additional information on the PtP link in the function manual CM PtP - Configurations for Point-to-Point Connections (http://support.automation.siemens.com/WW/view/en/59057093).
- You will find the description of the web server functionality in the function manual Web server (http://support.automation.siemens.com/WW/view/en/59193560).
- You will find information about the standard protocol SNMP on the Service & Support pages on the Internet (http://support.automation.siemens.com/WW/view/en/15166742).
- You can find information on time synchronization in the system manual S7-1500, ET 200MP (http://support.automation.siemens.com/WW/view/en/59191792).

3.2 Overview of connection resources

Connection resources

Some communications services require connections. Connections allocate resources on the CPUs, CPs and CMs involved (for example memory areas in the CPU operating system). In most cases one resource per CPU/CP/CM is allocated for a connection. In HMI communication, up to 3 connection resources are required per HMI connection.

The connection resources available depend on the CPU being used, the CPs and CMs and must not exceed a defined high limit for the automation system.

Available connection resources in a station

The maximum number of resources of a station is determined by the CPU.

Each CPU has reserved connection resources for PG, HMI and web server communication. There are also resources available that can be used for SNMP, e-mail connections, HMI, S7 communication as well as for open communication.

When are connection resources allocated?

The time for allocation of connection resources depends on how the connection is set up, automatic, programmed or configured (see section Setting up a connection (Page 18)).

Additional information

You will find more detailed information on the allocation of connection resources and the display of connection resources in STEP 7 in the section Connection resources (Page 71).

3.3 Setting up a connection

Automatic connection

STEP 7 sets up a connection automatically (for example PG or HMI connection) if you have connected the PG/PC interface to an interface of the CPU physically and have made the interface assignment in STEP 7 in the "Go online" dialog.

Setting up a programmed connection

You set up the programmed connection in the program editor of STEP 7 in the context of a CPU by assigning instructions for communication, for example TSEND_C.

When specifying the connection parameters (in the Inspector window, in the properties of the instruction), you are supported by the easy-to-use user interface.

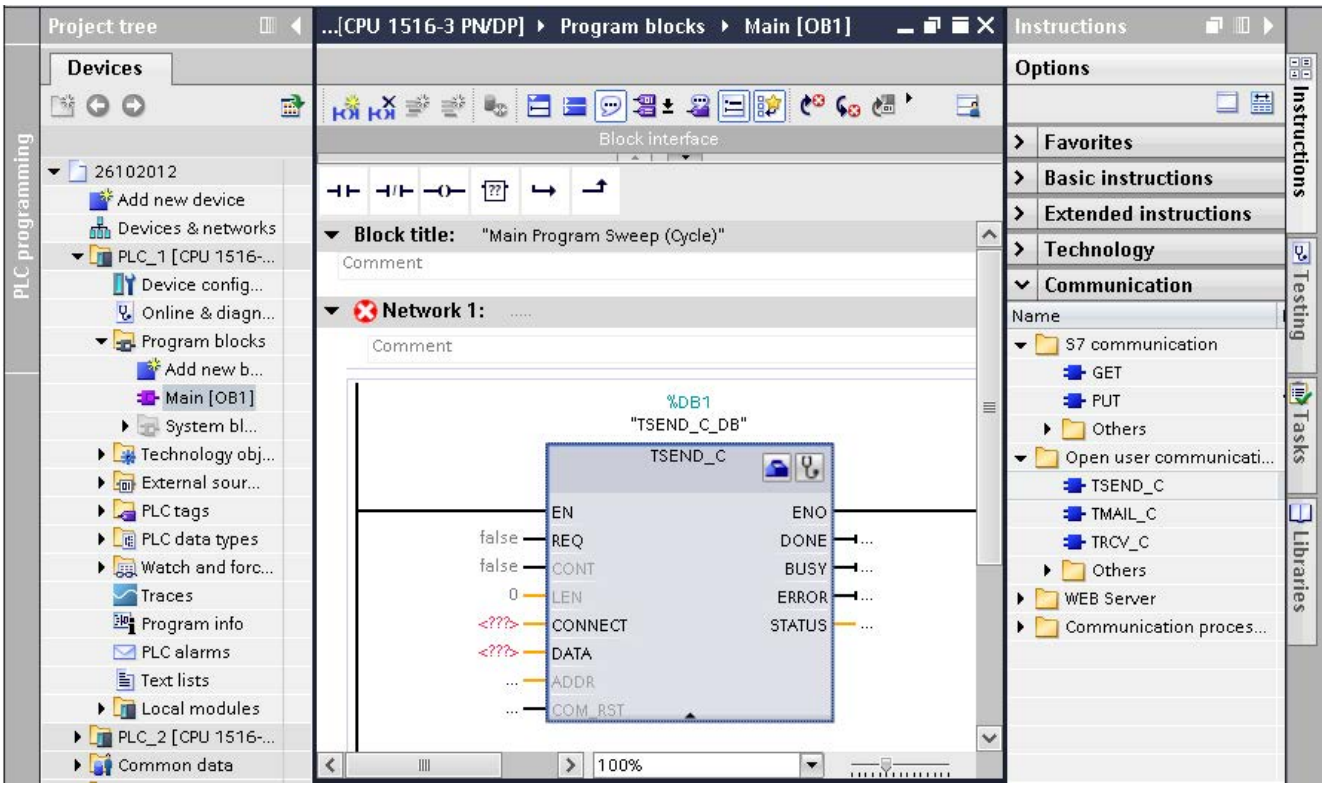


Figure 3-1 Programmed setup

Setting up a configured connection

You set up the configured connection in the network view of the Devices & networks editor of STEP 7 in the context of a CPU or a software controller.

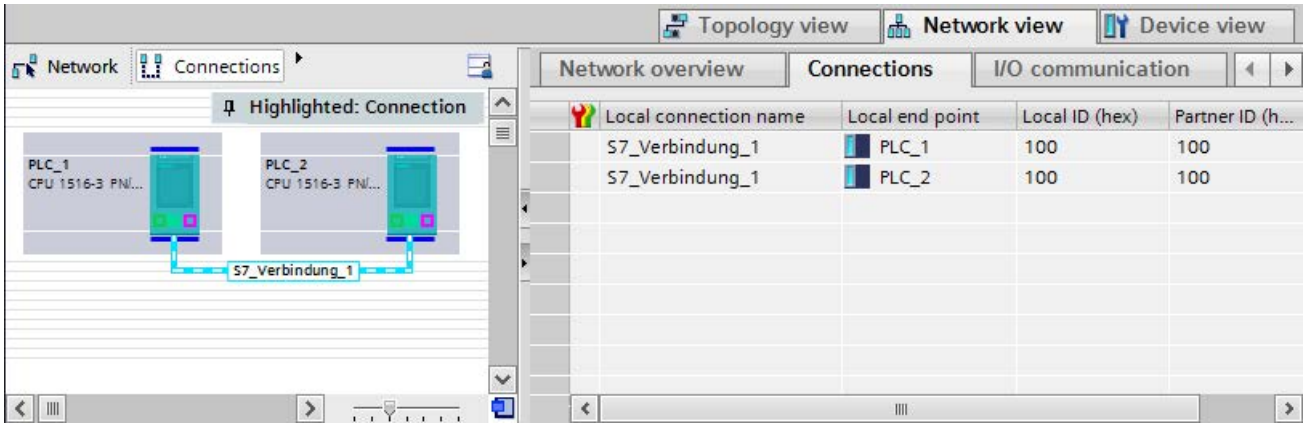


Figure 3-2 Configured setup

Summary

You can often choose between a configured or a programmed connection. Programmed connection setup allows connection resources to be released following data transfer. Programmed connections are not guaranteed as routed connections, i.e. they are not established when insufficient resources are available. With configured connection setup, the resource remains allocated after download of the configuration until the configuration changes again. Connection establishment via configured connections therefore cannot fail due to lack of resources. The "Connection resources" table in the Inspector window of the CPU displays an overview of connection resources already used and those still available.

Table 3- 2 Setting up the connection

Connection	Automatically	Programmed setup	Configured setup
Programming device connection	X	-	-
HMI connection	X	-	X
Open communication via TCP/IP connection	-	X	X
Open communication via ISO-on-TCP connection	-	X	X
Open communication via UDP connection	-	X	X
Open communication via ISO connection	-	X	X
Communication via Modbus TCP connection	-	X	-
E-mail connection	-	X	-
FTP connection	-	X	-
S7 connection	-	-	X

Additional information

You will find further information on the allocation of connection resources and the display of connection resources in STEP 7 in the section Connection resources (Page 71).

3.4 Data consistency

Definition of data consistency

A data block which cannot be modified by concurrent processes is called consistent data area. This means that a data block which belongs together and which is larger than the consistent data area can consist in part of new and of old data at the same time.

Example

An inconsistency can occur when an instruction for communication is interrupted, for example by a hardware interrupt OB with higher priority. If the user program in this OB now changes the data that has already been partly processed by the instruction, the transferred data originates:

- Partly from the time prior to hardware interrupt processing
- Partly from the time after the hardware interrupt processing.

This means that the date is inconsistent (processed at different points in time).

Effect

No inconsistency occurs if the system-specific maximum size of the consistent data is kept to. The S7-1500 CPUs allow a maximum of 462 bytes (see below).

If more data than the system-specific maximum size needs to be transferred consistently, you yourself must ensure that the data remains consistent in the application. This can, for example extend the interrupt reaction time of the CPU.

Data consistency with S7-1500

Use of instructions for access to common data:

If the user program contains instructions for communication that access common data, for example TSEND/TRCV, you can coordinate access to this data area yourself, for example using the "DONE" parameter. The data consistency of the data areas that are transferred locally with an instruction for communication can therefore be ensured in the user program.

Use of PUT/GET instructions or Write/Read via HMI communication:

In S7 communication with the PUT/GET instructions or Write/Read via HMI communication, you need to take into account the size of the consistent data areas during programming or configuration because there is no instruction in the user program of the target device (server) that can coordinate the data transfer in the user program.

System-specific maximum data consistency for S7-1500:

With an S7-1500, communication data is transferred in blocks of up to 462 bytes consistently into or out of the user memory during the program cycle. Data consistency is not ensured for larger data areas. Where defined data consistency is required, the length of communication data in the user program of the CPU must not exceed 462 bytes. You can then access these data areas consistently, for example from an HMI device using Read/Write tags.

Maximum data consistency for point-to-point CM:

With communication via a CM for a point-to-point connection, the data consistency is ensured by the Send/Receive instructions in the user program. The maximum data consistency is 4 KB, depending on the module type.

Additional information

- You will find the maximum amount of consistent data in the CPU, CM or CP manuals in the Technical specifications.
- You will find further information on data consistency in the description of the instructions in the STEP 7 online help.

3.5 Communications protocols and used port numbers

This section provides an overview of the protocols and port numbers used. For each protocol the address parameters, the respective communications layer as well as the communications role and the communications direction are specified.

This information makes it possible to match the security measures for protection of the automation system to the used protocols (for example firewall). Because security measures are limited to Ethernet or PROFINET networks, the tables do not include PROFIBUS protocols.

The tables below show the different layers and protocols that are being used.

The following table shows the protocols supported by the S7-1500 and ET 200SP CPUs. The S7-1500 software controllers also support the protocols listed in the following table for the Ethernet interfaces that are assigned to the software controller.

Table 3- 3 Layers and protocols

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
PROFINET protocols				
DCP Discovery and configuration protocol	Not relevant	(2) Ethertype 0x8892 (PROFINET)	Accessible devices PROFINET Discovery and configuration	DCP is used by PROFINET to discover PROFINET devices and provide basic settings.
LLDP Link Layer Discovery protocol	Not relevant	(2) Ethertype 0x88CC (LLDP)	PROFINET Link Layer Discovery protocol	LLDP is used by PROFINET to discover and manage neighbor relationships between PROFINET devices. LLDP uses the special multicast MAC address: 01-80-C2-00-00-0E
MRP Media Redun-dancy Protocol	Not relevant	(2) Ethertype 0x88E3 (IEC 62493-2-2010)	PROFINET medium redundancy	MRP provides control of redundant transmission paths by means of a ring topology. MRP uses multicast MAC addresses according to the standard
PTCP Precision Transparent Clock Protocol	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET send clock and time synchro-nization, based on IEEE 1588	PTC provides a time delay measurement between RJ45 ports and thus send clock synchronization and time synchronization. PTCP uses multicast MAC addresses according to the standard
PROFINET IO data	Not relevant	(2) Ethertype 0x8892 (PROFINET)	PROFINET Cyclic IO data transfer	The PROFINET IO frames are used to transmit IO data cyclically between PROFINET IO controller and IO devices via Ethernet.
PROFINET Context Manager	34964	(4) UDP	PROFINET connection less RPC	The PROFINET Context Manager provides an endpoint mapper in order to establish an application relation (PROFINET AR).

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
Connection-oriented communications protocols				
SMTP Simple mail transfer protocol	25	(4) TCP	Simple mail transfer protocol	SMTP is used for sending e-mail and SMS (depending on provider).
HTTP Hypertext transfer protocol	80	(4) TCP	Hypertext transfer protocol	HTTP is used for communication with the CPU-internal web server.
ISO on TCP (according to RFC 1006)	102	(4) TCP	ISO-on-TCP protocol	ISO on TCP (according to RFC 1006) is used for message-oriented data exchange to remote CPU or software controller. S7 communication with ES, HMI, OPC server, etc.
NTP Network time protocol	123	(4) UDP	Network time protocol	NTP is used for synchronization of the CPU system time with the time of an NTP server.
SNMP Simple network management protocol	161 162 (trap)	(4) UDP	Simple network management protocol	SNMP is used for reading and setting of network management data (SNMP managed Objects) by the SNMP Manager.
HTTPS Secure Hypertext transfer protocol	443	(4) TCP	Secure Hypertext transfer protocol	HTTPS is used for communication with the CPU-internal web server via Secure Socket Layer (SSL).
Modbus TCP Modbus Transmission Control Protocol	502	(4) TCP	Modbus/TCP protocol	Modbus/TCP is used by MB_CLIENT/MB_SERVER instructions in the user program.
OUC[1] Open User Communication	1 ... 1999 can be used to limited extent[2]	(4) TCP (4) UDP	Open User Communication (TCP/UDP)	OUC instructions provide connection establishment, connection termination and data transfer based on the socket layer.
	2000 ... 5000 Recommended			
	5001 ... 49151 can be used to limited extent[2]			

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
Reserved	49152 ... 65535	(4) TCP (4) UDP	-	Dynamic port area used for active connection end point if the application does not determine the local port number.

1 Note: The open communication provides direct access to the UDP/TCP for the user. The user is responsible for observing the port restrictions/definitions of the IANA (Internet Assigned Numbers Authority).

2 Do not use ports for OUC, which are already used by other protocols.

The following table shows the protocols that are supported by the S7-1500 software controller via the Ethernet interfaces assigned to Windows.

Table 3- 4 Layers and protocols

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
PROFINET protocols				
DCP Discovery and configuration protocol	Not relevant	(2) Ethertype 0x8892 (PROFINET)	Accessible devices PROFINET Discovery and configuration	DCP is used by PROFINET to discover PROFINET devices and provide basic settings.
Connection-oriented communications protocols				
SMTP Simple mail transfer protocol	25	(4) TCP	Simple mail transfer protocol	SMTP is used for sending e-mail and SMS (depending on provider).
HTTP Hypertext transfer protocol	Adjustable [1]	(4) TCP	Hypertext transfer protocol	HTTP is used for communication with CPU-internal web server. You can change the port number to avoid conflict with other web servers on Windows. If you want to use web server access, you must activate the port in the Windows Firewall.
ISO on TCP (according to RFC 1006)	102	(4) TCP	ISO-on-TCP protocol	ISO on TCP (according to RFC 1006) for S7 communication with PG/PC or HMI.
OUC[2] Open User Communica-tion	1 ... 1999 can be used to limited extent[3, 4]	(4) TCP (4) UDP	Open User Communica-tion (TCP/UDP)	OUC instructions provide connection establishment, connection termination and data transfer based on the socket layer. If you want to use OUC, you must activate the ports in the Windows Firewall.
	2000 ... 5000 recom-mended[4]			
	5001 ... 49151 can be used to limited extent[3, 4]			

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
Reserved	49152 ... 65535	(4) TCP (4) UDP	-	Dynamic port range that is used for the active connection end point, if the application does not determine the local port number. If you wish to use this communication, you must activate the ports in the Windows Firewall.

1 Default setting for Windows assigned interfaces: 81

2 Note: The open user communication provides direct access to the UDP/TCP for the user. The user is responsible for observing the port restrictions/definitions of the IANA (Internet Assigned Numbers Authority).

3 Do not use ports for OUC, which are already used by other protocols.

4 Do not use ports for OUC, which are already used by other Windows applications.

The following table shows the protocols that are supported in addition to those listed in the tables for the S7-1500 communications modules (e.g. CP 1543-1).

Table 3- 5 Layers and protocols

Protocol	Port number	(2) Link layer (4) Transport layer	Function	Description
PROFINET/Industrial Ethernet protocols				
Connection-oriented communications protocols				
FTP File transfer protocol	20 (data) 21 (control)	(4) TCP	File transfer protocol	FTP is used for the transmission of files (only in connection with CP).
secureFTP File transfer protocol	20 (data) 21 (control)	(4) TCP	File transfer protocol	SecureFTP is used for the transmission of files by means of a TSL connection (only in connection with CP).
DHCP Dynamic Host Configuration Protocol	68	(4) UDP	Dynamic Host Configuration Protocol	DHCP is used to retrieve the IP Address Suite from a DHCP server when starting up the IE interface.
Secure NTPv3 Network time protocol	123	(4) UDP	Network time protocol	NTP is used to synchronize the CM/CP internal system clock with an NTP server.
SNMP Simple network management protocol	161 162 (trap)	(4) UDP	Simple net-work man-agement protocol	SNMPv3 permits the CM/CP to read Network Management Data (MIBs) from SNMPv3 agent with authentication.

PG communication 4

Properties

Using PG communication, the CPU or another module capable of communication exchanges data with an engineering station (for example PG, PC). The data exchange is possible via PROFIBUS and PROFINET subnets. The gateway between S7 subnets is also supported.

PG communication provides functions needed to load programs and configuration data, run tests, and evaluate diagnostic information. These functions are integrated in the operating system of the module capable of communication.

A PG/PC can be connected to a CPU online. The PG/PC can operate a maximum of 4 online connections at one time (for example to 4 CPUs).

Requirements

- The PG/PC is physically connected to the communication-capable module.
- If the communication-capable module is to be reached via S7 routing, the hardware configuration has to be loaded in the participating stations (S7 router and end point).

Procedure for connecting online

You must establish an online connection to the CPU for the programming device communication:

1. Select the CPU in the project tree in STEP 7.
2. Select the "Online > Go online" menu command.

3. In the "Go online" dialog, make the following settings for your online connection:
   - Select interface type (e.g. PN/IE) in the "Type of PG/PC interface" drop-down list.
   - In the "PG/PC interface" drop-down list, select the PG/PC interface (e.g. Ind. Ethernet card) you want to use to establish the online connection.
   - Select the interface or the S7 subnet with which the PG/PC is physically connected from the "Connection to interface/subnet" drop-down list.
   - If the communication-capable module can be reached via an S7 router (gateway), select the S7 router that connects the subnets in question from the "1st Gateway" drop-down .

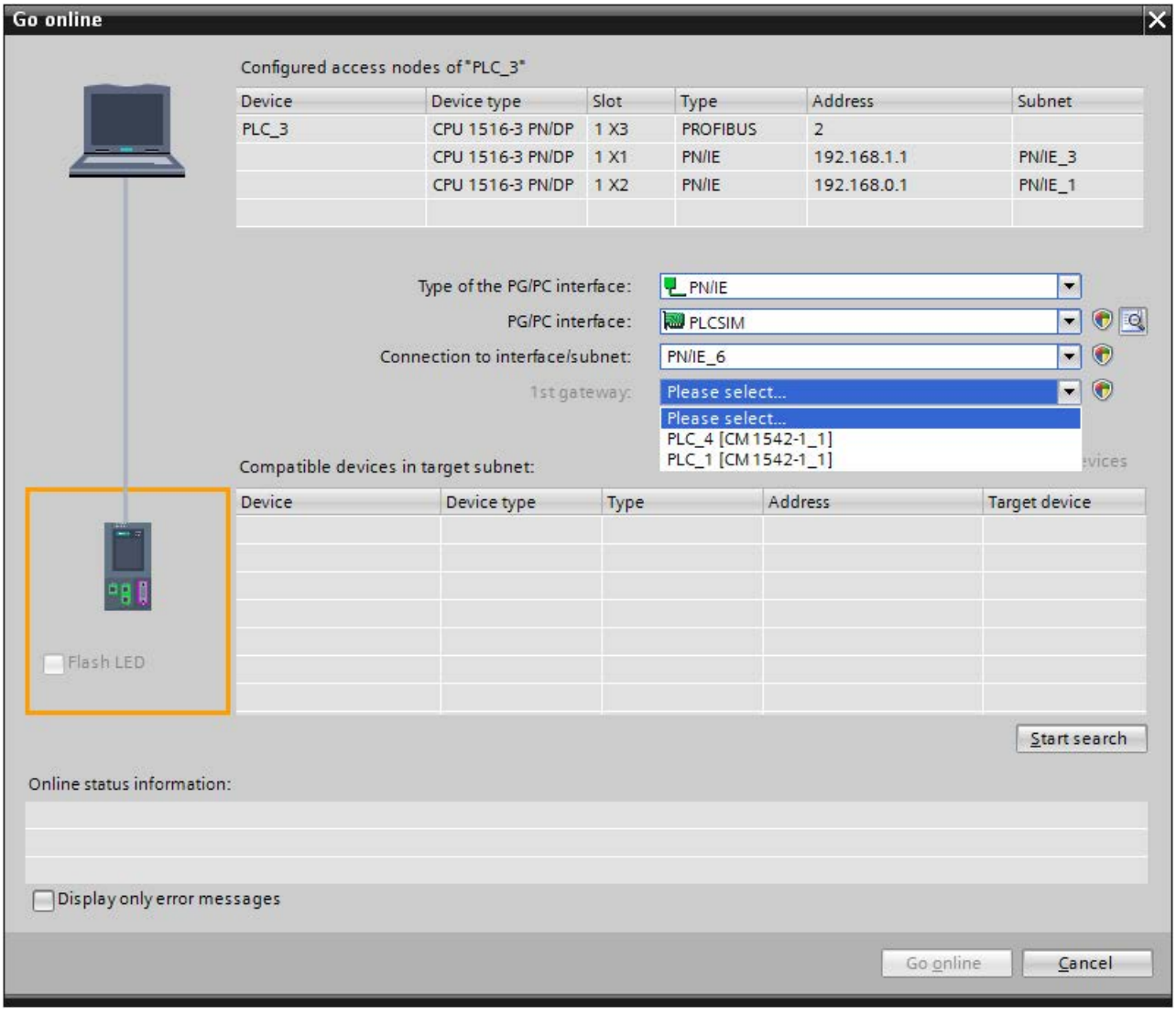


Figure 4-1 Setting up PG communication

4. In the "Compatible devices in target subnet" table, select the relevant CPU and confirm with "Go online".

Additional information

You can find more information on "Go online" in the STEP 7 online help.

HMI communication 5

Properties

Using HMI communication, one or more HMI devices (for example HMI Basic/Comfort/Mobile Panel) exchanges data with a CPU for operator control and monitoring with via the PROFINET or PROFIBUS DP interface. The data exchange is via HMI connections.

If you want to set up several HMI connections to a CPU, use for example:

- The PROFINET and PROFIBUS DP interfaces of the CPU
- CPs and CMs with the relevant interfaces

Procedure for setting up HMI communication

1. Configure the HMI device in an existing configuration with a CPU in the network view of the Devices & networks editor of STEP 7.
2. Select the "Connections" button and then "HMI connection" from the drop-down list.
3. Drag-and-drop a line between the end points of the connection (HMI device and CPU). The end points are highlighted in color. If the required S7 subnet does not yet exist, it is created automatically.

4. In the "Connections" tab, select the row of the HMI connection.

   In the "General" area of the "Properties" tab, you see the properties of the HMI connection, some of which you can change.

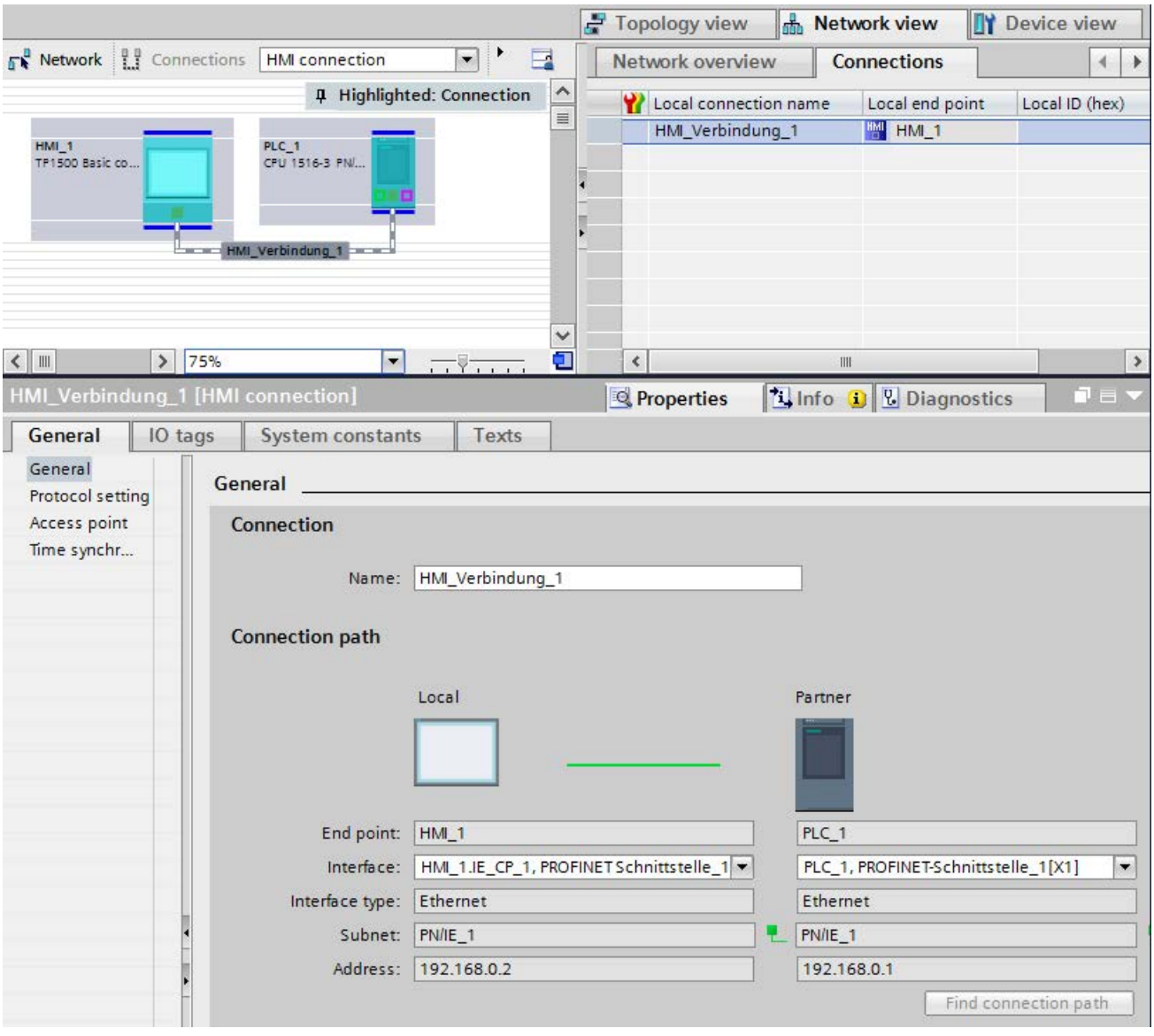


Figure 5-1 Setting up HMI communication

5. Download the hardware configuration to the CPU.
6. Download the hardware configuration to the HMI device.

Additional information

You can find information on S7 routing for HMI connections in the section S7 Routing (Page 64).

You can find more information on setting up HMI connections in the STEP 7 online help.

Open communication 6

6.1 Overview of open communication

Features of open communication

Using open communication, the CPU exchanges data with another module capable of communication. The main features of open communication are as follows:

- Open standard (communication partners can be two SIMATIC CPUs or a SIMATIC CPU and a suitable third-party device).
- Communication via various protocols (in STEP 7 known as "Connection types")
- High degree of flexibility in terms of the data structures transferred; this allows open data exchange with any communications devices as long as these support the connection types available.
- Open communication is possible in various automation systems, see technical specifications of the respective manuals.
  Examples:
  - Integrated PROFINET / Ind. Ethernet interfaces of CPUs (S7-1500, ET 200SP CPU, S7-1500 software controller)
  - PROFINET / Ind. Ethernet interfaces of communications modules (e.g. CP 1543-1, CM 1542-1)

6.2 Protocols for open communication

Protocols for open communication

The following protocols are available for open communication:

Table 6- 1 Transport protocols for open communication

Transport protocol	Via interface
TCP according to RFC 793	PROFINET/Industrial Ethernet
ISO-on-TCP according to RFC 1006 (Class 4)	PROFINET/Industrial Ethernet
ISO according to ISO/IEC 8073	Industrial Ethernet (only CP 1543-1)
UDP according to RFC 768	PROFINET/Industrial Ethernet

Table 6- 2 Application protocols for open communication

Application protocol	Used transport protocol
Modbus TCP	**TCP** according to RFC 793
E-mail	**TCP** according to RFC 793
FTP	**TCP** according to RFC 793

TCP, ISO-on-TCP, ISO, UDP

Prior to data transfer, these protocols (except UDP) establish a transport connection to the communications partner. Connection-oriented protocols are used when potential loss of data needs to be avoided.

The following is possible with UDP:

- Unicast to one device or broadcast to all devices on PROFINET via the PROFINET interface of the CPU or the Industrial Ethernet interface of the CP 1543-1
- Multicast to all recipients of a multicast group via the PROFINET/Industrial Ethernet interface of the CP 1543-1

Modbus TCP

The Modbus protocol is a communication protocol with linear topology based on a master/slave architecture. In the Modbus TCP (Transmission Control Protocol), the data is transmitted as TCP/IP packets.

Communication is controlled solely by suitable instructions in the user program.

E-mail and FTP

You can use email to send for example, data block contents (e.g. process data) as an attachment.

You can use the FTP connection (FTP = File Transfer Protocol) to transmit files to and from S7 devices.

The communication is controlled by instructions in the user program at the client end.

6.3 Instructions for open communication

Introduction

You set up open communication via the relevant connection (for example TCP connection) as follows:

- By programming in the user programs of the communications partners or
- By configuring the connection in STEP 7 in the hardware and network editor

Regardless of whether you set up the connection by programming or configuring, instructions are always required in the user programs of both communications partners for sending and receiving the data.

Setting up the connection via the user program

If the connection is set up by programming, the connection establishment and termination is implemented using instructions in the user program.

In certain areas of application it is an advantage not to set up the communications connections statically by configuring in the hardware configuration, but to have them set up by the user program. You can set up the connections via a specific application program-controlled and therefore when necessary. Programmed connection setup also allows connection resources to be released following data transfer.

A data structure is necessary for each communications connection that contains the parameters for establishing the connection (for example system data type "TCON_IP_v4" for TCP).

The system data types (SDT) are provided by the system and have a predefined structure that cannot be changed.

The various protocols have their own data structures (see table below). The parameters are stored in a data block ("connection description DB") for example of the system data type TCON_IP_v4.

There are two ways in which you can specify the DB with the data structure:

- Create the data block manually, assign parameters to it and write it directly to the instruction (necessary for e-mail and FTP)
- Recommendation: Have the data block created automatically in the properties in the program editor during configuration of the connection for the TSEND_C, TRCV_C and TCON instructions.

You can modify the connection parameters in the "connection description DB".

Protocols, system data types and employable instructions for programmed setup

Table 6- 3 Instructions for programmed setup of the connection

Protocol	System data type	Instructions for the user program
TCP	• TCON_IP_v4	Establish connection and send/receive data via: • TSEND_C/TRCV_C or • TCON, TSEND/TRCV (termination of the connection possible with TDISCON)
ISO-on-TCP	• TCON_IP_RFC	
ISO according to ISO/IEC 8073 (Class 4)	• TCON_ISOnative[1] • TCON_Configured	
UDP	• TCON_IP_v4 • TADDR_Param	Establish connection and send/receive data via: • TSEND_C/TRCV_C • TUSEND/TURCV (connection can be terminated via TDISCON)
Modbus TCP	• TCON_IP_v4	• MB_CLIENT • MB_SERVER
E-mail	• TMAIL_v4 • TMAIL_v6 • TMAIL_FQDN	• TMAIL_C
FTP	• FTP_CONNECT_IPV4[2] • FTP_CONNECT_IPV6[2] • FTP_CONNECT_NAME[2]	• FTP_CMD

1 This protocol can only be used with the CP 1543-1

2 User-defined data type

Setting up the connection with connection configuration

When setting up through the configuration of the connection, the address parameters of the connection are specified in the hardware and network editor of STEP 7.

To send and receive the data, use the same instructions as when the connections are set up by programming:

Table 6- 4 Instructions for sending/receiving with configured connections

Protocol	Send/receive with configured connections
Supported instructions:	
TCP	Send/receive data via: • TSEND_C/TRCV_C or • TSEND/TRCV
ISO-on-TCP	
ISO according to ISO/IEC 8073 (Class 4)	
UDP	Send/receive data via: • TSEND_C/TRCV_C • TUSEND/TURCV
Modbus TCP	Not supported
E-mail	Not supported
FTP	Not supported

Additional instructions for open communication

You can use the following instructions for connections set up in the user program as well for as configured connections:

- T_RESET: : Terminate and establish a connection
- T_DIAG: check connection

Additional information

The STEP 7 online help describes:

- The user and system data types
- The instructions for open communication
- The connection parameters

You will find information about the allocation and release of connection resources in the section Allocation of connection resources (Page 71).

6.4 Setting up open communication with TCP, ISO-on-TCP, UDP and ISO

Configuring a connection for the TSEND_C, TRCV_C or TCON instructions

Requirement: A TSEND_C, TRCV_C or TCON instruction is created in the programming editor.

1. Select a TCON, TSEND_C or TRCV_C block of Open User Communication in the program editor.
2. Open the "Properties > Configuration" tab in the inspector window.

3. Select the "Connection parameters" group. Until you select a connection partner, only the empty drop-down list for the partner end point is enabled. All other input options are disabled.

   The connection parameters already known are displayed:

   – Name of the local end point
   – Interface of the local end point
   – IPv4 address (for Ethernet subnet) or PROFIBUS address (for PROFIBUS subnet) of the local end point.

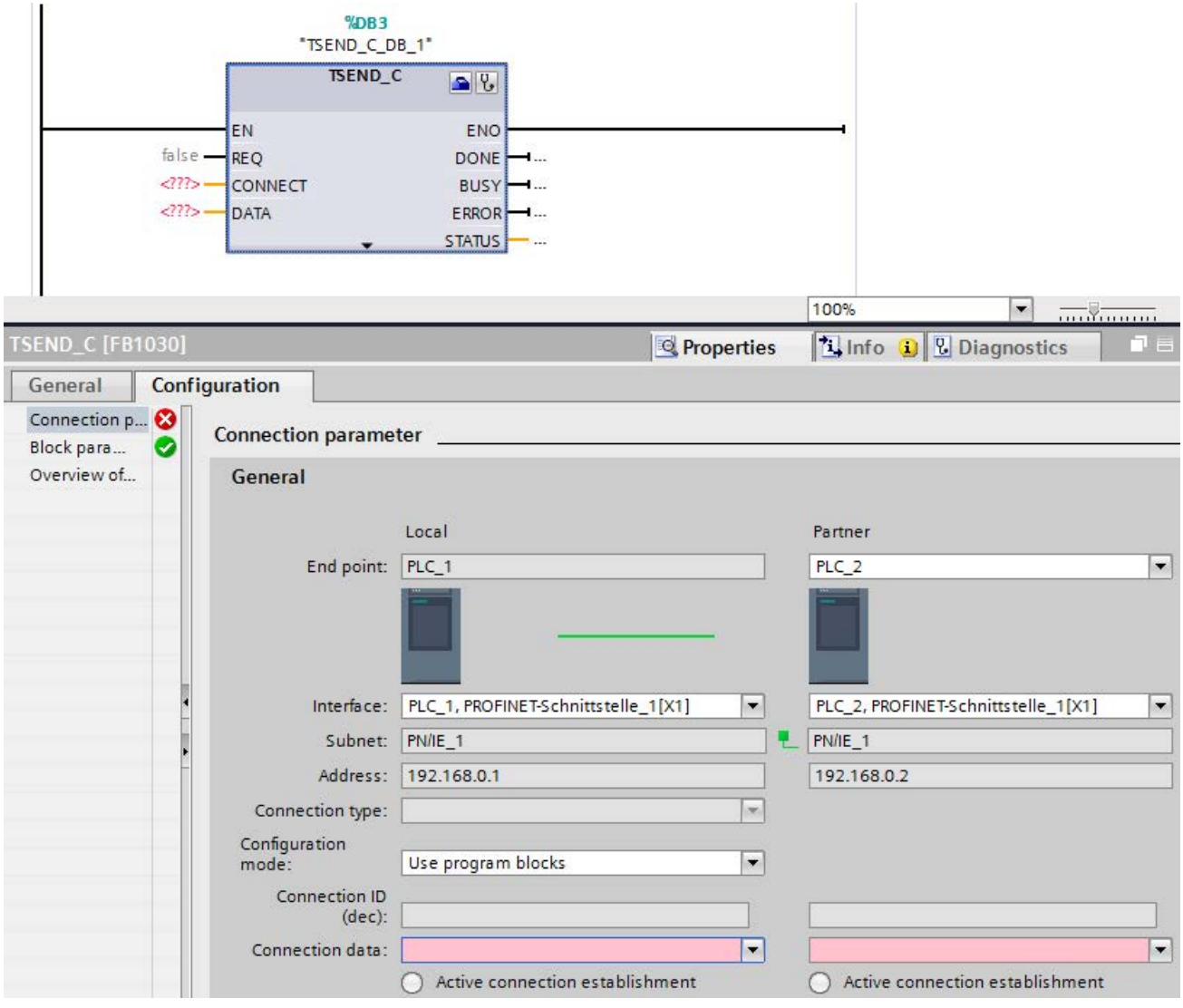


Figure 6-1 Connection parameters for TSEND_C

4. In the drop-down list box of the partner end point, select a connection partner. You can select an unspecified device or a CPU in the project as the communication partner. Certain connection parameters are then entered automatically.

   The following parameters are set:

   – Name of the partner end point
   – Interface of the partner end point
   – IPv4 address (for Ethernet subnet) or PROFIBUS address (for PROFIBUS subnet) of the partner end point.

   If the connection partners are networked, the name of the subnet is displayed.

5. In the "Configuration type" drop-down list, select between using program blocks or configured connections.
6. Select an existing connection description DB in the "Connection data" drop-down list or for configured connections select an existing connection under "Connection name". You can also create a new connection description DB or a new configured connection. Later, you can still select other connection description DBs or configured connections or change the names of the connection description DBs in order to create new data blocks:

   – You can also see the selected data block at the interconnection of the CONNECT input parameter of the selected TCON, TSEND_C or TRCV_C instruction.
   – If you have already specified a connection description DB for the connection partner using the CONNECT parameter of the TCON, TSEND_C or TRCV_C instruction, you can either use this DB or create a new DB.
   – If you edit the name of the displayed data block in the drop-down list, a new data block with the changed name but with the same structure and content is generated and used for the connection.
   – Changed names of a data block must be unique in the context of the communication partner.
   – A connection description DB must have the structure TCON_Param, TCON_IP_v4 or TCON_IP_RFC, depending on CPU type and connection.
   – A data block cannot be selected for an unspecified partner.

   Additional values are determined and entered after the selection or creation of the connection description DB or configured connection.

   The following is valid for specified connection partners:

   – ISO-on-TCP connection type
   – Connection ID with default of 1
   – Active connection establishment by local partner
   – TSAP ID
     for S7-1200/1500: E0.01.49.53.4F.6F.6E.54.43.50.2D.31
     for S7-300/400: E0.02.49.53.4F.6F.6E.54.43.50.2D.31

The following is valid for unspecified connection partners:

- TCP connection type
- Partner port 2000

The following applies for a configured connection with a specified connection partner:

- TCP connection type
- Connection ID with default of 257
- Active connection establishment by local partner
- Partner port 2000

The following applies for a configured connection with an unspecified connection partner:

- TCP connection type
- Local port 2000

7. Enter a connection ID as needed for the connection partner. No connection ID can be assigned to an unspecified partner.

Note

You must enter a unique value for the connection ID at a known connection partner. The uniqueness of the connection ID is not be checked by the connection parameter settings and there is no default value entered for the connection ID when you create a new connection.

8. Select the desired connection type in the relevant drop-down list. Default values are set for the address details depending on the connection type. You can choose between the following:
   - TCP
   - ISO-on-TCP
   - UDP
   - ISO (only with Configuration mode "Use configured connection")

   You can edit the input boxes in the address details. Depending on the selected protocol, you can edit the ports (for TCP and UDP) or the TSAPs (for ISO-on-TCP and ISO).
9. Use the "Active connection establishment" check box to set the connection establishment characteristics for TCP, ISO and ISO-on-TCP. You can decide which communication partner establishes the connection actively.

Changed values are checked immediately for input errors by the connection configuration and entered in the data block for the connection description.

Note

Open User Communication between two communication partners can only work when the program section for the partner end point has been downloaded to the hardware. To achieve fully functional communication, make sure that you load not only the connection description of the local CPU on the device but also that of the partner CPU as well.

Configuring connections, e.g. for TSEND/TRCV

If you want to use the instructions for TSEND/TRCV for open communication, for example, you first need to configure a connection (e.g. TCP connection).

To configure a TCP connection, follow these steps:

1. Configure the communications partners in the network view of the Devices & networks editor of STEP 7.
2. Click the "Connections" button and select the "TCP connection" connection type from the drop-down list.
3. Using drag-and-drop, connect the communication partner with each other (via an interface or local end point). If the required S7 subnet does not yet exist, it is created automatically.

   You can also set up a connection to unspecified partners.
4. Select the created connection in the network view.
5. Set the properties of the connection in the "Properties" tab in the "General" area, for example the name of the connection and the interfaces of the communications partner that will be used.

   For connections to an unspecified partner, set the address of the partner.
   You can find the local ID (reference of the connection in the user program) in the "Local ID" area.
6. In the Project tree, select the "Program blocks" folder for one of the CPUs and open OB1 in the folder by double-clicking on it. The program editor opens.
7. Select the required instruction from the "Instructions" task card, "Communication" area, "Open user communication", for example TSEND and drag it to a network of OB1.
8. At the ID parameter of the instruction, assign the local ID of the configured connection to be used for the transmission of data.
9. Interconnect the "DATA" parameter of the TSEND instruction with the user data, for example in a data block.
10. Download the hardware configuration and user program to the CPU.

Based on the procedure described above, set up the connection on the partner CPU with the instruction for receiving, TRCV, and download it to the CPU.

Point to note with ISO connections with CP 1543-1

If you use the "ISO connection" connection type, you will need to select the "Use ISO protocol" check box in the properties of the CP so that addressing using MAC addresses will work.

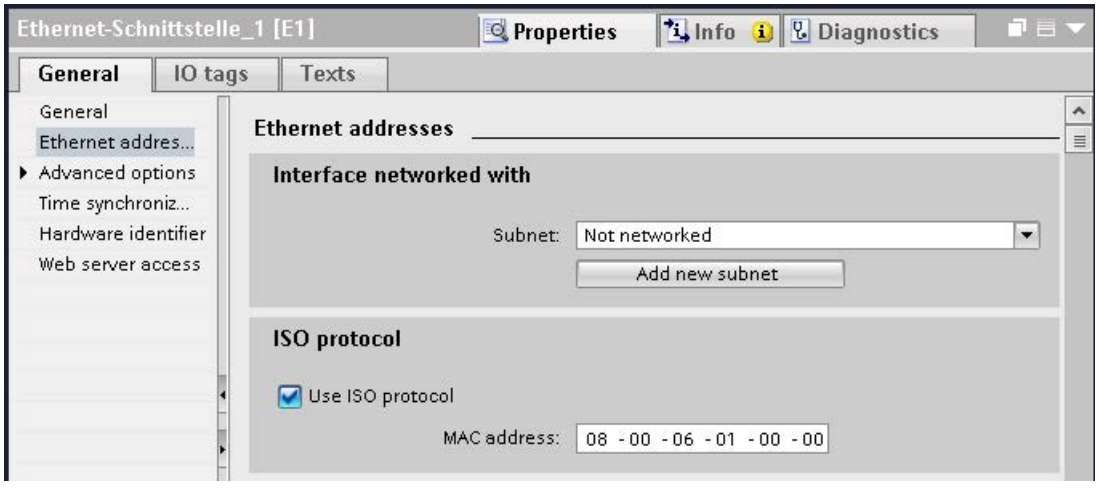


Figure 6-2 Select CP 1543-1 ISO protocol

Additional information

The STEP 7 online help describes:

- The instructions for open communication
- The connection parameters

6.5 Setting up communication with Modbus TCP

Setting up a connection for Modbus TCP via the user program

The parameter assignment takes place in the program editor at the instruction MB_CLIENT or MB_SERVER.

Procedure for setting up communication using Modbus TCP

The MB_CLIENT instruction communicates as a Modbus TCP client via the TCP connection. You establish a connection between the client and the server with the instruction, send Modbus requests to the server and receive the corresponding Modbus responses. You also control the setup of the TCP connection with this instruction.

The MB_SERVER instruction communicates as a Modbus TCP server via the TCP connection. The instruction processes connection requests of a Modbus client, receives and processes Modbus requests and sends responses. You also control the setup of the TCP connection.

Requirement: Client and server are connected via an S7 subnet (PROFINET) as far as IP is concerned.

1. Configure an S7-1500 automation system with CPU in the network view of the Devices & networks editor of STEP 7.
2. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.
3. Select the required instruction, for example MB_CLIENT, from the "Instructions" task card, "Communication" area, "Other", "MODBUS TCP" and drag it to a network of OB1.

4. Assign the parameters of the MB_CLIENT or MB_SERVER instruction. Observe the following rules:

   An IPv4 server address must be specified for each MB_CLIENT connection.

   Each MB_CLIENT or MB_SERVER connection must use a unique instance DB with the data structure TCON_IP_v4.

   Each connection requires a unique connection ID. The connection ID and instance DB belong together in pairs and must be unique for each connection.

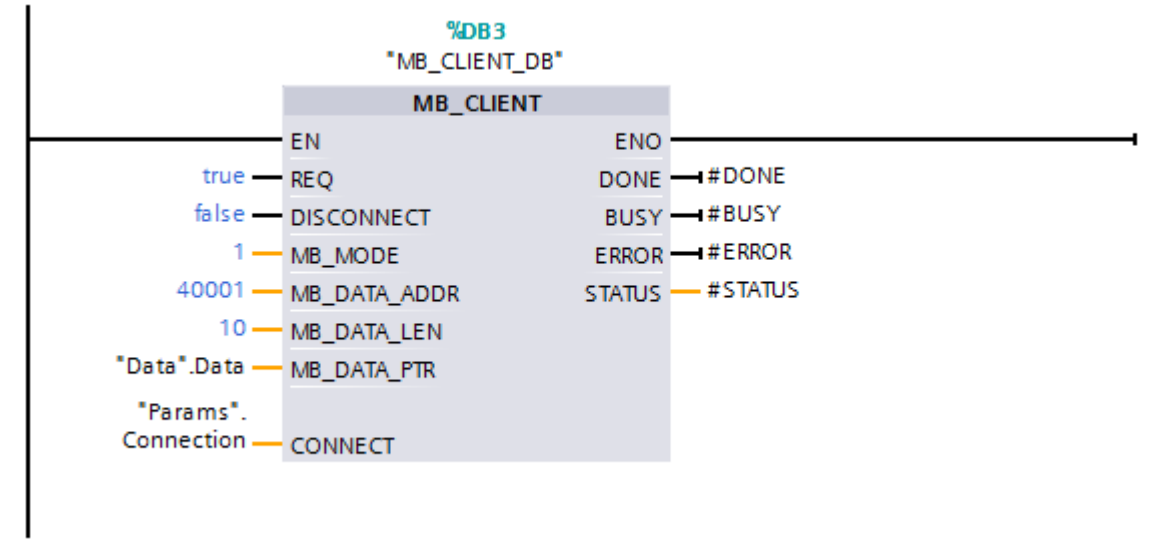


Figure 6-3 MB_CLIENT

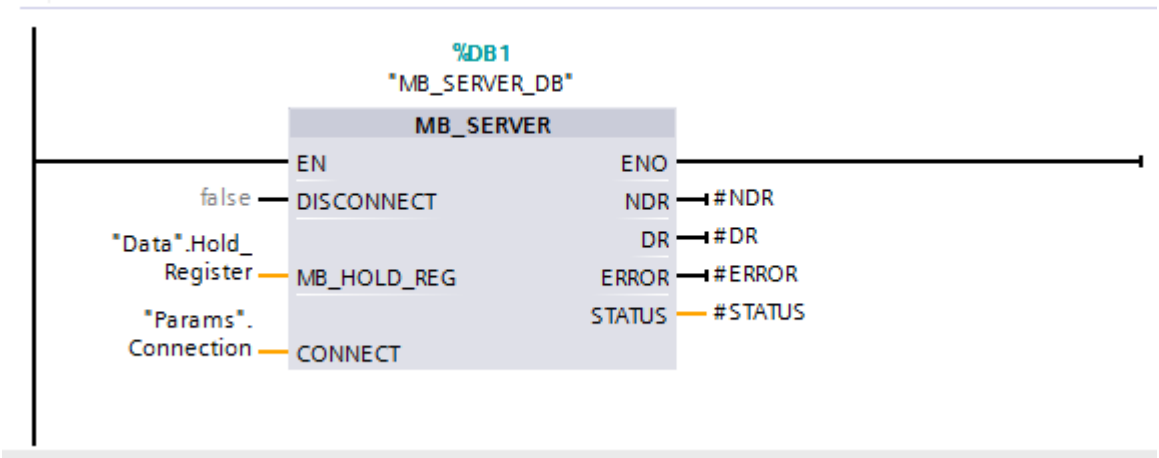


Figure 6-4 MB_SERVER

5. Download the hardware configuration and user program to the CPU.

Modbus TCP server as gateway to Modbus RTU

If you use a Modbus TCP server as a gateway to a Modbus RTU protocol, address the slave device in the serial network using the static parameter, MB_UNIT_ID. The MB_UNIT_ID parameter corresponds to the field of the slave address in the Modbus RTU protocol. The MB_UNIT_ID parameter in this case would forward the request to the correct Modbus RTU slave address.

You do not have to program the gateway function yourself.

You can find the MB_UNIT_ID parameter in the instance data block associated with MB_CLIENT instruction.

You can find more information on the MB_UNIT_ID parameter in the STEP 7 online help.

6.6 Setting up communication via e-mail

Setting up a connection for e-mail via the user program

For communication using e-mail, you need to create the data block of the relevant system data type yourself, assign parameters and call the instruction directly. This procedure is introduced below.

Procedure for setting up communication using e-mail

A CPU can send e-mails. To send e-mails from the user program of the CPU, use the TMAIL_C instruction.

Requirement: The SMTP server can be reached via the IPv4 network.

1. Configure an S7-1500 automation system with CPU in the network view of the Devices & networks editor of STEP 7.
2. Set the address parameters for the SMTP server in the TMAIL_C instruction. (Recommendation: Assign a name for the appendix.)
3. Create a global DB and within this DB a tag of the type TMAIL_v4, TMAIL_v6 (CP 1543-1 only) or TMAIL_FQDM (CP 1543-1 only).
4. Interconnect the variable to the MAIL_ADDR_PARAM parameter of the TMAIL_C instruction.
5. Download the hardware configuration and user program to the CPU.

Additional information

The STEP 7 online help describes:

- The system data types
- The instructions for open communication
- The connection parameters

6.7 Setting up communication via FTP

Setting up a connection for FTP via the user program

For communication via FTP, you need to create the data block of the relevant system data type yourself, assign parameters and call the instruction directly. This procedure is introduced below.

FTP client and server functionality

Files can be sent by a CPU to an FTP server and can be received from the FTP server. Communication with FTP is only possible for the S7-1500 using the CP 1543-1. The CP can be an FTP server, FTP client or both. FTP clients can also be third-party systems/PCs.

For the FTP server functionality, configure the CP accordingly in STEP 7.

You can use the FTP client functionality to implement, for example, the establishment and termination of an FTP connection, the transfer and deletion of files on the server. For the FTP client functionality, use the FTP_CMD instruction.

Procedure for setting up FTP server functionality

Requirement: The FTP server can be reached via the IPv4 network.

1. Configure an S7-1500 automation system with CPU and CP 1543-1 in the device view of the Devices & networks editor of STEP 7.

   At the same time, you need to select the check box "Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...)" in the HW configuration of the S7-1500 CPU under the "Protection" area navigation in the section "Connection mechanisms".

2. Make the following settings in the properties of the CP under "FTP configuration":
   - Select the "Use FTP server for S7 CPU data" check box.
   - Assign the CPU, a data block and a file name under which the DB for FTP will be stored.

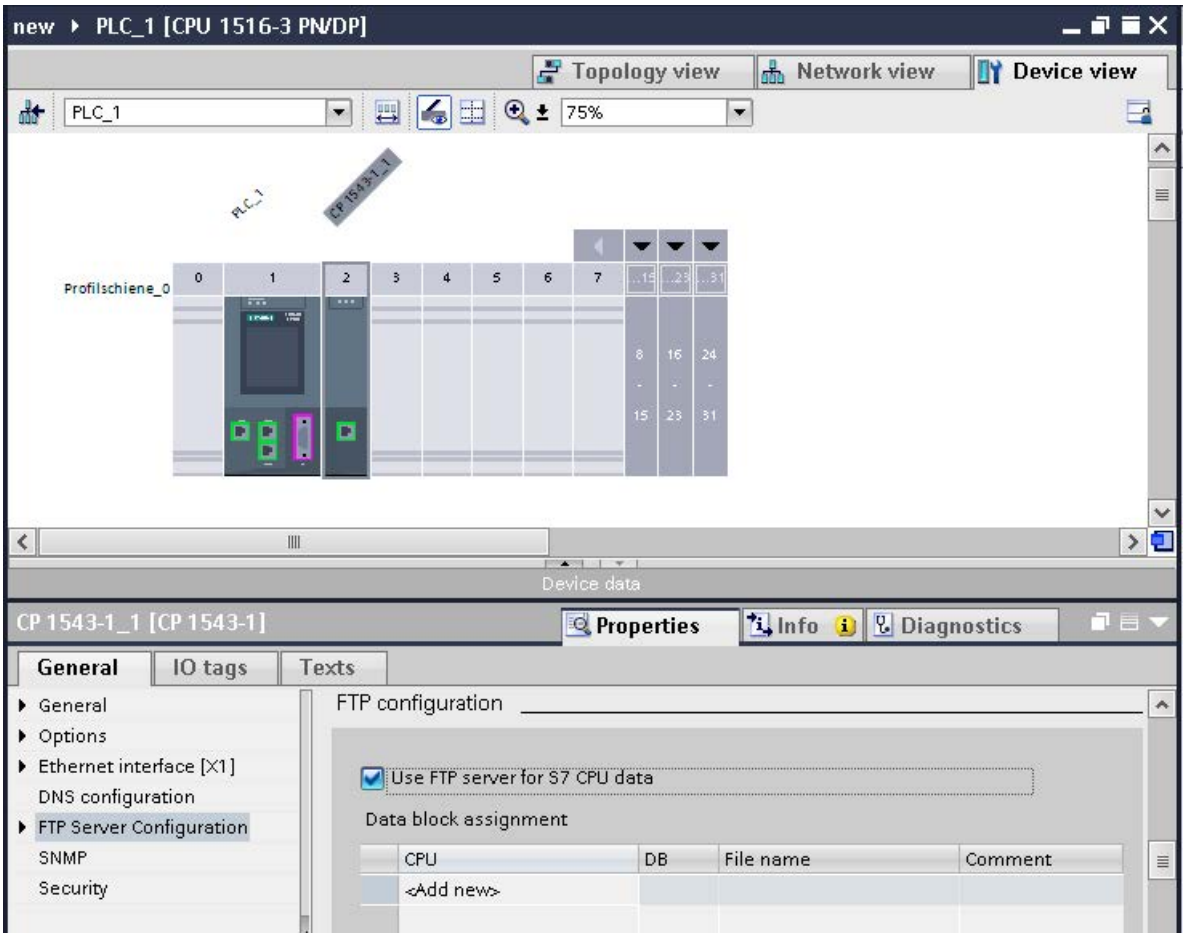


Figure 6-5 Setting up the FTP configuration

3. Download the hardware configuration to the CPU.

Procedure for setting up FTP client functionality

Requirement: The FTP server can be reached via the IPv4 network.

1. Configure an S7-1500 automation system with CPU and CP 1543-1 in the device view of the Devices & networks editor of STEP 7.

   At the same time, you need to select the check box "Permit access with PUT/GET communication from remote partner (PLC, HMI, OPC, ...)" in the HW configuration of the S7-1500 CPU under the "Protection" area navigation in the section "Connection mechanisms".
2. Call the FTP_CMD instruction in the user program of the CPU.
3. Set the connection parameters for the FTP server in the FTP_CMD instruction.
4. Create a global DB and within this DB a tag of the type FTP_CONNECT_IPV4, FTP_CONNECT_IPV6 or FTP_CONNECT_NAME.
5. Interconnect the tag within the data block with the FTP_CMD instruction.
6. For the connection to the FTP server, specify the following in the DB:
   - The user name, the password and the IP address for the FTP access in the relevant data type (FTP_CONNECT_IPV4, FTP_CONNECT_IPV6 or FTP_CONNECT_NAME)
7. Download the hardware configuration and user program to the CPU.

Additional information

The STEP 7 online help describes:

- The system data types
- The instructions for open communication
- The connection parameters

6.8 Establishment and termination of communications relations

Establishment and termination of communications

The table below shows the establishment and termination of communications as part of open communication.

Table 6- 5 Establishment and termination of communications

Setting up the connection	Establishing communication	Terminating communication
With the user program	After downloading the user program to the CPUs: The passive communications partner sets up the local connection access by calling TSEND_C/TRCV_C or TCON. Calling TSEND_C/TRCV_C or TCON on the active partner starts connection establishment. If the connection could be established, there is positive feedback to the instructions in the user program. After you have terminated a connection using the instruction T_RESET, the connection is reestablished. If the connection aborts, the active partner attempts to re-establish the connection. This applies only if the connection was successfully established beforehand with TCON.	• Using the TSEND_C/TRCV_C, TDISCON and T_RESET instructions • When the CPU changes from RUN to STOP mode • With POWER OFF/POWER ON on a CPU
By configuring a connection	After downloading the connection configuration and the user program to the CPUs.	By deleting the connection configuration in STEP 7 and downloading the changed configuration to the CPU.

S7 communication 7

Characteristics of S7 communication

S7 communication as homogeneous SIMATIC communication is characterized by vendor-specific communication between SIMATIC CPUs (not an open standard). S7 communication is used for migration and for connecting to existing systems (S7-300, S7-400).

For data transfer between two S7-1500 automation systems, we recommend that you use open communication (see section Open communication (Page 31)).

Properties of S7 communication

Using S7 communication, the CPU exchanges data with another CPU. Once the user has received the data at the receiver end, the reception data is automatically acknowledged to the sending CPU.

The data is exchanged via configured S7 connections. S7 connections can be configured at one end or at both ends.

S7 communication is possible via:

- Integrated PROFINET or PROFIBUS DP interface of a CPU
- Interface of a CP/CM

S7 connections configured at one end

For an S7 connection configured at one end, the configuration for this connection takes place in only one communication partner and is only downloaded to it.

A one-sided S7 connection can be configured to a CPU that is only a server of an S7 connection (e.g. CPU 315-2 DP). The CPU is configured and the address parameters and interfaces are thus known.

In addition, a one-sided S7 connection can be configured to a partner who is not in the project and whose address parameters and interface and therefore are not known. You need to enter the address; it is not checked by STEP 7. The partner is initially unspecified (no partner address is registered when you create the S7 connection). Once you enter the address, it is "unknown" (i.e. it is named, but the project is unknown).

This makes it possible to use S7 connections beyond the boundaries of a project. The communication partner is unknown to the local project (unspecified) and is configured in another STEP 7 or third-party project.

S7 connections configured at both ends

When an S7 connection is configured at both ends, the configuration and download of the configured S7 connection parameters takes place in both communication partners.

Instructions for S7 communication

For S7 communication with S7-1500, the following instructions can be used:

- PUT/GET

  You write data to a remote CPU with the PUT instruction. You can use the GET instruction to read data from a remote CPU. The PUT and GET instructions and are one-sided instructions, i.e. you need only an instruction in one communication partner. You can can easily set up the PUT and GET instructions via the connection configuration.

  Note

  Data blocks for PUT/GET instructions

  When using the PUT/GET instructions, you can only use data blocks with absolute addressing. Symbolic addressing of data blocks is not possible.

  You must also enable this service for protection in the CPU configuration in the "Protection" area.

- BSEND/BRCV

  The BSEND instruction sends data to a remote partner instruction of the type BRCV. The BRCV instruction receives data from a remote partner instruction of the type BSEND. You use the S7 communication via the BSEND/BRCV instruction pair for secure transmission of data.

- USEND/URCV

  The USEND instruction sends data to a remote partner instruction of the type URCV. The URCV instruction receives data from a remote partner instruction of the type USEND. You use the S7 communication via the BSEND/BRCV instruction pair for fast, non-secure transmission of data regardless of the timing of the processing by the communications partner; for example for operating and maintenance messages.

PROFIBUS DP interface in slave mode

You can find the "Test, commissioning, routing" check box in STEP 7 in the properties of the PROFIBUS DP interface of communications modules (e.g. CM 1542-5). Using this check box, you decide whether the PROFIBUS DP interface of the DP slave is an active or passive device on PROFIBUS.

- Check box selected: The slave is an active device on PROFIBUS. You can only set up S7 connections configured at both ends for this DP slave.
- Check box cleared: The DP slave is a passive device on PROFIBUS. You can only set up S7 connections configured at one end for this DP slave.

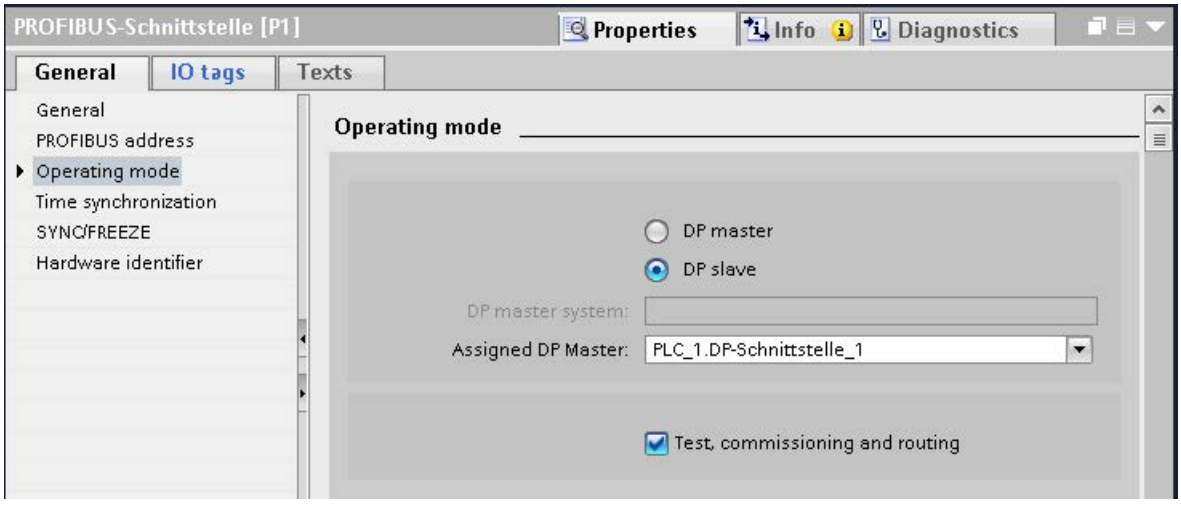


Figure 7-1 "Test, commissioning, routing" check box

Configuring S7 connections for PUT/GET instructions

You can create S7 connections and assign the parameters for these in the connection parameter assignment of the PUT/GET instructions. Changed values are checked immediately by the connection parameter assignment for input errors.

Requirement: A PUT or GET instruction is created in the programming editor.

To configure an S7 connection using PUT/GET instructions, follow these steps:

1. In the program editor, select the call of the PUT or GET instruction.
2. Open the "Properties > Configuration" tab in the inspector window.

3. Select the "Connection parameters" group. Until you select a connection partner, only the empty drop-down list for the partner end point is enabled. All other input options are disabled.

   The connection parameters already known are displayed:

   – Name of the local end point
   – Interface of the local end point
   – IPv4 address of the local end point

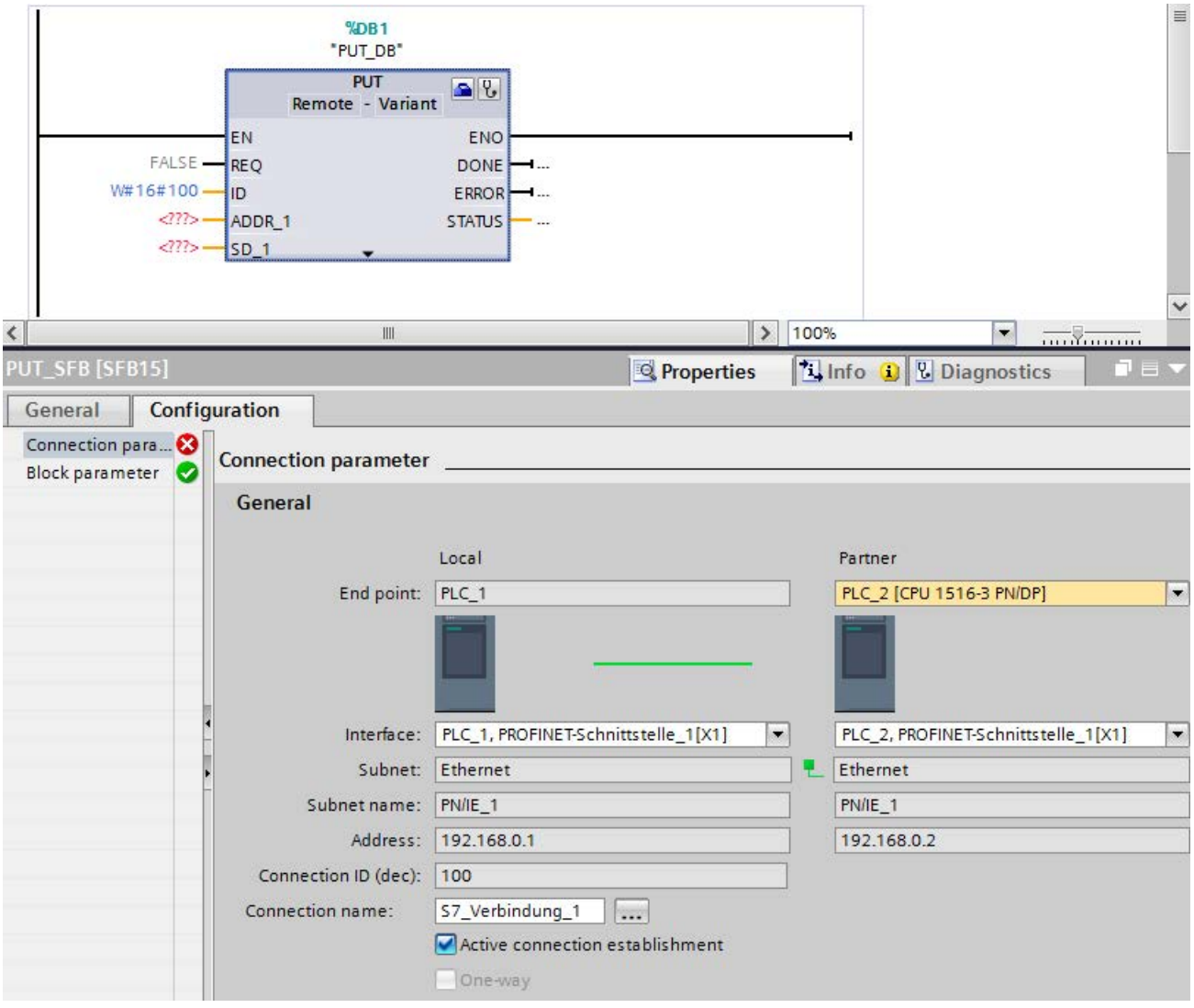


Figure 7-2 Connection configuration for PUT instruction

4. In the drop-down list box of the partner end point, select a connection partner. You can select an unspecified device or a CPU in the project as the communication partner.

   The following parameters are automatically entered as soon as you have selected the connection partner:

   – Name of the partner end point
   – Interface of the partner end point. If several interfaces are available, you can change the interface as required.
   – Interface type of the partner end point
   – Subnet name of both end points
   – IPv4 address of the partner end point
   – Name of the connection which is used for the communication.

5. If required, change the connection name in the "Connection name" input box. If you want to create a new connection or edit an existing connection, click on the "Create new connection" icon.

Note

The PUT and GET instructions between two communication partners can only run if both the hardware configuration and the program part for the partner end point have been loaded into the hardware. To achieve fully functional communication, make sure that you load not only the connection description of the local CPU on the device but also that of the partner CPU as well.

Configuring S7 connections for e.g. BSEND/BRCV

If you want to use the instructions for BSEND/BRCV for S7 communication, for example, you first need to configure an S7 connection.

To configure a S7 connection, follow these steps:

1. Configure the communications partners in the network view of the Devices & networks editor of STEP 7.
2. Select the "Connections" button and the "S7 connection" entry from the drop-down list.
3. Using drag-and-drop, connect the communication partner with each other (via an interface or local end point). If the required S7 subnet does not yet exist, it is created automatically.

   You can also set up a connection to unspecified partners.

4. In the "Connections" tab, select the row of the S7 connection.
5. Set the properties of the S7 connection in the "Properties" tab in the "General" area, for example the name of the connection and the interfaces of the communications partner that will be used.

   For S7 connections to an unspecified partner, set the address of the partner.
   You can find the local ID (reference of the S7 connection in the user program) in the "Local ID" area.

6. In the Project tree, select the "Program blocks" folder for one of the CPUs and open OB1 in the folder by double-clicking on it. The program editor opens.
7. In the program editor, call the relevant instructions for S7 communication in the user program of the communication partner (configured at one end) or in the user programs of the communication partners (configured at both ends). Select the BSEND and BRCV instructions from the "Communication" area of the "Instructions" task card, for example, and drag them to a network of OB1.
8. At the ID parameter of the instruction, assign the local ID of the configured connection to be used for the transmission of data.
9. Assign the parameters for the instructions indicating which data will be written to where and which data will be read from where.
10. Download the hardware configuration and user program to the CPU(s).

S7 communication via CP 1543-1

If you set up S7 communication via the Industrial Ethernet interface of the CP 1543-1, you can select the transport protocol for data transfer in the properties of the S7 connection under "General":

- "TCP/IP" check box selected (default): ISO-on-TCP (RFC1006): for S7 communication between S7-1500 CPUs
- "TCP/IP" check box cleared: ISO protocol (IEC8073): Addressing using MAC addresses

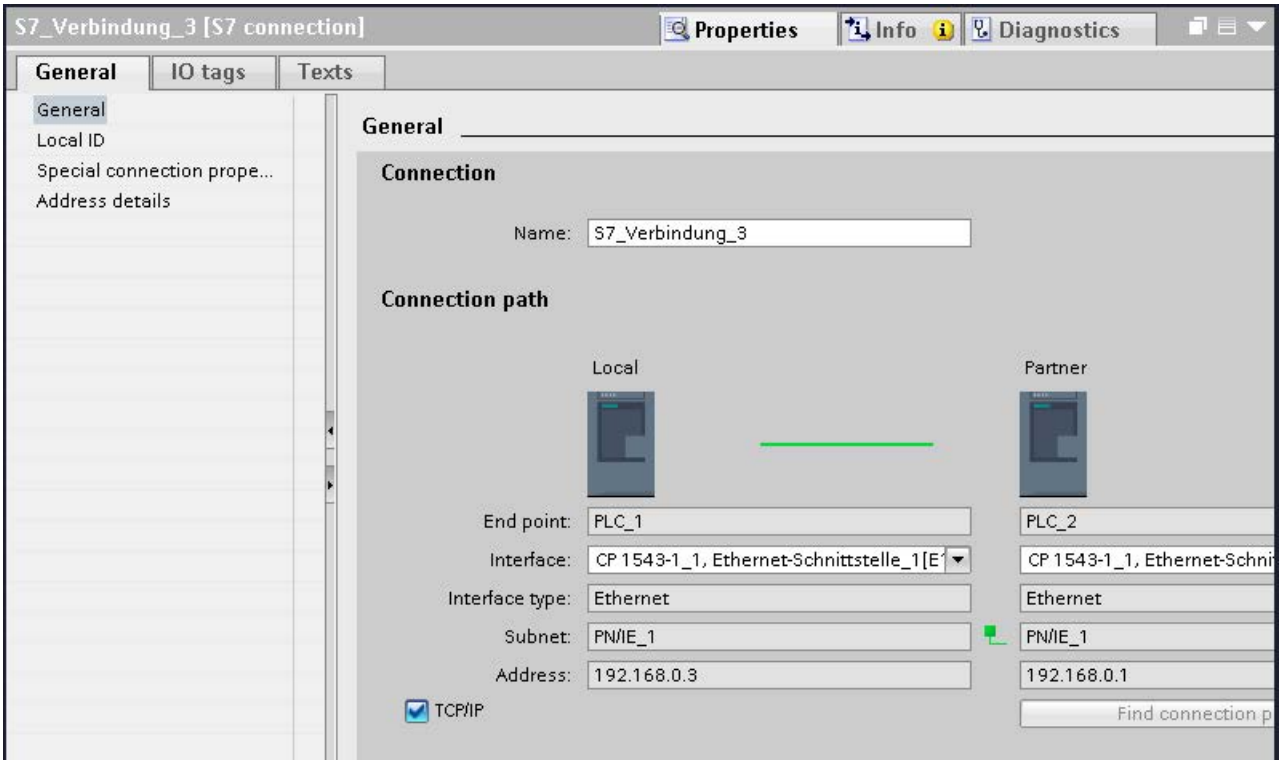


Figure 7-3 Selecting the CP 1543-1 transport protocol

Procedure for setting up an S7 connection via different S7 subnets

You have the option of using an S7 connection via multiple S7 subnets (PROFIBUS, PROFINET/Industrial Ethernet) (S7 routing).

1. Configure the communications partners in the network view of the Devices & networks editor of STEP 7.
2. Select the "Network" button.
3. Connect the relevant interfaces with the S7 subnets (PROFIBUS, PROFINET/Industrial Ethernet) using drag-and-drop.

4. Select the "Connections" button and the "S7 connection" entry from the drop-down list.
5. Using drag-and-drop in our example, connect PLC_1 in the left S7 subnet (PROFIBUS) to PLC_3 in the right S7 subnet (PROFINET).

   The S7 connection between CPU 1 and CPU 3 is configured.

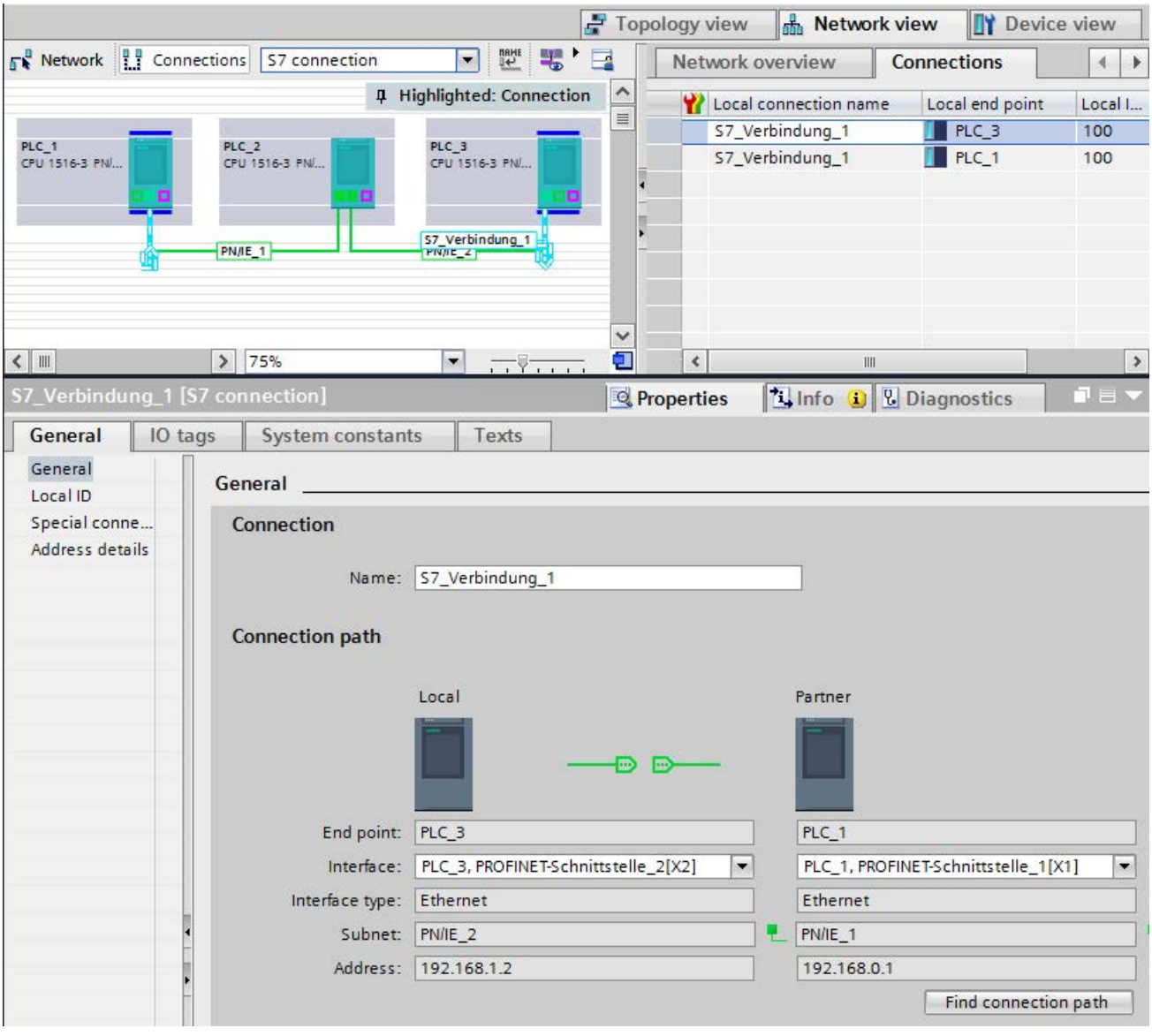


Figure 7-4 S7 connections via different subnets

CPU 1515SP PCas router for S7 connections

If you assign the "PROFINET onboard [X2]" interface to the CPU 1515SP PC of the SIMATIC PC station, the CPU 1515SP PC can be used as a router for S7 connections. With the setting "None, or a different Windows setting" on the CP interface "PROFINET onboard [X2]" , it is not possible to use the CPU 1515SP PC as a router for routed S7 connections.

An existing S7 connection routed by the CPU 1515SP PC becomes invalid if the assignment of the interface of the CPU 1515SP PC is changed from "SIMATIC PC station" to "None, or a different Windows setting". Since the PLC now no longer handles routing functions for this connection, when the CPU 1515SP PC is compiled, no message relating to the invalid connection is displayed. The invalid routed S7 connection is displayed only when the end points of the connection are compiled.

The interfaces required for routed S7 connections must remain explicitly assigned on the CPU 1515SP PC . You can edit the assignment of the interface of the CPU 1515SP PC in the properties under "PROFINET onboard [X2] > Interface assignment".

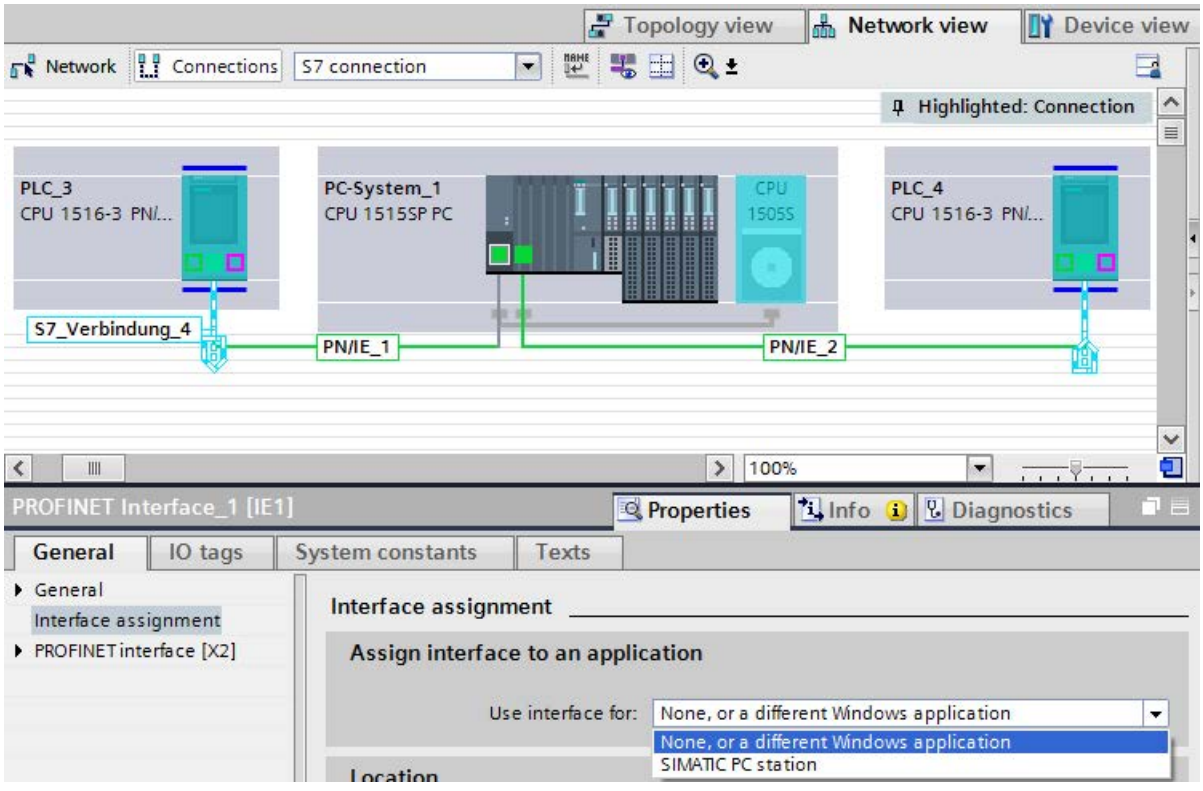


Figure 7-5 S7 routing PC station

Additional information

You can find detailed information on configuring S7 connections and how to use the instructions for S7 communication in the user program in the STEP 7 online help.

Point-to-point link 8

Functionality

A point-to-point connection for S7-1500, ET 200MP and ET 200SP is established via communications modules (CMs) with serial interfaces (RS232, RS422 or RS485):

- S7-1500/ET 200MP:
  - CM PtP RS232 BA
  - CM PtP RS422/485 BA
  - CM PtP RS232 HF
  - CM PtP RS422/485 HF
- ET 200SP:
  - CM PtP

The bidirectional data exchange via a point-to-point connection works between communications modules or third-party systems or devices capable of communication. At least 2 communication partners are required for communication ("point-to-point"). With RS422 and RS485, more than two communications partners are possible.

Protocols for communication via a point-to-point connection

- Freeport protocol (also called ASCII protocol)
- Procedure 3964 R)
- Modbus protocol in RTU format (RTU: Remote Terminal Unit)
- USS protocol (universal serial interface protocol)

The protocols use different layers according to the ISO/OSI reference model:

- Freeport: Uses layer 1 (physical layer)
- 3964 (R), USS and Modbus: Use layer 1 and 2 (physical layer and data link layer; therefore greater transmission reliability than with Freeport). USS and Modbus use additionally layer 4.

Properties of the Freeport protocol

- The recipient recognizes the end of the data transfer by means of a selectable end criterion (e.g. character delay time elapsed, receipt of end character, receipt of a fixed amount of data).
- The sender cannot recognize whether the sent data arrived free of errors at the recipient.

Properties of procedure 3964 (R)

- When the data is sent, control characters are added (start, end and block check characters). Make sure that these control characters are not included as data in the frame.
- Connection establishment and termination makes use of control characters.
- If transfer errors occur, data transfer is automatically repeated.

Data exchange using Freeport or 3964 (R) communication

The data to be sent is stored in the user program of the corresponding CPU in data blocks (send buffer). A receive buffer is available on the communications module for the received data. Check the properties of the receive buffer and adapt them if necessary. You must create a data block for receiving in the CPU.

In the user program of the CPU, the "Send_P2P" and "Receive_P2P" instructions handle the data transfer between the CPU and CM.

Procedure for setting up Freeport or 3964 (R) communication

1. Configure an S7-1500 configuration with CPU and CM in the device view of the hardware and network editor of STEP 7.
2. Assign the parameters for the interface of the CP (protocol, port parameters) in the "General" area in the "Properties" tab.

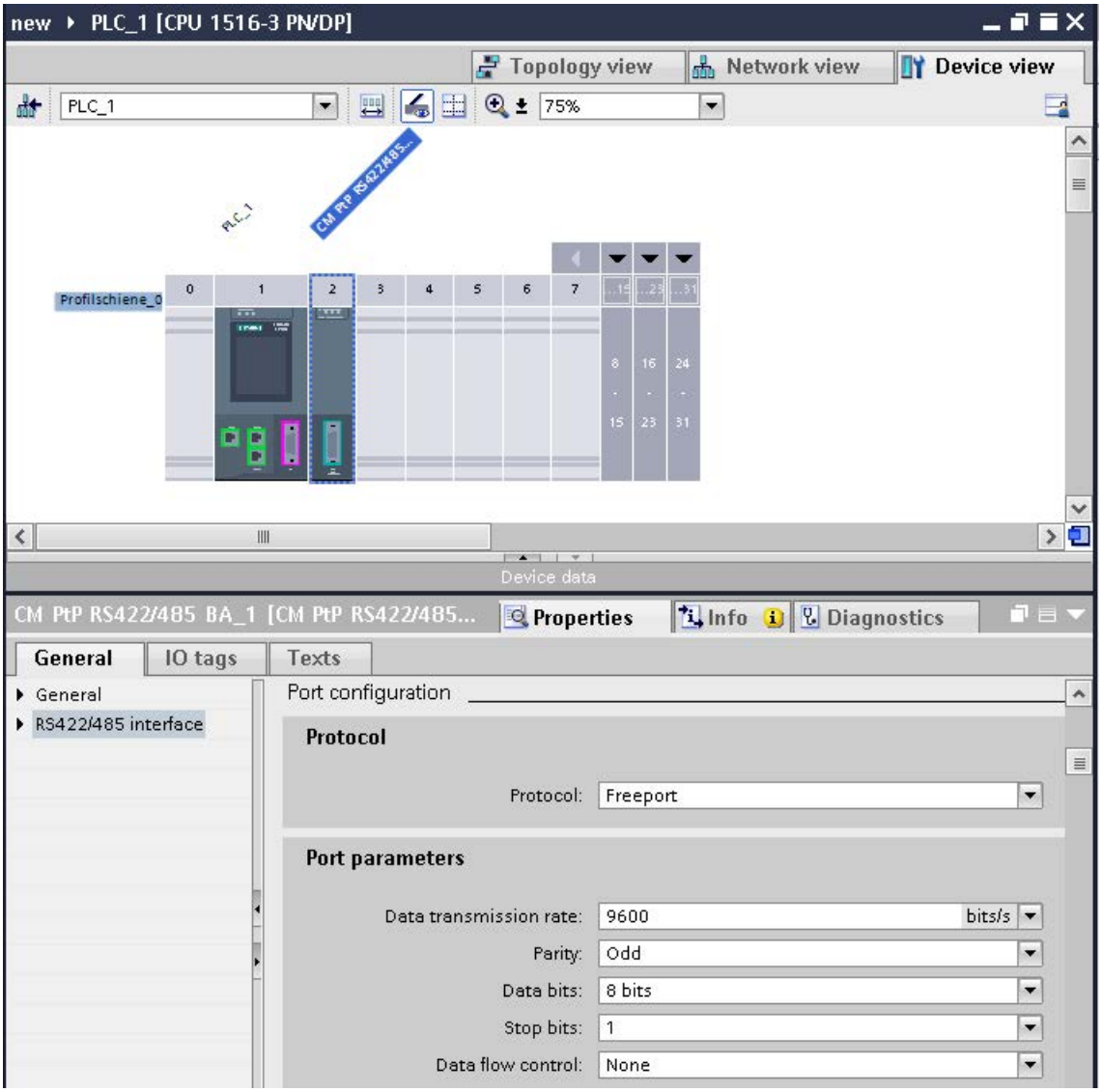


Figure 8-1 Setting up PtP communication

3. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.
4. Select the "Send_P2P" and "Receive_P2P" instructions from the "Communication" area of the "Instructions" task card and drag them to a network of OB1.
5. Assign the parameters for the instructions according to your configuration.
6. Download the hardware configuration and user program to the CPU.

Otherwise: Dynamic configuration via the user program

In certain types of application it is an advantage to set up communication dynamically; in other words, program-controlled by a specific application.

Typical applications for this, could be, for example manufacturers of serial machines. To make the user interfaces as convenient as possible for their customers, these manufacturers adapt the communications services to the particular operator entries.

Instructions for Freeport communication

There are 3 instructions available for the dynamic configuration in the user program for Freeport communication. The following applies to all 3 instructions: the previously valid configuration data is overwritten but not stored permanently in the target system.

- The "Port_Config" instruction is used for the program-controlled configuration of the relevant port of the communications module.
- The "Send_Config" instruction is used for the dynamic configuration, for example of time intervals and breaks in transmission (serial transmission parameters) for the relevant port.
- The "Receive_Config" instruction is used for dynamic configuration, for example of conditions for the start and end of a message to be transferred (serial receive parameters) for the relevant port.

Instructions for 3964 (R) communication

There are 2 instructions available for dynamic configuration in the user program for 3964 (R) communication. The following applies to the instructions: the previously valid configuration data is overwritten but not stored permanently in the target system.

- The "Port_Config" instruction is used for the program-controlled configuration of the relevant port of the communications module.
- The "P3964_Config" instruction is used for the dynamic configuration of protocol parameters.

Properties of the USS protocol

- Simple, serial data transfer protocol with cyclic message frame traffic in half duplex mode that is tailored to the requirements of drive technology.
- Data transfer works according to the master-slave principle.
  - The master has access to the functions of the drive and can, among other things, control the drive, read status values and read and write the drive parameters.

Data exchange using USS communication

The communications module is the master. The master continuously sends frames (job frames) to the up to 16 drives and expects a response frame from each addressed drive.

A drive sends a response frame under the following conditions:

- When a frame is received without errors
- When the drive is addressed in this frame

A drive must not send if these conditions are not met or the drive was addressed in the broadcast.

The connection to the relevant drive exists for the master once it receives a response frame from the drive after a specified processing time (response delay time).

Procedure for setting up USS communication

1. Configure an S7-1500 configuration with CPU and CM in the device view of the hardware and network editor of STEP 7.
2. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.
3. Select the instructions for USS communication according to your task in the "Communication" area, "Communications processor" folder of the "Instructions" task card and drag them to a network of OB1:
   - The "USS_Port_Scan" instruction allows you to communicate via the USS network.
   - The "USS_Drive_Control" instruction prepares send data for the drive and evaluates the response data of the drive.
   - The "USS_Read_Param" instruction is used to read out parameters from the drive.
   - The "USS_Write_Param" instruction is used to change parameters on the drive.
4. Assign the parameters for the instructions according to your configuration.
5. Download the hardware configuration and user program to the CPU.

Properties of the Modbus protocol (RTU)

- Communication takes the form of serial, asynchronous transfer with a transmission speed of up to 115.2 kbps, half duplex.
- Data transfer works according to the master-slave principle.
- The Modbus master can send jobs for reading and writing operands to the Modbus slave:
  - Reading inputs, timers, counters, outputs, memory bits, data blocks
  - Writing outputs, memory bits, data blocks
- Broadcast to all slaves is possible.

Data exchange using Modbus communication (RTU)

The communications module can be a Modbus master or Modbus slave. A Modbus master can communicate with one or more Modbus slaves (the number depends on the physical interface). Only the Modbus slave explicitly addressed by the Modbus master is permitted to return data to the Modbus master. The slave detects the end of the data transfer and acknowledges it. If an error occurs, it provides an error code to the master.

Procedure for setting up Modbus communication (RTU)

1. Configure an S7-1500 configuration with CPU and CM in the device view of the hardware and network editor of STEP 7.
2. In the Project tree, select the "Program blocks" folder and open OB1 in the folder by double-clicking on it. The program editor opens.
3. Select the instructions for Modbus communication according to your task in the "Communication" area, "Communications processor" folder of the "Instructions" task card and drag them to a network of OB1:
   - The "Modbus_Comm_Load" instruction configures the port of the CM for Modbus communication.
   - The "Modbus_Master" instruction is used for Modbus master functionality.
   - The "Modbus_Slave" instruction is used for Modbus slave functionality.
4. Assign the parameters for the instructions according to your configuration.
5. Download the hardware configuration and user program to the CPU.

Additional information

- You can find more detailed information on communication via point-to-point connections and basics of serial data transmission in the function manual CM PtP communication module - Configurations for point-to-point connections (http://support.automation.siemens.com/WW/view/en/59057093).
- You can find a description of how to use the instructions for point-to-point connections in the user program in the STEP 7 online help.
- You can find information about the communications modules with a serial interface in the manual of the particular communications module.

Routing 9

9.1 S7 routing

Definition of S7 routing

S7 routing is the transfer of data beyond S7 subnet boundaries. You can send information from a transmitter to a receiver across several s7 subnets. The gateway from one S7 subnet to one or more other subnets is provided by the S7 router The S7 router is a device which has interfaces to the respective S7 subnets. S7 routing is possible via various S7 subnets (PROFINET/Industrial Ethernet and/or PROFIBUS).

Requirements for S7 routing

- All devices that can be reached in a network have been configured in a project in STEP 7 and downloaded.
- All devices involved in the S7 routing must receive routing information about the S7 subnets that can be reached through specific S7 routers. The devices obtain the routing information by downloading the hardware configuration to the CPUs, since the CPUs play the role of an S7 router.

  In a topology with several consecutive S7 subnets, the following order must be kept to when downloading: First download the hardware configuration to the CPU(s) directly connected to the same S7 subnet as the PG/PC, then download one by one the CPUs of the S7 subnets beyond this starting with the nearest S7 subnet through to the S7 subnet furthest away.
- The PG/PC you want to use to establish a connection via a S7 router must be assigned to the S7 subnet it is physically connected to. You can assign the PG/PC to a PG/PC in STEP 7 under Online & Diagnostics > Online accesses > Connection to interface/subnet.
- For S7 subnets of the type PROFIBUS: Either the CPU must be configured as DP master or, if it is configured as a DP slave, the "Test, commissioning, routing" check box must be selected in the properties of the DP interface of the DP slave.
- S7 routing for HMI connections is possible as of STEP 7 V13 SP1.

S7 routing for online connections

With the PG/PC, you can reach devices beyond S7 subnets, for example to do the following:

- Download user programs
- Download a hardware configuration
- Execute test and diagnostics functions

In the following figure, CPU 1 is the S7 router between S7 subnet 1 and S7 subnet 2.

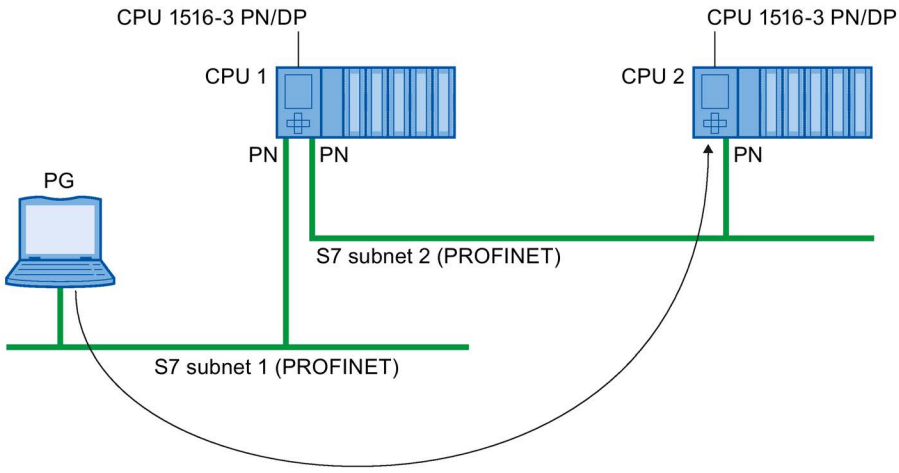


Figure 9-1 S7 routing: PROFINET - PROFINET

The following figure shows the access from a PG via PROFINET to PROFIBUS. CPU 1 is the S7 router between S7 subnet 1 and S7 subnet 2; CPU 2 is the S7 router between S7 subnet 2 and S7 subnet 3.

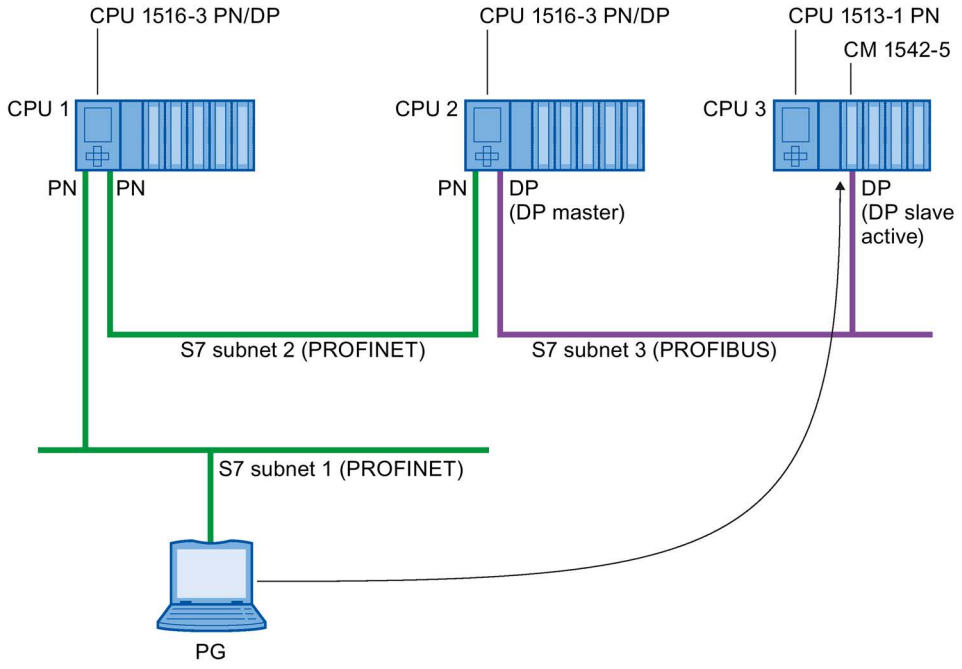


Figure 9-2 S7 routing: PROFINET - PROFIBUS

S7 routing for HMI connections

You have the option of setting up an S7 connection from an HMI to a CPU via different subnets (PROFIBUS and PROFINET or Industrial Ethernet). In the following figure, CPU 1 is the S7 router between S7 subnet 1 and S7 subnet 2.

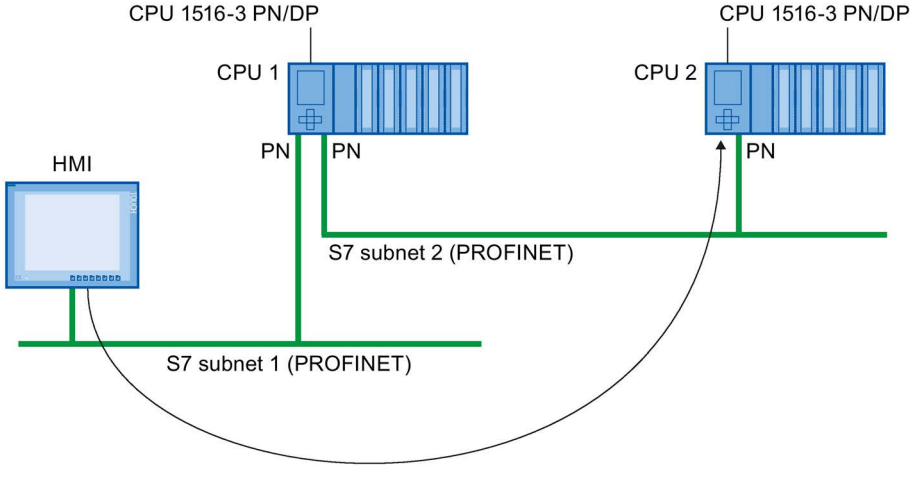


Figure 9-3 S7 routing via HMI connections

S7 routing for CPU-CPU communication

You have the option of setting up an S7 connection from a CPU to another CPU via different subnets (PROFIBUS and PROFINET or Industrial Ethernet). The procedure is described based on an example in the section S7 communication (Page 49).

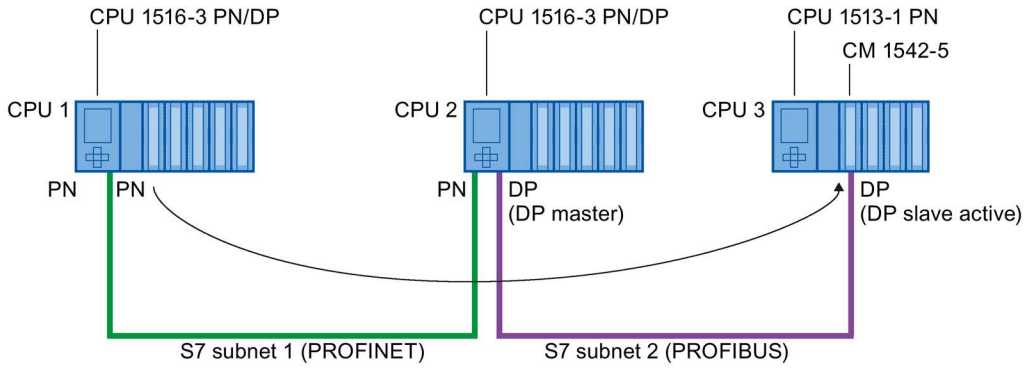


Figure 9-4 S7 routing via CPU-CPU communication

Using S7 routing

For the CPU, select the PG/PC interface and the S7 subnet in the "Go online" dialog of STEP 7. S7 routing is performed automatically.

Number of connections for S7 routing

The number of connections available for S7 routing in the S7 routers (CPUs, CMs or CPs) can be found in the technical specifications in the manuals of the relevant CPU/CM/CP.

S7 routing: Example of an application

The figure below shows the example of an application for remote maintenance of a system using a PG. The connection is made here beyond two S7 subnets via a modem connection.

You configure a remote connection via TeleService in STEP 7 using "Online access" or "Go online".

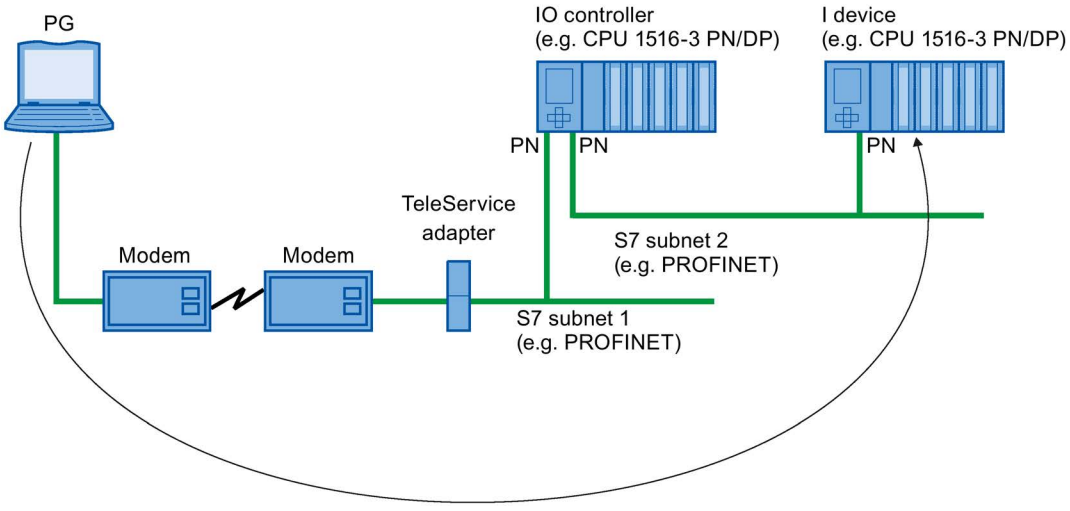


Figure 9-5 Remote maintenance of a plant using TeleService

Additional information

- The allocation of connection resources with S7 routing is described in the section Allocation of connection resources (Page 71).
- You can find more information on setting up TeleService in the STEP 7 online help.
- You can find more information on S7 routing and TeleService adapters when you search the Internet using the following links:
  - Device manual Industrial Software Engineering Tools TS Adapter IE Basic (http://support.automation.siemens.com/WW/view/en/51311100)
  - Downloads for the TS Adapter (http://support.automation.siemens.com/WW/view/en/10805406/133100)

See also

HMI communication (Page 29)

9.2 Data record routing

Definition of data record routing

Data can be sent over PROFINET from an engineering station to field devices via multiple networks. Since the engineering station addresses the field devices using standardized records and these records are routed via S7 devices, the term "data record routing" is used to refer to this type of routing.

The data sent using data record routing include the parameter assignments for the participating field devices (slaves) and device-specific information (e.g. setpoint values, limit values).

Data record routing is used, for example, when field devices of different manufacturers are used. The field devices are addressed using standardized data records (PROFINET) for configuration and diagnostics.

Data record routing with STEP 7

You can perform data routing with STEP 7 by calling a device tool (for example, PCT) via the TCI interface (Tool Calling Interface) and passing call parameters. The device tool uses the communication paths that STEP 7 also uses for communication with the field device.

No configuration is required for this type of routing except the installation of the TCI tools on the STEP 7 computer.

Example: Data record routing with the Port Configuration Tool (PCT)

You can use the Port Configuration Tool (PCT) to configure the IO link master of the ET200 and assign parameters to connected IO link devices. The subnets are connected via data record routers. Data record routers are, for example, CPUs, CPs, IMs, IO link masters.

You can learn about the constellations of data record routers supported by the PCT here (http://support.automation.siemens.com/WW/view/en/87611392).

The figure below shows an example configuration with the data record routing with PCT.

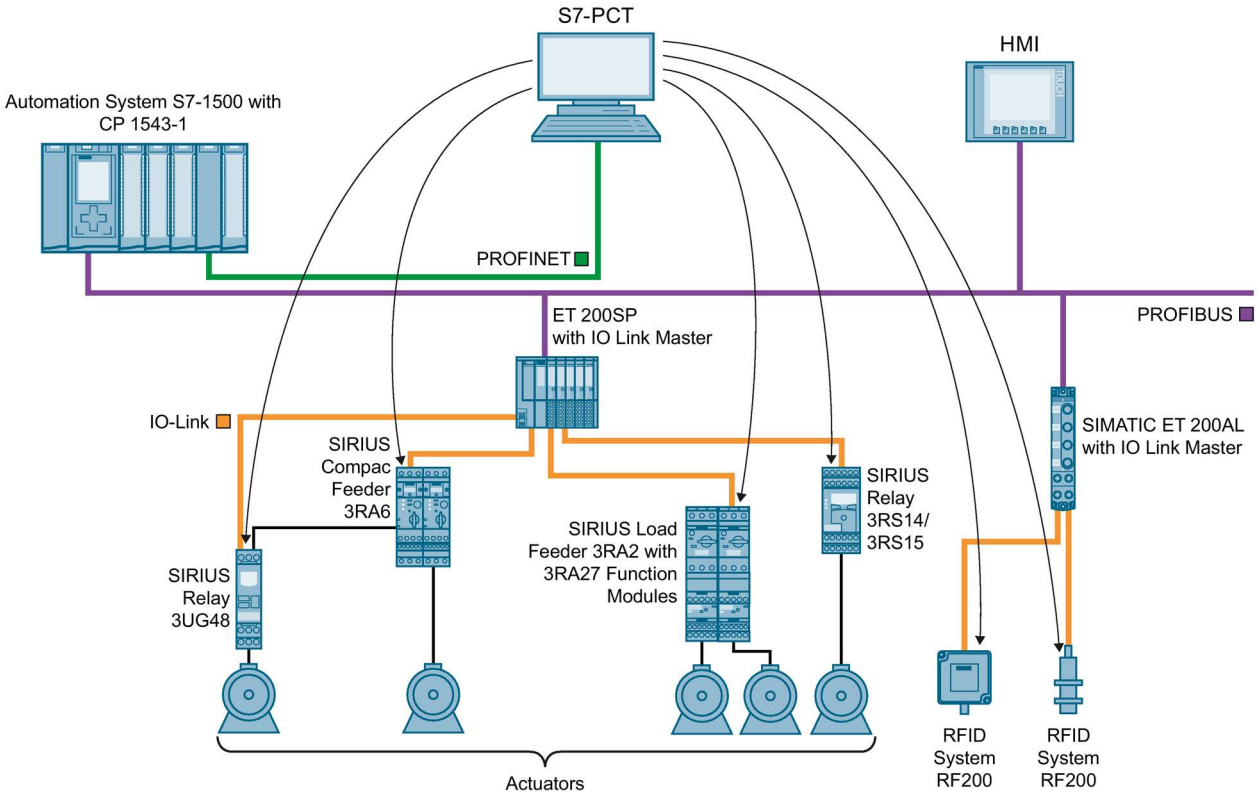


Figure 9-6 Example configuration for data record routing with PCT

Additional information

- Whether or not the CPU, CP or CM you are using supports data record routing can be found in the relevant manuals.
- The allocation of connection resources with data record routing is described in the section Allocation of connection resources (Page 71).
- You can find additional information on configuration with STEP 7 in the STEP 7 online help.

Connection resources 10

10.1 Allocation of connection resources

Allocation of connection resources with automatic connection

As soon as you have connected the PG or HMI device to a CPU physically and have gone online in STEP 7, connection resources are allocated.

Allocation of connection resources with programmed connection setup

With programmed connections, a connection resource is allocated when the instruction for establishing the connection (TSEND_C/TRCV_C or T_CON) is called.

With suitable parameter assignment of the CONT parameter of the TSEND_C/TRCV_C instructions or by calling the TDISCON instruction, the connection can be terminated following data transfer and the connection resource is available again. If the connection is terminated, the connection resources on the CPU/CP/CM are available again. If the connection remains, the execution time of the instructions during the next data transfer is shorter because the connection does not need to be established again. If the CPU goes to STOP, these connection resources are available again.

Allocation of connection resources with configured connection setup

With configured connections, the connection resource is allocated as soon as the hardware configuration is downloaded to the CPU.

After using a configured connection for transfer of data, the connection is not terminated. The connection resource is permanently allocated. To release the connection resource again, you need to delete the configured connection in STEP 7 and download the modified configuration to the CPU.

Monitoring the maximum possible number of connection resources

With **automatic** connections, the CPU monitors the use of connection resources in the automation system. Once the reserved connection resources have been exhausted, additional resources can be used (as long as connection resources are available for the automation system).

If the establishment and termination of the connections is **programmed** in the user program, you yourself will need to make sure that the limits of the connection resources are kept to on the automation system. If you use more connection resources that those provided by the automation system. the CPU acknowledges the instruction to establish connection with an error.

If you have **configured** connections in STEP 7, STEP 7 monitors use of the connection resources to ensure that the maximum possible number on an automation system is not exceeded. STEP 7 signals a violation of this with a suitable warning.

Configured connections: Display of the connection resources in STEP 7 (offline view)

You can display the reserved and available connection resources of an automation system in the hardware configuration. You can find the connection resources in the Inspector window in the properties of the CPU.

516-3 PN/DP]

IO tags | Texts

Connection resources

	Station resources			Module resour...	Module reso...	Module reso...
	Reserved		Dynamic ⚠	PLC_2 [CPU 15..	CP 1543-1_1..	CM 1542-5_1..
Maximum number of resources:		10	246	128	118	48
	Maximum	Configured	Configured	Configured	Configured	Configured
PG communication:	4	-	-	-	-	-
HMI communication:	4	4	6	6	4	0
S7 communication:	0	-	23	2	0	21
Open user communication:	0	-	118	39	52	27
Web communication:	2	-	-	-	-	-
Other communication:	-	-	-	-	-	-
Total resources used:		4	147	47	56	48
Available resources:		6	99	81	62	0

Figure 10-1 Reserved and available connection resources (offline view)

Module-specific connection resources (offline view)

The columns of the module-specific connection resources contain the following for the CPU, CPs and CMs of an automation system:

- How many connection resources are available as maximum for CPU/CP/CM
- How many of these were configured for which communications connections
- How many connection resources were configured in total and therefore used up
- How many connection resources are still available

The display is per module and not per interface.

In the example, the CPU provides a maximum of 128 connection resources. 6 HMI, 2 S7 and 39 open communication connections were configured for the CPU via the interfaces occupying a total of 47 resources on the CPU. 81 resources of the CPU remain available. For the CP 1543-1, 56 of the 118 available resources are allocated, 62 resources remain available. All 48 available resources are used for the CM 1542-5.

Station-specific connection resources (offline view)

The maximum number of available connection resources on the automation system (in the station) depends on the CPU being used. If the CPU-dependent limit is reached, it does not matter whether the CPU, CPs and CMs have further module-specific connection resources. For this station, the connection resources are used up.

In the example there are 246 + 10 reserved connection resources available for the automation system.

The 10 connection resources are reserved:

- 4 for PG communication required by STEP 7, for example, for test and diagnostics functions or downloading to the CPU
- 4 for HMI communication which are allocated by the first HMI connections configured in STEP 7
- 2 for communication with the web server that are allocated after connecting a Web browser if the web server of the CPU is activated

A maximum of 246 connection resources are dynamic; in other words, available for various communications services on the automation system. In this example, 147 of these connection resources are already configured for various communications services and modules. This leaves 99 connection resources available for the automation system.

The warning triangle in the column of the dynamic station resources is therefore displayed because the sum of the maximum available connection resources of CPU, CP and CM (= 294 connection resources) exceeds the station limit of 256.

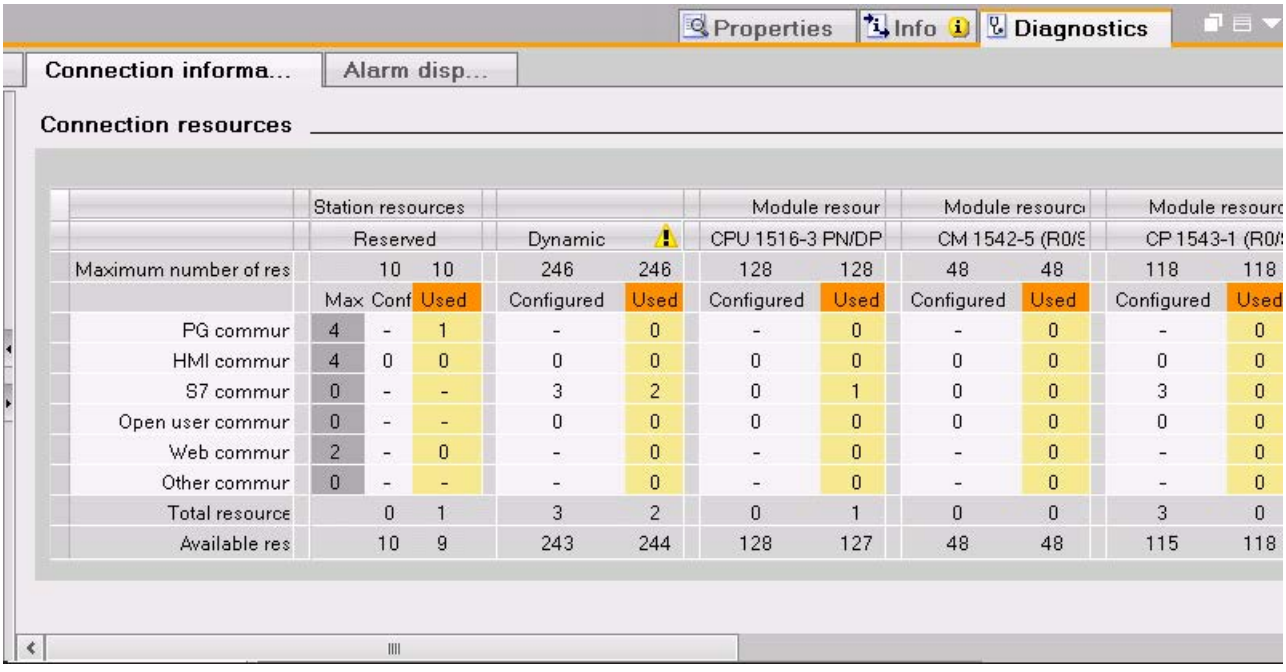
Note

Available connection resources exceeded

STEP 7 signals the exceeding of the station-specific connection resources with a warning. In this case, either use a CPU with a higher maximum number of available station-specific connection resources or reduce the number of communications connections.

Display of the connection resources in STEP 7 (online view)

If you have selected a CPU in the network view of the Devices & networks editor of STEP 7 that is connected online, you can display the current status of the allocated and available resources for this automation system in the "Connection information" tab in the "Diagnostics" area of the Inspector window.



	Station resources					Module resour		Module resourc		Module resourc	
	Reserved			Dynamic		CPU 1516-3 PN/DP		CM 1542-5 (R0/S		CP 1543-1 (R0/	
Maximum number of res		10	10	246	246	128	128	48	48	118	118
	Max	Conf	Used	Configured	Used	Configured	Used	Configured	Used	Configured	Used
PG commur	4	-	1	-	0	-	0	-	0	-	0
HMI commur	4	0	0	0	0	0	0	0	0	0	0
S7 commur	0	-	-	3	2	0	1	0	0	3	0
Open user commur	0	-	-	0	0	0	0	0	0	0	0
Web commur	2	-	0	-	0	-	0	-	0	-	0
Other commur	0	-	-	-	0	-	0	-	0	-	0
Total resource		0	1	3	2	0	1	0	0	3	0
Available res		10	9	243	244	128	127	48	48	115	118

Figure 10-2 Connection resources - online

The online view of the "Connection resources" table also contains the reserved and configured connection resources of the offline view columns with the connection resources currently allocated on the CPU. In the online view, **all** allocated connection resources on the automation system are displayed regardless of whether they were set up automatically, programmed or configured. In the "Other communication" row, allocated connection resources for communication with third-party devices and communication via data record routing are displayed. The table is updated automatically.

Note

If a routed S7 connection goes through a CPU, the required connection resources of the CPU do not appear in the table of connection resources!

Connection resources for HMI communication

You can find information about the availability and allocation of connection resources for HMI connections in the offline view in the context of the HMI device (in the Inspector window in the properties in the "Connection resources" area).

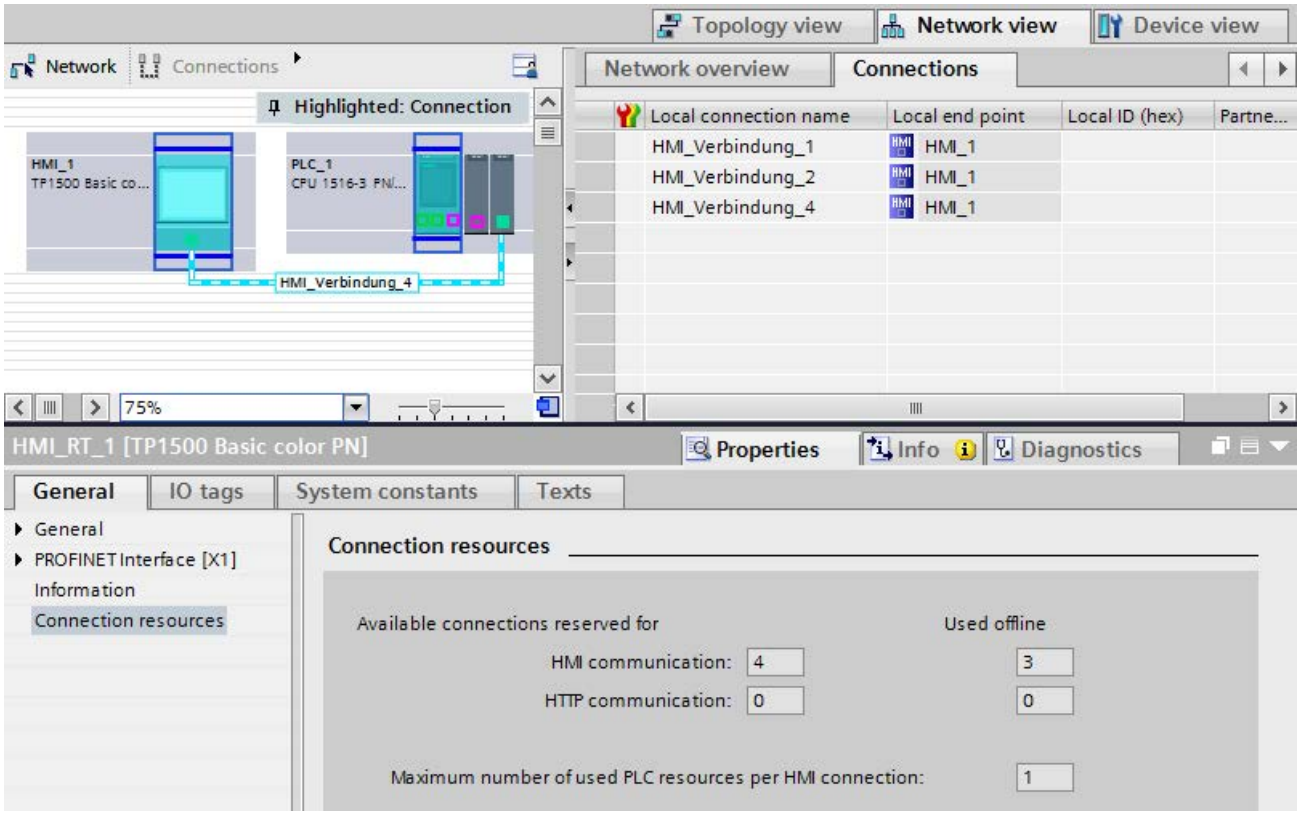


Figure 10-3 Connection resources - HMI communication

The following is displayed under "Offline used":

- The number of the connection resources used for HMI communication

  If the maximum number of available connection resources for an HMI device is exceeded, a corresponding message is output by STEP 7.

- The maximum number of connection resources allocated by the configured HMI connections

  With HMI communication, the allocation of connection resources in the CPU depends on the HMI device.

The following table shows the relationship between the HMI device used and the maximum allocated connection resources per HMI connection.

HMI device	Max. required connection resources of the CPU per HMI connection
Basic Panel	1
Comfort Panel	2[1]
RT Advanced	2[1]
RT Professional	3

[1] If you do not use system diagnostics and a message configuration, the CPU requires only one connection resource per HMI connection.

Connection resources for S7 routing

To transfer data beyond S7 subnets ("S7 routing"), an S7 connection is established between two CPUs. The S7 subnets are connected via gateways known as S7 routers. CPUs, CMs and CPs in S7-1500 are S7 routers.

The following applies for a routed S7 connection:

- A connection resource is allocated in each end point and displayed in the table of connection resources.
- In the S7 router, two connection resources are allocated, but they are not shown in the table of connection resources.

Connection resources for data record routing

Data record routing also enables transfer of data beyond S7 subnets from an engineering station connected to PROFINET to various field devices via PROFIBUS.

Two connection resources are allocated in each data record router for data record routing.

Note

Connection resources with data record routing

Two connection resources are allocated for data record routing in the data record router. Neither the data record connection nor the allocated connection resources are displayed in the table of connection resources.

Additional information

- S7 routing is described in the section S7 routing (Page 64).
- You can find the number of connection resources that an HMI device requires on the CPU in the documentation of the HMI device.

Connection diagnostics

11

Connections table in the online view

After selecting a CPU in the Devices & networks editor of STEP 7, you will see the status of your connections displayed in the online view of the connections table.

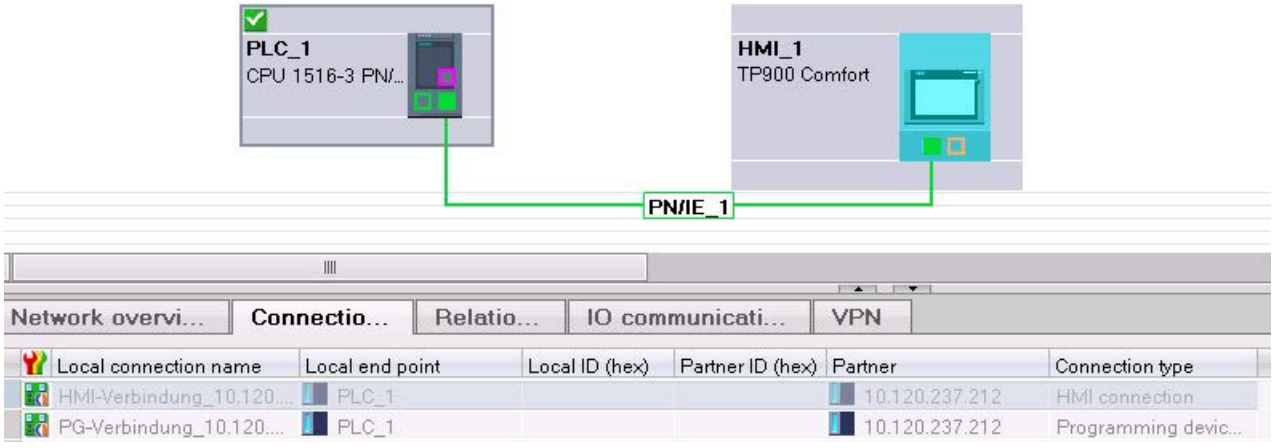


Figure 11-1 Online view of the connections table

After selecting the connection in the connections table, you obtain detailed diagnostic information in the "Connection information" tab.

"Connection information" tab: Connection details

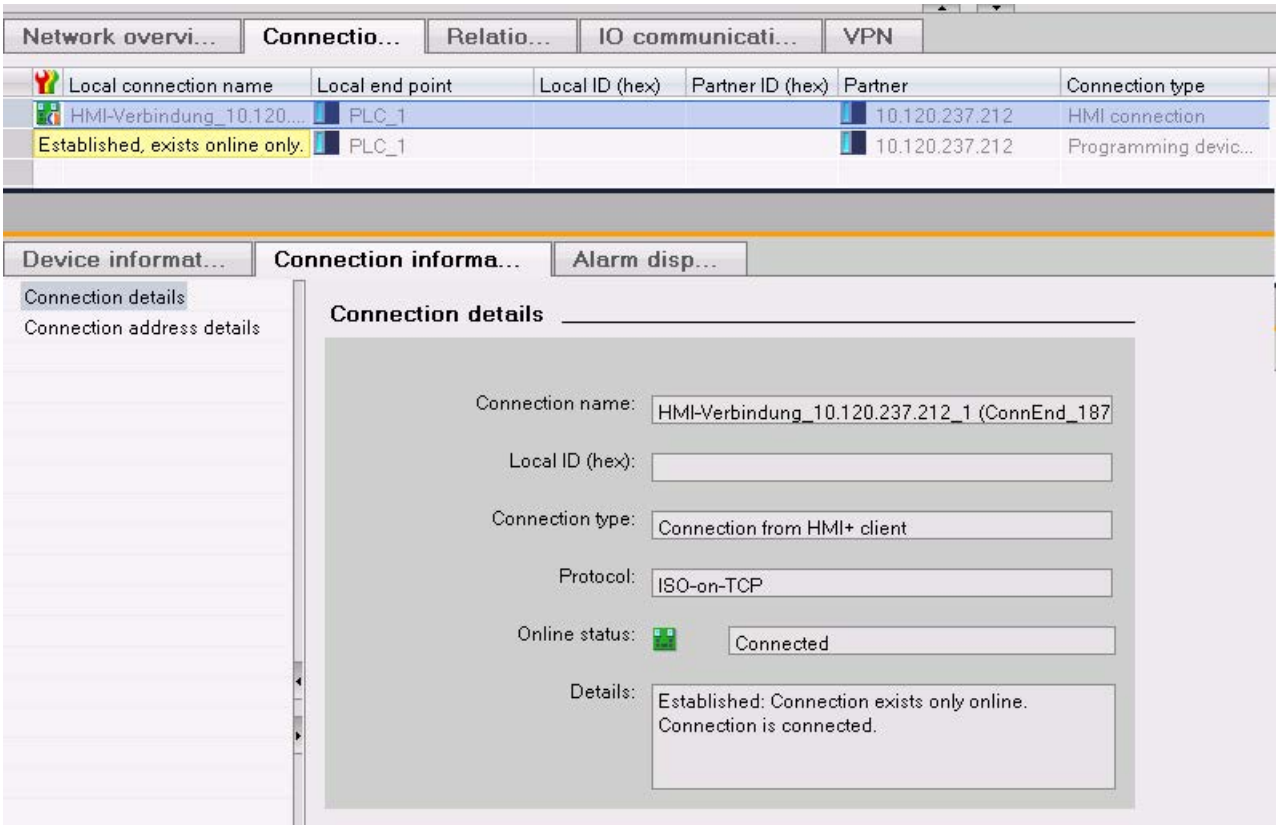


Figure 11-2 Diagnostics of connections - connection details

"Connection information" tab: Address details

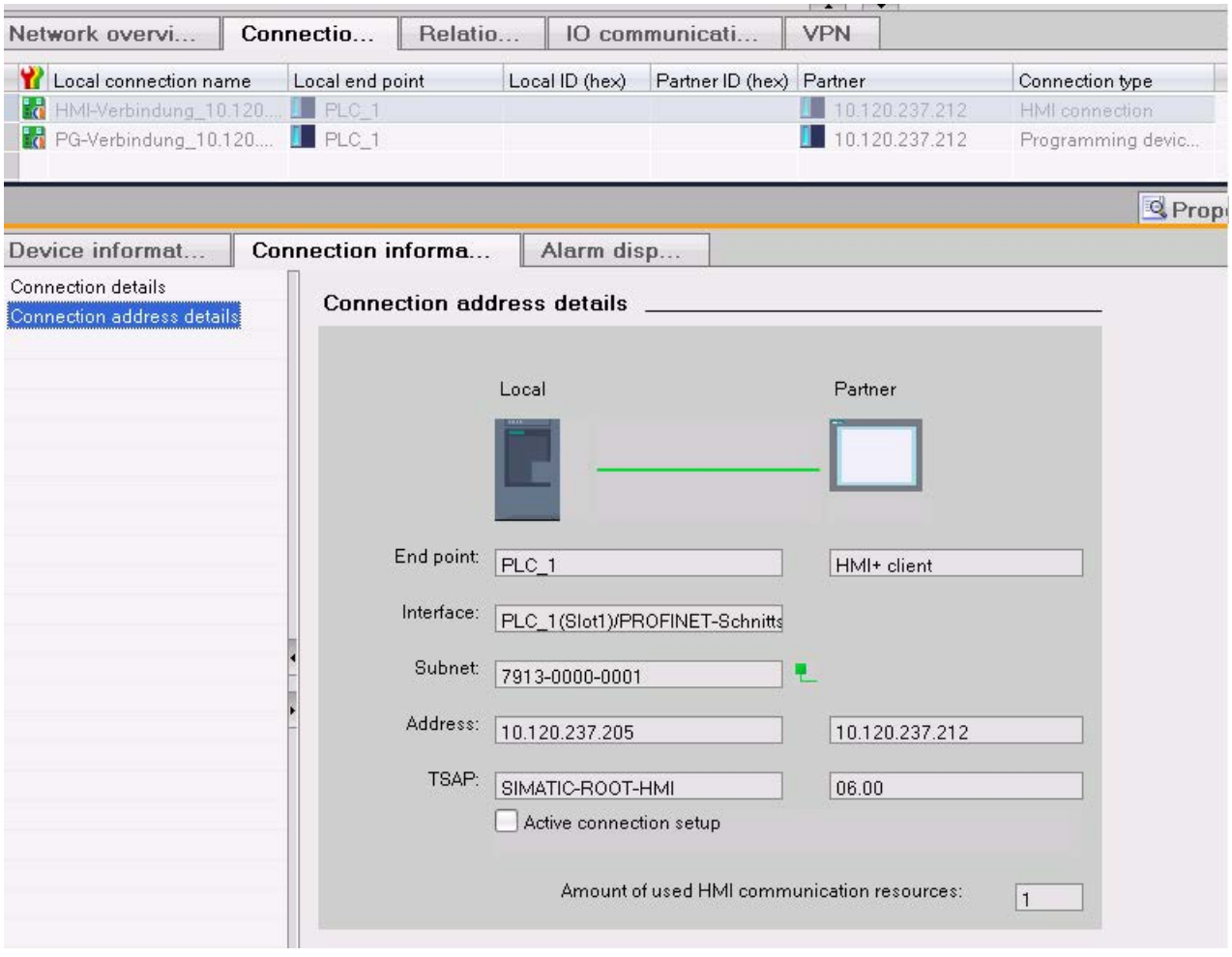


Figure 11-3 Diagnostics of connections - address details

Diagnostics via web server

You can evaluate diagnostic information from the CPU using a web browser via the integrated web server of a CPU.

On the "Communication" Web page, you will find the following information about communication via PROFINET in various tabs:

- Information on the PROFINET interfaces of the CPU (for example addresses, subnets, physical properties).
- Information on the quality of the data transfer (for example number of data packets sent/received error-free).
- Information about the allocation/availability of connection resources.
- The "Connections" page is similar to the online view in STEP 7 and also provides an overview of all connections with detail view.

Diagnostics with the user program

When you program the T_DIAG instruction, you can evaluate diagnostic information about the configured and programmed connections of the CPU using the user program.

Additional information

You will find the description of the web server functionality in the function manual Web server (http://support.automation.siemens.com/WW/view/en/59193560).

Industrial Ethernet Security 12

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. Data transfer can also be protected by a combination of different security measures:

- Data espionage
- Data manipulation
- Unauthorized access

Security measures

- 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

All network nodes located in the internal network segment of a CP 1543-1 are protected by its firewall.

- 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.
- HTTPS

  For encrypted transfer of Web pages, for example during process monitoring.
- 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.

12.1 Firewall

Tasks of the firewall

The purpose of the firewall functionality is to protect networks and stations from outside influences and disturbances. This means that only certain previously specified communications relations are permitted.

To filter the data traffic, IPv4 addresses, IPv4 subnets, port numbers or MAC addresses among other things can be used.

The firewall functionality can be configured for the following protocol levels:

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

Firewall rules

Firewall rules describe which packets are permitted or forbidden in which direction.

12.2 Logging

Functionality

For test and monitoring purposes, the security module has diagnostics and logging functions.

- Diagnostics functions

  These include various system and status functions that you can use in online mode.

- Logging functions

  This involves the recording of system and security events. Depending on the event type, the recording is made in volatile or non-volatile local buffer areas of the CP 1543-1. As an alternative, it is also possible to record on a network server.

  The parameter assignment and evaluation of these functions is only possible with a network connection.

Recording events with logging functions

You specify which events should be recorded with the log settings. Here you can configure the following recording variants:

- Local logging

  With this variant, you record the events in local buffers of the CP 1543-1. In the online dialog of the Security Configuration Tool, you can then access these recordings, visualize them and archive them on the service station.

- Network Syslog

  With the network Syslog, you use a Syslog server in the network. This records the events according to the configuration in the log settings.

12.3 NTP client

Functionality

To check the time validity of a certificate and the time stamp of log entries, the date and time are maintained on the CP 1543-1 as on the CPU. This time can be synchronized with NTP. The CP 1543-1 forwards the synchronized time to the CPU via the backplane bus of the automation system. This way the CPU also receives a synchronized time for the time events in program execution.

The automatic setting and periodic synchronization of the time takes place either via a secure or non-secure NTP server. You can assign a maximum of 4 NTP servers to the CP 1543-1. A mixed configuration of non-secure and secure NTP servers is not possible.

12.4 SNMP

Functionality

The CP 1543-1 supports the transfer of management information using the Simple Network Management Protocol (SNMP) just like on the CPU. To achieve this, an "SNMP agent" is installed on the CP that receives and responds to the SNMP queries. Information about the properties of devices capable of SNMP is contained in so-called MIB files (Management Information Base) for which the user needs to have the appropriate rights.

With SNMPv1, the "community string" is also sent. The "community string" is like a password that is sent along with the SNMP query. The requested information is sent when the "community string" is correct. The request is discarded when the string is incorrect.

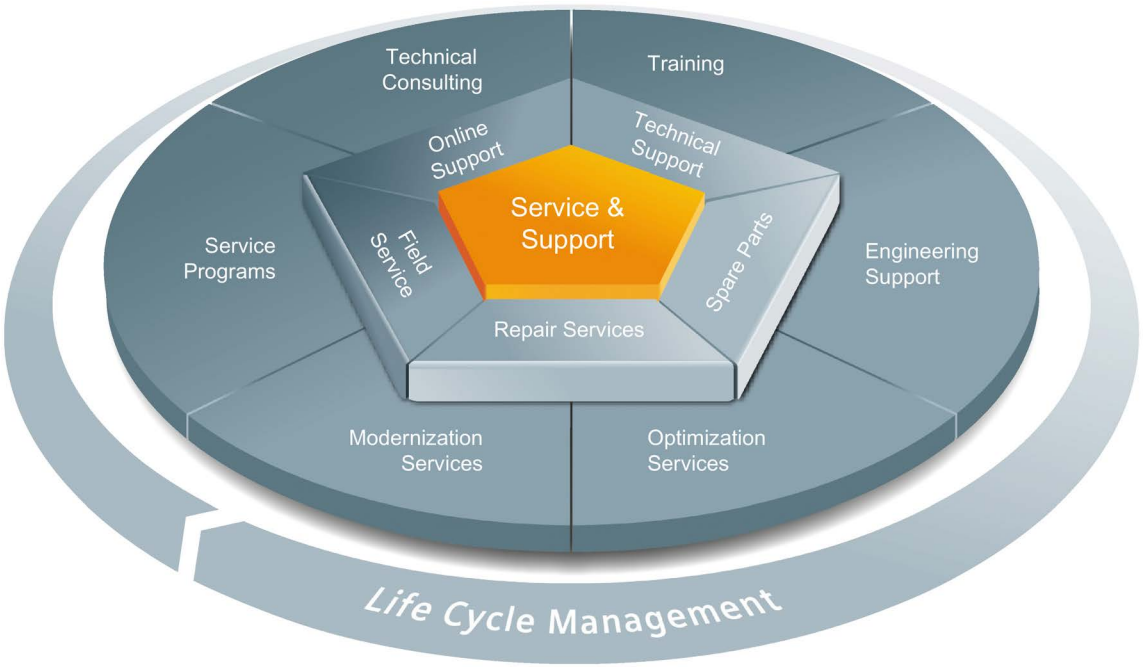
With SNMPv3, data can be transferred encrypted. To do this, select either an authentication method or an authentication and encryption method.

Possible selection:

- Authentication algorithm: none, MD5, SHA-1
- Encryption algorithm: none, AES-128, DES

Service & Support

A



The unmatched complete service for the entire life cycle

For machine constructors, solution providers and plant operators: The service offering from Siemens Industry Automation and Drive Technologies includes comprehensive services for a wide range of different users in all sectors of the manufacturing and process industry.

To accompany our products and systems, we offer integrated and structured services that provide valuable support in every phase of the life cycle of your machine or plant – from planning and implementation through commissioning as far as maintenance and modernization.

Our Service & Support accompanies you worldwide in all matters concerning automation and drive technology from Siemens. We provide direct on-site support in more than 100 countries through all phases of the life cycle of your machines and plants.

You have an experienced team of specialists at your side to provide active support and bundled know-how. Regular training courses and intensive contact among our employees – even across continents – ensure reliable service in the most diverse areas

Online Support

The comprehensive online information platform supports you in all aspects of our Service & Support at any time and from any location in the world.

You can find Online Support on the Internet at the following address: Internet (http://www.siemens.com/automation/service&support).

Technical Consulting

Support in planning and designing your project: From detailed actual-state analysis, definition of the goal and consultation on product and system questions right through to the creation of the automation solution.

Technical Support

Expert advice on technical questions with a wide range of demand-optimized services for all our products and systems.

You can find Technical Support on the Internet at the following address: Internet (http://www.siemens.com/automation/support-request).

Training

Extend your competitive edge – through practical know-how directly from the manufacturer.

You can find the training courses we offer on the Internet at the following address: Internet (http://www.siemens.com/sitrain).

Engineering Support

Support during project engineering and development with services fine-tuned to your requirements, from configuration through to implementation of an automation project.

Field Service

Our Field Service offers you services for commissioning and maintenance – to ensure that your machines and plants are always available.

Spare parts

In every sector worldwide, plants and systems are required to operate with constantly increasing reliability. We will provide you with the support you need to prevent a standstill from occurring in the first place: with a worldwide network and optimum logistics chains.

Repairs

Downtimes cause problems in the plant as well as unnecessary costs. We can help you to reduce both to a minimum – with our worldwide repair facilities.

Optimization

During the service life of machines and plants, there is often a great potential for increasing productivity or reducing costs.

To help you achieve this potential, we are offering a complete range of optimization services.

Modernization

You can also rely on our support when it comes to modernization – with comprehensive services from the planning phase all the way to commissioning.

Service programs

Our service programs are selected service packages for an automation and drives system or product group. The individual services are coordinated with each other to ensure smooth coverage of the entire life cycle and support optimum use of your products and systems.

The services of a Service Program can be flexibly adapted at any time and used separately.

Examples of service programs:

- Service contracts
- Plant IT Security Services
- Life Cycle Services for Drive Engineering
- SIMATIC PCS 7 Life Cycle Services
- SINUMERIK Manufacturing Excellence
- SIMATIC Remote Support Services

Advantages at a glance:

- Reduced downtimes for increased productivity
- Optimized maintenance costs due to a tailored scope of services
- Costs that can be calculated and therefore planned
- Service reliability due to guaranteed response times and spare part delivery times
- Customer service personnel will be supported and relieved of additional tasks
- Comprehensive service from a single source, fewer interfaces and greater expertise

Contact

At your service locally, around the globe: your partner for consultation, sales, training, service, support, spare parts... for the entire range of products supplied by Industry Automation and Drive Technologies.

You will find your personal contact in our contacts database at: Internet (http://www.siemens.com/automation/partner).

Glossary

Automation system

Programmable logic controller for the open-loop and closed-loop control of process chains of the process engineering industry and manufacturing technology. The automation system consists of different components and integrated system functions according to the automation task.

Bus

Transmission medium that connects several devices together. Data transmission can be performed electrically or via optical fibers, either in series or in parallel.

Client

Device in a network that requests a service from another device in the network (server).

CM

→ *Communications module*

Communications module

Module for communications tasks used in an automation system as an interface expansion of the CPU (for example PROFIBUS) and providing additional communications options (PtP).

Communications processor

Module for expanded communications tasks covering special applications, for example in the area of security.

Consistent data

Data that belongs together in terms of content and must not be separated when transferred.

CP

→ *Communications processor*

CPU

Central **P**rocessing **U**nit - Central module of the S7 automation system with a control and arithmetic unit, memory, operating system and interface for programming device.

Device

Generic term for:

- Automation systems (PLC, PC, for example)
- Distributed I/O systems
- Field devices (for example, PLC, PC, hydraulic devices, pneumatic devices) and
- Active network components (for example, switches, routers)
- Gateways to PROFIBUS, AS interface or other fieldbus systems

DP master

Within PROFIBUS DP, a master in the distributed I/O that behaves according to the EN 50170 standard, Part 3.

→ *See also DP slave*

DP slave

Slave in the distributed I/O that is operated on PROFIBUS with the PROFIBUS DP protocol and behaves according to the EN 50170 standard, Part 3.

→ *See also DP master*

Duplex

Data transmission system; a distinction is made between full and half duplex.

Half duplex: One channel is available for alternate data exchange (sending or receiving alternately but not at the same time).

Full duplex: Two channels are available for simultaneous data exchange in both directions (simultaneous sending and receiving in both directions).

Ethernet

International standard technology for local area networks (LAN) based on frames. It defines types of cables and signaling for the physical layer and packet formats and protocols for media access control.

Ethernet network adapter

Electronic circuitry for connecting a computer to an Ethernet network. It allows the exchange of data / communication within the network.

FETCH/WRITE

Server services using TCP/IP, ISO-on-TCP and ISO for access to system memory areas of S7 CPUs. Access (client function) is possible from a SIMATIC S5 or a third-party device/PC. FETCH: Read data directly; WRITE: Write data directly.

Field device

→ *Device*

Freeport

Freely programmable ASCII protocol; here for data transfer via a point-to-point connection.

FTP

File **T**ransfer **P**rotocol; a network protocol for transferring files via IP networks. FTP is used to download files from the server to the client or to upload files from the client to the server. FTP directories can also be created and read out and directories and files can be renamed or deleted.

HMI

Human **M**achine **I**nterface, device for visualization and control of automation processes.

IE

→ *Industrial Ethernet*

IM

→ *Interface module*

Industrial Ethernet

Guideline for setting up an Ethernet network in an industrial environment. The essential difference compared with standard Ethernet is the mechanical ruggedness and immunity to noise of the individual components.

Instruction

The smallest self-contained unit of a user program characterized by its structure, function or purpose as a separate part of the user program. An instruction represents an operation procedure for the processor.

Interface module

Module in the distributed I/O system. The interface module connects the distributed I/O system via a fieldbus to the CPU (IO controller/DP master) and prepares the data for the I/O modules.

IO controller, PROFINET IO controller

Central device in a PROFINET system, usually a classic programmable logic controller or PC. The IO controller sets up connections to the IO devices, exchanges data with them, thus controls and monitors the system.

IO device, PROFINET IO device

Device in the distributed I/O of a PROFINET system that is monitored and controlled by an IO controller (for example distributed inputs/outputs, valve islands, frequency converters, switches).

IP address

Binary number that is used as a unique address in computer networks in conjunction with the Internet Protocol (IP). It makes these devices uniquely addressable and individually accessible. An IPv4 address can be evaluated using a binary subnet mask that results in a network part or a host part as a structure. The textual representation of an IPv4 address is made up, for example, of 4 decimal numbers with a range of values from 0 to 255. The decimal numbers are separated by dots.

IPv4 subnet mask

Binary mask, with which an IPv4 address (as a binary number) is divided into a "network part" and a "host part"

ISO protocol

Communications protocol for message or packet-oriented transfer of data in an Ethernet network. This protocol is hardware-oriented, very fast and allows dynamic data lengths. The ISO protocol is suitable for medium to large volumes of data.

ISO-on-TCP protocol

Communications protocol capable of S7 routing for packet-oriented transfer of data in an Ethernet network; provides network addressing. The ISO-on-TCP protocol is suitable for medium and large volumes of data and allows dynamic data lengths.

Linear bus topology

Network topology characterized by the arrangement of the devices in a line (bus).

MAC address

Worldwide unique device identification for all Ethernet devices. The MAC address is assigned by the manufacturer and has a 3-byte vendor ID and 3-byte device ID as a consecutive number.

Master

Higher-level, active participant in the communication/on a PROFIBUS subnet. The master has rights to access the bus (token), requests data and sends it.

→ *See also DP master*

Modbus RTU

Remote **T**erminal **U**nit; Open communications protocol for serial interfaces based on a master/slave architecture.

Modbus TCP

Transmission **C**ontrol **P**rotocol; Open communications protocol for Ethernet based on a master/slave architecture. The data are transmitted as TCP/IP packets.

Network

A network consists of one or more interconnected subnets with any number of devices. Several networks can exist alongside each other.

NTP

The **N**etwork **T**ime **P**rotocol (NTP) is a standard for synchronizing clocks in automation systems via Industrial Ethernet. NTP uses the connectionless UDP transport protocol for the Internet.

Operating system

Software that allows the use and operation of a computer. The operating system manages resources such as memory, input and output devices and controls the execution of programs.

PG

→ *Programming device*

PNO

→ *PROFIBUS user organization*

Point-to-point connection

Bidirectional data exchange via communications modules with a serial interface between two communications partners (and two only).

Port

Physical connector to connect devices to PROFINET. PROFINET interfaces have one or more ports.

Process image

Address area of a programmable logic controller (PLC), in which the signal states of the inputs and the logical states of the outputs from the connected modules are stored digitally.

PROFIBUS

Process **Fi**eld **Bus** - European Fieldbus standard.

PROFIBUS address

Unique identifier of a device connected to PROFIBUS. The PROFIBUS address is sent in the frame to address a device.

PROFIBUS device

Device with at least one PROFIBUS interface either electrical (for example RS-485) or optical (for example Polymer Optical Fiber).

PROFIBUS user organization

Technical committee dedicated to the definition and development of the PROFIBUS and PROFINET standard.

PROFIBUS DP

A PROFIBUS with DP protocol that complies with EN 50170. DP stands for distributed I/O = fast, real-time capable, cyclic data exchange. From the perspective of the user program, the distributed I/O is addressed in exactly the same way as the centralized IO.

PROFINET

Open component-based industrial communications system based on Ethernet for distributed automation systems. Communications technology promoted by the PROFIBUS user organization.

PROFINET device

Device that always has a PROFINET interface (electrical, optical, wireless).

PROFINET interface

Interface of a module capable of communication (for example CPU, CP) with one or more ports. A MAC address is assigned to the interface in the factory. Along with the IP address and the device name (from the individual configuration), this interface address ensures that the PROFINET device is identified uniquely in the network. The interface can be electrical, optical or wireless.

PROFINET IO

IO stands for input/output; distributed I/O (fast, cyclic data exchange with real-time capability). From the perspective of the user program, the distributed I/O is addressed in exactly the same way as the centralized IO.

PROFINET IO as the Ethernet-based automation standard of PROFIBUS & PROFINET International defines a cross-vendor communication, automation, and engineering model.

With PROFINET IO, a switching technology is used that allows all devices to access the network at any time. In this way, the network can be used much more efficiently through the simultaneous data transfer of several devices. Simultaneous sending and receiving is enabled via the full-duplex operation of Switched Ethernet.

PROFINET IO is based on switched Ethernet with full-duplex operation and a bandwidth of 100 Mbps.

Programming device

Programming devices are essentially compact and portable PCs which are suitable for industrial applications. They are identified by a special hardware and software configuration for programmable logic controllers.

Protocol

Agreement on the rules by which the communication between two or more communication partners transpires.

PtP

Point-**t**o-**P**oint, interface and/or transmission protocol for bidirectional data exchange between two (and only two) communications partners.

Ring topology

All devices of a network are connected together in a ring.

Router

Network node with a unique identifier (name and address) that connects subnets together and allows transportation of data to uniquely identified communications nodes in the network.

RS232, RS422 and RS485

Standard for serial interfaces.

RTU

Modbus RTU (RTU: **R**emote **T**erminal **U**nit, transfers the data in binary form; allows a good data throughput. The data must be converted to a readable format before it can be evaluated.

S7 routing

Communication between S7 automation systems, S7 applications or PC stations in different S7 subnets via one or more network nodes functioning as S7 routers.

SDA service

Send Data with Acknowledge. SDA is an elementary service with which an initiator (for example DP master) can send a message to other devices and then receives acknowledgment of receipt immediately afterwards.

SDN service

Send Data with No Acknowledge. This service is used primarily to send data to multiple stations and the service therefore remains unacknowledged. Suitable for synchronization tasks and status messages.

Security

Generic term for all the measures taken to protect against

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability due to the destruction of data

Server

A device or more generally an object that can provide certain services; the service is performed at the request of a client.

Slave

Distributed device in a fieldbus system that can only exchange data with a master after the master has requested this.

→ *See also DP slave*

SNMP

Simple Network Management Protocol, uses the wireless UDP transport protocol. SNMP works in much the same way as the client/server model. The SNMP manager monitors the network nodes. The SNMP agents collect the various network-specific information in the individual network nodes and makes this information available in a structured form in the MIB (Management Information Base). This information allows a network management system to run detailed network diagnostics.

Subnet

Part of a network whose parameters must be matched up on the devices (for example in PROFINET). A subnet includes the bus components and all connected stations. Subnets can be linked together, for example using gateways or routers to form one network.

Switch

Network components used to connect several terminal devices or network segments in a local network (LAN).

TCP/IP

Transmission Control Protocol / Internet Protocol, connection-oriented network protocol, generally recognized standard for data exchange in heterogeneous networks.

Time-of-day synchronization

Capability of transferring a standard system time from a single source to all devices in the system so that their clocks can be set according to the standard time.

Tree topology

Network topology characterized by a branched structure: Two or more bus nodes are connected to each bus node.

Twisted-pair

Fast Ethernet via twisted-pair cables is based on the IEEE 802.3u standard (100 Base-TX). The transmission medium is a shielded 2x2 twisted-pair cable with an impedance of 100 Ohms (22 AWG). The transmission characteristics of this cable must meet the requirements of category 5.

The maximum length of the connection between the terminal and the network component must not exceed 100 m. The connectors are designed according to the 100Base-TX standard with the RJ-45 connector system.

UDP

User Datagram Protocol; communications protocol for fast and uncomplicated data transfer, without acknowledgment. There are no error checking mechanisms as found in TCP/IP.

User program

In SIMATIC, a distinction is made between the CPU operating system and user programs. The user program contains all instructions, declarations and data by which a system or process can be controlled. The user program is assigned to a programmable module (for example, CPU, FM) and can be structured in smaller units.

USS

Universal Serial Interface protocol (**U**niverselles **S**erielles **S**chnittstellen-Protokoll); defines an access method according to the master-slave principle for communication via a serial bus.

Web server

Software/communications service for data exchange via the Internet. The web server transfers the documents using standardized transmission protocols (HTTP, HTTPS) to a Web browser. Documents can be static or put together dynamically from different sources by the web server on request from the Web browser.

Index

A

Allocation of connection resources, 71

B

BRCV, 50
BSEND, 50

C

CM, 10
Communication
    Data record routing, 69
    HMI communication, 29
    Open communication, 31
    PG communication, 26
    Point-to-point connection, 58
    S7 communication, 49
    S7 routing, 64
Communication options
    Overview, 15
Communication via PUT/GET instruction
    Creating and configuring a connection, 51
Communications
    Communication protocols, 32
    Establishment and termination, 48
Communications module, 10
Communications processor, 10
Communications services
    Connection resources, 17
Connection
    Diagnostics, 77
    Instructions for open communication, 33
Connection diagnostics, 77
Connection resources
    Data record routing, 76
    Display in STEP 7, 72
    HMI communication, 75
    Module specific, 72
    Overview, 17
    Pin assignments, 71
    S7 routing, 76
    Station specific, 73
Consistency of data, 20
CP, 10

D

Data consistency, 20
Data record routing, 69
    Connection resources, 76

E

E-mail, 15, 33, 44
Establishment and termination of communications, 48

F

Fetch, 15
Firewall, 82
Freeport protocol, 58
FTP, 15, 33, 44, 45

G

GET, 50

H

HMI communication, 15, 29

I

IM, 14
Industrial Ethernet Security, 81
Instructions for open communication, 33
Interface module, 14
Interfaces for communication, 11
Interfaces of communications modules
    Point-to-point connection, 13
Interfaces of communications processors, 12
ISO, 15, 32
ISO-on-TCP, 32, 36

L

Logging, 82

M

Modbus protocol (RTU), 58
Modbus TCP, 32

N

NTP, 15, 83

O

Open communication
  Connection configuration, 36
  Instructions, 33
  Properties, 31
  Protocols, 32
  Setting up e-mail, 44
  Setting up FTP, 45
  Setting up TCP, ISO-on-TCP, UDP, 36

P

PCT, 70
PG communication, 15, 26
Point-to-point connection, 15, 58
Procedure 3964(R), 58
Protocols of open communication, 32
PUT, 50

S

S7 communication, 15, 49, 76
S7 routing, 64
  Connection resources, 76
Security, 81
Security measures, 81
  Firewall, 82
  Logging, 82
  NTP, 83
  SNMP, 83
Setting up a connection, 18
  By configuring, 40
  ISO connection with CP 1543-1, 41
SNMP, 15, 83
Syslog, 83
System data type, 34

T

TCON, 33
TCP, 15, 32, 36
TDISCON, 33
Time-of-day synchronization, 15
TRCV, 33
TRCV_C, 33
TSEND, 33
TSEND_C, 33

U

UDP, 15, 32, 36
URCV, 50
USEND, 50
USS protocol, 58

W

Web server, 15
Write, 15