SIEMENS

SIMATIC

S7-1500/ET 200MP
Automation system

System Manual

11/2024
A5E03461182-AM

S7-1500/ET 200MP Automation system

System Manual

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

Introduction

<div align="right">

1

</div>

Purpose of the documentation

> This documentation provides important information on configuring, installing, wiring and commissioning the S7-1500 automation system/ET 200MP distributed I/O system.

Basic knowledge required

> General knowledge in the field of automation engineering is required to understand this documentation.

Validity of the documentation

> This documentation applies to all products of the SIMATIC S7-1500 and SIMATIC ET 200MP product families.

Conventions

> STEP 7: In this documentation, "STEP 7" is used as a synonym for all versions of the configuration and programming software "STEP 7 (TIA Portal)".
>
> Please also observe notes marked as follows:
>
> ---
> **NOTE**
>
> A note contains important information on the product described in the documentation, on the handling of the product or on the section of the documentation to which particular attention should be paid.
>
> ---

ID link for the digital nameplate

>
>
> The ID link is a globally unique identifier according to IEC 61406-1, which you will find in the future as a QR code on your product.

The figure shows an example of an ID link for the digital output module
DQ 16x24VDC/0.5A BA.

You can recognize the ID link by the frame with a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product.

Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call the ID link.

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

Special information

NOTE

Important note for maintaining the operational safety of your plant

Plants with safety-related features are subject to special operational safety requirements on the part of the operator. The supplier is also required to comply with certain measures for product monitoring. Siemens informs system operators in the form of personal notifications about product developments and properties which may be or become important issues in terms of operational safety.

You need to subscribe to the corresponding notifications to ensure that you always remain up-to-date and are able to make any necessary changes to your plant regarding operational safety should the need arise.

Register with Industry Online Support. Follow the links below and click on "Email on update" on the right-hand side in each case:

- SIMATIC S7-300/S7-300F (https://support.industry.siemens.com/cs/ww/en/ps/13751)
- SIMATIC S7-400/S7-400H/S7-400F/FH
  (https://support.industry.siemens.com/cs/ww/en/ps/13828)
- SIMATIC WinAC RTX (F) (https://support.industry.siemens.com/cs/ww/en/ps/13915)
- SIMATIC S7-1500/SIMATIC S7-1500F
  (https://support.industry.siemens.com/cs/ww/en/ps/13716)
- SIMATIC S7-1200/SIMATIC S7-1200F
  (https://support.industry.siemens.com/cs/ww/en/ps/13683)
- Distributed I/O (https://support.industry.siemens.com/cs/ww/en/ps/14029)
- STEP 7 (TIA Portal) (https://support.industry.siemens.com/cs/ww/en/ps/14667)

NOTE

Increased safety measures

Anywhere that errors can cause injury or property damage, special standards must be applied to the safety of the entire plant. Special, plant-specific rules exist for this purpose, which must also be taken into account by the owner when setting up the controller.

For electronic controllers with safety responsibility, the measures that must be taken to prevent or control errors are based on the risk posed by the plant. For this, the owner must ensure implementation of additional measures for the plant, e.g. use of safety-related controllers such as the S7-1500 F fail-safe automation system.

NOTE

When using F-CPUs in safety mode and fail-safe modules, note the description of the fail-safe system SIMATIC Safety Programming and Operating Manual SIMATIC Safety - Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126).

NOTE

Product information

The Product Information for the S7-1500 automation system/ET 200MP distributed I/O system contains:

- Module overview of SIMATIC S7-1500 and ET 200MP

- Additions to the documentation

The product information can be found on the Internet (https://support.automation.siemens.com/WW/view/en/68052815).

Industry Mall

The Industry Mall is the catalog and order system of Siemens AG for automation and drive solutions on the basis of Totally Integrated Automation (TIA) and Totally Integrated Power (TIP).

You can find catalogs for all automation and drive products on the Internet (https://mall.industry.siemens.com).

1.1 S7-1500/ET 200MP documentation guide

1.1.1 Information classes S7-1500/ET 200MP

The documentation for the SIMATIC S7-1500 automation system and the ET 200MP distributed I/O system is arranged into three areas.

This arrangement enables you to access the specific content you require. Changes and supplements to the manuals are documented in a Product Information.

You can download the documentation free of charge from the Internet (https://support.industry.siemens.com/cs/ww/en/view/109742691).

Basic information

The System Manual and Getting Started describe in detail the configuration, installation, wiring and commissioning of the SIMATIC S7-1500 and ET 200MP systems.

The STEP 7 online help supports you in the configuration and programming.

Examples:

- Getting Started S7-1500

- S7-1500/ET 200MP System Manual

- Online help TIA Portal

Device information

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

Examples:

- Equipment Manuals CPUs
- Equipment Manuals Interface Modules
- Equipment Manuals Digital Modules
- Equipment Manuals Analog Modules
- Equipment Manuals Communications Modules
- Equipment Manuals Technology Modules
- Equipment Manuals Power Supply Modules

General information

The function manuals contain detailed descriptions on general topics relating to the SIMATIC S7-1500 and ET 200MPsystems.

Examples:

- Function Manual Diagnostics
- Function Manual Communication
- Function Manual Motion Control
- Function Manual Web Server
- Function Manual Cycle and Response Times
- PROFINET Function Manual
- PROFIBUS Function Manual

Product Information

Changes and supplements to the manuals are documented in a Product Information. The Product Information takes precedence over the device and system manuals.

You can find the latest Product Information on the S7-1500 and ET 200MP systems on the Internet (https://support.industry.siemens.com/cs/de/en/view/68052815).

Manual Collection S7-1500/ET 200MP

The Manual Collection contains the complete documentation on the SIMATIC S7-1500 automation system and the ET 200MP distributed I/O system gathered together in one file.

You can find the Manual Collection on the Internet. (https://support.industry.siemens.com/cs/ww/en/view/86140384)

Manual Collection fail-safe modules

The Manual Collection contains the complete documentation on the fail-safe SIMATIC modules, gathered together in one file.

You can find the Manual Collection on the Internet. (https://support.industry.siemens.com/cs/de/en/view/109806400)

SIMATIC S7-1500 comparison list for programming languages

The comparison list contains an overview of which instructions and functions you can use for which controller families.

You can find the comparison list on the Internet (https://support.industry.siemens.com/cs/ww/en/view/86630375).

1.1.2 SIMATIC Technical Documentation

Additional SIMATIC documents will complete your information. You can find these documents and their use at the following links and QR codes.

The Industry Online Support gives you the option to get information on all topics. Application examples support you in solving your automation tasks.

Overview of the SIMATIC Technical Documentation

Here you will find an overview of the SIMATIC documentation available in Siemens Industry Online Support:

Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/view/109742705)

Watch this short video to find out where you can find the overview directly in Siemens Industry Online Support and how to use Siemens Industry Online Support on your mobile device:

Quick introduction to the technical documentation of automation products per video (https://support.industry.siemens.com/cs/us/en/view/109780491)

YouTube video: Siemens Automation Products - Technical Documentation at a Glance (https://youtu.be/TwLSxxRQQsA)

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:

   – Industry Online Support International: (https://support.industry.siemens.com)

   The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.

   – ID link:

   Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.

2. Retain this version of the documentation.

Updating the documentation

The documentation of the product is updated in digital form. In particular in the case of function extensions, the new performance features are provided in an updated version.

1. Download the current version as described above via the Industry Online Support or the ID link.

2. Also retain this version of the documentation.

mySupport

With "mySupport" you can get the most out of your Industry Online Support.

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAx data	The CAx data area gives you access to the latest product data for your CAx or CAe system. You configure your own download package with a few clicks: • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

You can find "mySupport" on the Internet. (https://support.industry.siemens.com/My/ww/en)

Application examples

The application examples support 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 on individual products.

You can find the application examples on the Internet. (https://support.industry.siemens.com/cs/ww/en/ps/ae)

Safety information

2

2.1 Warnings in this document

You can find explanations of the warnings used in this document in the "Legal information" section.

2.2 Safety-related symbols

2.2.1 Devices without explosion protection

The following table contains an explanation of the symbols located in your SIMATIC device, its packaging or the accompanying documentation.

Symbol	Meaning
⚠	General warning sign **Caution/Notice** You must read the product documentation. The product documentation contains information about the potential risks and enable you to recognize risks and implement countermeasures.
📖	Read the information provided by the product documentation. ISO 7010 M002
⚡	Ensure the device is only installed by electrically skilled person. IEC 60417 No. 6182
CABLE SPEC.	Note that connected mains lines must be designed according to the expected minimum and maximum ambient temperature.
EMC	Note that the device must be constructed and connected in accordance with EMC regulations.
230V MODULES	Note that a 230 V device can be exposed to electrical voltages which can be dangerous. ANSI Z535.2

Symbol	Meaning
24V MODULES	Note that a device of Protection Class III may only be supplied with a protective low voltage according to the standard SELV/PELV. IEC 60417-1-5180 "Class III equipment"
INDOOR USE ONLY INDUSTRIAL USE ONLY	Be aware that the device is only approved for the industrial field and only for indoor use.
	Note that an enclosure is required for installing the device. Enclosures are considered: • Standing control cabinet • Serial control cabinet • Terminal boxes • Wall enclosure

2.2.2 Devices with explosion protection

The following table contains an explanation of the symbols located in your SIMATIC device, its packaging or the accompanying documentation.

Symbol	Meaning
ONLY EX MODULES	The assigned safety symbols apply to devices **with Ex approval**. You must read the product documentation. The product documentation contains information about the potential risks and enable you to recognize risks and implement countermeasures.
	Read the information provided by the product documentation. ISO 7010 M002
	Ensure the device is only installed by electrically skilled person. IEC 60417 No. 6182
F<2N DISPLAY F<4N HOUSING	Observe the mechanical rating of the device.
CABLE SPEC.	Note that connected mains lines must be designed according to the expected minimum and maximum ambient temperature.
EMC	Note that the device must be constructed and connected in accordance with EMC regulations.
U = 0V	When the device is under voltage, note that it may not be installed or removed, or plugged or pulled.

Symbol	Meaning
230V MODULES	Note that a 230 V device can be exposed to electrical voltages which can be dangerous. ANSI Z535.2
III 24V MODULES	Note that a device of Protection Class III may only be supplied with a protective low voltage according to the standard SELV/PELV. IEC 60417-1-5180 "Class III equipment"
INDOOR USE ONLY INDUSTRIAL USE ONLY	Be aware that the device is only approved for the industrial field and only for indoor use.
ZONE 2 INSIDE CABINET IP54	For Zone 2 potentially explosive atmospheres, be aware that the device may only be used when it is installed in an enclosure with a degree of protection ≥ IP54.
ZONE 22 INSIDE CABINET IP6x	For Zone 22 potentially explosive atmospheres, be aware that the device may only be used when it is installed in an enclosure with a degree of protection ≥ IP6x.

2.3 Intended use

The system is used to control machines and plants.

Intended use also includes observance of this documentation, in particular the safety instructions and conditions of use. See Technical specifications (Page 401) section.

2.4 Changes to the device and spare parts

Modifications to the device can impair the safety and function of the device:

* Do not make any changes or modifications to the device.
* Do not remove or paste over safety instructions on the device.
* Do not tape over, cover or install ventilation slots.
* Only use original spare parts and accessories.
* Only use the software provided by Siemens.

2.5 Knowledge and personnel qualification

All persons working with this device require the following knowledge:

- Contents of this document as well as contents of the enclosed documents.
- Handling the device (after instruction)
- Relevant standards and regulations
- Accident prevention regulations

The following activities are reserved for specially qualified personnel:

Working on electrical parts

Work on electrical parts may only be performed by the following persons:

- Qualified electricians
- Persons trained in electrical engineering under the direction and supervision of qualified personnel.

Commissioning and configuration

Commissioning and configuration requires general knowledge in the field of automation technology.

2.6 Personal protective equipment

The personal protective equipment depends on the activity and is determined by the operator.

To avoid material damage during packing, unpacking and installation activities we recommend:

- ESD wrist strap
- ESD shoes

2.7 Open Source Software

This product, solution or service ("Product") contains third-party software components. These are either open source software licensed under a license recognized by the Open Source Initiative (https://opensource.com/) or a license defined by Siemens as comparable ("OSS") and/or commercial software or freeware. With respect to the OSS components, the applicable OSS license conditions prevail over any other terms and conditions covering the Product. The OSS portions of this Product are provided royalty-free and can be used at no charge.

If SIEMENS has combined or linked certain components of the Product with/to OSS components licensed under the GNU LGPL version 2 or later as per the definition of the applicable license, and if use of the corresponding object file is not unrestricted ("LGPL Licensed Module", whereas the LGPL Licensed Module and the components that the LGPL Licensed Module is combined with or linked to is the "Combined Product"), the following additional rights apply, if the relevant LGPL license criteria are met: (i) you are entitled to modify the Combined Product for your own use, including but not limited to the right to modify the Combined Product to relink modified versions of the LGPL Licensed Module, and (ii) you may reverse-engineer the Combined Product, but only to debug your modifications.

The modification right does not include the right to distribute such modifications and you shall maintain in confidence any information resulting from such reverse-engineering of a Combined Product.

Certain OSS licenses require SIEMENS to make source code available, for example, the GNU General Public License, the GNU Lesser General Public License and the Mozilla Public License. If such licenses are applicable and this Product is not shipped with the required source code, a copy of this source code can be obtained by anyone in receipt of this information during the period required by the applicable OSS licenses by contacting the following address:

Siemens Aktiengesellschaft
LC DI FA SL
Werner-von-Siemens Str. 60
91052 Erlangen
Germany

Keyword: Open Source Request (please specify Product name and version, if applicable)

SIEMENS may charge a handling fee of up to 5 EUR to fulfil the request.

Warranty regarding further use of the Open Source Software

SIEMENS' warranty obligations are set forth in your agreement with SIEMENS. If you modify the product or the OSS components or use them in a way other than that specified by SIEMENS, the warranty will be voided and no technical support will be provided. The following license terms may contain limitations of liability that apply between you and the respective licensor. For the avoidance of doubt, SIEMENS does not make any warranty commitment on behalf of or binding upon any third-party licensor. The Open Source Software used in the product and the license agreements concerning this software can be found in the Readme_OSS.

2.8 Safe working

2.8.1 Working on electrical parts

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualification).
- Always observe the country-specific safety rules.
- Notify all those who will be affected by the procedure.
- Follow the 5 safety rules according to DIN EN 50110-1 (VDE 0105-1):

1. Disconnect
2. Secure to prevent reconnection
3. Verify safe isolation from the supply (all poles)
4. Ground and short-circuit
5. Erect barriers around or cover adjacent live parts

The 5 safety rules must be applied in the above order prior to starting work on an electrical system. After completing the work, proceed in the reverse order.

It is assumed that every electrician is familiar with the 5 rules.

2.9 Residual risks

Despite all the technical and procedural risk reductions that have been carried out, not all dangers can be avoided.

The following sections describe these residual risks and measures to avoid them.

2.9.1 Live parts

Electrocution on contact with live parts leads to life-threatening injuries (death).

Operation

- Do not open the device.
- Never use damaged devices.
- Pull the plug and not the cable.

Installation and connection

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualification (Page 22)).
- Adhere to the protective measures for safe working on electrical parts (see section Working on electrical parts (Page 23))
- Fuse the connection cables according to the current-carrying capacity of the cable used, taking into account the applicable standards.
- Install the device in a control cabinet. The enclosures, cabinets or electrical equipment rooms must guarantee protection against electric shock and spread of fire.
- Ground the device in compliance with the applicable regulations.
- For the 24 V DC supply (SELV/PELV), only use power supply units that provide safe electrical extra-low voltage in accordance with IEC 61131-2 or IEC 61010-2-201.

Maintenance

- Only work on electrical parts if you are a qualified specialist (see section Target group and personnel qualification (Page 22)).
- Adhere to the protective measures for safe working on electrical parts (see section Working on electrical parts (Page 23))

2.9.2 External power supply to modules

Even if the main supply to the plant is disconnected, externally supplied modules can continue to carry voltage. An electric shock on contact with live parts can lead to death or serious injury.

For special SIMATICmodules, e.g. relay modules, you can connect or switch voltages larger than 24 V DC, e.g. 230 V AC. In some applications, these modules are supplied with voltages from outside the system (external power supply). In the event of an external power supply, a dangerous voltage may still be present on these modules even if the system is disconnected.

Maintenance

Ensure the following points before starting work:

- The plant is completely disconnected from the power supply.
- All externally supplied plant units are disconnected from the power supply

2.9.3 Voltage dangerous to touch due to permissible electric potential difference

Due to the permissible electric potential difference, a dangerous voltage may be present at the inputs of modules. An electric shock on contact with live parts can lead to death or serious injury.

Special SIMATIC modules, such as analog input modules, have isolated channels. In this case, there is no connection between the potential of the sensor and the potential of the module. If a dangerous voltage within the permissible electric potential difference occurs at the sensor, this voltage may also be present at the measurement channel of the module.

You can find the permissible electric potential differences in the technical specifications section of the modules' Equipment Manuals.

Maintenance

Ensure the following points before starting work:

- The plant is completely disconnected from the power supply.
- All externally supplied plant units are disconnected from the power supply

2.9.4 Conductive pollution

Electrocution during transmission of electrical energy via conductive contamination to the body leads to life-threatening injuries (death).

- Install the device in a control cabinet.
- Keep the control cabinet free of conductive contamination.

2.9.5 Overheating

Smoke development and fire due to overheating of the device and lines lead to burns and life-threatening injuries (death).

To avoid overheating:

• Ensure the correct installation position.

• Ensure sufficient air supply (for example, do not mask or cover ventilation slots, maintain mounting clearances).

• Only use undamaged cables.

Installation and connection

• Follow the instructions for the mounting position.

• Adhere to the specified ventilation clearances.

• Fuse the connecting cables according to the cable cross-section.

Maintenance

• Check plug-in connections and cables regularly for damage.

2.9.6 Uncontrolled movements

Uncontrolled movements of driven machine or system parts during commissioning, operation, maintenance and repair.

• Follow the safety instructions described in the function manuals.

2.9.7 Unsafe operating states

Unsafe operating states may result in personal injury of unknown extent.
The following factors can be triggers:

• Manipulation of the software, e.g. viruses, trojans or worms.

Manipulation of the software, e.g. viruses, trojans or worms.

• Adhere to the protective measures against tampering with the software (see section Industrial cybersecurity).

• Perform available updates in a timely manner.

• Protect files stored on removable media from malware with appropriate protective measures, e.g. virus scanner.

• Set up access protection for the CPU.

2.10   Behavior in case of emergency

- Force EMERGENCY OFF.

When the safe operating state has been restored:

- Unlock the EMERGENCY OFF mechanism.
- The person responsible for the system ensures that the system starts up in a controlled and defined manner.

2.11   Material damage

2.11.1   Transport and storage

- Only pack, store, transport and ship electronic components, modules or devices in the original product packaging or in other suitable materials, e.g. conductive foam rubber or aluminum foil.
- Observe the limits during transport and storage. See Technical specifications (Page 401) section.

2.11.2   Installation and connection

- We recommend touching components, modules and devices only if they are grounded by one of the following measures:
  - With an ESD wrist strap.
  - With ESD shoes or ESD grounding strips in ESD areas with conductive flooring.
- Place electronic components, modules and devices only on conductive surfaces (e.g. tables with ESD coating, conducting ESD plastic foam, ESD packing bags, ESD transport containers).
- Ensure that there is sufficient overvoltage protection.
- Do not install/remove the following elements when the power is on:
  - Front connectors
  - I/O modules
  - CPU

New properties/functions 3

What's new in the S7-1500, ET 200MP System Manual, Edition 11/2024 since the previous version 11/2023?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Extension of the CPU portfolio	The following CPUs have been added to the CPU portfolio: • 1517(F)-3 PN • 1518(F)-3 PN • 1516T(F)-3 PN • 1517T(F)-3 PN • 1518T(F)-3 PN The CPUs mentioned above have 2 ports at the PROFINET interface X2 and the same PROFINET functionalities as at the PROFINET interface X1. In addition these CPUs provide higher performance and make more data work memory available.	As of section System overview (Page 77)
	Configurable ambient conditions	In the case of the following CPUs, you can specify the ambient conditions at the operating location in the hardware configuration and thus optimize the program processing of the CPU: • 1518(F)-3 PN • 1518T(F)-3 PN	Cycle and response times (https://support.industry.siemens.com/cs/us/en/view/59193558) Function Manual
	Integrated safety		
	Central user management	System-wide, central management of users and user groups outside TIA Portal via UMC server. User management for comprehensive automation solutions with multiple projects, users, and user groups can work in all projects in which they are activated and the appropriate rights have been assigned to them. During operation, users can be added to or removed from a group or their passwords can be changed – All without the CPU configuration having to be changed or loaded.	Section Central user management (Page 282)
	Retentive memory area for Syslog messages	S7-1500 CPUs store Syslog messages retentively as of FW Version V4.0. This means that events that require a restart of the CPU also remain in the Syslog storage.	Section Industrial cybersecurity (Page 40)
	Programming the CPU		

What's new?		What are the customer benefits?	Where can I find the information?
New contents	SIMATIC Controller Profiling	You start or stop the profiling of an S7-1500 CPU as of firmware version V4.0 using the new "Profiling" instruction. When starting the profiling, specify the configuration with which the profiling data is to be recorded.	STEP 7 online help
	Programming the CPU	For S7-1500 CPUs as of firmware version V4.0, the nesting depth has been extended for the following elements: • PLC data types • Tags of the STRUCT data type • Tags of the ARRAY of STRUCT / ARRAY of UDT data type Previously, the maximum nesting depth was 8 elements. You can now nest up to 26 elements inside each other. An ARRAY of STRUCT/UDT requires three hierarchy levels in each case. If you use these data types, the maximum nesting depth is reduced accordingly.	
	Communication of the CPU		
	New function for OPC UA	Enables cross-vendor communication.	Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) Function Manual
	Configuring SNMP and DCP	As of STEP 7 V20, you can centrally configure the SNMP settings for an entire PROFINET IO system.IO-devices that support the SNMP automatically synchronize the SNMP settings of the PROFINET interface of your higher-lever IO-controller.If IO-controllers and IO-devices support the DCP protocol, the write-protected mode is activated by default for DCP. Easier configuration of the SNMP settings through central specification at the CPU for the connected PROFINET IO system.	PROFINET (https://support.industry.siemens.com/cs/ww/en/view/49948856) Function Manual
	Web server of the CPU		
	System web pages	Introduction of the system web pages with new design and functionality for: • Overview • Diagnostics • User program • Messages and DataLogs • Maintenance	Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) Function Manual
	New Web API methods	The Web API has been expanded to include the following functions: • Reading out basic information of the CPU • Reading out API session information • Reading out technology objects and their values • Configuring the HTTP response header • Further options for configuring web applications	

What's new?		What are the customer benefits?	Where can I find the information?
New contents		The extended scope of functions of the Web API offers additional access options. The configuration of the HTTP header also extends access to the web server via HMI Unified Panels.	
	Technology functions of the CPU		
	Axis functions	Defining the motion transition Extended scope of functions	Axis functions (https://support.industry. siemens. com/cs/us/en/view/109817884) Function Manual
		Stopping the basic motion Extended scope of functions	
	Synchronous operation functions (T-CPU only)	New cyclic cam types with larger definition ranges Extended scope of functions	Synchronous operation functions (https://support.industry. siemens. com/cs/us/en/view/109817888) Function Manual
		Directly set a following axis synchronously at a specified leading value position in camming. New synchronization mode of the following axis in camming: • Direct synchronous setting at the specified leading value position Extended scope of functions	
		New synchronization modes of the following axis in gearing: • Subsequent synchronization using leading value distance starting from current leading value position with calculated synchronous position • Subsequent synchronization using leading value distance with calculated synchronous position Extended scope of functions	
		Reversal tolerance of the leading value adjustable in gearing and camming. Synchronization and desynchronization are not aborted with a fluctuating leading value.	
		Cross-PLC synchronous operation with communication via PN/PN coupler Extended scope of functions	
		Cross-PLC synchronous operation across multiple projects Use of externally supplied projects possible.	
	Kinematics functions (T-CPU only)	Extension of the kinematics control panel Improved commissioning	Kinematics functions (https://support.industry.

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Kinematics functions (T-CPU only)	Display of effective dynamic limits Extension of the kinematics control panel	siemens.com/cs/us/en/view/109817886) Function Manual
	Interpreter functions (T-CPU only)	"Debug" program mode The execution of the Interpreter program can be tested.	Interpreter functions (https://support.industry.siemens.com/cs/us/en/view/109817891) Function Manual
	Trace functionality of the CPU		
	Named value data types in Traces	"Named values" are values that are assigned a unique name. In TIA Portal, you declare named values within "named value data types". They contain a set of values to which a unique set of names is assigned. Named values are easily referenced throughout the program and increase the readability and maintainability of the program. Among other things, this makes it easy to monitor/analyze the named value data types in the trace.	Using the trace and logic analyzer function (https://support.industry.siemens.com/cs/us/en/view/64897128) Function Manual
	Recording as binary file for long-term trace and long-term project trace	Recording as binary file instead of a CSV file and saving in a DAT file. This makes it possible to monitor/analyze long-term traces and long-term project traces directly in TIA Portal.	
	Acquiring events from technology objects in the Trace recording	Detecting events in the Trace recording, which occur at a Motion Control technology object as of V9.0 during recording. Monitoring/analyzing of the correct sequence and parameterization of Motion Control jobs in complex applications.	
	Cross-project Trace	Recording of values from multiple projects with a PN/PN coupler. Monitoring/analyzing of signals and events from multiple projects.	

What's new in the S7-1500, ET 200MP System Manual, Edition 11/2023 since the previous version 01/2023?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	"Industrial Cybersecurity" section	Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.	Section Industrial cybersecurity (Page 40)

What's new?		What are the customer benefits?	Where can I find the information?
New contents		The section contains the following information: • Basic information on the subject of industrial cybersecurity • Measures to protect individual components and the entire system against manipulation and unwanted access.	Section Industrial cybersecurity (Page 40)
	Syslog messages	As of TIA Portal version V19 and FW version V3.1, you can forward the syslog messages of an S7-1500 CPU to a syslog server.	
	CPU 1511(F)-1 PN	Expansion of the code work memory: 300 KB (standard CPU), 450 KB (F-CPU).	Section System overview (Page 77)
	Compact CPUs	Expansion of the work memory: • Code work memory: 300 KB (CPU 1511C-1 PN), 400 KB (CPU 1512C-1 PN) • Data work memory: 1.5 MB (CPU 1511C-1 PN), 2 MB (CPU 1512C-1 PN)	
	Local user management	As of TIA Portal version V19 and FW version V3.1, S7-1500 CPUs have improved management of users, roles, and CPU function rights (User Management & Access Control, UMAC). As of the above-mentioned version, you manage all project users with their rights (e.g. access rights) for all CPUs in the project. Management is performed in the editor for users and roles in the TIA Portal.	Section Local user management (Page 272)
	"Random" instruction	The "Random" instruction is supported as of FW version V3.1: You can use this instruction to generate a 32-bit random number.	STEP 7 online help
	SIMATIC Controller Profiling	With SIMATIC Controller Profiling you can analyze and evaluate the runtime behavior of your user program on an S7-1500 CPU as of FW Version V3.1. All the relevant information can be displayed graphically and evaluated in a web browser.	Application example SIMATIC Controller Profiling (https://support.industry.siemens.com/cs/us/en/view/109750245)
	Appendix "Use over 2,000 m above sea level and extended temperature range"	The previously permissible ambient temperature range has been extended for many modules. The permissible installation heights have been extended to installation heights of up to 5000 m, depending on the module.	Appendix Use over 2 000 m above sea level and extended temperature range (Page 429)

What's new in the S7-1500, ET 200MP System Manual, Edition 01/2023 since the previous version 11/2022?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	General safety instructions	This section contains a compilation of general safety instructions for the SIMATIC S7-1500/ET 200MP automation system.	Section General safety instructions

What's new in the S7-1500, ET 200MP System Manual, Edition 11/2022 since the previous version 05/2021?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	S7-1500 Motion Control KinPlus	The "S7-1500T Motion Control KinPlus" software enables control of kinematics with 5 or 6 interpolating axes.	S7-1500T Motion Control (https://support.industry.siemens.com/cs/ww/en/view/109751049) Function Manuals
	Technology and standard CPUs	Expansion of the work memory	Section Technical specifications of CPUs (Page 103)
	Increase in the number of simultaneously active jobs for asynchronous instructions (OUC and S7 communication)	The CPU can process a larger number of asynchronous instructions in parallel with the cyclic user program.	Section Asynchronous instructions (Page 258)
	Management of web server certificates during CPU runtime	You can load or update web server certificates not only in STOP mode but also in RUN mode.	Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) Function Manual
	New Web API methods	Many new API methods extend your access options to the CPU via the Web API.	

What's new in the S7-1500, ET 200MP System Manual, Edition 05/2021 since the previous version 11/2019?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Active backplane bus	The active backplane bus is used in applications with high availability requirements. Applications in which even short plant downtimes would result in significant economic damage. The active backplane bus provides you with the following advantages: • Reaction-free pulling and plugging of I/O modules during operation • Reserve capacity (= gaps in system configuration) for later use	Section Components (Page 94) Active backplane bus (https://support.industry.siemens.com/cs/de/de/view/109778694/-en) manual

What's new?		What are the customer benefits?	Where can I find the information?
New contents	CPU 1518(F)-4 PN/DP MFP	A Linux-based operating system (SIMATIC Industrial OS) is pre-installed on the CPUs 1518(F)-4 PN/DP MFP (multifunctional platform) to allow you to use Linux-based apps and software, for example.	Starting from section System overview (Page 77)
	CPU 1518(F)-4 PN/DP	Expansion of work memory and motion control resources: • Code work memory: 6 MB (standard CPU), 9 MB (F-CPU) • Data work memory: 60 MB • Motion control resources: 15360 This expansion allows you to implement larger and more extensive applications with the CPUs.	Starting from section System overview (Page 77)
	CPU 1518T-4 PN/DP	Extension of the CPU portfolio with the CPU 1518T-4 PN/DP: CPU 1518T-4 PN/DP offers a very large program and data memory for demanding usage in applications that contain central I/O in addition to distributed automation structures. CPU 1518T-4 PN/DP features high-performance, extended motion control functions, for example: • Synchronous operation functions • Kinematics functions Important technical specifications: • Code work memory: 9 MB • Data work memory: 60 MB • Motion control resources: 15360 • Extended motion control resources: 512	Starting from section System overview (Page 77)
	CPU 1518TF-4 PN/DP	Extension of the CPU portfolio with the CPU 1518TF-4 PN/DP: CPU 1518TF-4 PN/DP offers a very large program and data memory for demanding usage in applications that contain central I/O in addition to distributed automation structures. The CPU can also be used for safety functions according to IEC 61508 up to SIL-3 and ISO 13849 up to PLe for safety applications. CPU 1518TF-4 PN/DP features high-performance, extended motion control functions, for example: • Synchronous operation functions • Kinematics functions Important technical specifications: • Code work memory: 9 MB • Data work memory: 60 MB • Motion control resources: 15360 • Extended motion control resources: 512	Starting from section System overview (Page 77)

What's new?		What are the customer benefits?	Where can I find the information?
New contents	New motion control technology functions for the following tasks: • Desynchronization of gearing or camming • Following value shift in gearing or camming • Simulation of the kinematic motions • Copying the calculated cam elements	Extended areas of application	Motion Control (Page 138) section
Changed contents	With the introduction of DHCP (Dynamic Host Configuration Protocol), NTP servers can also be obtained via DHCP. This changes the configuration, in order to define where the NTP server obtains its configuration from: • via the hardware configuration of the CPU • via DHCP • via the block T_CONFIG	More assignment options from NTP servers to the CPU.	Section Time synchronization (Page 345)

What's new in the S7-1500, ET 200MP System Manual, Edition 11/2019 since the previous version 12/2017?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	DIN-rail adapter	You can install the SIMATIC S7-1500/ET 200MP automation system on a standard 35 mm DIN rail using the DIN rail adapter.	Sec. Installing the DIN-rail adapter (Page 183)
	Communication module IO-Link Master	With the IO-Link master, you can do the following during operation: • Changing parameters for the production and processing of product variants and batches down to sensor/actuator level • Specify remote diagnostics or detailed diagnostics up to the sensor/actuator	Section Communication module IO-Link Master (Page 135)
	Communications processor CP 1545-1	Communication processors connect the SIMATIC S7-1500 automation system securely with networks. With the integrated security functions, communication processors protect the S7-1500 automation system and lower-level networks from unauthorized access. Communication processors use encryption to protect data transfer against manipulation and espionage.	Section CM communication modules / CP communications processors (Page 133)

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Technology module TM NPU	With the TM NPU technology module, you can: • Process large amounts of data via neural networks • Perform visual quality check • Control robot systems via screen • Using pick-and-place applications	Section Technology Module TM NPU (Page 148)
	Basic analog input module	The new, simple and inexpensive analog input module provides data for temperature measurement with RTD via 8 channels.	Section Analog input modules (Page 125)

What's new in the S7-1500, ET 200MP System Manual, Edition 12/2017 since the previous version 09/2016?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Technology CPUs	• Extension of the technology CPU portfolio by the CPUs 1516T(F)-3 PN/DP • All technology CPUs feature the new technology object TO_Kinematics. With the TO_Kinematics, you can implement complex motion control applications for controlling 2D, 3D and 4D kinematics.	Starting from section System overview (Page 77)
	CPU1518(F)-4 PN/DP MFP	• Extension of the CPU portfolio by the CPUs 1518(F)-4 PN/DP MFP (multifunctional platform) • The CPU can execute STEP 7 blocks of the "usual" user program as well as blocks and applications programmed with C/C++. • The multifunctional platform offers you the option of running C/C++ code synchronously in the CPU cycle (via the CPU function library). In addition, the multifunctional platform can run C/C++ applications as separate applications in parallel to CPU runtime. • With C/C++ applications you can implement parallel processes for the STEP 7 user program, e.g. for pre-processing or sending data via Industrial Ethernet. A CPU can perform several tasks at the same time, the complexity of functions is reduced and the time required for implementation is reduced. • You can re-use existing technological know-how in C/C++ code synchronously and asynchronously to the STEP 7 user program.	Starting from section System overview (Page 77)

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Password provider	As an alternative to manual password entry, you can link a password provider to STEP 7. A password provider offers you the following advantages: • More convenient handling of passwords. STEP 7 automatically imports the password for the blocks. This saves you time • Optimum block protection as the users do not know the password themselves	Section Know-how protection (Page 296)
	GetSMCinfo instruction	With the help of the GetSMCinfo instruction you can respond to information provided by the memory card in the user program and if required, replace the memory card as a precautionary measure. This process makes sense if you write to the card often in your application, for example if you use data logs.	Section Overview of SIMATIC Memory Card
	Testing with breakpoints	When testing with breakpoints, you execute a program from one breakpoint to another. Testing with breakpoints provides you with the following advantages: • Testing SCL and STL program code with the help of breakpoints • Localization of logic errors step by step • Simple and quick analysis of complex programs prior to actual commissioning • Recording of current values within individual executed loops • Use of breakpoints for program validation also possible in SCL/STL networks within LAD/FBD blocks	Section Test functions (Page 393)
Changed contents	PS 60W 24/48/60VDC HF system power supply	The PS 60W 24/48/60VDC HF enables extended retentivity of the CPU's data work memory. In the event of failure of the supply voltage, the PS 60W 24/48/60VDC HF supplies sufficient power for the CPU to back up the entire data work memory (without retentive data) to the SIMATIC Memory Card.	Section Use of system power supplies (Page 165)
	Time synchronization	For all applications that require the exact time, you update the CPU time using the NTP method. This also automatically sets the CPU time beyond subnet limits.	Section Time synchronization (Page 345)
	Reading out the identification and maintenance data using the Get_IM_Data instruction	With the Get_IM_Data instruction you can read out the identification and maintenance data of the modules without much programming work.	Section Reading out and entering I&M data (Page 349)

What's new?		What are the customer benefits?	Where can I find the information?
		With the Get_IM_Data instruction you can access identification and maintenance data (I&M) of a module in the user program. I&M data is information saved in a module. This allows you to • Check the system configurations • React to hardware changes • React to hardware faults in the user program. Finding and elimination of hardware errors is easier.	

What's new in the S7-1500, ET 200MP System Manual, Edition 09/2016 since the previous version 12/2014?

What's new?		What are the customer benefits?	Where can I find the information?
New contents	Compact CPUs	You can use compact CPUs for smaller to medium-sized applications. The compact CPUs have integrated analog and digital on-board I/O as well as integrated technology functions.	Starting from section System overview (Page 77)
	Technology CPUs	You can use technology CPUs for demanding applications. Technology CPUs are equipped with expanded motion control functions.	Starting from section System overview (Page 77)
	Fail-safe modules	With fail-safe modules, you replace the conventional safety engineering technical setup. For example, this involves replacement of switching devices for EMERGENCY OFF, protective door monitoring and two-hand operation.	Starting from section System overview (Page 77)
	Formatting, erasing or converting a SIMATIC Memory Card via the display	Your SIMATIC Memory Card is formatted, erased or converted to a program card directly via the display without having to use STEP 7. You save time.	Section SIMATIC Memory Card
Changed contents	Asynchronous instructions	You are given an overview of the resource consumption of asynchronous instructions. This ensures adequate resources in the CPU.	Section Asynchronous instructions (Page 258)
	Configuration control	Configuration control provides you with the following advantages: • Different configuration levels of a standard machine can be handled in a single project. • No changes to the hardware configuration or user program are needed. • Centralized/distributed configuration of a system is flexibly variable • Easy handling during maintenance, versioning and upgrades. • Hardware savings: You only use the I/O modules that you currently need. • Potential savings when building, commissioning and creating documentation for standard machines.	Section Configuration control (Page 303)

What's new?		What are the customer benefits?	Where can I find the information?
Changed contents	Wiring rules for the power supply elements	You are given information on proper connection of the power supply elements.	Section Wiring rules (Page 211)
	Connecting the CPU/interface module to the load current supply	You are given information on proper connection of the CPU/interface module to the load current supply.	Section. Connecting the CPU/interface module to the load current supply (Page 219)
	Firmware update via accessible devices	You are given information on fast firmware updates via accessible devices in the network.	Section Firmware update (Page 377)

Industrial cybersecurity

4

Due to the digitalization and increasing networking of machines and industrial plants, the risk of cyber attacks is also growing. Appropriate protective measures are therefore mandatory, particularly in the case of critical infrastructure facilities.

In the first part of this section you will find basic information on the subject of industrial cybersecurity. Subsequent sections describe recommended measures for protecting the entire system and the individual components from manipulation and unwanted access.

NOTE

Security-relevant changes to software or devices are documented in the section New properties/functions (Page 28).

4.1 Cybersecurity information

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

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

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

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

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under
https://new.siemens.com/cert.

4.2 Security update notification

Read the special information on maintaining the operational safety of your plant in the Introduction (Page 12) section.

Set up notification of security updates

To receive notifications about security updates, proceed as follows:

1. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home).

2. Enter the keyword "Security" in the search engine.

3. Choose the "Search in Knowledge base" option.

4. Select your product or product group in the "Master tree" filter menu, e.g. "S7-1500" > "Central modules".

5. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".

6. Select the document with which you want to create notifications.

   For example, if you would like to be informed about all firmware versions of the S7-1500 CPUs, select the entry "Firmware update S7-1500 CPUs incl. Displays and ET 200 CPUs (ET 200SP, ET 200pro)".

7. Select "Add to my favorites" using the 3 dots on the right.

8. In the following dialog, select the name, the storage location and the "Notify me" option for the favorite. Then click on the "+ Add to my favorites" button.

Result: You will be notified by email each time the document is changed.

Under "mySiePortal" > "Lists & notifications" > "My notifications", you can display your notifications and delete them if necessary.

4.3 Basic information on industrial cybersecurity

4.3.1 Definition of industrial cybersecurity

Industrial cybersecurity is generally understood to mean all measures to protect against the following threats:

- Loss of confidentiality due to unauthorized access to data
- Loss of integrity due to manipulation of data
- Loss of availability (e.g. due to the destruction of data or denial of service (DoS))

4.3.2 Objectives of industrial cybersecurity

The objectives of industrial cybersecurity are:

- Ensuring trouble-free operation of industrial plants and production processes
- Preventing threats to people and production from cybersecurity attacks
- Protection of industrial plants against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Provision of a practical and cost-effective concept for securing existing plants and devices that do not have their own security functions
- Use of existing, open, and proven industrial cybersecurity standards
- Compliance with legal requirements

An optimized and adapted security concept applies to automation and drive technology. The security measures must not impede or endanger production.

4.4 Integrated security concept and security strategies

4.4.1 Comprehensive security concept "Defense in Depth"

With Defense in Depth, Siemens provides a multi-layer security concept that offers industrial plants comprehensive and far-reaching protection in accordance with the recommendations of the IEC 62443 international standard.

Productivity and know-how are protected on 3 levels:

Plant security

Plant security uses various methods to safeguard critical components from physical access by people. This starts with classic building access and extends to securing sensitive areas using access control (for example, code card, iris scan, fingerprint or access code).

Network security

Automation networks must be protected against unauthorized access. This is achieved through security measures on the product, but also those in the product-related environment.

System integrity

Targeted measures must be taken to protect existing know-how or to prevent unauthorized access to automation processes. The measures protect against unauthorized configuration changes, and highlight attempts at manipulation.

You can find more information on the topics of Defense in Depth, plant security, network security, and system integrity on the SIEMENS Industrial cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) Web page.

You can also visit the download center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) to obtain more information on the topic of industrial cybersecurity. The "Operational Guidelines", for example, provide recommendations on basic security measures for secure machine and plant operation in an industrial environment.

4.4.2   Security management

The ISO 27001 and IEC 62443 standards call for a comprehensive approach in information technology (IT) and operational technology (OT) to protect against cyber attacks.

Responsibility for cybersecurity and IT security

Every operator of machinery and equipment is responsible for:

- Defining cybersecurity and IT security as an important criterion in the procurement and selection of machines and software applications
- Use of suitable measures to protect production resources, data, and communication from manipulation and theft
- Providing all necessary resources and training to employees to fully support these goals

For this purpose, suitable measures must be selected after a risk assessment and a cost-benefit analysis in order to protect material and intellectual property and prevent damage from occurring. These measures should be integrated into corporate processes and procedures, evaluated regularly, and firmly anchored in the corporate culture. In addition to protecting intellectual property, the protection of personal data must be ensured at all organizational units and levels.

Siemens will provide you with information and support. Subscribe to the Security feeds (https://www.siemens.com/cert) for information on vulnerabilities. Register with mySiePortal (https://sieportal.siemens.com/en-ww/home) and create filters to be notified when important information is published. The procedure is described in the section Notification of security updates (Page 41). Consider using Siemens Cybersecurity Services.

Responsibility in the digital supply chain

Cybersecurity should play a critical role in the evaluation and procurement process. The entire life cycle of a product should be considered to ensure protection against current and future risks. These include, for example, security updates throughout the product life cycle, including guidelines for secure disposal of the product.

Siemens plans and announces the provision of security updates, as well as total discontinuation of products, as part of product support.

Employee awareness

Regular training in cybersecurity and continuous testing of training success are essential so that cybersecurity measures are internalized in processes and work instructions. This involves general training in the use of software and IT hardware for company communication and as work equipment, e.g.:

- secure handling of USB devices
- encrypted communication
- use of VPN
- rules for passwords and use of access
- setting up two-factor authentication
- Educating employees about the dangers posed by malware, phishing, social engineering and other factors

Furthermore, if applicable, production equipment and software training should always include the topic of cybersecurity.

Maintaining the security concept through updates

Keeping software up-to-date is essential, for example, to benefit from the following measures:

- Implementation of new security strategies, protocols and techniques
- Closing of security vulnerabilities
- Elimination of security vulnerabilities

To this end, it is necessary to keep a constant eye on the further development of protective measures and, if necessary, the expansion of requirements.

Recommendations:

- Set up notifications for (security) updates
- Subscribe to information on vulnerabilities
- Monitor and implement the further development of the technology, especially in the area of cybersecurity

Always keep technology and knowledge up to date.

Consideration of the risks posed by cyber attacks in the Threat and Risk Assessment (TRA)

Make an inventory of all software, hardware, and infrastructure devices, in order to identify risks to the location or organization. Incident response procedures must be incorporated into all IT and manufacturing processes. The choice of risk mitigation measures should be based on a cost-benefit analysis and classification of risks. This is followed by the introduction of cybersecurity rules and procedures and the training of personnel.

Living the concept

> Technical solutions alone are not sufficient to effectively counter threats.
>
> Cybersecurity must be part of the corporate culture and process landscape and must be internalized and lived by all employees.

Continuously monitoring the security situation

> You have the following options to monitor the cybersecurity situation continuously:
>
> - Setting anomaly references and creating allow and deny lists based on normal network communication and production machine behavior. The SINEC software family offers you reliable security tools (https://www.siemens.com/global/en/products/automation/industrial-communication/sinec-network-software/cybersecurity.html) to detect potential vulnerabilities in OT networks, quickly initiate suitable measures and resolve security vulnerabilities in a targeted manner.
>
> - Establishment of an intrusion detection system (IDS) that generates alarms when unusual behavior occurs in the network
>
> - Introduction of a Security Information and Event Management (SIEM) system to collect, analyze, and evaluate events in real time to enable early countermeasures
>
> - Measures regarding network security: e.g. network segmentation, firewalls, VPN, DMZ (demilitarized zones)

4.5 Operational application environment and security assumptions

4.5.1 Intended use

> SIMATIC products are intended for use in industry. If you plan to use the product in a different environment, check the conditions required for such use.
>
> The product may be operated only by personnel qualified for the specific task in accordance with the relevant documentation, in particular its warning notices and safety information. 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.

Operational reliability and intended use

> Read the "Special information" in the Introduction (Page 12) section.

Area of application

> Observe the section Areas of application SIMATIC S7-1500 and ET 200MP (Page 81).

4.5.2 Requirements for the operational application environment and security assumptions

Siemens recommends the following security measures:

- Threat and Risk Assessments (as part of security management)
- Network security concepts
  - Network segmentation
  - Asset and network management
  - Network protection
  - Remote access
- Access control concepts (utilizing access control systems)
  - Physical protection
  - Physical corporate security
  - Physical product security

Threat and Risk Assessment

Vulnerabilities and risks are identified, and countermeasures are proposed to ensure the security of the system, networks, and data.

Network security concepts

You can find information on network security in the whitepaper "Industrial Network Security Architecture", available at the Download Center (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html) on the Industrial Cybersecurity (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html) website.

Access control concepts

Physical protection
In addition to closing off and/or monitoring entire production facilities, it may be necessary to physically secure cabinets or even individual components such as circuit breakers.

Physical corporate security
You can ensure physical corporate security by the following measures, among others:

- Closed off and monitored company premises
- Access control, locks/card readers, and/or security personnel
- Accompaniment of non-employees by company personnel
- Employees are trained on and embrace security processes within the company

Physical production security

You can ensure the physical production security by, among others, the following measures:

- Separate access control for critical areas, such as production zones.

- Installation of critical components in lockable cabinets/control rooms with monitoring and alarm capabilities. The cabinets/control rooms must be secured with a cylinder lock. Do not use simple locks, such as universal, triangular/square, or double-bit locks.

- Radio field planning to limit WLAN coverage areas, preventing them from extending beyond defined zones (e.g. factory floor).

- Guidelines that prohibit the use of external data storage media (such as USB flash drives) and IT devices (such as laptops) classified as unsafe on systems.

4.6 Security properties of the devices

The security properties of the individual devices are listed in the Equipment Manuals.

4.7 Secure operation of the system

This section describes measures recommended by Siemens to protect your system from manipulation and unauthorized access.

4.7.1 Hardening measures

System hardening, also simply referred to as hardening, is the secure configuration of products or systems. The aim is to close security gaps and take various measures to reduce the attack surfaces for cyberattacks.

Measures for system hardening include, for example:

- Secure configuration in which only necessary software components and services are installed or activated for proper operation.

- Access control, by which a restrictive user and rights management system is implemented.

4.7.2 Secure configuration

Secure configuration involves control over all software components, along with their interfaces, ports, and services.

Activated services and ports pose a risk, for example of unauthorized access to the network and to programs.

To minimize the risk, activate solely the required services at all the automation components. Take all activated services (especially Web servers, FTP, remote maintenance etc.) into account in the security concept. Consider the default states of ports and services in your security concept.

You can find an overview of all ports and services used in the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

4.7.3   Access control

In addition to physical protection, also establish logical safeguards to control access to your system:

- Use a restrictive user and rights management system, e.g. for accessing the CPUs and TIA Portal.
- Refer to the information about password management in the section Protection (Page 269) and in the STEP 7 online help (TIA Portal).

4.7.4   Handling of sensitive data

Data protection information

Siemens Aktiengesellschaft observes the applicable data protection laws, including the General Data Protection Regulation (GDPR), in particular the rules of data minimization and data-protection-friendly default settings (privacy by design, privacy by default).

This means for the products in this system:

Products with user management save user names and passwords to manage access rights. User names are also saved in logging alarms. These logging alarms are provided with a time stamp and stored in the internal cache of the CPU. They can be forwarded to a central syslog server. You can find more information in the section Syslog messages (Page 62).

In addition, the products do not store any personal data.

If you establish a reference to an identifiable person by linking these data with other data (such as shift schedules), or if you store personal data on the same medium (such as a hard disk), you must yourself ensure that the data protection regulations are observed.

Information on the secure removal of data from the CPU, interface module and SIMATIC Memory Card is provided in the section Secure decommissioning (Page 50).

Storage of security-relevant data

When storing your security-relevant data on your PC, independently ensure secure data storage.

Also observe the section Sensitive data (Page 60).

4.7.5 Regular firmware updates

NOTE

Outdated firmware versions might not be monitored for security vulnerabilities.

- Always keep your plant/products up to date to benefit from troubleshooting and to minimize potential risks.

- Use email notifications to be automatically informed about firmware updates.

You can find more information in the following:

- The section Firmware update

- The section Notification of security updates

4.7.6 Notifications about security vulnerabilities (Siemens Security Advisories)

A vulnerability is a security vulnerability in information security. It can pose a threat as it provides intruders with the opportunity to access system resources and manipulate or steal data. Many vulnerabilities allow availability to be impaired.

Siemens ProductCERT

If Siemens identifies or fixes security gaps (Vulnerabilities) in the products, this will be published in the Security Advisories.

You can find the documents for SIMATIC on the following Siemens AG web page: Siemens ProductCERT and Siemens CERT (https://new.siemens.com/global/en/products/services/cert. html?s=SIMATIC#SecurityPublications)

"Search Security Advisories" is the default entry in the "SIMATIC" search field. You can also enter other product names or other terms in the search field and search for them.

On this page, you will also find all the required information on how to deal with vulnerabilities:

- Contact persons for matters related to vulnerabilities

- Options for automated notifications regarding vulnerabilities

- Notifications are also possible in CSAF format

- Option to subscribe to RSS feeds and newsletters

- List of all current vulnerabilities and detailed information such as:

  - Description

  - Classification according to Common Vulnerability Scoring System (CVSS)

  - Measures

  - Availability

  - Etc.

Set up Security feeds (https://www.siemens.com/cert) to receive notifications about security-related topics.

If you suspect or have discovered a vulnerability in a Siemens product, please let us know immediately. To do this, press the "Contact" button on the CERT Services page (https://www.siemens.com/cert) and follow the instructions.

4.7.7 Data backup

Secure your configuration and parameter settings so that you can quickly restore this data if needed.

4.7.8 Security checks

Security checks for data, files, and archives serve to ensure data integrity at the storage location and during file transmission, protecting against manipulation and transmission errors. This is often achieved using digital checksums that are provided alongside the data. Tools (such as SHA-256 or SHA-512) for calculating and verifying these checksums are provided in many systems and named according to their respective calculation methods.

File Integrity Guidelines describe the prescribed procedure for integrity checks.

Integrity protection is a protection function for engineering data and firmware files.

Communication integrity means protecting communication against unauthorized manipulations to ensure high system availability. A central element in this regard is, for example, the use of digital checksums when accessing controllers. (Source: Industrial Cyber-security website (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html))

4.7.9 Secure decommissioning

In the following section, you will find information on how to properly decommission individual components of your automation system. Decommissioning is necessary when the component has reached the end of its service life.

Decommissioning includes environmentally sound disposal and secure removal of all digital data of electronic components with storage medium.

4.7.9.1 Securely removing data

Before disposing of components of your automation system, you should securely delete all data from the storage media of these components. How to securely delete data from the devices so that it cannot be recovered is described below.

NOTICE
Data misuse resulting from non-secure deletion of data
Incomplete or non-secure deletion of data from data memories can result in data misuse by third parties.
For this reason, ensure secure deletion of data from all storage media used before disposing of the product.

Secure erasure of data from the CPU and SIMATIC Memory Card

To delete all data from the data memories of the CPU, reset the CPU to factory settings. The function deletes all information that was saved internally on the module.

For secure deletion of the data, follow these steps in the order given:

1. Format the SIMATIC Memory Card.

   The formatting deletes all contents from the SIMATIC Memory Card.

   Formatting with STEP 7:

   – Establish an online connection.

   – Open the online and diagnostics view of the CPU (either from the project context or via "Accessible devices").

   – In the dialog window, select "Functions > Format memory card" and then click the "Format" button.

   Formatting using the display of a CPU:

   – In the display of the CPU, select the menu "Settings" > "Card functions" > "Format card" and confirm with OK.

2. Restore the factory settings of the CPU.

   We recommend resetting the CPU in STEP 7. When you reset a CPU to factory settings, select the options shown in the figure before the reset.
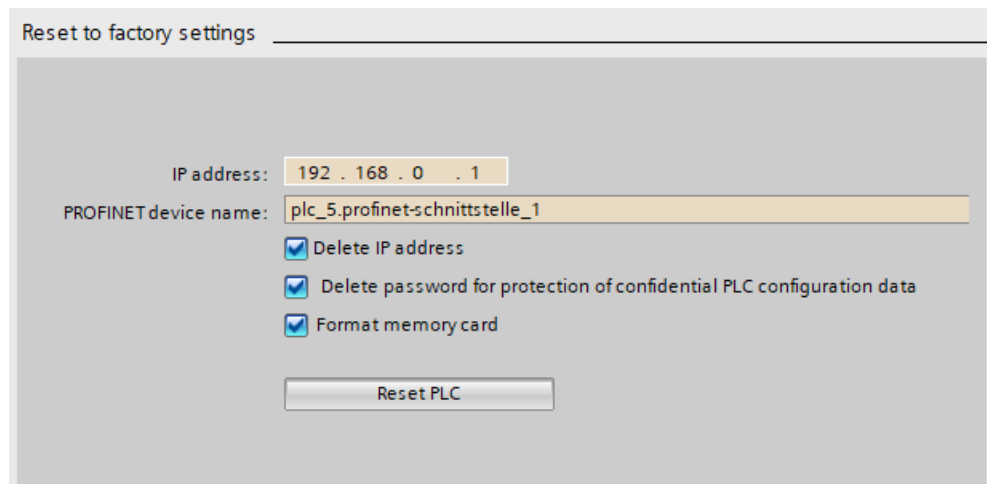
Figure 4-1 Resetting the CPU to factory settings

NOTE

If you reset the CPU using STEP 7 and you have selected the "Format memory card" option, you can skip step 1 of the described sequence of steps.

Result: All data that was still contained in the data memories of the modules and the SIMATIC Memory Card has been deleted. You can now dispose of the components.

For more information on resetting the CPU to factory settings, refer to the section Resetting the CPU to factory settings (Page 383).

NOTE

If you no longer plan to use the SIMATIC Memory Card after formatting it, destroy it before disposing of it.

A secure destruction method is to shred the card to such a degree that it cannot be reconstructed. For this, you can also use a waste disposal service that specializes in data storage medium destruction.

Secure erasure of data from the interface module

With the following tools, you can securely erase the data from the interface module:

- STEP 7 < V19
- SIMATIC Automation Tool
- MultiFieldbus Configuration Tool (MFCT)
- PRONETA

Follow these steps in the order given:

1. Establish an online connection.

2. Open the Online and Diagnostics view of the IM (either from the project context or via "Accessible devices").

3. In the dialog box "Functions > Reset to factory settings", select the option "Delete I&M data" and then the "Reset" button.
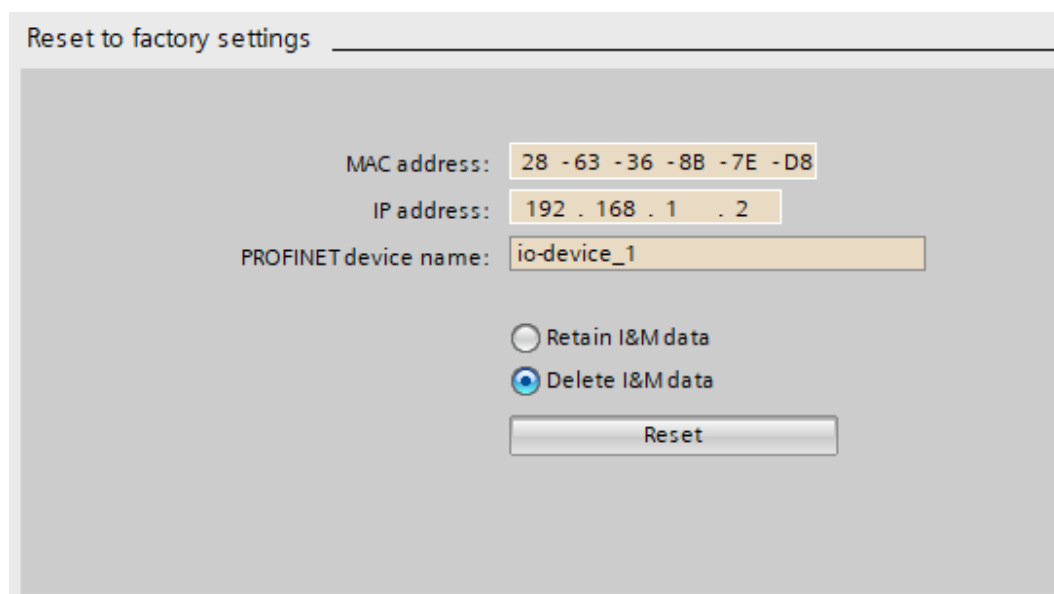
Figure 4-2 Resetting an interface module to factory settings

Result: All the data that was still in the data memories of the interface module was deleted. You can now dispose of the components.

For more information on resetting the interface module to factory settings, refer to the section Resetting an interface module to factory settings (Page 388).

NOTE

STEP 7 ≥ V19

Only the communication parameters will be securely deleted on "Reset to factory settings" with the "Delete I&M data" option enabled when you use STEP 7 ≥ V19.

Deleted communication parameters:

- IP address
- Device name
- PROFINET configuration data

If you want to securely remove all data, use one of the tools listed above for this purpose.

4.7.9.2 Recycling and disposal

For environmentally sustainable recycling and disposal of your old equipment, contact a certified electronic waste disposal service and dispose of the equipment according to the applicable regulations in your country.

4.8 Secure operation of the engineering software

For more information on secure operation of the engineering software, refer to the TIA Portal online help.

4.9 Secure operation of CPUs

This section describes measures recommended by Siemens to protect your device from manipulation and unauthorized access.

4.9.1 Secure configuration

Information about ports, services, and default states can be found in the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925) and the Equipment Manual.

4.9.2 User management and access control

4.9.2.1 Administration of user accounts

Creating and managing user accounts with appropriate usage rights is an important measure, as every active user represents a potential security risk.

Take the following security measures:

- Train your personnel in understanding their rights and password assignment
- Regularly check the user accounts

You can find information on creating and managing user accounts in the Protection (Page 269) section under "User management" and in the online help for STEP 7 (TIA Portal).

4.9.2.2 Assigning secure passwords

Using non-secure passwords can easily lead to data misuse. Non-secure passwords can be easily guessed or decrypted.

- Therefore, always change the default passwords during commissioning and use different passwords for different users, functions and devices.
- When changing the password, do not use passwords (or parts of passwords) that were used in the past.
- Also, change passwords for functions you don't personally use to prevent misuse of such unused functions.
- Always keep your passwords confidential and ensure that only authorized individuals have access to the respective passwords.
- Go over the required minimum password length and use a mixture of lower- and upper-case letters, numbers and characters.

The STEP 7 online help (TIA Portal) provides information on creating secure passwords.

Overview of all components and functions with password protection

Components and functions with password protection	Comment
SIMATIC S7 app	See section SIMATIC S7 app (Page 158)
CPU	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section Secure Communication
OPC UA	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section OPC UA communication
SNMP Community-String (similar to a password)	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section SNMP
Secure communication (with certificate protection)	See the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section Secure Communication
Web server	See the Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59193560)

4.9.2.3 Password management

- You can find comprehensive recommendations for creating secure passwords in the Industrial security Configuration Manual (https://support.industry.siemens.com/cs/us/en/view/108862708).

- Establish guidelines for assigning passwords and intervals for password changes.

- Settings for checking guidelines during password assignment or changes can be configured in the TIA Portal. For more information, please refer to the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

- Modify and reset the password for protecting confidential configuration data.

  You can find information on the following topics in the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925):

  - Description of how to change the password

  - Description of how to delete or reset the password

  - Description of how to assign the password via a SIMATIC Memory Card

- Access to a password-protected CPU can be configured through the display, if the CPU has a display; see section Using the display to set additional password protection (Page 294).

- For user management and access control, use the Local/central user management (Page 272).

- Using a password provider: In STEP 7, you can set up a password provider; see section Know-how protection (Page 296).

- In addition, you can use commercially available password management programs.

Setting password protection without engineering system

You can change your password for a user account in the user management via the web server of the CPU:

- API method Api.ChangePassword: Changing a password in runtime

You can find more information about the available methods of the web server's Web API in the Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) Function Manual.

4.9.2.4 Setting protection levels

For detailed information about setting up protection levels for the CPU and assigning user authorizations, refer to the section Configuring access protection for the CPU (Page 290) and the STEP 7 online help (TIA Portal).

4.9.2.5 Certificate management

You can create, assign, and manage certificates with TIA Portal for the following functions of the S7-1500 CPUs:

- Secure Open User Communication
- OPC UA communication
- Secure PG/HMI communication
- Web server

You can find all relevant information about "Certificate management" in the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

4.9.3 Protection functions

Integrated protection functions of the CPU protect against unauthorized access.

You can find an overview of the protection functions supported by your CPU in the respective Equipment Manual.

A description of the protection functions and their activation can be found in the section Protection (Page 269).

4.9.4 Signed firmware update for CPUs

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Principle of the signed firmware updates for CPUs

Firmware updates for CPUs contain a digital signature.

The digitally signed firmware update files are available for download on the Siemens Support Web page (https://support.industry.siemens.com/cs/de/en/view/109478459).

The CPU verifies the authenticity and integrity of the firmware update file before installation using the digital signature with standardized asymmetric cryptography methods. As a result, the CPU can detect a manipulated or corrupted firmware update file and reject it.

Note that the CPU performs the verification only after the complete firmware download has taken place.

The procedure for carrying out firmware updates for CPUs is described in the section Firmware update (Page 377).

Diagnostics alarms and remedy

The success/failure of the signed firmware update is reported:

- In the diagnostics buffer of the CPU
- On the display of the CPU if the CPU has a display
- In the Syslog storage of the CPU

In case of firmware update rejection, proceed as follows:

1. Check whether the firmware update file used by you originates from a secure source and was downloaded unchanged. As a check calculate the hash value of the downloaded firmware update file and compare it with the value specified on the download page.
2. Download the firmware again from the Siemens Support Web page.
3. Repeat the firmware update.

Information on the procedure for calculating and comparing hash values is available on the Internet (https://support.industry.siemens.com/cs/de/de/view/109483101/en).

4.9.5 Secure Boot for CPUs

Secure Boot

Secure Boot verifies, before the boot process, whether firmware has been falsified, for example through manipulation or accidental falsification.
Secure Boot ensures the authenticity and integrity of the firmware executed by the device.

Principle of "Secure Boot" for CPUs

CPUs as of article number 6ES751x-xxx03-0AB0 and as of 6ES751x-xxx10-0AB0 verify the authenticity and integrity of the firmware to be executed using "Secure Boot" before their startup.

The verification is carried out using standardized asymmetric cryptography methods.

In addition to the signed firmware update for CPUs (Page 58), Secure Boot prevents a manipulation of the firmware by a physical intervention into the CPU.

Secure Boot is integrated in the CPU and cannot be deactivated for security reasons.

4.9.6 Web server

The CPUs of the S7-1500 series have an integrated Web server.

It comes with built-in security features:

- Activation for specific interfaces
- Access via the secure transmission protocol "HTTPS" using the CA-signed or self-signed web server certificate
- Authentication via local or central user management
- Changing the password of local users during runtime using Web-API

The functions are described in detail in the Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) Function Manual.

4.9.7 Secure communication/OPC UA

Additional protection is provided by the protection functions of the secure communication and OPC UA protocols.

Information about the protocols Secure Communication and OPC UA can be found in the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

4.9.8 Sensitive data

Security-relevant and sensitive data can be protected through appropriate measures such as passwords and protection functions.

For certain data, protection is already essential and implemented within the system (e.g. certificate management in the TIA Portal).

Sensitive data	Comment	Where can I find more information?
Confidential configuration data (private keys, passwords/access data)	Protection by using a strong password	Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925), section Protection of confidential configuration data
User management data	-	Protection (Page 269) section STEP 7 online help
Configuration of CPUs and interface modules	Protection through PROFINET Security Class 1	Function manual PROFINET with STEP 7 (https://support.industry.siemens.com/cs/ww/en/view/49948856)
Blocks (data blocks, logic blocks)	Know-how protection, copy protection, write protection	Protection (Page 269) section
Data deemed sensitive by the operator	Backups, other configuration data, analysis data	Backing up and restoring the CPU configuration (Page 341) section

4.9.9 Backups and data backups

Regular backups or data backups after successful installation should be part of a successful security concept. Whether for restoring a project if required, if the changes made do not yield the desired results, or for saving an installation in an emergency.

Options for backing up STEP 7 project:

- Project backup via online backup, see article Online backup (https://support.industry.siemens.com/cs/us/en/view/109759862/91508694411)

- Project backup via the TIA Portal, see article What options are there in STEP 7 (TIA Portal) for backing up projects and what is the significance of the backup files of the projects? (https://support.industry.siemens.com/cs/us/en/view/92561565)

You can find more information in the section Backing up and restoring the CPU configuration (Page 341).

4.9.10 Additional protective measures for network security

To secure a CPU via further measures, the following options are available:

- Use of the CP 1543-1 or CP 1545-1 with security functions

  The use of an Ethernet CP provides you with additional access protection through a firewall and possibilities to establish secure VPN connections. See also operating instructions SIMATIC NET: S7-1500 - Industrial Ethernet CP 1543-1 (https://support.industry.siemens.com/cs/us/en/view/67700710) and S7-1500 - Industrial Ethernet SIMATIC CP 1545-1 (https://support.industry.siemens.com/cs/us/en/view/109771664).

- Various measures increase protection against unauthorized access to functions and data of the CPU from external sources and via the network. For information on the protection functions, refer to the Overview of protective functions (Page 269) section, under Further measures for protection of the CPU.

- You can find information on network security and network components for protection against unauthorized access in the Network security section of the PROFINET Function Manual (https://support.industry.siemens.com/cs/ww/en/view/49948856).

4.9.11 Remote access to CPU

4.9.11.1 Using a Web server

When using Web servers, traditional firewalls are no longer sufficient to protect modern networks.

Information about potential risks when using Web servers can be found in the Web server Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59193560).

4.9.12 Recording Security events

Syslog storage

Syslog stands for "System Logging Protocol," a standard for transmitting log messages triggered by security events. Predefined events in a network device are collected as security events in the device (syslog client) and stored as syslog messages in the local cache.

A syslog server collects and categorizes syslog messages, which can then be analyzed and filtered and displayed in various ways. Additionally, notifications for critical events can be configured.

The following security events, for example, are collected in the CPU diagnostic buffer:

- Going online with the correct or incorrect password
- Manipulated communication data detected
- Manipulated data detected on memory card
- Manipulated firmware update file detected
- Changed protection level (access protection) downloaded to the CPU
- Password legitimization restricted or enabled (via an instruction or, if applicable, the CPU display)

- Online access denied due to the possible number of simultaneous access attempts being exceeded

- Timeout when an existing online connection is inactive

- Logging on to the Web server with the correct or incorrect password

- Creating a backup of the CPU

- Restoring the CPU configuration (Restore)

The above-listed security events are also stored as syslog messages in the local cache of a CPU as of firmware version V3.1. You can find an overview of all syslog messages in the following Entry (https://support.industry.siemens.com/cs/ww/en/view/109823696).
The content of a syslog message is based on IEC 62443-3-3.

You can find more information in the section Syslog messages .

Connection to a SIEM system

A SIEM system (Security Information and Event Management) analyzes security events in real time and can be installed, for example, on the syslog server.

4.9.13 Syslog messages

Using syslog messages

International standards and national regulations for the IT security of automation components require, for example, the ability to log safety-related events.
Syslog (System Logging) is an IETF standard protocol (RFC 5424) for the transfer of recorded events and meets this requirement. A CPU records the following events, for example:

- Security events

- Firmware updates

- Changes to the user program

- Changes to the configuration

- Changes to the operating mode

The collecting of security-relevant events cannot be deactivated. Each CPU as of FW version saves V3.1 syslog messages in a local cache. By querying this cache, you can view the syslog messages and identify potential security risks.

For CPUs as of FW version V4.0, the local cache is located in the retentive memory area. As a result, syslog messages are retained after a POWER OFF/POWER ON transition or when the CPU is switched off. As a result, events that require one or more CPU restarts are also retained in syslog storage, such as restoring the CPU configuration.

The cache of a CPU is organized as a ring buffer. If the storage limit of the cache is reached and additional security events occur, the oldest messages in the cache are overwritten.

You have the option of transferring the events collected by the CPU to a syslog server in the network.

NOTE

Deleting the retentive syslog storage

If you want to expand or store a CPU as of FW version V4.0, the syslog messages are retained in the syslog storage of the CPU. To prevent unwanted transmission of saved syslog messages, return the CPU to factory settings (reset to factory settings) before removing or storing.

After a successful reset, the syslog storage only contains one boot up entry, which provides information about the reset to factory settings.

Forwarding to a syslog server

From STEP 7 V19 and a CPU as of FW version V3.1, it is possible to transfer syslog messages to a server, e.g. SINEC INS. The syslog messages are transferred to the syslog server via the syslog protocol. The syslog server saves all syslog messages from its connected devices. Messages of system and network events are stored centrally in a storage location in the syslog server. At the syslog server interface, you can view the collected syslog messages and thereby determine the source of potential security risks or problems.

Syslog messages are sent to the syslog server via port 514 (UDP) or port 6514 (TLS over TCP) by default.

NOTE

If you are using UDP as the transport protocol, the data is transmitted unencrypted. Authentication is also omitted with UDP.

Processing in a Security Information and Event Management system (SIEM system)

In order to be able to accept and process the incoming syslog messages, a SIEM system must "understand" the syslog protocol according to RFC 5424.

The SIEM system breaks down the incoming syslog messages into individual elements. These elements are assigned to their own event within the SIEM system. Within this event, it is analyzed whether there are connections between the individual syslog messages. In this way, the SIEM system detects possible attack vectors and, if necessary, informs the user, e.g. in the event of multiple attacks at several points in the system.

① CPUs
② Syslog messages
③ Syslog server, e.g. SINEC INS
④ SIEM system
⑤ Notify user
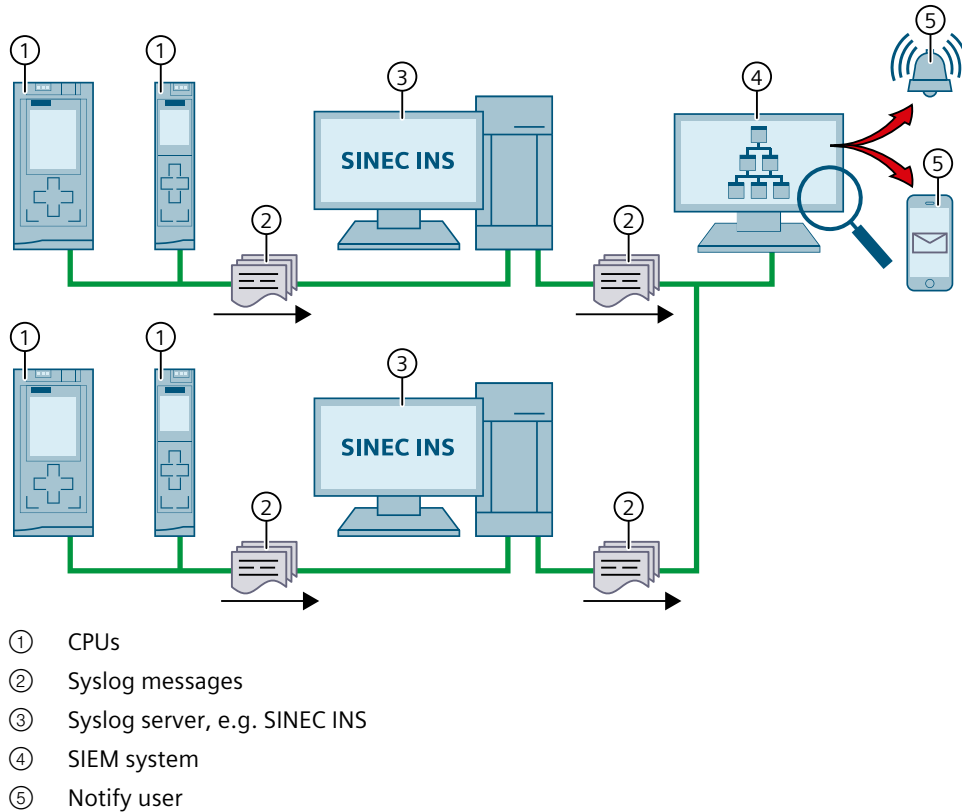
Figure 4-3 Forwarding and processing of syslog messages

More information

More information on network management with SINEC INS is available in the "SIMATIC NET: Network management SINEC INS V1.0 SP2" (https://support.industry.siemens.com/cs/us/en/view/109781023) manual.

You can find information on the structure of syslog messages in the Structure of the Syslog messages (Page 68) section.

4.9.13.1 Transfer the syslog messages to a syslog server

A CPU can send syslog messages to a syslog server via a TLS or UDP connection.

Transmitting syslog messages via a TLS connection

A TLS connection ensures that all syslog messages from a CPU are securely transmitted to the syslog server. If the TLS connection is interrupted, the syslog messages are cached in the CPU cache. The CPU only sends the cached syslog messages when the TLS connection to the syslog server is established again.

Each syslog message is transferred to a syslog server only once. If you address another syslog server in the settings for the syslog server, syslog messages that have already been transferred are not transferred to a newly configured syslog server.

Since the cache of a CPU is organized as a ring buffer, the oldest messages are overwritten as soon as the memory limit is reached and further security events occur. Overwriting syslog messages that have not yet been transferred to a syslog server is reported as a security event (overflow event) in syslog storage. If syslog messages are overwritten over a long period of time, the overflow event is repeated regularly. As soon as the first message is sent back to the syslog server, another security event is generated. This security event confirms that syslog messages are being transferred back to the syslog server.

Message in the diagnostics buffer of the CPU

If a syslog server is configured in the CPU properties, the CPU also records overwriting of non-transmitted syslog messages in the diagnostics buffer.

As soon as a non-transmitted syslog message is overwritten, the CPU reports maintenance demanded as an incoming event in the diagnostics buffer. In addition, the MAINT LED of the CPU also signals incoming maintenance demanded.

As soon as the syslog messages are sent back to the syslog server, the CPU reports maintenance demanded as an outgoing event in the diagnostics buffer. If the CPU does not report any further maintenance demanded, the MAINT LED also turns off again.

Information on the status and error display of the CPU can be found in the respective device manuals.

Requirements

If you want to transfer the syslog messages of a CPU to a syslog server, the following requirements must be met:

- STEP 7 as of version V19
- CPU as of FW version V3.1
- A project has been created in STEP 7
- The device or network view of STEP 7 is open

Procedure

To configure the CPU to transfer syslog messages to a syslog server, following these steps:

1. Select the required CPU in the device or network view of STEP 7.

2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Syslog server".

3. In the "Connection to syslog server" area, select the "Enable transfer of syslog messages to a syslog server" option. The selection options below become editable.

4. Select one of the following options from the "Transport protocol" drop-down list:

   – "Transport Layer Security (TLS) - server and client authentication": Encrypted data transfer, syslog server and client (CPU) must authenticate themselves.

   – "Transport Layer Security (TLS) - only server authentication": Encrypted data transfer, only the syslog server needs to authenticate itself.

   – "UDP": Unencrypted data transfer, syslog server and client (CPU) do not need to authenticate themselves.

   In the next sections you can read how to select the certificates for authentication (logon) depending on the settings specified.

5. In the "Addresses of the syslog servers" column, enter a valid server address.

6. In the "Port" column, enter a valid port number.
   By default, STEP 7 uses the following port numbers:

   – Standard TCP port for TLS: 6514

   – Standard UDP port: 514

Result: You have configured the transfer of syslog messages to a syslog server.
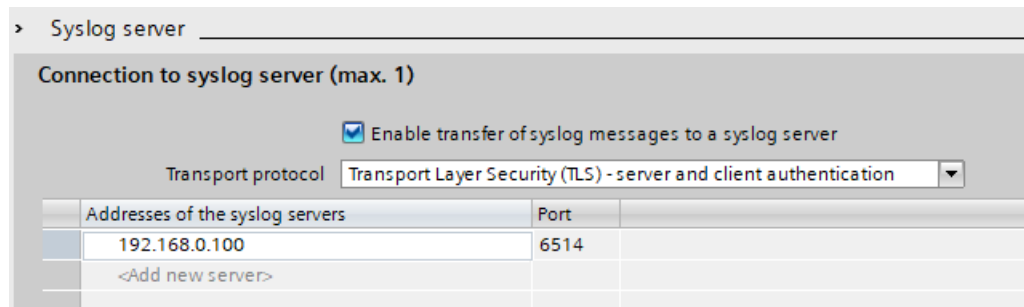
Figure 4-4 Transfer of syslog messages to a syslog server configured

Selecting the client certificate

STEP 7 provides the required client certificate for a CPU for the TLS transport protocol. If the certificate is managed within the CPU, you can either choose an existing certificate or create a new certificate. To do so, follow these steps:

1. Select the required CPU in the device or network view of STEP 7.

2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Certificates for Syslog".

3. Select the appropriate certificate in the "Client certificate" field.
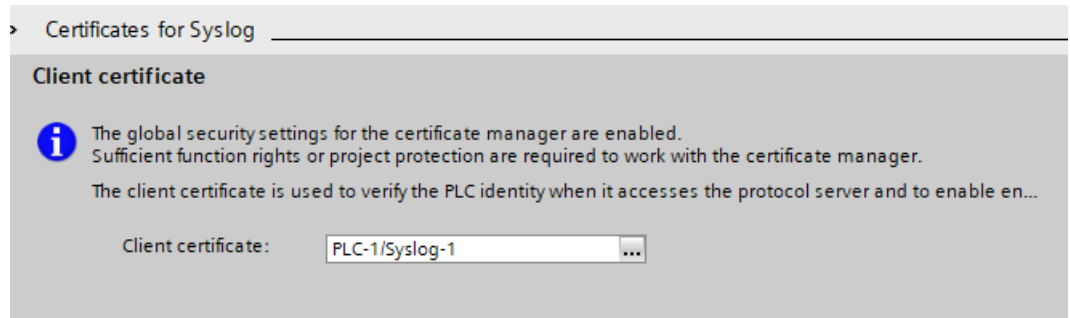
Selecting the server authentication

After selecting the TLS transport protocol, the configured syslog server must authenticate itself. This ensures that the CPU only connects to a trusted server. If you want to waive server authentication, activate the automatic acceptance of server certificates during runtime. To configure these settings, follow these steps:

1. Select the required CPU in the device or network view of STEP 7.

2. In the Inspector window, navigate to "Properties > Protection & Security > Syslog > Certificates for Syslog".

3. In the "Trusted servers" area, specify whether the connected syslog server is to be authenticated. In this case, it is necessary to complete the following information:

    – Add trusted server: Add a valid server certificate in the "Common name of subject" column.

    – Automatically accept certificates during runtime: Activate the "Automatically accept server certificates during runtime" option. Editing in the table is then not possible.

NOTE

No authentication with automatically accepted server certificates

If you enable the "Automatically accept server certificates during runtime" option, a server does not need to authenticate itself. This means that the CPU can also connect to unknown servers that could represent a security risk.

Only select this option during commissioning or in a protected environment.

4.9.13.2 Structure of the Syslog messages

A CPU collects syslog messages in a local cache. These syslog messages are structured according to the syslog protocol (RFC 5424) and consist of the following elements:

- HEADER
- STRUCTURED-DATA
- MSG (Message)

The following sections describe the structure and parameters of the individual elements.

Structure of the HEADER element

The header contains all the data required for further processing of the syslog message. A space separates the individual parts of the header (exception: No space between PRI and VERSION). A CPU transmits the following header in syslog messages, for example:
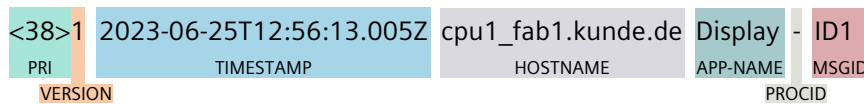
Figure 4-5 Example: HEADER of the syslog message of a CPU

The following table describes the parameters in the prescribed order.

Parameter	Description

PRI	PRI encodes the priority of the syslog message, divided into Severity (severity of the message) and Facility (origin of the message).
	The PRI value is formed as follows:
	• PRI = Facility x 8 + Severity
	Possible values:
	• Severity
	  – 0 = Emergency: system is unusable
	  – 1 = Alert: action must be taken immediately
	  – 2 = Critical: critical conditions
	  – 3 = Error: error conditions
	  – 4 = Warning: warning conditions
	  – 5 = Notice: normal but significant condition
	  – 6 = Informational: informational messages
	  – 7 = Debug: debug-level messages
	• Facility
	  – 1 = User-level messages
	  – 2 = Mail system
	  – 3 = System daemons
	  – 4 = Security/authorization messages
	  – 5 = Messages generated internally by syslog
	  – 6 = Line printer subsystem
	  – 7 = Network news subsystem
	  – 8 = UUCP subsystem
	  – 9 = Clock daemon
	  – 10 = Security/authorization messages
	  – 11 = FTP daemon
	  – 12 = NTP subsystem
	  – 13 = Log audit
	  – 14 = Log alert

Parameter	Description
	A CPU does not use all of the listed severity/facility values.
VERSION	Version number of the syslog specification.
TIMESTAMP	The device sends the time stamp in the format "2023-06-25T12:56:13.005Z" as UTC time without time zone and correction for daylight-saving/standard time.
HOSTNAME	Contains the name or the IP address (PROFINET interface X1) of the device or system from which the syslog message has been sent. IPv4 address according to RFC1035: Bytes in decimal representation: XXX.XXX.XXX.XXX IPv6 address according to RFC4291 Section 2.2 "-" is output if information is missing.
APP-NAME	Contains the component (device part or application) from which the message has been generated. "-" is output if information is missing.
PROCID	The process ID serves to clearly identify the individual processes, for example during analysis and troubleshooting. "-" is output if information is missing.
MSGID	ID to identify the message. "-" is output if information is missing.

Structure of the STRUCTURED-DATA element

STRUCTURED-DATA provides information in an interpretable and decomposable data format. The following applications are possible, for example:

- More information about the syslog message

- Application specific information

STRUCTURED-DATA can contain one or more elements (SD-ELEMENT). Each SD element must be enclosed in square brackets. If STRUCTURED-DATA consists of multiple SD elements, the individual SD elements are separated by a space.

Each SD-ELEMENT consists of its name (SD-ID) and one or more name-value pairs (SD-PARAM). Each name-value pair consists of a parameter name (PARAM-NAME) and the associated value (PARAM-VALUE). A space separates the individual components (SD-ID and SD-PARAM) within an SD element.

A CPU transmits the following SD ELEMENT in a syslog message, for example:
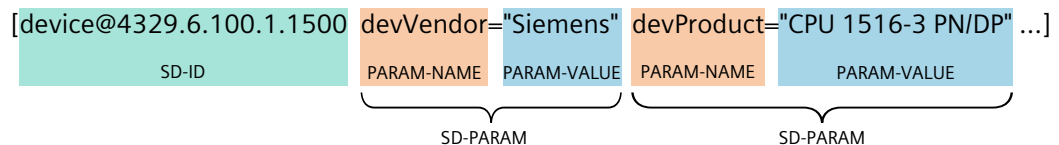
Figure 4-6 Example: SD ELEMENT of the syslog message of a CPU

Structure of the MSG element

In the MSG (MESSAGE) element, a CPU transmits the simplified name of the event in English. The following table shows what the content of a message of the MESSAGE element can look like.

MESSAGE	Description
SE_LOCAL_SUCCESSFUL_LOGON	The local logon has been successful (e.g. on the operator display of the CPU).

More information

You can read more information about the structure and transmission of syslog messages in the following RFCs (Request for Comments):

- The syslog protocol (RFC 5424) (https://tools.ietf.org/html/rfc5424)
- Transferring syslog messages via Transport Layer Security (RFC 5425) (https://tools.ietf.org/html/rfc5425)
- Transferring syslog messages via UDP (RFC 5426) (https://tools.ietf.org/html/rfc5426)

4.10 Secure operation of interface modules

Device-specific security information and instructions for interface modules can be found in the respective Equipment Manual.

4.10.1 Data integrity for interface modules

Data integrity refers to the completeness and correctness (integrity) of data, which is an essential prerequisite for the proper functioning of systems.

Measures for data privacy, data consistency, and data security ensure that data used within devices cannot be damaged, altered (manipulated), or deleted during processing or transmission, and at the very least, any changes to the data are detected.

Data integrity for interface modules

To detect intentional or accidental changes to data within an interface module and its associated modules, the possibility of dynamic integrity checking is introduced for PROFINET interface modules.

The ability to detect integrity breaches enhances the resilience of the distributed I/O system.

Data integrity within a distributed I/O system is entirely covered within the interface module and does not pertain to other components of the automation system.

Principle

The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as parameter settings, IP address, device name, MAC address and I&M data. The interface module stores the checksums in the I&M4 data area.

A CRC (Cyclic Redundancy Check) is always the same for a specific, unchanged memory content. When the memory content changes, the interface module (IM) calculates a different checksum for this content by reading and comparing the I&M4 data. By comparing with the initial CRC, you can determine whether the data in the memory has been modified or not:

- CRC stayed the same: No change in the data within this memory area of the interface module IM

- CRC changed: The data within this memory area of the IM was modified

Only you, as the user, know whether changes to the data of an interface module were intentional or not. If changes were not intentional, you can detect that the data of the interface module has been compromised through changed CRCs and respond accordingly.

I&M data

PROFINET devices provide Identification and Maintenance data (I&M data), which is a set of predefined data structures containing the internal module status. With this data, a module can be identified, its serial number can be determined, etc.

The CRC checksums are mapped in the maintenance data **I&M4** of the interface module.

NOTE

Requirements for calculating the CRCs

The CRCs via the memory contents of the interface module are calculated only when you request to read the I&M4 data.

The CRCs cover not only the interface module itself but can also take into consideration combined checksums from associated modules (refer to the section on the structure of the data record for I&M data). Process data is not included in the calculation of CRCs.

Example:

- You put your distributed I/O system into operation and read the CRC CHK_OVERALL with the value "0x55AAA678" ("16#55AAA678") from the interface module via the I&M4 data.

- As long as no changes have been made to the data of the interface module or the associated modules, each subsequent read will give the value "0x55AAA678" or "16#55AAA678".

- Once you read a different CRC CHK_OVERALL, for example, "0xCC9876FF", you will realize that there must have been changes to the data of the interface module or the associated modules.

The quality of the statement regarding the data integrity of the distributed I/O system improves with each module associated with the interface module that supports I&M4 data. Refer to the Equipment Manual of the respective module to find out if and from which firmware version the module supports I&M4 data.

The structure of the I&M data 0 to 4 is described in the section Record structure for I&M data

Spare parts scenario

The spare parts scenario is still ensured. This means that you can replace interface modules with the same article number. For the "new" interface module, the static data such as the serial number and MAC addresses will change. Note that this is why the replacement will be reflected in the changed identification data CHK_STATIC_LOCAL and consequently also in CHK_OVERALL.

More information on the spare parts scenario and compatibility can be found in the Equipment Manual of the interface module.

4.10.2   Signed firmware update for interface modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Information on whether your interface module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

Principle of the signed firmware update for interface modules

Firmware updates for interface modules may include a digital signature. The digitally signed firmware update files are available for download on the Siemens Support Web page.

The interface module verifies the authenticity and integrity of the firmware update file before installation using the digital signature with standardized asymmetric cryptography methods. As a result, the interface module can detect a manipulated or corrupted firmware update file and reject it.

Note that the interface module performs the verification only after the complete firmware download has taken place.

Subsequently, a notification is sent to the firmware update tool regarding the success or failure of the signature verification.

You still have all the options for firmware updates, as described in the Firmware update (Page 377) section, when performing signed firmware updates for modules. If the firmware update was not successful, the module will continue to run with the previous firmware.

Diagnostics alarms and remedy

When performing a firmware update for a module with an established connection between the IM and CPU, the following options for notifications are available in the CPU's diagnostic buffer:

- Successful integrity check of the firmware for the module
- Rejection of non-secure firmware for the module

You can find more information in the section on diagnostics alarms in the equipment manual for the respective module.

In case of firmware update rejection, proceed as follows:

1. Check whether the firmware update file used by you originates from a secure source and was downloaded unchanged. As a check calculate the hash value of the downloaded firmware update file and compare it with the value specified on the download page.

2. Download the firmware again from the Siemens Support website.

3. Repeat the firmware update.

Information on the procedure for calculating and comparing hash values is available on the Internet (https://support.industry.siemens.com/cs/de/de/view/109483101/en).

4.10.3 Secure Boot for interface modules

Secure Boot

Secure Boot verifies, before the boot process, whether firmware has been falsified, for example through manipulation or accidental falsification.
Secure Boot ensures the authenticity and integrity of the firmware executed by the device.

Information on whether your interface module supports Secure Boot is available in the Technical specifications section of the corresponding Equipment Manual.

Principle of "Secure Boot" for interface modules

Interface modules verify the authenticity and integrity of the firmware to be executed using "Secure Boot" before being executed.

The verification is carried out using standardized asymmetric cryptography methods.

In addition to signed firmware updates for interface modules, Secure Boot also prevents manipulation of the firmware through physical intervention in the interface module.

Secure Boot is integrated into the interface module and cannot be deactivated for security reasons.

NOTE

Longer startup duration of the interface module

The signature verification of Secure Boot significantly extends the startup time of the interface module. You can find time specifications in the Equipment Manual of the interface module, in the Technical specifications section.

LED display on the interface module

> If the Secure Boot verification results in an invalid signature, the LEDs RUN, ERROR, and MAINT on the interface module will flash. In this case, you need to replace the interface module.

4.11 Secure operation of I/O modules

> Device-specific security information and instructions for I/O modules can be found in the respective Equipment Manual.

4.11.1 Data integrity for I/O modules

Data integrity for I/O modules

> In order to detect intentional or accidental changes to the data of an interface module and the assigned modules, the dynamic integrity check for I/O modules is introduced. Information on whether your I/O module supports the data integrity check is available in the Technical specifications section of the corresponding Equipment Manual.

Principle

> The interface module calculates checksums based on its used data and the supplied data from the associated modules, such as serial numbers, parameter settings, calibration data and I&M data of I/O modules. The interface module stores the checksums in the I&M4 data area.

> You can find more information on the principle of data integrity and I&M4 data in the section Data integrity for interface modules (Page 70).

Spare parts scenario

> The spare parts scenario is still ensured. This means that you can replace I/O modules with the same article number. For the "new" I/O module, the static data such as the serial number will change. Note that the replacement is therefore reflected in the following modified I&M4 data of the interface module:

> - CHK_STATIC_SUBS
> - CHK_OVERALL_SUBS
> - CHK_OVERALL

> You can find the structure of I&M data in the section Record structure for I&M data (Page 351).

4.11.2 Signed firmware update for I/O modules

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

- Firmware was modified
- Firmware was downloaded from an incorrect Internet source

Signed firmware update for I/O modules

Firmware updates for I/O modules can contain a digital signature. Information on whether your I/O module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

The digitally signed firmware update files are available for download on the Siemens Support Web page.

Principle, diagnostics alarms, and remedies

The principle and diagnostics of the signed firmware update are the same for interface modules and I/O modules. The information in the section Signed firmware update for interface modules applies.

4.12 Secure operation of power supply modules

Device-specific security information and instructions for the power supply modules can be found in the respective Equipment Manual.

4.12.1 Signed firmware update for system power supplies (PS)

Signed firmware update

A signed firmware update ensures the authenticity and integrity of the firmware loaded onto a device.

It protects you against installing malicious firmware in case:

• Firmware was modified

• Firmware was downloaded from an incorrect Internet source

Signed firmware update for system power supplies (PS)

Firmware updates for system power supplies (PS) can contain a digital signature. Information on whether your power supply module supports signed firmware updates is available in the Technical specifications section of the corresponding Equipment Manual.

The digitally signed firmware update files are available for download on the Siemens Support Web page.

Principle, diagnostics alarms, and remedies

The principle and diagnostics of the signed firmware update are the same for interface modules and I/O modules. The information in the section Signed firmware update for interface modules (Page 72) applies.

System overview

5

5.1 Overview of the SIMATIC S7-1500 automation system

5.1.1 The SIMATIC automation systems

You need optimum solutions for every application in order to automate your machines and plants economically and flexibly.

The SIMATIC controller portfolio includes a variety of systems:

- The SIMATIC S7-1200 Basic Controller is the intelligent choice for compact automation solutions with integrated communication and technology functions.

- If plant complexity and system performance are priorities, the SIMATIC S7-1500 automation system is the right choice for you. The SIMATIC S7-1500 controller builds on the more simple functionality of the SIMATIC S7-1200 Basic Controller and fulfills the highest demands on performance, flexibility and networking capability.

- The SIMATIC ET 200SP Distributed Controller combines the advantages of the S7-1500 and the very compact design of the ET 200SP with high channel density. By using distributed intelligence, you save costs and space in the control cabinet.

- For use outside the cabinet, the CPU 1513pro-2 PN and CPU 1516pro-2 PN offer you SIMATIC S7-1500 functionality in the design of the ET 200pro in the degree of protection IP65/IP67.

- If you require PC-based automation, use the SIMATIC S7-1500 software controller. The PC-based controller is autonomous from the operating system during operation.

- If you want to increase the availability of your system, use the redundant system S7-1500R/H. In the system, two CPUs (primary and backup CPU) process the user program in parallel and permanently synchronize all relevant data. In the event of failure of the primary CPU, the backup CPU takes over control of the process at the point of interruption.

The SIMATIC controllers are integrated into the Totally Integrated Automation Portal and offer consistent data management and a uniform operating concept. With its integrated functions, engineering in the TIA Portal ensures consistent functionality.
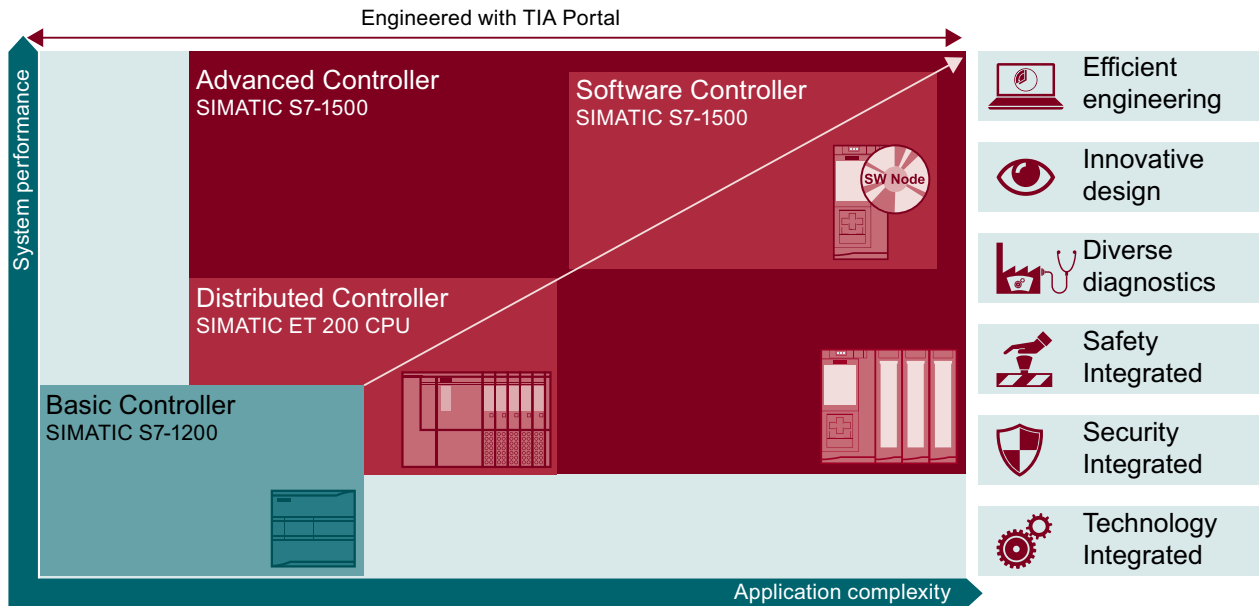
Figure 5-1 Overview of SIMATIC automation systems

The SIMATIC S7-1500 automation system supports all conventional communication standards.

All the SIMATIC S7-1500 CPUs offer integrated motion control functions. Technology CPUs are available for extended motion control functions.

The SIMATIC S7-1500 CPUs are also available as fail-safe controllers.

Diagnostic functions across all components simplify troubleshooting. Changes to the parameter assignment can be implemented quickly and easily with the integrated display.

Integrated security functions help against:

- Manipulation
- Theft of know-how

Integrated security functions offer additional security mechanisms for the configuration of secured networks.

5.1.2 Comparison of SIMATIC automation systems

The tables below compare the main technical specifications of the SIMATIC systems.

	Basic Controller	Controller	
	SIMATIC S7-1200	**SIMATIC ET 200SP CPU**	**SIMATIC ET 200SP Open Controller CPU 1515SP PC2**
Data work memory, max.	150 KB	3.5 MB	5 MB
Code work memory, max.	150 KB	900 KB	1 MB
Load memory/mass storage, max.	32 GB (via SIMATIC Memory Card)	32 GB (via SIMATIC Memory Card)	320 MB
I/O address area, max.	1024/1024 bytes	32/32 KB	32/32 KB
Integrated interfaces, max.	1 x PROFINET IO (2-port switch)	1 x PROFINET IO (2-/3-port switch, support of BusAdapters) 1 x PROFINET IO	1 x PROFINET IO (2-port switch)
Controller with integrated inputs and outputs	X	---	---
Configuration control	---	X	X
Web server	X	X	X
Isochronous mode	---	Distributed	Distributed
Integrated display	---	---	As Windows application
Technology integrated	Motion Control PID Control	Motion Control PID Control	Motion Control PID Control
Extended motion control functions	---	In T-CPUs	In T-CPUs
Security integrated	X	X	X
Integrated system diagnostics	X	X	X
Integrated safety functionality	In F-CPUs	In F-CPUs	In F-CPUs
Degree of protection	IP20	IP20	IP20

	Distributed Controller	Advanced Controller		
	SIMATIC ET 200pro	**SIMATIC S7-1500**	**Software Controller SIMATIC S7-1500**	**SIMATIC S7-1500R/H**
Data work memory, max.	7.5 MB	150 MB	20 MB	150 MB
Code work memory, max.	2 MB	18 MB	5 MB	18 MB
Load memory/mass storage, max.	32 GB (via memory card)	32 GB (via memory card)	320 MB	32 GB
I/O address area, max.	32/32 KB	32/32 KB	32/32 KB	32/32 KB

	Distributed Controller	Advanced Controller			
	SIMATIC ET 200pro	SIMATIC S7-1500		Software Controller SIMATIC S7-1500	SIMATIC S7-1500R/H
Integrated interfaces, max.	1 x PROFINET IO (3-port switch) 1 x PROFINET IO	1 x PROFINET IO (2-port switch) 1 x PROFINET IO 1 x PROFINET 1 x PROFIBUS	2 x PROFINET IO (2-port switch) 1 x PROFINET	Support the hardware interfaces	2 x PROFINET IO (2-port switch) 1 x PROFINET 2 x H-Sync interface (only H/HF-CPUs)
Controller with integrated inputs and outputs	---	C-CPU		---	---
Configuration control	X	X		X	---
Web server	X	X		X	X (only Web API)
Isochronous mode	Distributed	Centralized and distributed		Distributed (support using CP 1625)	---
Integrated display	---	X		As Windows application	X
Technology integrated	Motion Control PID Control	Motion Control PID Control C-CPUs: High-speed counters, PWM, PTO, frequency output		Motion Control PID Control	PID Control
Extended motion control functions	---	In T-CPUs		In T-CPUs	
Security integrated	X	X		X	X
Integrated system diagnostics	X	X		X	X
Integrated safety functionality	In F-CPUs	In F-CPUs		In F-CPUs	In F-CPUs
Degree of protection	IP65/67	IP20		Depending on hardware	IP20
Redundancy connections (synchronization link)	---	---		---	PROFINET ring (R-CPUs) Fiber-optic cable (H-CPUs)
System redundancy	---	---		---	X

5.1.3   Areas of application SIMATIC S7-1500 and ET 200MP

Area of application SIMATIC S7-1500

The SIMATIC S7-1500 automation system offers you the required flexibility and performance for a wide range of controller applications in machine and plant engineering. The scalable configuration makes it possible for you to adapt your PLC onsite to the local conditions.

As well as the standard motion control and technology functions available in the S7-1500, SIMATIC S7-1500 technology CPUs offer you additional features such as enhanced synchronous operation and kinematics functions.

The SIMATIC S7-1500 automation system conforms with IP20 degree of protection and is intended for use in a dry environment and installation in a control cabinet.

SIMATIC S7-1500R/H CPUs (redundant or fault-tolerant CPUs) offer you the option to increase the availability of your system. In order to be able to switch from the primary CPU to the backup CPU in case of need, the user program is processed synchronously on two CPUs.

Area of application Distributed I/O system ET 200MP

SIMATIC ET 200MP is a modular, scalable and universally usable distributed I/O system. SIMATIC ET 200MP offers the same system benefits as the SIMATIC S7-1500. A central controller accesses the I/O modules of the ET 200MP as central I/O modules via PROFINET or PROFIBUS.

SIMATIC ET 200MP convinces with its high performance:

* For shortest response times

* For large configuration limits

* For fastest applications

This is also accompanied by the high-speed backplane bus, special input/output modules and the consistent use of PROFINET mechanisms.

Area of application F-system SIMATIC Safety with S7-1500 and ET 200MP

By using fail-safe SIMATIC S7-1500 CPUs and modules, you can implement applications for safety engineering. This enables you to achieve almost seamless integration of machine safety into the SIMATIC S7-1500 and ET 200MP. You use one system at the same time for both your standard and fail-safe automation. This provides you with economic benefits, reliability as well as potential savings on hardware, engineering tasks and storage costs.

5.1.4 Plant components and automation levels

The Advanced Controllers SIMATIC S7-1500 are used for complete production automation and in applications for medium-sized and high-end machines. The combination of the individual SIMATIC components offers powerful and flexible automation solutions that cover all ranges of control applications:

- The process signals are connected to the central controller via fieldbus
- All modules are located directly in the automation system or in the distributed I/O system
- F-CPUs with integrated safety functionality ensure fail-safe processes
- SIMATIC S7-1500 is intended for installation in the control cabinet with IP20 degree of protection

The SIMATIC S7-1500 is integrated across all communication standards consistently in the various automation levels.
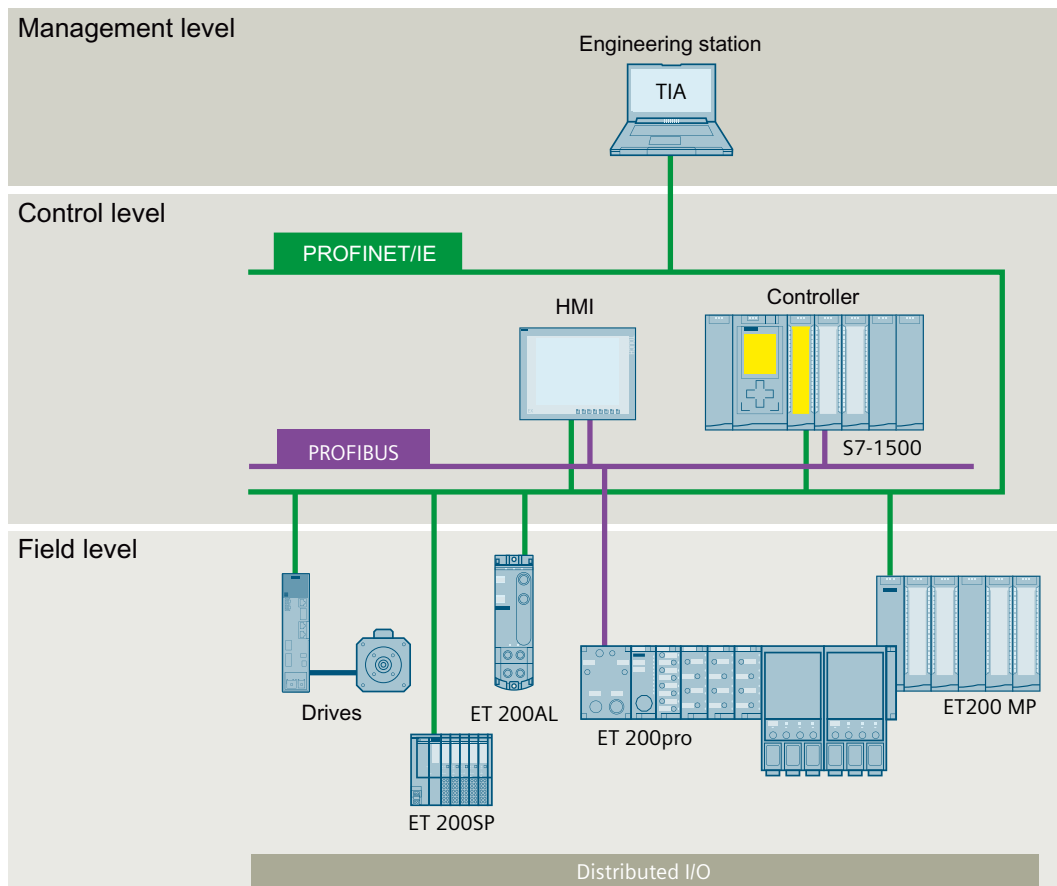
Figure 5-2 Basic structure: SIMATIC S7-1500 at management, control and field level

You can also find an overview of the SIMATIC S7-1500 automation system on the Internet (https://www.siemens.com/global/en/products/automation/systems/industrial/plc/simatic-s7-1500.html).

5.1.5   Scalability

In order to suit the requirements of your plant planning, the SIMATIC S7-1500 controllers can be scaled in their processing speed and configuration limits. They also offer networking facilities via different communications standards.

Safety Integrated, Motion Control, and other technology functions can be used for all plant sizes.

Different example applications with different SIMATIC S7-1500 CPUs are shown in the following:

SIMATIC S7-1500 with integrated I/O
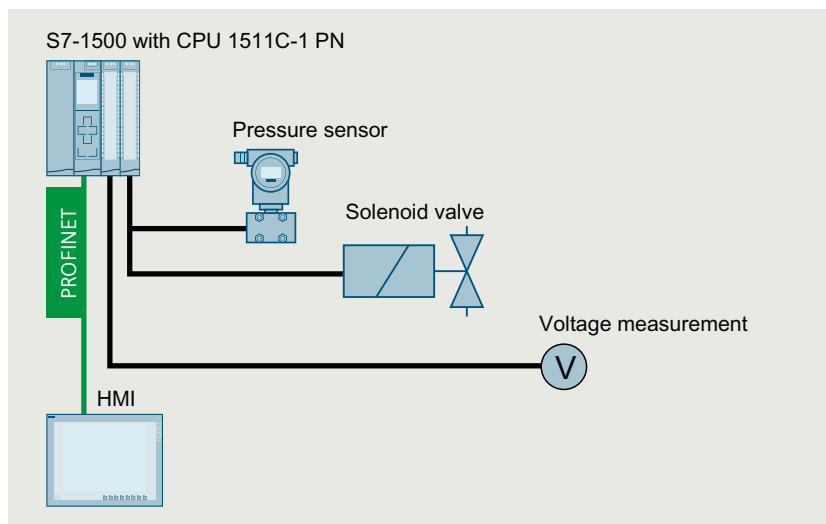
Figure 5-3 Example: Plant configuration with SIMATIC S7-1500 with integrated I/O

SIMATIC S7-1500 with I/O, ET 200MP and HMI device
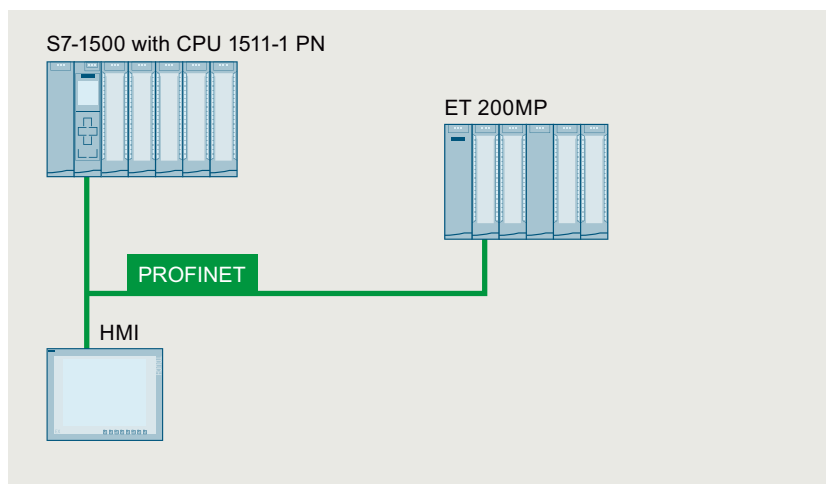
Figure 5-4 Example: Plant configuration with SIMATIC S7-1500 with I/O, ET 200MP and HMI device

SIMATIC S7-1500 with Motion Control, distributed I/O and IO-Link devices
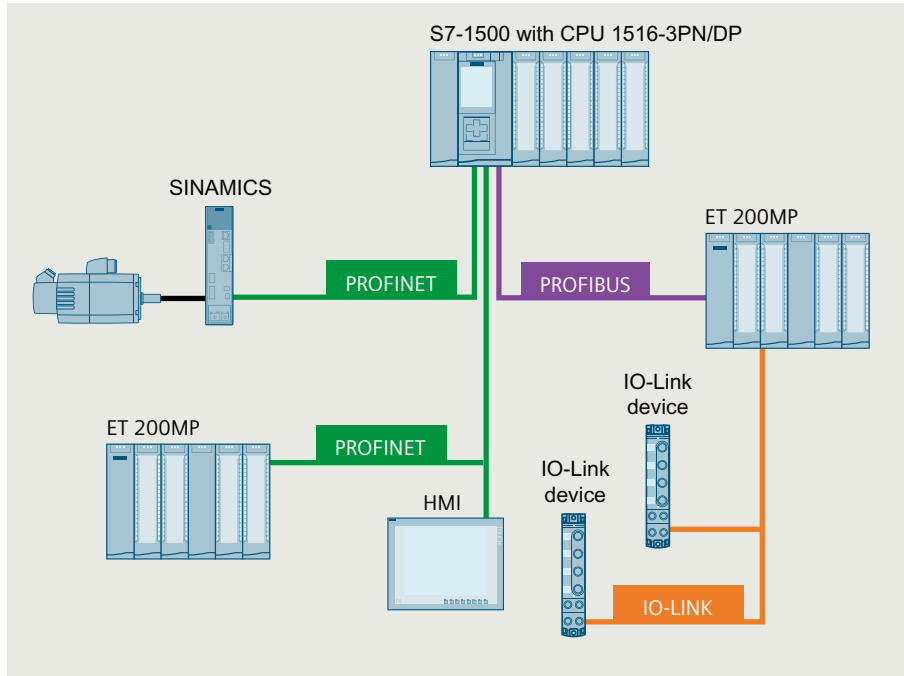
Figure 5-5 Example: Plant configuration with SIMATIC S7-1500, Motion Control, distributed I/O and IO-Link devices

SIMATIC S7-1500 with safety und WLAN integration

Figure 5-6 Example: Plant configuration with SIMATIC S7-1500 and Safety on PROFINET

5.1.6 Overview of features

Automation system SIMATIC S7-1500

Through the integration of numerous new performance features, the S7-1500 automation system offers you excellent operability and the highest performance.

Important properties and functions

Easy to use

- Uniform front connectors

- Pre-wiring position enables easy connecting and reconnecting

- Integrated shield for high signal measurement quality

High performance

- Fast signal processing for faster reaction times and high productivity

- Fast backplane bus for high baud rate and efficient transmission protocol

- Location-independent information acquisition thanks to integrated web server

- High number of connections and PROFINET ports

- Variety of networking options in systems (IO controller, I-device, shared device)

Wide range of diagnostics

- Integrated system diagnostics for uniform display concept without additional programming effort

- User-defined interrupts

- Evaluate system errors using system blocks

Innovative design

- Onboard display for diagnostics and first commissioning

- High degree of variability through scalability up to 30 I/O modules per rack

- Innovative labeling system maximizes organization in very limited spaces

- Compact CPUs with integrated analog and digital on-board I/O and integrated technology functions

Communication standards

- PROFINET IO

- PROFIBUS DP

- Point-to-point (RS232, RS485)

Efficient engineering

- STEP 7 language innovations while maintaining proven functions

- Support of different programming languages (STL, LAD, FBD, SCL, CFC, GRAPH)

- Consistency check by STEP 7 instead of in the CPU

Safety Integrated

- Easy integration of fail-safe CPUs (F-CPUs) and fail-safe modules (F-modules)

- One F-CPU for fail-safe and non-fail-safe applications

- Setting of all F parameters via software

Security Integrated

- Protection level concept for greater access protection

- Know-how protection against unauthorized access and modifications

- Copy protection on the SIMATIC Memory Card against copying of user programs

Technology Integrated

- Motion control functionality supports the connection of PROFIdrive-capable drives

- Technology CPUs with advanced motion control functions

- Easy programming of motion sequences with PLCopen motion control blocks

- Temperature controller

- PID control for continuous and discrete closed-loop control processes with autotuning for easy commissioning and optimal control performance

- Seamless integration into TIA Portal for synchronous configuration and uniform operating concept

- TRACE support for effective commissioning, diagnostics and fast optimization of drives and closed-loop controls

Figure 5-7 SIMATIC S7-1500 automation system - Properties and functions

Distributed I/O system ET 200MP

The ET 200MP distributed I/O system is a scalable and flexible system for connecting the process signals to a CPU via a fieldbus.

The modules have a very high channel density and a low variety of parts. This simplifies ordering, logistics and spare parts handling significantly.

Important properties and functions

Easy to use

- With I/O modules of the S7-1500 automation system

- Screw-type or push-in terminal connections

- Configuration adjustment for future configuration levels through integrated configuration control

- Uniform front connectors

- Pre-wiring position enables easy connecting and reconnecting

High performance

- Isochronous PROFINET IO with send clocks as fast as 250 µs

Innovative design

- High channel density (e.g. 32 channels on 25 mm wide I/O module)

- High degree of variability through scalability up to 30 I/O modules per station

- Innovative labeling system maximizes organization in very limited spaces

Safety Integrated

- Easy integration of fail-safe modules (F-modules)

- Setting of all F parameters via software

Interface modules

- IO device with PROFINET IO interface (2 ports)

- DP device with PROFIBUS DP interface

Powerful technology

- Technology modules for counting, position detection, and time-based IO functionality

Communication standards

- PROFINET IO

- PROFIBUS DP

- Point-to-point (RS232, RS485)

Figure 5-8 SIMATIC ET 200MP distributed I/O system - Properties and functions

5.2 Configuration

5.2.1 Configuration of the SIMATIC S7-1500 Automation System

Configuration

The SIMATIC S7-1500 automation system is made up of the following components:

- CPU (standard, fail-safe, compact or technology CPU)
- Digital and analog I/O modules
- Communications modules (PROFINET/Ethernet, PROFIBUS, point-to-point)
- Technology modules (counting, position detection, time-based IO)
- Load current supply
- System power supply (optional)

You install the S7-1500 automation system on a mounting rail. You can install up to 32 modules (CPU, system power supply and 30 I/O modules) on the mounting rail. You connect the modules to each other with U connectors.

Configuration example
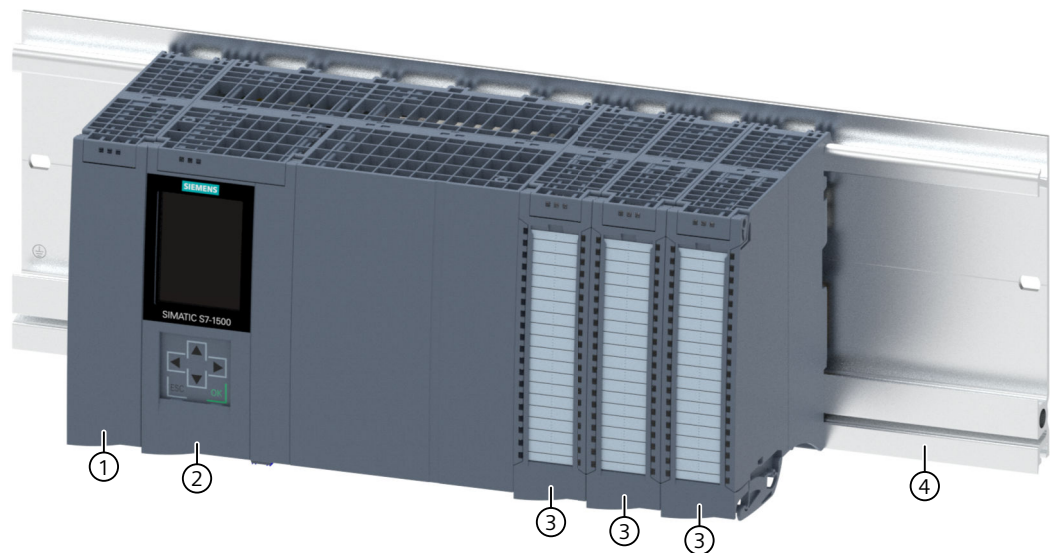
① System power supply
② CPU
③ I/O modules
④ Mounting rail with integrated DIN rail profile

Figure 5-9 Example configuration of an S7-1500 automation system

5.2.2 Configuration of the distributed I/O system SIMATIC ET 200MP

Configuration

The SIMATIC ET 200MP distributed I/O system is made up of the following components:

- Interface module (PROFINET or PROFIBUS)
- Digital and analog I/O modules
- Communications modules (point-to-point)
- Technology modules (counting, position detection, time-based IO)
- System power supply (optional)

The ET 200MP distributed I/O system is installed on a mounting rail like the S7-1500 automation system.
The I/O modules of the SIMATIC ET 200MP distributed I/O system can be used in a decentralized configuration (with an ET 200MP interface module) or in a centralized configuration (with an S7-1500 CPU).

Example of a configuration with the IM 155-5 PN ST interface module
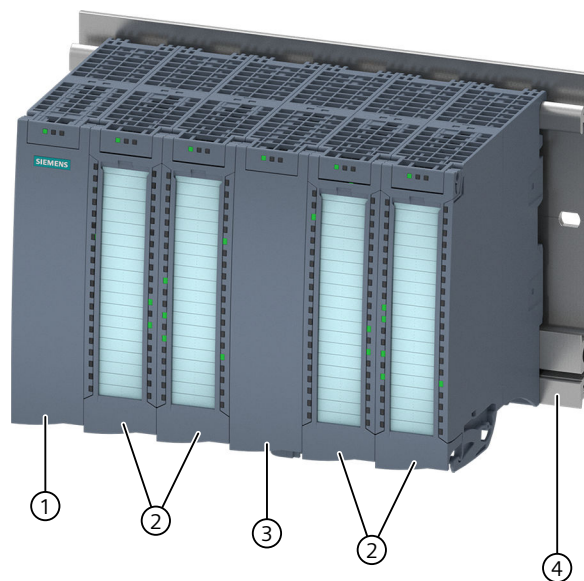
①   Interface module
②   I/O modules
③   System power supply
④   Mounting rail with integrated DIN rail profile

Figure 5-10   Example of a configuration of the ET 200MP with IM 155-5 PN ST

Example of a configuration with the IM 155-5 DP ST interface module
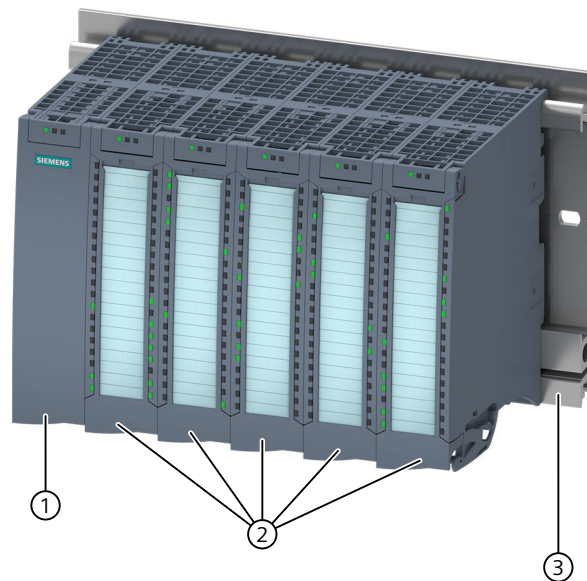
①   Interface module

②   I/O modules

③   Mounting rail with integrated DIN rail profile

Figure 5-11 Example of a configuration of the ET 200MP with IM 155-5 DP ST

5.2.3   Configuration of a fail-safe system with SIMATIC S7-1500

Fail-safe automation systems

Fail-safe automation systems (F-systems) are used in systems with higher safety requirements. F-systems control processes and ensure that they are in a safe state immediately after shutdown. In other words, F-systems control processes in which an immediate shutdown does not endanger persons or the environment.

Safety Integrated

Safety Integrated is the integrated safety concept for automation and drive technology from Siemens.

Proven technologies and systems from automation technology, such as SIMATIC S7-1500 in this case, are used for safety systems. Safety Integrated includes the complete safety sequence, ranging from sensor, actuator and fail-safe modules right through to the controller, including safety-related communication via standard fieldbuses. Drives and controllers handle safety tasks in addition to their actual functions.

SIMATIC Safety F-system with S7-1500 and ET 200MP

The figure below contains an example of an F-system SIMATIC Safety with S7-1500, ET 200MP, and PROFINET IO.

You can combine fail-safe I/O modules and non-fail-safe I/O modules in a can be combined in a S7-1500/ET 200MPconfiguration.

The fail-safe IO controller (F-CPU) exchanges:

- Safety-related data with fail-safe modules.

- Non-safety-related data with non-fail-safe modules.
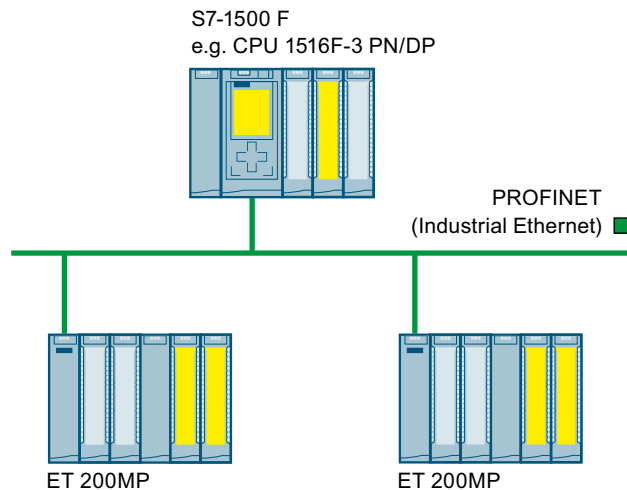
Figure 5-12 Fail-safe automation system SIMATIC Safety (example)

Fail-safe I/O modules S7-1500/ET 200MP

The following fail-safe I/O modules are available for S7-1500/ET 200MP:

- Fail-safe digital input modules detect the signal states of safety-related sensors and send the relevant safety frames to the F-CPU.

- Fail-safe digital output modules control actuators for safety-oriented tasks.

Configuration example of the ET 200MP with fail-safe I/O modules
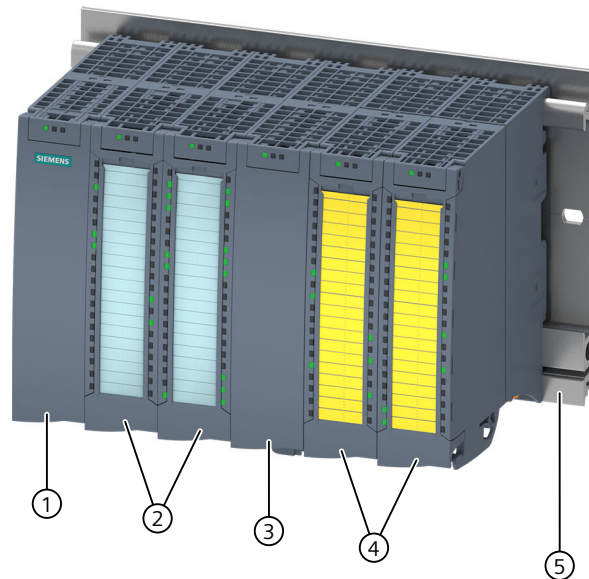
①   Interface module
②   I/O modules
③   Power supply (optional)
④   Fail-safe I/O modules
⑤   Mounting rail with integrated DIN rail profile

Figure 5-13   Configuration example of the ET 200MP with fail-safe I/O modules

Hardware and software requirements

You use the S7-1500/ET 200MP fail-safe I/O modules:

- In S7-1500 with S7-1500 F-CPUs as of firmware version V1.7

- Distributed in ET 200MP with S7-1500 F-CPUs as of firmware version V1.5 and all F-CPUs that can be selected in the hardware catalog of the TIA Portal

Fail-safe I/O modules in ET 200MP require the following interface modules:

- IM 155-5 PN BA, as of firmware version V4.3

- IM 155-5 PN ST, as of firmware version V3.0.0

- IM 155-5 PN HF, as of firmware version V3.0.0

- IM 155-5 DP ST, as of firmware version V3.0.0

To configure and program fail-safe I/O modules S7-1500/ET 200MP , you need:

- STEP 7, V13 SP1 or higher

- Option package STEP 7 Safety Advanced as of V13 SP1 + HSP0086

Use in safety mode only

You can only use the S7-1500/ET 200MP fail-safe I/O modules in safety mode. They cannot be used in non-fail-safe mode, i.e. standard mode.

Achievable safety classes

Fail-safe I/O modules are equipped with integrated safety functions for safety mode.

You can achieve the safety classes of the table below:

- By corresponding parameter assignment of the safety functions in STEP 7
- With a specific combination of fail-safe and non-fail-safe I/O modules as well as
- With a special arrangement and wiring of the sensors and actuators

Table 5-1 Safety classes that can be achieved with S7-1500/ET 200MP in safety mode

Safety class in safety mode		
According to IEC 61508:2010	According to ISO 13849-1:2015	
SIL3	Category 3	(PL) Performance Level d
SIL3	Category 4	(PL) Performance Level e

More information

An overview of the technical specifications of the fail-safe I/O modules can be found in section Fail-safe digital modules (Page 124).

The applications and wiring for the particular safety class are described in the manuals of the fail-safe I/O modules.
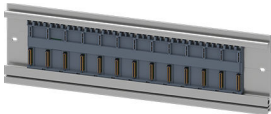
5.3 Components

Components of the S7-1500 automation system/ET 200MP distributed I/O system

Table 5-2 Components S7-1500/ET 200MP

Components	Function	Diagram
Mounting rail	The mounting rail is the module rack of the SIMATIC S7-1500/ET 200MP automation system. You can use the entire length of the mounting rail (marginless assembly). The mounting rails can be ordered as Accessories/spare parts (Page 425) accessories.	
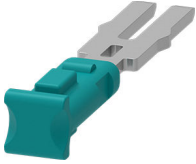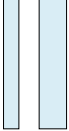
* Additionally the PS 60W 24/48/60V DC HF keeps the complete work memory of the CPU retentive.

Components	Function	Diagram
DIN-rail adapter	The SIMATIC S7-1500/ET 200MP automation system is installed on a standard 35 mm DIN rail using the DIN-rail adapter. The DIN-rail adapter can be ordered as an accessory/spare part (Page 425).	
Active backplane bus	Properties of the active backplane bus: • Reaction-free pulling and plugging of I/O modules during operation • Reserve capacity for later use The active backplane bus can be used with the following interface modules: • IM 155-5 PN HF (6ES7155-5AA00-0AC0 as of firmware version V4.4) • IM 155-5 MF HF (6ES7155-5MU00-0CN0 as of firmware version V5.0) You can find more information on the active backplane bus (e.g. installing, configuring, technical specifications) in the Active backplane bus (https://support.industry.siemens.com/cs/de/de/view/109778694/en) Equipment Manual. The active backplane bus can be ordered as an accessory/spare part (Page 425).	
PE connection element for mounting rail	The set of screws is threaded into the mounting rail's T-profile groove, and is required for grounding the mounting rail. The set of screws is contained in the scope of delivery of the mounting rails in the standard lengths (160 to 830 mm) and can be ordered as Accessories/spare parts (Page 425).	
CPU (standard, fail-safe, compact or technology CPU)	The CPU executes the user program. The integrated system power supply of the CPU supplies the modules used via the backplane bus. Further features and functions of the CPU: • Communication via Ethernet • Communication via PROFIBUS/PROFINET • HMI communication • Integrated web server • OPC UA server • OPC UA client • Integrated technology (e.g. motion control functions, trace functionality) • Integrated system diagnostics • Integrated protection functions (access, know-how and copy protection) • Safety mode (when using fail-safe CPUs)	

* Additionally the PS 60W 24/48/60V DC HF keeps the complete work memory of the CPU retentive.

Components	Function	Diagram
Interface module for PROFINET IO	The interface module: • Is used as an IO device on PROFINET IO. • Links the ET 200MP distributed I/O system with the IO controller. • Exchanges data with the I/O modules via the backplane bus. • Can be used with the BusAdapters of the ET 200SP (only IM 155-5 MF HF).	
Interface module for PROFIBUS DP	The interface module: • Is used as a DP Device on PROFIBUS DP. • Links the ET 200MP distributed I/O system with the DP master. • Exchanges data with the I/O modules via the backplane bus.	
I/O module/ fail-safe I/O module	The I/O modules form the interface between the controller and the process. The controller detects the current process state via the connected sensors and actuators, and triggers the corresponding reactions. I/O modules are divided into the following module types: • Digital input (DI, F-DI) • Digital output (DQ, F-DQ) • Digital input/digital output (DI/DQ) • Analog input (AI) • Analog output (AQ) • Analog input/analog output (AI/AQ) • Technology module (TM) • Communication module (CM) • Communication processor (CP) A U connector is included in the scope of delivery for each I/O module. For fail-safe I/O modules, an additional electronic coding element for saving the PROFIsafe address is included in the scope of delivery and can be ordered as spare part Accessories/spare parts (Page 425).	
U connector	The individual modules are connected to one another with the U connector. The U connector provides the mechanical and electrical connection between the modules. The U connector is included in the scope of delivery of all modules (exceptions: CPU, interface module) and can be ordered as Accessories/spare parts (Page 425).	
Front connectors	The front connectors are used to wire the I/O modules. The front connectors for technology and analog modules must be supplemented with a shielding bracket, power supply element, and shield connection clamp. The components are included in the scope of delivery of the technology modules, analog modules and compact CPUs (for onboard I/O) and can be ordered as Accessories/spare parts (Page 425) accessories. There are front connectors with screw terminals and push-in terminals for 35 mm modules, and with push-in terminals for 25 mm modules. The front connectors for 25 mm modules are included in the scope of delivery of the I/O modules and compact CPUs (for onboard I/O). Four potential bridges and one cable tie are included in the scope of delivery of the front connectors for 35 mm modules. The front connect-	

Components	Function	Diagram
	ors for 25 mm modules have no potential bridges due to the compact module design.	
Potential bridges for front connector	You jumper two terminals with potential bridges. The potential bridges are included in the scope of delivery of the front connector and can be ordered as Accessories/spare parts (Page 425). The front connectors for 25 mm modules have no potential bridges. Therefore, you should also observe the information in the product manual for the respective digital or analog module.	
Shielding bracket	The shielding bracket is an insertable bracket for modules with EMC-critical signals (e.g. analog modules, technology modules), and, together with the shield connection clamp, permits the low impedance application of shielding with minimal installation times. The shielding bracket is included in the scope of delivery of the analog modules, technology modules, and compact CPUs (for onboard I/O) and can be ordered as Accessories/spare parts (Page 425).	
Shield clamp	The shield connection clamps are used to attach cable shielding to the shielding bracket. The shield connection clamp is included in the scope of delivery of the analog modules, technology modules, and compact CPUs (for onboard I/O) and can be ordered as Accessories/spare parts (Page 425).	
Power supply element	The power supply element is inserted in the front cable connector, and serves to supply power to modules with EMC-critical signals (analog modules, technology modules). The power supply element (connection technology: screw terminal) is included in the scope of delivery of the analog and technology modules and can be ordered as Accessories/spare parts (Page 425).	
Labeling strips for the exterior of the front cover of the I/O modules	The labeling strips are used to label the modules for specific plants. You can label the labeling strips using a machine. The labeling strips are available in different colors: • Al gray: Non-fail-safe modules • Yellow: Fail-safe modules The labeling strips are included in the scope of delivery of the I/O modules and compact CPUs (for onboard I/O). Additional labeling strips can be ordered as Accessories/spare parts (Page 425).	

* Additionally the PS 60W 24/48/60V DC HF keeps the complete work memory of the CPU retentive.

Components	Function	Diagram
4-pole connection plug for supply voltage of the CPU/interface module	The supply voltage is supplied by means of the 4-pole connection plug.	
System power supply (PS)	The system power supply is a diagnostics-capable power supply module, that can be connected with the backplane bus using a U connector. A system power supply is required when the power fed from the CPU/interface module into the backplane bus is not sufficient to supply the connected modules with power. System power supplies are available in various models: • PS 25 W 24 V DC • PS 60 W 24/48/60 V DC • PS 60W 24/48/60V DC HF* • PS 60 W 120/230 V AC/DC A power cable connector with coding element and U connector is included in the scope of delivery of the system power supply and may be ordered as spare part.	
Load current supply (PM)	The load current supply (PM) supplies the system power (PS), central modules (CPU), interface module and input and output circuits of the I/O modules with 24 V DC. If you are using load current supplies, we recommend the devices from our SIMATIC series. These devices can be mounted on the mounting rail. Load current supplies are available in various models: • PM 70 W 120/230 V AC • PM 190 W 120/230 V AC As an alternative to the SIMATIC load current supplies (PM), you can also use SITOP smart power supplies. Use of a SITOP smart power supply is recommended in these cases, among others: • Higher power requirement • Redundancy • Uninterruptible power supply For more information on the SITOP modules, refer to an FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/96998532).	

* Additionally the PS 60W 24/48/60V DC HF keeps the complete work memory of the CPU retentive.

Reference

You can find more information on the different function classes (for example, basic, standard) of the interface and I/O modules in an FAQ on the Internet (https://support.industry.siemens.com/cs/de/de/view/109476914/en).

5.4 CPUs

Figure 5-14 Controller

SIMATIC S7-1500 controllers are characterized by maximum performance capability thanks to a high-performance backplane bus, very short terminal-to-terminal response time and extremely fast signal processing.

The controller (CPU) executes the user program. The integrated system power supply of the controller provides power to the modules used through the backplane bus.

A fail-safe version is available for each SIMATIC S7-1500 controller (except compact CPUs and the redundant CPU 1513R-1 PN and CPU 1515R-2 PN). To use the safety functions in the TIA Portal, you need the "STEP 7 Safety Advanced" option package.

During commissioning of the plant you can, for example, change the IP address of the CPU directly via the display, thus saving time and costs. In the event of a service call, the plant downtimes are minimized by quick access to diagnostics alarms.

For effective commissioning and fast optimization of drives and controls, the SIMATIC S7-1500 supports extensive trace functions for all CPU tags.

A SIMATIC S7-1500 controller also offers additional functions:

- Communication via Ethernet/PROFINET
- Communication via PROFIBUS
- HMI communication
- Communication via OPC UA
- Web server, technology functions, system diagnostics, protection functions integrated
- When using an F-CPU: Safety mode
- When using a S7-1500 R/H CPU: Redundancy
- When using a T-CPU: Extended motion control functions

5.4.1 What can you do with the CPU?

SIMATIC S7-1500 provides you with a variety of CPUs that can be integrated. You can expand each CPU with I/O, communications and technology modules.

Example: The performance of a CPU 1511-1 PN with 1.5 MB data work memory is sufficient for your application. If you require additional communication interfaces, you can extend the CPU with communication modules for Industrial Ethernet, PROFINET and PROFIBUS. Modules for serial communication are also available.

The following overview supports you in selecting the CPU and shows the respective maximum size of the data work memory:
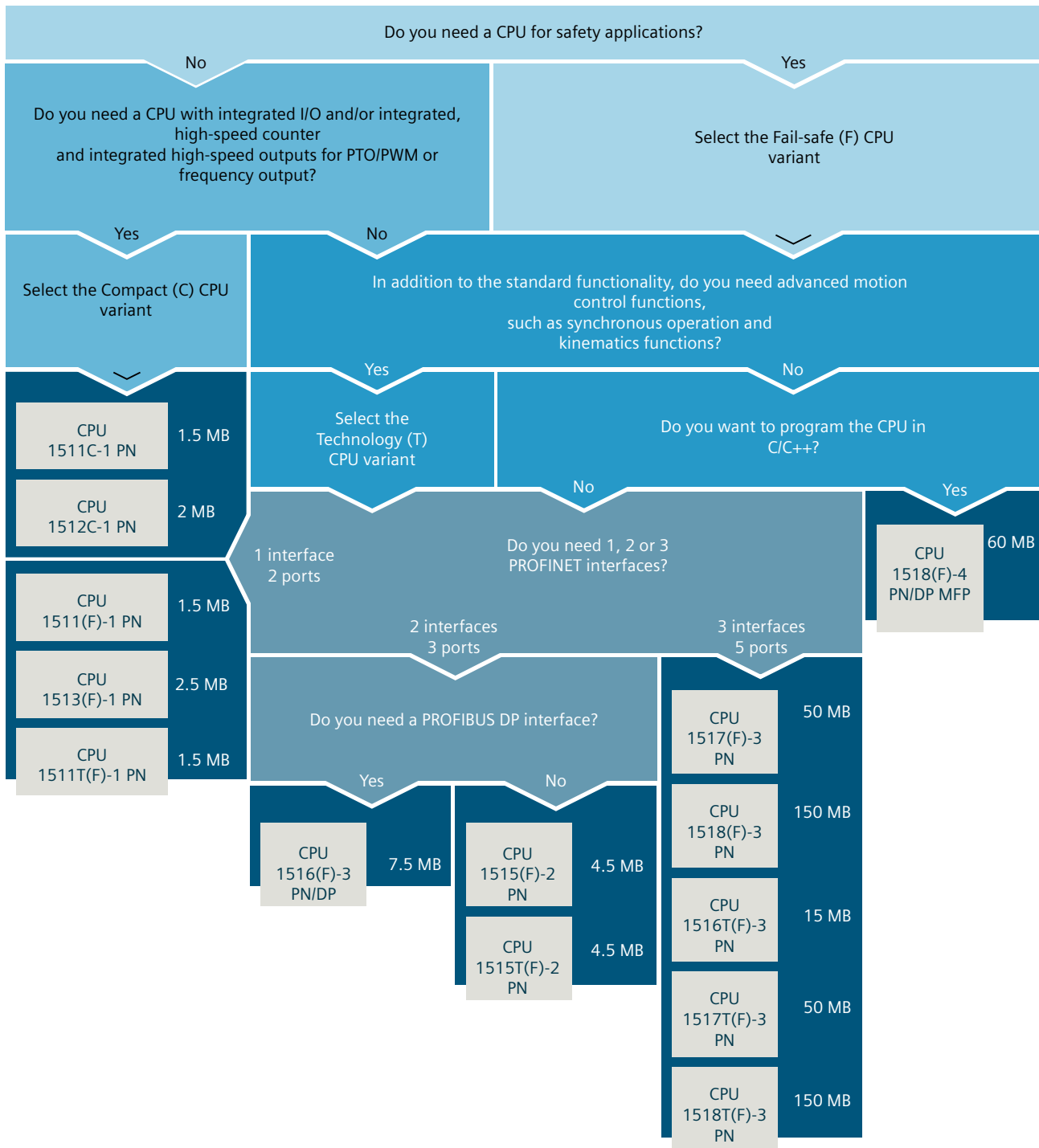
Figure 5-15   Selection guide for CPUs

5.4.2 Technical specifications of CPUs

Table 5-3 Standard CPUs and F-CPUs

CPU	1511-1 PN 1511F-1 PN 1511T-1 PN 1511TF-1 PN	1513-1 PN 1513F-1 PN	1515-2 PN 1515F-2 PN 1515T-2 PN 1515TF-2 PN	1516-3 PN/DP 1516F-3 PN/DP	1517-3 PN 1517F-3 PN	1518-3 PN 1518F-3 PN 1518T-3 PN 1518TF-3 PN
				1516T-3 PN 1516TF-3 PN	1517T-3 PN 1517TF-3 PN	1518-4 PN/DP M-FP 1518F-4 PN/DP MFP
Article number						
Standard CPU:	6ES7511-1AL03-0AB0 (https://mall.industry.siemens.com/mall/de/de/-Catalog/Product/6ES7-511-1AL03-0AB0)	6ES7513-1AM0-3-0AB0 (https://mall.industry.siemens.com/mall/en/de/-Catalog/Product/6ES-7513-1AM03-0-AB0)	6ES7515-2AN03-0AB0 (https://mall.industry.siemens.com/mall/en/de/C-atalog/Product/6ES7-515-2AN03-0AB0)	6ES7516-3AP03-0AB0 (https://mall.industry.siemens.com/mall/en/de/-Catalog/Product/6ES-7516-3AP03-0A-B0)	6ES7517-3AQ10-0AB0 (https://mall.industry.siemens.com/mall/en/us/Ca-talog/Product/6ES-7517-3AQ10-0AB0)	6ES7518-3AT10-0AB0 (https://mall.industry.siemens.com/mall/en/us/C-atalog/Product/6ES7-518-3AT10-0AB0)
F-CPU	6ES7511-1FL03-0AB0 (https://mall.industry.siemens.com/mall/en/de/-Catalog/Product/6ES7-511-1FL03-0AB0)	6ES7513-1FM0-3-0AB0 (https://mall.industry.siemens.com/mall/en/de/-Catalog/Product/6ES-7513-1FM03-0A-B0)	6ES7515-2FN03-0AB0 (https://mall.industry.siemens.com/mall/en/de/C-atalog/Product/6ES7-515-2FN03-0AB0)	6ES7516-3FP03-0AB0 (https://mall.industry.siemens.com/mall/en/de/-Catalog/Product/6ES-7516-3FP03-0AB-0)	6ES7517-3FQ10-0-AB0 (https://mall.industry.siemens.com/mall/en/us/Ca-talog/Product/6ES-7517-3FQ10-0AB0)	6ES7518-3FT10-0-AB0 (https://mall.industry.siemens.com/mall/en/us/C-atalog/Product/6ES7-518-3FT10-0AB0)
T-CPU	6ES7511-1TL03-0AB0 (https://mall.industry.siemens.com/mall/en/en/-Catalog/Product/6ES7-511-1TL03-0AB0)	---	6ES7515-2TN03-0AB0 (https://mall.industry.siemens.com/mall/en/en/C-atalog/Product/6ES7-515-2TN03-0AB0)	6ES7516-3TP10-0AB0 (https://mall.industry.siemens.com/mall/en/us/-Catalog/Product/6ES-7516-3TP10-0AB-0)	6ES7517-3TQ10-0-AB0 (https://mall.industry.siemens.com/mall/en/us/Ca-talog/Product/6ES-7517-3TQ10-0AB0)	6ES7518-3TT10-0-AB0 (https://mall.industry.siemens.com/mall/en/us/C-atalog/Product/6ES7-518-3TT10-0AB0)
TF-CPU	6ES7511-1UL03-0AB0 (https://mall.industry.siemens.com/mall/en/de/-Catalog/Product/6ES7-511-1UL03-0AB0)	---	6ES7515-2UN03-0AB0 (https://mall.industry.siemens.com/mall/en/de/C-atalog/Product/6ES7-515-2UN03-0AB0)	6ES7516-3UP10-0AB0 (https://mall.industry.siemens.com/mall/en/us/-Catalog/Product/6ES-7516-3UP10-0A-B0)	6ES7517-3UQ10-0AB0 (https://mall.industry.siemens.com/mall/en/us/Ca-talog/Product/6ES-7517-3UQ10-0AB0)	6ES7518-3UT10-0AB0 (https://mall.industry.siemens.com/mall/en/us/C-atalog/Product/6ES7-518-3UT10-0AB0)
CPU 1518 MFP	---	---	---	---	---	6ES7518-4AX00-1AB0 (https://mall.industry.siemens.com/mall/en/de/C-atalog/Product/6ES7-518-4AX00-1AB0)

CPU	1511-1 PN 1511F-1 PN 1511T-1 PN 1511TF-1 PN	1513-1 PN 1513F-1 PN	1515-2 PN 1515F-2 PN 1515T-2 PN 1515TF-2 PN	1516-3 PN/DP 1516F-3 PN/DP 1516T-3 PN 1516TF-3 PN	1517-3 PN 1517F-3 PN 1517T-3 PN 1517TF-3 PN	1518-3 PN 1518F-3 PN 1518T-3 PN 1518TF-3 PN 1518-4 PN/DP M-FP 1518F-4 PN/DP MFP
CPU 1518F MFP	---	---	---	---	---	6ES7518-4FX00--1AB0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7-518-4AX00-1AB0)
Equipment Manual						
Standard CPU:	↓ (https://support.industry.siemens.com/cs/ww/en/view/109752841)	↓ (https://support.siemens.com/cs/ww/en/view/109752842)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109767406)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109767407)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109963203)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109963204)
T-CPU	↓ (https://support.industry.siemens.com/cs/ww/en/view/109739188)	---	↓ (https://support.industry.siemens.com/cs/ww/en/view/109739189)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109963205)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109963206)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109963207)
CPU 1518 MFP	---	---	---	---	---	↓ (https://support.industry.siemens.com/cs/ww/en/view/109749061)
F-CPU	↓ (https://support.industry.siemens.com/cs/de/en/view/109478599)					
Supply voltage, permissible range of all the CPUs 19.2 V DC ... 28.8 V DC						
Code work memory						
Standard CPU:	300 KB	600 KB	1 MB	2 MB	4 MB	12 MB
T-CPU	450 KB	---	1.5 MB	6 MB	6 MB	18 MB
F-CPU	450 KB	900 KB	1.5 MB	6 MB	6 MB	18 MB
TF-CPU	450 KB	---	1.5 MB	6 MB	6 MB	18 MB
MFP-CPU	---					6 MB
FMFP-CPU	---					9 MB
Data work memory	1.5 MB	2.5 MB	4.5 MB	7.5 MB 25 MB	50 MB	150 MB 60 MB
Processing times						
Bit operations	6 ns	6 ns	6 ns	6 ns 1.2 ns	0.6 ns	0.3 ns 1 ns
Word operations	7 ns	7 ns	7 ns	7 ns 2.6 ns	1.3 ns	0.8 ns 2 ns

CPU	1511-1 PN 1511F-1 PN 1511T-1 PN 1511TF-1 PN	1513-1 PN 1513F-1 PN	1515-2 PN 1515F-2 PN 1515T-2 PN 1515TF-2 PN	1516-3 PN/DP 1516F-3 PN/DP 1516T-3 PN 1516TF-3 PN	1517-3 PN 1517F-3 PN 1517T-3 PN 1517TF-3 PN	1518-3 PN 1518F-3 PN 1518T-3 PN 1518TF-3 PN 1518-4 PN/DP M-FP 1518F-4 PN/DP MFP
Integrated interfaces						
PROFINET I-O	1	1	2	2	2	2
PROFINET	---	---	---	--- 1	1	1
Number of PROFINET ports	2	2	3	3 5	5	5 4
PROFIBUS DP	---	---	---	1 ---	---	--- 1
Technology						
Motion control resources*	1120	1120	2400	2400 12800	20480	30720 15380
Typical number of positioning axes (at 4 ms servo/IPO cycle)	5	5	7	110 11	70 T(F)-CPU: 140	1518(F): 140 1518T(F): 280 140
Extended motion control resources (T-CPUs only)	90	---	120	540	720	1560 512
Max. number of positioning axes	14	14	30	30	128	128
Additional functions						
Isochronous mode	Centralized and distributed	Centralized and distributed	Centralized and distributed	Centralized and distributed	Centralized and distributed	Centralized and distributed
Web server	X	X	X	X	X	X

* See Motion Control (Page 138) section

Table 5-4 Compact CPUs

Controller	1511C-1 PN	1512C-1 PN
Article number	6ES7511-1CL03-0AB0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7511-1-1CL03-0AB0)	6ES7512-1CM03-0AB0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7512-2-1CM03-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/109963074)	↓ (https://support.industry.siemens.com/cs/de/en/view/109963073)
Supply voltage, permissible range	19.2 V DC to 28.8 V DC	19.2 V DC to 28.8 V DC
Code work memory	300 KB	400 KB
Data work memory	1.5 MB	2 MB
Processing time for bit operations	6 ns	6 ns
Processing time for Word operations	7 ns	7 ns
PROFINET interfaces	1	1
Number of PROFINET ports	2	2
Integrated analog inputs/outputs	5 inputs/2 outputs	5 inputs/2 outputs
Integrated digital inputs/outputs	16 inputs/16 outputs	32 inputs/32 outputs
Technology		
Motion control resources*	1120	1120
Typical number of positioning axes (at 4 ms servo/IPO cycle)	5	5
Max. number of positioning axes	10	10
Isochronous mode	Distributed	Distributed
High-speed counters	6 (max. 100 kHz)	6 (max. 100 kHz)
Frequency meter	6 (max. 100 kHz)	6 (max. 100 kHz)
Period duration measurement	6 channels	6 channels
Pulse generators (pulse width modulation, Pulse Train Output, frequency output)	4	4
Web server	X	X

* See Motion Control (Page 138) section

Code work memory: Volatile memory that contains runtime-relevant parts of the program code.

Data work memory: Volatile memory that contains the runtime-relevant parts of the data blocks and technology objects.

5.4.3 Web server

The SIMATIC S7-1500 CPUs have an integrated web server.

You can display the CPU status without additional software installation via a web browser and control it to a limited extent. Graphically visualized process variables and user-defined websites facilitate information acquisition and diagnostics of plant states.

Figure 5-16 Home page web server

Example: Web server simplifies maintenance of treatment plants

Automation task:

Implementation of a user interface for fault management of a treatment plant.

Feature:

Treatment plants operate fully automatically, they are not manned. The operator optionally receives an SMS if a fault occurs. For diagnostics, the operator directly accesses the corresponding web sites.

Solution:

Creation of user sites for the web server of a SIMATIC S7-1500 CPU. The customer can make changes to the web sites himself, e.g. the mobile number for the SMS messages, settings in the CPU or the message texts.

Benefits

The web server provides you with the following advantages:

- Access via web browsers to a SIMATIC S7-1500 with plant-relevant operating data
- Display of service and diagnostics information over large distances
- Access restrictions for unauthorized users

Additional information

A detailed description of handling the web server can be found in the Function Manual "SIMATIC S7-1500 web server" SIMATIC S7-1500 Web server (https://support.industry.siemens.com/cs/de/en/view/59193560).

5.4.4 Safety

For fail-safe operation of your plant, program the F-CPUs of the SIMATIC S7-1500. Use the "STEP 7 Safety Advanced" option package of the TIA Portal for this purpose. In combination with the TIA Portal, the F-CPUs offer optimal integration of fail-safe systems into your engineering environment; one controller, one communication system, and one engineering platform for standard and fail-safe automation:

- Integration of safety technology
- Instructions approved by German Technical Inspectorate for frequently required safety applications
- Integration of safety-related functions up to SIL 3 according to IEC 61508:2010 or PL e and category 4 according to ISO 13849-1:2015 or according to EN ISO 13849-1:2015
- Uniform engineering for standard and safety automation
- Simple documentation of safety-related changes via the F-change history in STEP 7 Safety
- Support in the acceptance of the safety program and no renewed acceptance of the safety program after changes in the standard program

Example: Production cell with access protection

Automation task:

A laser scanner monitors access to a production area. The maintenance area is secured by a protective door. Entering the production area or opening the protective door, just like an emergency stop, results in the shutdown or stopping of the production cell.
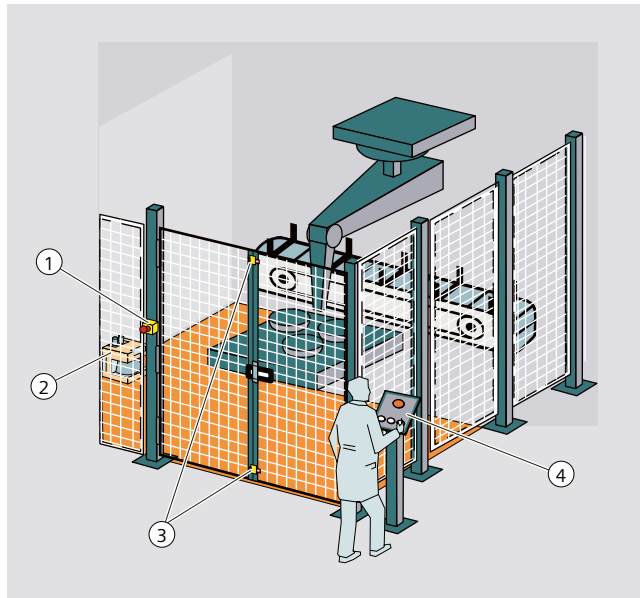
①   Emergency stop

②   Laser scanner

③   Protective door

④   Control panel with start and acknowledgment key

Figure 5-17 Production cell with access protection

Feature:

Start-up of the system is only possible with unlocked emergency stop, closed protective door and free protection area of the laser scanner. After activating the emergency stop, opening the protective door or addressing the protection area, a user acknowledgement is required to restart production operations again. Access protection to the F-CPU and the safety program is essential for productive operation.

Solution:

Use of a SIMATIC S7-1500 F-CPU with fail-safe modules in the distributed I/O system ET 200SP on the PROFINET IO.

The F modules ET 200SP take over the connections for emergency stop, monitoring of the protective door, monitoring of the access area, the motor and the user acknowledgment. Perform the relevant programming in STEP 7. The safety program runs in the CPU.

Benefits

SIMATIC Safety Integrated provides you with the following advantages:

- Engineering with SIMATIC STEP 7 Safety Advanced in the TIA Portal, same engineering and operating concept for standard and fail-safe automation task

- Use of instructions approved by the German Technical Inspectorate from the system library Safety in the safety program, e.g. for protective door, emergency stop, monitored feedback loop circuit and user acknowledgment, saves time and reduces the error rate

- Simple connections of PROFIsafe devices via PROFINET and PROFIBUS

- Additional password protection for F-CPU and safety program is set up for IT security.

- Integration in integrated system diagnostics

Additional information

A detailed description of the topic "Safety Integrated" is available in the programming and operating manual SIMATIC Safety - Configuring and Programming SIMATIC Safety - Configuration and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126).

5.4.5 Diagnostics

Integrated diagnostics across all levels of the automation is incorporated in the SIMATIC S7-1500 automation system. All SIMATIC products have integrated diagnostic functions which you can use to analyze and localize faults and errors efficiently. This reduces the commissioning periods required and minimizes standstill times in production.

A uniform display concept ensures that error messages in the STEP 7, on the HMI, the Web server and in the display of the CPU are visualized identically as plain text information.

You can optionally configure machine and plant diagnostics. This means that the logic of these process diagnostic messages or monitoring depends directly on the state of the plant and is defined by you.
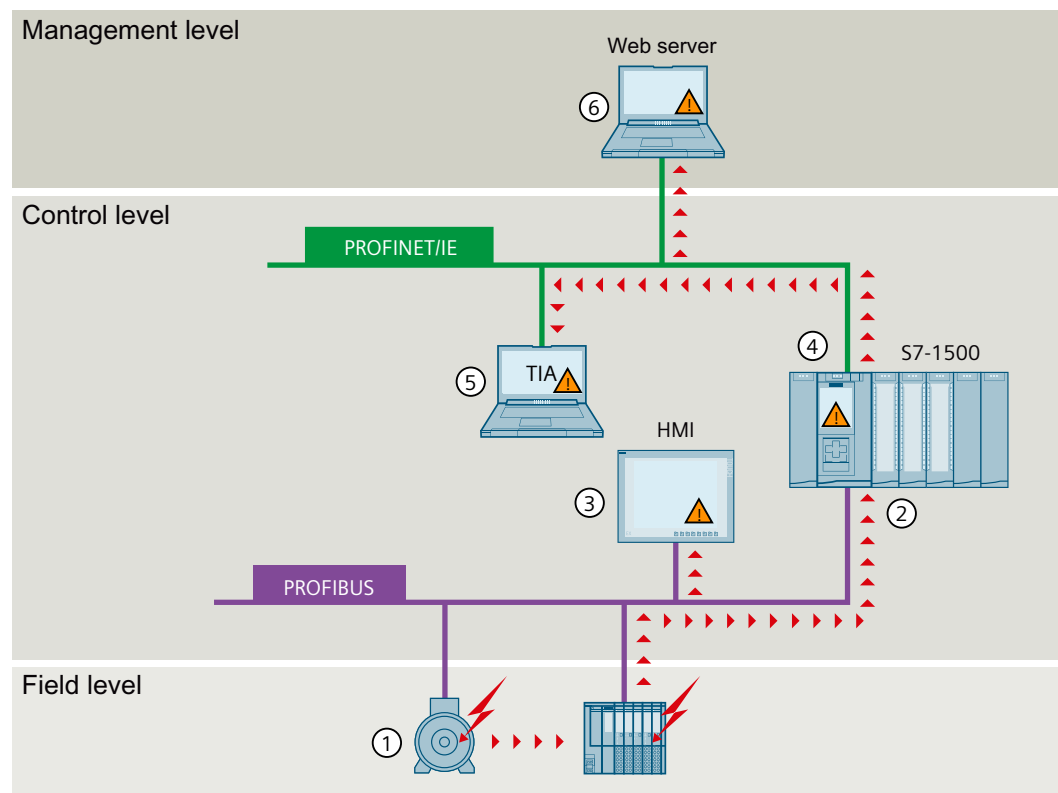
①	Monitoring functions are integrated in the hardware as standard.
②	Diagnostics is implemented system-wide across bus limits.
③	Output of the cause of the error in plain text, archiving and logging of alarms
④	Automatic localization of the error source
⑤	Configurability of alarms
⑥	Plant-wide, uniform display of system status

Figure 5-18 *Display of diagnostic information*

Faults in the plant are immediately detected and reported on the display devices, even in STOP mode. As a result, system diagnostics is always consistent with the actual state of the plant.

Advantages and customer benefits

Integrated system diagnostics offers the following advantages:

- Diagnostics is always consistent with the actual state of the plant. The system diagnostics also works in the STOP mode of the CPU.

- The uniform display concept enables efficient error analysis.

- The immediate identification of the error source in the event of an error speeds up commissioning and minimizes production downtimes.

- By configuring diagnostics events, you tailor the diagnostics to the requirements of your automation task.

5.4.6 Trace

for effective commissioning and optimization of drives and closed-loop controls, the SIMATIC S7-1500 CPUs feature integrated trace functionality. The trace function records the CPU tags, depending on the settable trigger conditions. Tags are, for example, drive parameters or system and user tags of a CPU. You can display and evaluate the saved recordings with STEP 7.

By visualizing the entire process with real-time trace, you identify, for example, sporadic events in the system during commissioning and service.
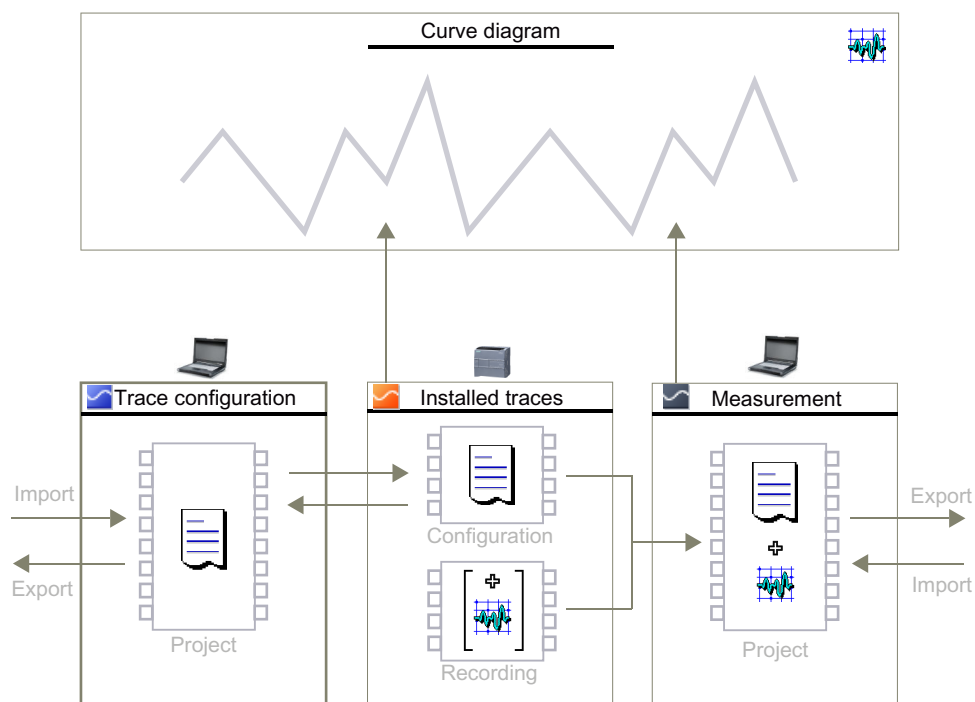
Figure 5-19 Schematic overview

Example: Trace optimizes the commissioning of packaging machines

Automation task:

At what speed does a plant reach its maximum productivity? How do you quickly determine the optimum settings?

The packaging machine ensures quick and reliable packaging of ECG electrodes on a rotary table which is loaded and unloaded by a conveyor belt.

Feature:

After filling is the correct time for further transport of the packaged electrodes. Light barriers trace the position of the electrodes for this.

Solution:

The Trace function of a SIMATIC S7-1500 CPU visualizes the exact sequence of selected signals over a short period of time. It supports the start-up engineer in finding the exact light barrier positions and the optimum speed for belts and the rotary table.

The trace recordings are supplied to the customer as part of the plant project. In the event of a fault, the customer recognizes whether changes to the basic settings have caused the fault.

In addition, the trace recordings are stored as a "measurement" on the SIMATIC memory card, up to 999 trace recordings are available for evaluation.

Advantages and customer benefits

The Trace function provides you with the following advantages:

- Cost-effective and easy evaluation as the signals are available in the CPU
- Monitoring of highly dynamic processes
- Up to 8 independent trace jobs simultaneously
- Recordings of individual cycles for up to 64 different tags in a .csv file over a longer period (e.g. hours, days) → Long-term trace.
- recording in separate CPU memory area for easy localization of sporadic errors
- Various trigger options
- Various zoom and cursor measuring functions
- Saving trace recordings on the SIMATIC memory card
- export of measurements, e.g. for user-specific processing

Project trace

A project trace includes trace configurations of multiple devices and records the signals across devices.

Synchronization takes place via a global trigger that can be triggered by any device. After receiving the global trigger, the devices with valid project trace configuration start the recording.

More information

You can find a detailed description of the "Trace" function in the Function Manual SIMATIC/SINAMICS Using the trace and logic analyzer function SIMATIC/SINAMICS Trace and logic analyzer function (https://support.industry.siemens.com/cs/ww/en/view/64897128).

5.5 Interface modules for SIMATIC S7-1500 I/O devices

An interface module connects the SIMATIC S7-1500 I/O devices as ET 200MP distributed I/O system via PROFINET or PROFIBUS with the controller. The interface module exchanges the data between the higher-level controller and the I/O modules.

Interface modules

Short designation	IM 155-5 MF HF	IM 155-5 PN HF IM 155-5 PN ST	IM 155-5 PN BA	IM 155-5 DP ST
Article number				
High Feature (HF)	6ES7155-5MU00-0CN0 (https://mall.industry.siemens.com/mall/en/us/Catalog/Product/6ES7155-5MU00-0CN0)	6ES7155-5AA00-0AC0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7155-5AA00-0AC0)	---	---
Standard (ST)	---	6ES7155-5AA01-0AB0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7155-5AA01-0AB0)	---	6ES7155-5BA00-0AB0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7155-5BA00-0AB0)
Basic (BA)	---	---	6ES7155-5AA00-0AA0 (https://mall.industry.siemens.com/mall/en/de/Catalog/Product/6ES7155-5AA00-0AA0)	---
Equipment Manual				
High Feature (HF)	↓ (https://support.industry.siemens.com/cs/us/en/view/109-826205)	↓ (https://support.industry.siemens.com/cs/ww/en/view/89-261636)	---	---
Standard (ST)	---	↓ (https://support.industry.siemens.com/cs/ww/en/view/59-193106)	---	↓ (https://support.industry.siemens.com/cs/ww/en/view/78-324181)
Basic (BA)	---	---	↓ (https://support.industry.siemens.com/cs/ww/de/view/10-9745036)	---
Supply voltage	24 V DC	24 V DC	24 V DC	24 V DC
Number of IO modules	30	30	12	12

Short designation	IM 155-5 MF HF	IM 155-5 PN HF IM 155-5 PN ST	IM 155-5 PN BA	IM 155-5 DP ST
Interfaces	1 x PROFINET IO; integrated 2-port switch, 2 ports via BusAdapter	1 x PROFINET IO; integrated 2-port switch	1 x PROFINET IO; integrated 2-port switch	1 x PROFIBUS
Min. slave interval	---	---	---	100 µs
Isochronous real-time communication (IRT)	X	X	---	---
Isochronous mode	---	X (shortest cycle 250 µs)	---	---
Prioritized startup	---	X	---	---
Device replacement without programming device	X (LLDP; addressing via a tool, e.g. STEP 7)	X (LLDP; address assignment by a tool, for example, STEP 7)	X (LLDP; address assignment by a tool, for example, STEP 7)	---
Shared device	4 IO controllers	High Feature: 4 IO controllers Default: 2 IO controllers	2 IO controllers	---
Identification and maintenance data	I&M 0 to 3	I&M 0 to 3	I&M 0 to 3	I&M 0 to 3
Media redundancy (MRP)	X	X	X	---
Media redundancy with planned duplication (MRPD)	X	High Feature: X Default:	---	---
System redundancy on S7-400H	with GSD file	High Feature: With GSD file and STEP 7 V5.5 SP3 or higher Default:	---	---
System redundancy in S7-1500R/H	X	High Feature: X Default:	---	---
GSD file for ET 200MP	PROFINET (https://support.industry.siemens.com/cs/ww/en/view/68-189683)	PROFINET (https://support.industry.siemens.com/cs/ww/en/view/68-189683)	PROFINET (https://support.industry.siemens.com/cs/ww/en/view/68-189683)	PROFIBUS (https://support.industry.siemens.com/cs/ww/en/view/80-206700)

5.6 Input and output modules

The I/O modules form the interface between the controller and the process. The controller detects the current process state via the connected sensors and actuators, and triggers the corresponding reactions.

Digital and analog modules provide the inputs/outputs that are required for the respective task.

The input/output modules are divided into function classes.

Function classes of input/output modules

The table below shows selected properties and technical specifications of different function classes of input/output modules.

Function class		
High Speed (HS)	Special modules for extremely fast applications Shortest input delays Shortest conversion times Isochronous mode	
High Feature (HF)	Flexible use Even for complex applications Parameters for each channel Diagnostics for each channel Add-on functions	With analog modules • Highest accuracy (< 0.1%) • High common mode voltage (e. g. 60 V DC / 30 V AC), with single-channel electrical isolation if required
Standard (ST)	Medium price range Parameter per load group / module Diagnostics per load group / module	With analog modules • Universal modules • Accuracy ≥ 0.3% • Common-mode voltage approx. 10 V to 20 V
Basic (BA)	Inexpensive, simple modules No parameters No diagnostics	

5.6.1 Which I/O devices are the correct ones?

SIMATIC S7-1500 offers a wide range of I/O modules. Depending on the complexity of your plant and the technical and functional requirements, you perform your planning flexibly and in a modular manner with SIMATIC components.
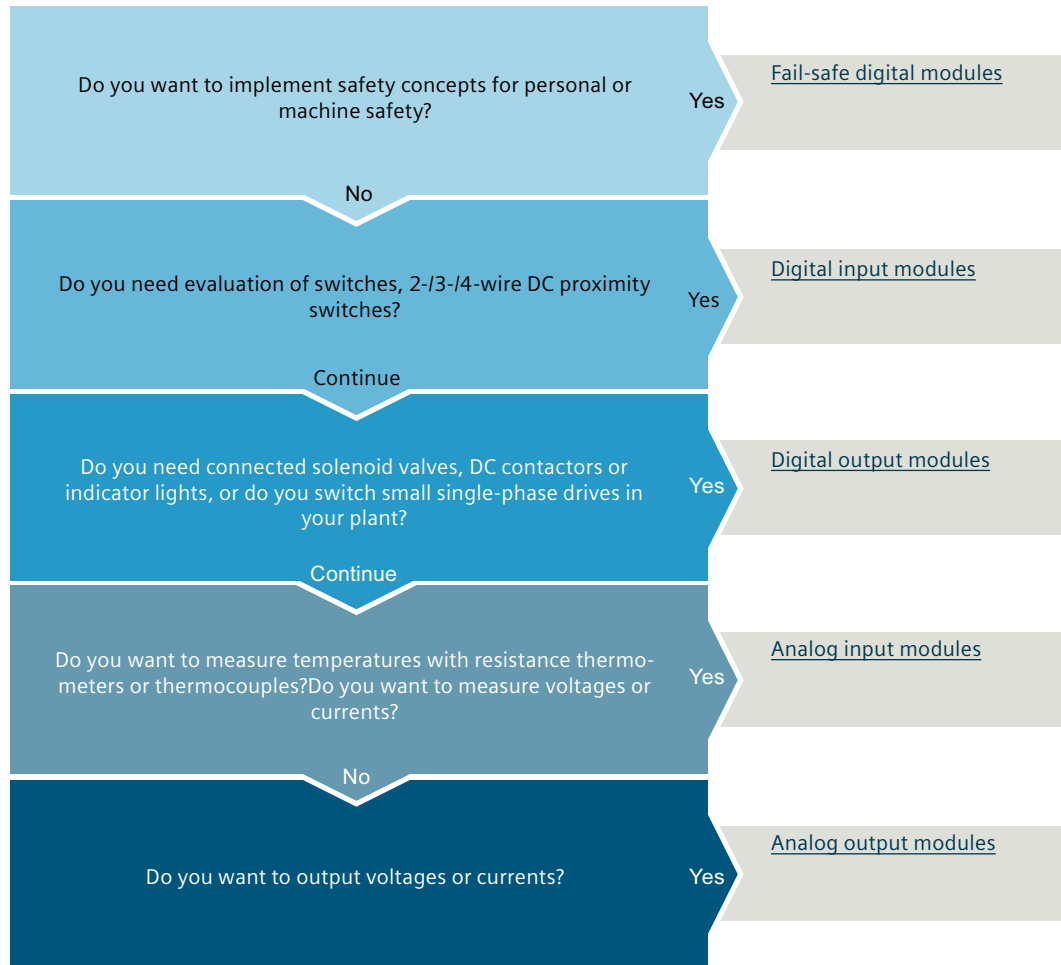
Figure 5-20 Selection guide for input/output modules

5.6.2 Digital input modules

Digital input modules

Short designation	DI 16x24VDC HF DI 16x24VDC BA	DI 32x24VDC HF DI 32x24VDC BA	DI 16x24VDC SRC BA	DI 16x24...125VUC HF
Article number				
High Feature (HF)	6ES7521-1BH00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-1B-H00-0AB0)	6ES7521-1BL00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-1BL-00-0AB0)	---	6ES7521-7EH00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-7E-H00-0AB0)

Short designation	DI 16x24VDC HF DI 16x24VDC BA	DI 32x24VDC HF DI 32x24VDC BA	DI 16x24VDC SRC BA	DI 16x24...125VUC HF
Basic (BA)	6ES7521-1BH10-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-1BH10-0AA0)	6ES7521-1BL10-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-1BL10-0AA0)	6ES7521-1BH50-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-1BH50-0AA0)	---
Equipment Manual				
High Feature (HF)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59-193001)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59-192896)	---	↓ (https://support.industry.siemens.com/cs/ww/zh/view/10-9480460)
Basic (BA)	↓ (https://support.industry.siemens.com/cs/ww/en/view/83-501190)	↓ (https://support.industry.siemens.com/cs/ww/en/view/83-499481)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59-191844)	---
Width				
High Feature (HF)	35 mm	35 mm	---	35 mm
Basic (BA)	25 mm	25 mm	35 mm	---
Number of inputs	16	32	16	16
Electrical isolation between channels	---	X	---	X
Number of potential groups	1	2	1	1
Rated input voltage	24 V DC	24 V DC	24 V DC	24 V UC to 125 V UC
Diagnostic interrupt	Only with HF	Only with HF	---	X
Hardware interrupt	Only with HF	Only with HF	---	X
Isochronous mode	Only with HF	Only with HF	---	---
Input delay				
High Feature (HF)	0.05 ms to 20 ms (configurable)		---	0.05 ms to 20 ms (configurable with DC) 20 ms (fixed at AC)
Basic (BA)	Typ. 3 ms (fixed)	Typ. 3 ms (fixed)	Typ. 3 ms (fixed)	---
Integrated counting function (Two channels can optionally be used as counter with 3 kHz)	Only with HF: Counting up to 3 kHz	Only with HF: Counting up to 1 kHz	---	---

Digital input modules

Short designation	DI 16x230VAC BA	DI 16xNAMUR HF	DI 16x24VDC HS
Article number			
High Feature (HF)	---	6ES7521-7TH00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-7TH00-0AB0)	---
Basic (BA)	6ES7521-1FH00-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-1FH00-0AA0)	---	---
High Speed (HS)	---	---	6ES7521-7BH00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7521-7BH00-0AB0)
Equipment Manual			
High Feature (HF)	---	↓ (https://support.industry.siemens.com/cs/ww/en/view/1097983-82)	---
Basic (BA)	↓ (https://support.industry.siemens.com/cs/de/en/view/59193398)	---	---
High Speed (HS)	---	---	↓ (https://support.industry.siemens.com/cs/ww/en/view/1098068-01)
Width			
High Feature (HF)	---	35 mm	---
Basic (BA)	35 mm	---	---
High Speed (HS)	---	---	35 mm
Number of inputs	16	16	16
Electrical isolation between channels	X	---	---
Number of potential groups	4	2	2
Rated input voltage	120/230 V AC	24 V DC	24 V DC
Diagnostic interrupt	---	X	X
Hardware interrupt	---	X	X
Isochronous mode	---	X	X
Input delay			
High Feature (HF)	---	0.05 ms to 20 ms (configurable)	---

Short designation	DI 16x230VAC BA	DI 16xNAMUR HF	DI 16x24VDC HS
Basic (BA)	Typ. 25 ms (fixed)	---	---
High Speed (HS)	---	---	0.05 ms to 20 ms (configurable)
Integrated counting function (Two channels can optionally be used as counter with 3 kHz)	---	Counting up to 20 kHz	Counting up to 20 kHz

Digital input/output module

Short designation	DI 16x24VDC / DQ 16x24V/0.5A BA
Article number	
High Feature (HF)	---
Basic (BA)	6ES7523-1BL00-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7523-1BL00-0AA0)
Equipment Manual	
High Feature (HF)	---
Basic (BA)	↓ (https://support.industry.siemens.com/cs/ww/en/view/83501523)
Width	
High Feature (HF)	---
Basic (BA)	25 mm
Number of inputs	16
Electrical isolation between channels	---
Number of potential groups	DI: 1 / DQ: 2
Rated input voltage	24 V DC
Diagnostic interrupt	---
Hardware interrupt	---
Isochronous mode	---
Input delay	
High Feature (HF)	---
Basic (BA)	Typ. 3 ms (fixed)
Integrated counting function (Two channels can optionally be used as counter with 3 kHz)	---

Benefits

The digital input modules provide you with the following advantages:

- High channel density with low variety of parts, therefore less effort for ordering, logistics and storage of spare parts

- Modules in 25 mm size without parameter assignment and diagnostics, therefore simple commissioning

- Front connector in screw-type connection system or in push-in system (35 mm width) or push-in system for 25 mm modules

- Same mechanical design, same handling and same accessories for all modules

- Same pin assignment for wiring, which means that circuit diagrams and wiring plans can be universally used

- Any combination of narrow and wide modules

- Can be used centrally in SIMATIC S7-1500 and in the ET 200MP distributed I/O system

- Cost-effective implementation of simple counting tasks with two counter inputs each of the high-feature modules DI16x24VDC HF and DI 32x24V DC HF

5.6.3   Digital output modules

Digital output modules and digital input/output module (DC)

Short designation	DQ 8x24VDC/2A HF	DQ 32x24VDC/0.5A H DQ 32x24VDC/ 0.5A BA	DQ 16x24VDC/0.5A HF DQ 16x24VDC/ 0.5A BA	DI 16x24VDC / DQ16x24V/0.5A BA
Article number				
High Feature (HF)	6ES7522-1BF00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7522-1BF-00-0AB0)	6ES7522-1BL01-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7522-1BL-01-0AB0)	6ES7522-1BH01-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7522-1B-H01-0AB0)	---
Basic (BA)	---	6ES7522-1BL10-0AA0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7522-1BL-10-0AA0)	6ES7522-1BH10-0AA0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7522-1B-H10-0AA0)	6ES7523-1BL00-0AA0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7523-1BL-00-0AA0)
Equipment Manual				
High Feature (HF)	↓ (https://support. industry.siemens. com/cs/ww/en/view/59-193089)	↓ (https://support. industry.siemens. com/cs/ww/en/view/10-9480716)	↓ (https://support. industry.siemens. com/cs/ww/en/view/10-9480717)	---
Basic (BA)	---	↓ (https://support. industry.siemens. com/cs/ww/en/view/83-500404)	↓ (https://support. industry.siemens. com/cs/ww/en/view/83-500415)	↓ (https://support. industry.siemens. com/cs/ww/de/view/83-501523)
Width				
High Feature (HF)	35 mm	35 mm	35 mm	---

Short designation	DQ 8x24VDC/2A HF	DQ 32x24VDC/0.5A H DQ 32x24VDC/ 0.5A BA	DQ 16x24VDC/0.5A HF DQ 16x24VDC/ 0.5A BA	DI 16x24VDC / DQ16x24V/0.5A BA
Basic (BA)	---	25 mm	25 mm	25 mm
Number of outputs	8	32	16	16
Type	Transistor	Transistor	Transistor	Transistor
Electrical isolation between channels	X	Only with BA	Only with BA	X
Number of potential groups	2	4; only with BA	2; only with BA	DQ: 2 / DI: 1
Rated output voltage	24 V DC	24 V DC	24 V DC	24 V DC
Rated output current	2 A	0.5 A	0.5 A	0.5 A
Diagnostic interrupt	X	Only with HF	Only with HF	---
Hardware interrupt	---	---	---	---
Isochronous mode	---	Only with HF	Only with HF	---
Pulse-width modulation (PWM)	X	---	---	---
Switching cycle counter	X	---	Only with HF	---

Digital output modules (UC, AC)

Short designation	DQ 16x24 ...48VUC/ 125VDC/0.5A ST	DQ 8x230VAC/5A ST relay	DQ 16x230VAC/2A ST relay	DQ 8x230VAC/2A ST Triac	DQ 16x230VAC/1A ST Triac
Article number	6ES7522-5EH00-0-AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7522-5EH00-0AB0)	6ES7522-5HF00-0-AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7522-5HF00-0AB0)	6ES7522-5HH00-0-AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7522-5HH00-0AB0)	6ES7522-5FF00-0A-B0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7522-5FF00-0AB0)	6ES7522-5FH00-0-AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7522-5FH00-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view-/109480462)	↓ (https://support.industry.siemens.com/cs/ww/en/view-/59192915)	↓ (https://support.industry.siemens.com/cs/ww/en/view-/109475445)	↓ (https://support.industry.siemens.com/cs/ww/en/view-/59193088)	↓ (https://support.industry.siemens.com/cs/ww/en/view-/109475446)
Width	35 mm	35 mm	35 mm	35 mm	35 mm
Number of outputs	16	8	16	8	16
Type	Transistor	Relay	Relay	Triac	Triac
Electrical isolation between channels	X	X	X	X	X
Number of potential groups	1	16	8	8	8
Relay coil supply voltage	---	24 V DC	24 V DC	---	---

Short designation	DQ 16x24 ...48VUC/ 125VDC/0.5A ST	DQ 8x230VAC/5A ST relay	DQ 16x230VAC/2A ST relay	DQ 8x230VAC/2A ST Triac	DQ 16x230VAC/1A ST Triac
Rated output voltage	24 V DC to 125 V DC / 24 V AC to 48 V AC	24 V DC to 120 V DC / 24 V AC to 230 V AC	24 V DC to 120 V DC / 24 V AC to 230 V AC	230 V AC	230 V AC
Rated output current	0.5 A	5 A	2 A	2 A	1 A
Diagnostic interrupt	---	X	X	---	---
Hardware interrupt	---	---	---	---	---

Benefits

The digital output modules provide you with the following advantages:

- High channel density with low variety of parts, therefore less effort for ordering, logistics and storage of spare parts

- Modules in 25 mm size without parameter assignment and diagnostics, therefore simple commissioning

- Front connector in screw-type connection system or in push-in system (35 mm width) or push-in system for 25 mm modules

- Same mechanical design, same handling and same accessories for all modules

- Same pin assignment for wiring, which means that circuit diagrams and wiring plans can be universally used

- Any combination of narrow and wide modules

- Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system

- High feature module DQ 8x24VDC/2A HF: You can use pulse width modulation (PWM) to easily generate periodic pulses with a constant rated voltage and a variable pulse duration.

  Typical use:

  – Control of proportional valves and way values (e.g. energy saving by reducing the holding current).

  – Heating control e.g. via an external additional power unit.

5.6.4 Fail-safe digital modules

Fail-safe digital modules

Fail-safe digital modules are available for implementing safety concepts in the area of equipment and personnel safety (for example, for emergency stop devices in the operation of processing machines).

The fail-safe modules ensure safe processing of field information (sensors: e.g., EMERGENCY OFF buttons, light barriers; actuators, e.g. motor control). You are provided with all the hardware and software components required for safe processing, according to the required safety class. The following table shows the available fail-safe modules.

Short designation	F-DI 16x 24VDC PROFIsafe	F-DQ 8x24VDC/2A PPM
Article number	6ES7526-1BH00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7526-1BH00-0AB0)	6ES7526-2BF00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7526-2BF00-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/109482426)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109482427)
Width	35 mm	35 mm
Number of inputs	16	---
Number of outputs	---	8
Type output	---	Transistor
Electrical isolation between channels	---	---
Rated input voltage	24 V DC	---
Rated output voltage	---	24 V DC
Rated output current	---	2 A
Maximum achievable safety class in safety mode	PLe/SIL 3	PLe/SIL 3
Low demand mode: PFD according to SIL3	< 5.00E-05	< 6.00E-05
High demand/continuous mode: PFH according to SIL3	< 1.00E-09 1/h	< 2.00E-09 1/h
Diagnostic interrupt	X	X
Hardware interrupt	---	---
Input delay	0.4 ms to 20 ms (configurable by channel)	---

Benefits

The fail-safe input and output modules S7-1500 provide you with the following advantages:

- High-channel, fail-safe inputs and outputs
- Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system
- processing of standard and safety programs
- Uniform engineering for standard and safety automation in the TIA Portal
- Integration of safety-related functions up to SIL 3 according to IEC 61508:2010 or PL e and category 4 according to ISO 13849-1:2015 or according to EN ISO 13849-1:2015

5.6.5 Analog input modules

Analog input modules and analog input/output module

Short designation	AI 8xU/I HF AI 8xU/I HS	AI 8xU/R/RTD/TC HF AI 8xU/I/RTD/TC ST	AI 4xU/I/RTD/TC ST AI 8xU/I/R/RTD BA	AI 4xU/I/RTD/TC / AQ 2xU/I ST
Article number				
High Feature (HF)	6ES7531-7NF00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7531-7N-F00-0AB0)	6ES7531-7PF00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7531-7PF-00-0AB0)	---	---
High Speed (HS)	6ES7531-7NF10-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7531-7N-F10-0AB0)	---	---	---
Standard (ST)	---	6ES7531-7KF00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7531-7KF-00-0AB0)	6ES7531-7QD00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7531-7Q-D00-0AB0)	6ES7534- 7QE00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7534-7Q-E00-0AB0)
Basic (BA)	---	---	6ES7531-7QF00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalo-g/Product/6ES7531-7Q-F00-0AB0)	---
Equipment Manual				
High Feature (HF)	↓ (https://support. industry.siemens. com/cs/ww/en/view/10-9483587)	↓ (https://support. industry.siemens. com/cs/ww/en/view/10-9483586)	---	---
High Speed (HS)	↓ (https://support. industry.siemens. com/cs/ww/en/view/59-193206)	---	---	---

Short designation	AI 8xU/I HF AI 8xU/I HS	AI 8xU/R/RTD/TC HF AI 8xU/I/RTD/TC ST	AI 4xU/I/RTD/TC ST AI 8xU/I/R/RTD BA	AI 4xU/I/RTD/TC / AQ 2xU/I ST
Standard (ST)	---	↓ (https://support. industry.siemens. com/cs/ww/en/view/59-193205)	↓ (https://support. industry.siemens. com/cs/ww/en/view/91-688401)	↓ (https://support. industry.siemens. com/cs/ww/en/view/91-688109)
Basic (BA)	---	---	↓ (https://support. industry.siemens. com/cs/de/en/view/109-763142)	---
Width	35 mm	35 mm	25 mm	25 mm
Number of inputs	8	8	4	4
Resolution	16 bits including sign	16 bits including sign	16 bits including sign	16 bits including sign
Measurement type	Voltage, current	Voltage, current, resistance, thermal resistor, thermocouple	Voltage, current, resistance, resistance thermometer, thermocouple	Voltage, current, resistance, thermal resistor, thermocouple
Electrical isolation between channels	Only with HF	Only with HF	---	---
Number of potential groups	1	1	---	---
Rated supply voltage	24 V DC	24 V DC	24 V DC	24 V DC
Permissible potential difference between inputs (UCM)	HF: 60 V DC / 30 V AC HS: 10 V DC	HF: 60 V DC / 30 V AC ST: 10 V DC	20 V DC	20 V DC
Diagnostic interrupt	X	X	X	X
Hardware interrupt	X Two high limits and two low limits in each case	X Two high limits and two low limits in each case	X Two high limits and two low limits in each case	X Two high limits and two low limits in each case
Isochronous mode	Only HS	---	---	---
Conversion time (per channel)	HF: Fast mode: 4/18/22/102 ms; Standard mode: 9/52/62/302 ms HS: 62.5 µs, per module, regardless of number of activated channels	HF: Fast mode: 4/18/22/102 ms; Standard mode: 9/52/62/302 ms ST: 9/23/27/107 ms	9/23/27/107 ms	9/23/27/107 ms
Calibration in RUN mode	Only with HF	Only with HF	X	X
Oversampling	Only with HS	---	---	---
Measuring range adaptation	Only with HF	---	---	---
Scale measured values	Only with HF	---	---	---
Scale temperatures	---	Only with HF	---	---

Short designation	AI 8xHART HF	AI 24xCVM HF
Article number		
High Feature (HF)	6ES7531-7TF00-0AB0 (https://mall.industry.siemens.com/mall/en/us/Catalog/Product/6ES753-1-7TF00-0AB0)	6ES7531-7LK00-0AB0 (https://mall.industry.siemens.com/mall/en/us/Catalog/Product/6ES753-1-7LK00-0AB0)
Equipment Manual		
High Feature (HF)	↓ (https://support.industry.siemens.com/cs/us/en/view/109821074)	↓ (https://support.industry.siemens.com/cs/us/en/view/109963246)
Width	35 mm	25 mm
Number of inputs	8	24
Resolution	16 bits including sign	16 bits including sign
Measurement type	Current	Voltage
Electrical isolation between channels	X	---
Number of potential groups	1	1
Rated supply voltage	24 V DC	24 V DC
Permissible potential difference between inputs (UCM)	60 V DC / 30 V AC	---
Diagnostic interrupt	X	X
Hardware interrupt	X Two high limits and two low limits in each case	X Two high limits and two low limits in each case
Isochronous mode	---	---
Conversion time (per channel)	Fast mode: 7/21/25/106 ms; Standard mode: 12/55/65/307 ms	8/22/25/105 ms
Calibration in RUN mode	X	X
Oversampling	---	---
Measuring range adaptation	---	---
Scale measured values	---	---
Scale temperatures	---	---

Advantages

Analog input modules detect process signals, e.g. pressure or temperature and pass the process signals on in digitalized form (16 bit format) to the CPU. You use the analog input modules to measure current (2-wire and 4-wire transducer), voltages, resistances (resistance thermometer) and temperatures (thermoelements). The measurement types depend on the module used.

The analog input modules provide you with the following advantages:

- Front connector in screw-type connection system or in push-in system (35 mm width) or push-in system for 25 mm modules

- Same mechanical design, same handling and same accessories for all modules

- Components required for shielding are included in the scope of delivery and allow simple and quick installation without the use of tools

- Same pin assignment for wiring, which means that circuit diagrams and wiring plans can be universally used

- Any combination of narrow and wide modules

- Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system

Overview of functions

In the following you will find a brief overview of special functions of the modules. You can find a detailed description of the functions in the equipment manual of the module.

Measuring range adjustment of the analog input module AI 8xU/I HF

The function adjusts the measuring range to the sensor. You can increase the resolution for a configurable part of the measuring range in S7 format. The measured signal is resolved precisely to more decimal places around a specific operating point.

Scaling of the measured values of the analog input module AI 8xU/I HF

With measured value scaling, you display the user data of the module in REAL format (32-bit floating point) instead of S7 format. You can thus directly assign a technological variable to the analog value of the module. The conversion is made directly in the module, which saves power and cycle time in the CPU.

You can combine the measured value scaling with the measuring range adjustment. In this case, the measuring range is adjusted first and then the representation of the measured value is scaled.

Calibration in runtime

The following analog modules offer you the calibration function at runtime:

- AI 4xU/I/RTD/TC ST

- AI 8xU/I/RTD BA

- AI 8xU/I/RTD/TC ST

- AI 8xU/I HS

- AI 8xU/I HF

- AI 8xHART HF

- AI 8xU/R/RTD/TC HF

- AI 16xU BA

- AI 16xI BA

- AI 24xCVM HF

- AI 4xU/I/RTD/TC / AQ 2xU/I ST

The calibration compensates for influences on the measuring result by cables and/or temperature. A calibration checks the process values output by the analog input module, determines the deviation from the actual values and compensates for measuring errors.

Typical use:

- For plants in which sensors detect relatively small voltages or currents
- For applications which require regular calibration for all components in a measuring circuit.

Oversampling of the AI 8xU/I HS analog input module

Oversampling divides a PROFINET bus cycle into equidistant bus sub-cycles. This requires isochronous mode.

Oversampling acquires data with high time resolution but without using an extremely short PROFINET bus cycle and thus fast CPU cycles. Use for quality-monitoring measurements, for example when recording pressure trends during the blowing process of PET bottle production.

5.6.6   Analog output modules

Analog output modules and analog input/output module

Short designation	AQ 8xU/I HS	AQ 4xU/I HF AQ 4xU/I ST	AQ 2xU/I ST	AI 4xU/I/RTD/TC / AQ 2xU/I ST
Article number				
High Feature (HF)	---	6ES7532-5ND00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catal- og/Product/6ES7532-5- ND00-0AB0)	---	---
High Speed (HS)	6ES7532-5HF00-0AB0 (https://mall.industry. siemens. com/mall/de/WW/Catalo- g/Product/6ES7532-5HF- 00-0AB0)	---	---	---
Standard (ST)	---	6ES7532-5HD00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catal- og/Product/6ES7532-5- HD00-0AB0)	6ES7532-5NB00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catal- og/Product/6ES7532-5- NB00-0AB0)	6ES7534-7QE00-0AB0 (https://mall.industry. siemens. com/mall/en/WW/Catalog/- Product/6ES7534-7QE00-- 0AB0)
Equipment Manual				
High Feature (HF)	---	↓ (https://support. industry.siemens. com/cs/ww/en/view/10- 9483585)	---	---

Short designation	AQ 8xU/I HS	AQ 4xU/I HF AQ 4xU/I ST	AQ 2xU/I ST	AI 4xU/I/RTD/TC / AQ 2xU/I ST
High Speed (HS)	↓ (https://support.industry. siemens. com/cs/ww/en/view/591- 93551)	---	---	---
Standard (ST)	---	↓ (https://support. industry.siemens. com/cs/ww/de/view/59- 191850)	↓ (https://support. industry.siemens. com/cs/ww/en/view/91- 688388)	↓ (https://support.industry. siemens. com/cs/ww/en/view/9168- 8109)
Width	35 mm	35 mm	25 mm	25 mm
Number of outputs	8	4	2	2
Resolution	16 bits including sign	16 bits including sign	16 bits including sign	16 bits including sign
Output type	Voltage/current	Voltage/current	Voltage/current	Voltage/current
Electrical isolation between channels	---	Only with HF	---	---
Number of potential groups	---	1	---	---
Rated supply voltage	24 V DC	24 V DC	24 V DC	24 V DC
Diagnostic interrupt	X	X	X	X
Isochronous mode	X	Only with HF	---	---
Conversion time (per channel)	50 µs, regardless of number of activated channels	HF: 125 µs, regardless of number of activated channels ST: 0.5 ms	0.5 ms	0.5 ms
Calibration in RUN mode	X	Only with ST	X	X
Oversampling	X	---	---	---

Short designation	AQ 8xHART HF
Article number	
High Feature (HF)	6ES7532-8TF00-0AB0 (https://mall.industry.siemens. com/mall/en/us/Catalog/Product/6ES7532-8TF00-0AB0)
Equipment Manual	
High Feature (HF)	↓ (https://support.industry.siemens. com/cs/us/en/view/109954408)
Width	35 mm
Number of outputs	8
Resolution	16 bits including sign
Output type	Current
Electrical isolation between channels	---
Number of potential groups	---
Rated supply voltage	24 V DC

Short designation	AQ 8xHART HF
Diagnostic interrupt	X
Isochronous mode	X
Conversion time (per channel)	---
Calibration in RUN mode	X
Oversampling	---

Advantages

Analog output modules convert a 16-bit digital value into current or voltage and output it at the process. With the analog output modules you control, for example, proportional valves or small servo drives.

The analog output modules provide you with the following advantages:

• Front connector in screw-type connection system or in push-in system (35 mm width) or push-in system for 25 mm modules

• Same mechanical design, same handling and same accessories for all modules

• Components required for shielding are included in the scope of delivery and allow simple and quick installation without the use of tools

• Same pin assignment for wiring, which means that circuit diagrams and wiring plans can be universally used

• Any combination of narrow and wide modules

• Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system

Overview of functions

In the following you will find a brief overview of special functions of the modules. A detailed description of the functions is available in the device manual of the module.

Calibration in runtime

The following analog modules offer you the calibration function at runtime:

• AQ 2xU/I ST

• AQ 4xU/I ST

• AQ 4xU/I HF

• AQ 8xU/I HS

• AQ 8xHART HF

• AI 4xU/I/RTD/TC / AQ 2xU/I ST

The calibration compensates for influences on the measuring result by cables and/or temperature. A calibration checks the process values output by the analog output module, determines the deviation from the actual values and compensates for output errors.

Typical use:

- For plants in which sensors process relatively small voltages or currents.
- For applications which require regular calibration for all components in a measuring circuit.

Oversampling of the AQ 8xU/I HS analog output module

Oversampling divides a PROFINET bus cycle into equidistant bus sub-cycles. This requires isochronous mode.

Oversampling acquires data with high time resolution but without using an extremely short PROFINET bus cycle and thus fast CPU cycles. Used, for example, for controlling a feed valve, the output data is controlled exactly at the current position of the machine.

5.7 Communication

5.7.1 Interfaces for communications

Interfaces for communication via PROFINET and PROFIBUS DP (as of CPU 1516) are already integrated in the CPUs. Additional communication modules enhance the communication capabilities of the SIMATIC S7-1500 with additional functions or interfaces, e.g. 8xIO-Link. The following communications options are available for your automation task:

Communication options	PN/IE	DP	Serial
PG communication for commissioning, testing, diagnostics	X	X	---
HMI communication for operator control and monitoring	X	X	---
Open User Communication	X	---	---
Secure Open User Communication	X	---	---
Data exchange via OPC UA as server	X	---	---
Data exchange via OPC UA as client	X	---	---
Direct data exchange between IO controllers	X	---	---
Communication via Modbus TCP	X	---	---
Communication via UDP Multicast	X	---	---
Sending process alarms via e-mail	X	---	---
File management and file access via FTP (File Transfer Protocol); CP may be the FTP client and FTP server	X	---	---
S7 communication	X	X	---
Serial point-to-point or multi-point connection Data exchange via point-to-point with Freeport, 3964 (R), USS or Modbus protocol	---	---	X
Web server Data exchange via HTTP(S), for example for diagnostics	X	---	---
SNMP (Simple Network Management Protocol)	X	---	---
Time synchronization	X	X	---

5.7.2 CM communication modules / CP communications processors

For special requirements of your plant, use communications processors (CPs) for security functions to secure Industrial Ethernet networks.

If your system requires additional interfaces, communication modules (CM) expand your S7-1500 CPU with other interfaces of an interface type such as PROFINET, PROFIBUS or point-to-point connection. The CMs for point-to-point connection allow, for example, Freeport or Modbus communication via their RS232, RS422 and RS485 interfaces.

Communication modules for PROFINET and Industrial Ethernet

Short designation	CM 1542-1	CP 1543-1	CP 1545-1
Article number	6GK7542-1AX00-0XE0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK7542-1AX00-0XE0)	6GK7543-1AX00-0XE0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK7543-1AX00-0XE0)	6GK7545-1GX00-0XE0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK7545-1GX00-0XE0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/ps/21885/man)	↓ (https://support.industry.siemens.com/cs/ww/en/ps/15340/man)	↓ (https://support.industry.siemens.com/cs/us/en/view/109-771664)
Bus system	PROFINET	Industrial Ethernet	Industrial Ethernet
Interface	RJ45	RJ45	RJ45
Data transmission rate	10/100 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
Functionality and protocols	TCP/IP, ISO-on-TCP, UDP, Modbus TCP, S7 communication, IP Broadcast/Multicast, IP routing, SNMPv1	TCP/IP, ISO, UDP, Modbus TCP, S7 communication, IP Broadcast/Multicast, Security, Secure Open User Communication, SMTPS, diagnostics SNMPV1/V3, DHCP, FTP client/server e-mail, IPV4/IPV6	TCP/IP, ISO, UDP, Modbus TCP, S7 communication, IP Broadcast/Multicast, Security, Secure Open User Communication, SMTPS, diagnostics SNMPV1/V3, DHCP, FTP client/server e-mail, IPV4/IPV6
Diagnostic interrupt	X	X	X
Hardware interrupt	X	---	---
Isochronous mode	---	---	---
Link to cloud systems via MQTT	---	---	X
OPC UA PubSub via UDP	---	---	---

Communication modules for PROFIBUS

Short designation	CM 1542-5	CP 1542-5
Article number	6GK7542-5DX00-0XE0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK7-542-5DX00-0XE0)	6GK7542-5FX00-0XE0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6GK7-542-5FX00-0XE0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/ps/15671/man)	↓ (https://support.industry.siemens.com/cs/ww/en/ps/15672/man)
Bus system	PROFIBUS	PROFIBUS
Interface	RS485	RS485
Data transmission rate	9600 bps to 12 Mbps	9600 bps to 12 Mbps
Functionality and protocols	DPV1 master/device S7 communication PG/OP communication Open User Communication	DPV1 master/device S7 communication PG/OP communication FDL
Diagnostic interrupt	X	X
Hardware interrupt	X	X
Isochronous mode	---	---

Communication modules for point-to-point connection

Short designation	CM PtP RS232 HF CM PtP RS232 BA	CM PtP RS422/485 HF CM PtP RS422/485 BA
Article number		
High Feature (HF)	6ES7541-1AD00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES75-41-1AD00-0AB0)	6ES7541-1AB00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES75-41-1AB00-0AB0)
Basic (BA)	6ES7540-1AD00-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES75-40-1AD00-0AA0)	6ES7540-1AB00-0AA0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES75-40-1AB00-0AA0)
Equipment Manual		
High Feature (HF)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59057160)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59061372)
Basic (BA)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59057152)	↓ (https://support.industry.siemens.com/cs/ww/en/view/59057390)
Interface	RS232	RS422/485
Data transmission rate		
High Feature (HF)	300 to 115 200 bps	300 to 115 200 bps
Basic (BA)	300 to 19 200 bps	300 to 19 200 bps
Frame length, max.		
High Feature (HF)	4 KB	4 KB

Short designation	CM PtP RS232 HF CM PtP RS232 BA	CM PtP RS422/485 HF CM PtP RS422/485 BA
Basic (BA)	1 KB	1 KB
Diagnostic interrupt	X	X
Hardware interrupt	---	---
Isochronous mode	---	---
Protocols		
High Feature (HF)	Freeport, 3964 (R), Modbus RTU master, Modbus RTU device	Freeport, 3964 (R), Modbus RTU master, Modbus RTU device
Basic (BA)	Freeport, 3964 (R)	Freeport, 3964 (R)

Benefits

The communication modules point-to-point connection S7-1500 provide you with the following advantages:

- Connection of legacy and external systems possible

- Connection of data readers or special sensors

- Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system

- Variety of physical interfaces, e.g. RS232 and RS422 or RS485

- Predefined protocols, e.g. 3964(R), Modbus RTU or USS

- Application-specific protocols based on Freeport (ASCII)

- Uniform programming interface for all modules

- Diagnostic interrupt for simple fault rectification

5.7.3 Communication module IO-Link Master

Communication module IO-Link Master

An 8-port IO-link master module CM 8xIO-link is available for the S7-1500 automation system/ET 200MP distributed I/O system.

IO-Link is a point-to-point connection between a master and a device. Both conventional and intelligent sensors/actuators can be used as devices at the IO link via unshielded standard cables using proven 3-wire technology.

You can use the 8-port IO link master as follows:

- Central, directly behind a S7-1500 CPU (a total of 30 I/O modules, plug-in type)

- Distributed with ET 200MP to PROFINET and PROFIBUS

With the IO link, you can easily change the parameters for the production and processing of different product variants and batches up to sensor/actuator level during CPU runtime. A considerably more detailed diagnostics up to sensor or actuator or a remote diagnostics is possible.

Table 5-5 Communication module IO-Link Master

Short designation	CM 8x IO-Link
Article number	6ES7547-1JF00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7547-1JF00-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/109763143)
Bus system	IO-Link
Interface	8 ports
Data transmission rate	COM1 (4.8 kbaud), COM2 (38.4 kbaud), COM3 (230.4 kbaud)
Functionality and protocols	IO-Link Protocol 1.0 IO-Link Protocol 1.1
Diagnostic interrupt	X
Hardware interrupt	---
Isochronous mode	---

Benefits:

- Simplified and reduced wiring, engineering and commissioning
- Time savings
- Higher availability due to pre-assembled cable
- Avoidance of plant downtimes through preventive maintenance
- High diagnostics capability
- Configurable diagnostics can be set for each channel

5.7.4   Safety-related communication via fail-safe modules

The figure below provides an overview of the possibilities of safety-related communication via PROFINET IO in SIMATIC Safety fail-safe systems with S7-1500 F-CPUs.
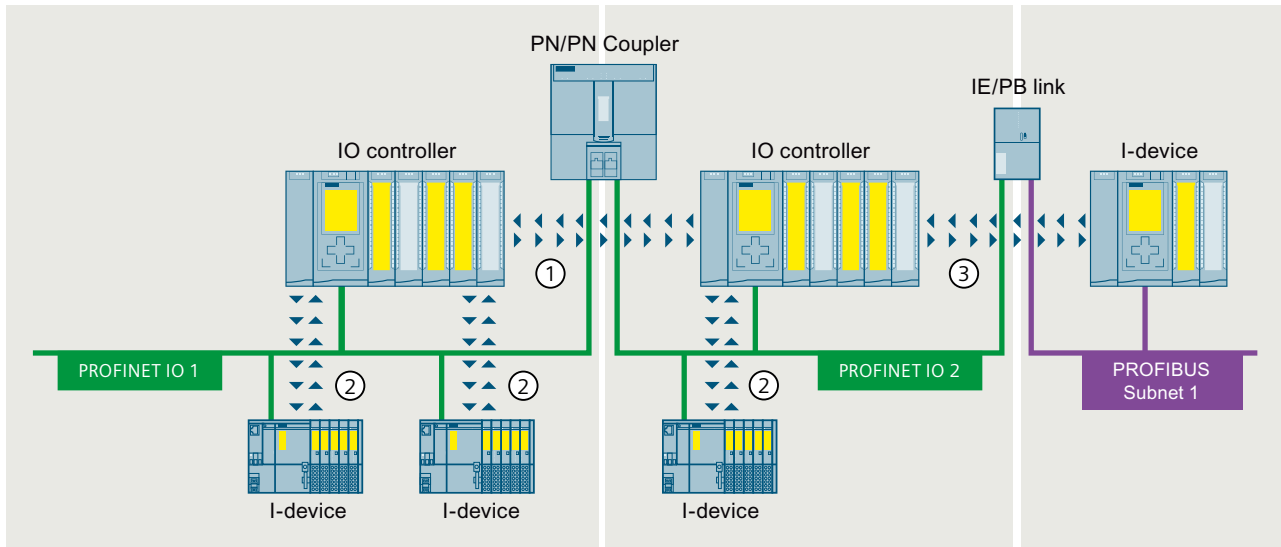
1	Safety-related IO controller - IO controller communication
2	Safety-related IO controller - I-device communication
3	Safety-related IO controller-I-device communication (via IE/PB link to PROFIBUS)

Figure 5-21 Example of safety-related communication

5.8 Technology functions

5.8.1 Motion control

You use the integrated Motion Control functionality of SIMATIC S7-1500 for positioning and moving axes. Depending on the CPU, the SIMATIC S7-1500 automation system supports different configuration limits for motion control technology objects.

With Motion Control instructions according to PLCopen, you control PROFIdrive-capable drives and drives with analog setpoint interface.

Motion control technology objects

The table below shows the technology objects that are supported by the SIMATIC S7-1500 and S7-1500T. * They occupy Motion Control resources or Extended Motion Control resources in the CPU.

Technology objects	SIMATIC S7-1500	SIMATIC S7-1500T	Resource requirements per technology object
Speed-controlled axis	X	X	40
Positioning axis	X	X	80
Synchronous axis	X	X	160
External encoder	X	X	80
Measuring input	X	X	40
Output cam	X	X	20
Cam track	X	X	160
Cam of type "TO_Cam"	---	X	2*
Cam of type "TO_Cam_10k"	---	X	20*
Cam of the type "TO_Cam_600Seg"	---	X	2*
Cam of the type "TO_Cam_6kSeg"	---	X	20*
Kinematics	---	X	30*
Interpreter	---	X	60*
Interpreter program	---	X	0
Interpreter mapping	---	X	0
Leading axis proxy	---	X	3*

* They occupy Extended Motion Control resources in the CPU.

Motion control technology functions

The table below shows the technology functions offered by both SIMATIC S7-1500 and S7-1500T and the extended Motion Control functions of the technology CPUs.

Technology functions	SIMATIC S7-1500	SIMATIC S7-1500T
Enable, disable technology objects	X	X
Acknowledge alarms, restart technology object	X	X
Reference technology objects, set reference point	X	X
Pause axis	X	X
Position axis absolutely	X	X
Position axis relatively	X	X
Move axis at set velocity/speed	X	X
Move axis in jog mode	X	X
Positioning axis overlapping	X	X
Set alternative encoder as operationally active encoder	---	X
Pause superimposed motions on the axis	X	X
Hold and disable axis	X	X
Activate/deactivate hardware limit switch	X	X
Controlling bits of control word 1 and 2	X	X
Save absolute encoder adjustment for device replacement	X	X
Start one-time measuring	X	X
Start cyclic measuring	X	X
Abort active measuring	X	X
Activate/deactivate output cam	X	X
Activate/deactivate cam track	X	X
Start gearing	X	X
Start gearing with specified synchronous positions	---	X
Start velocity synchronous operation	---	X
Absolute shift of master value on the following axis	---	X
Relative shift of master value on the following axis	---	X
Relative shift of following value on the following axis	---	X
Absolute shift of following value on the following axis	---	X
Start camming	---	X
Simulate synchronous operation	---	X
Desynchronize gearing	---	x
Desynchronize camming	---	x
Specify additive master value	---	X
Interpolate cam	---	X
Read out slave value of a cam	---	X
Read master value of a cam	---	X
Copy calculated cam elements	---	X

Technology functions	SIMATIC S7-1500	SIMATIC S7-1500T
Specify motion setpoints	---	X
Specify superimposed motion setpoints	---	X
Activate and deactivate force/torque limiting / fixed stop detection	X	X
Specify additive torque	X	X
Specify upper and lower torque limits	X	X
Interrupt motion control of kinematics	---	X
Continue motion control of kinematics	---	X
Stop motion of kinematics	---	X
Position kinematics with linear motion	---	X
Position kinematics relatively with linear motion	---	X
Position kinematics with circular motion	---	X
Position kinematics relatively with circular motion	---	X
Move kinematics with synchronous "point-to-point" motion, absolute	---	X
Move kinematics with synchronous "point-to-point" motion, relative	---	X
Start conveyor tracking	---	X
Set kinematics to simulation mode	---	X
Define workspace zones	---	X
Define kinematics zones	---	X
Activate workspace zones	---	X
Deactivate workspace zones	---	X
Activate kinematics zones	---	X
Deactivate kinematics zones	---	X
Re-define tool	---	X
Change active tool	---	X
Redefine object coordinates system	---	X
Transform axis coordinates into cartesian coordinates	---	X
Transforming Cartesian coordinates into axis coordinates	---	X

Motion Control configuration example

The SINAMICS Startdrive engineering tool is available in the TIA Portal for easy commissioning and optimization of SINAMICS drives. SINAMICS Startdrive enables efficient commissioning by means of the integrated axis control panel and extensive diagnostic functions.
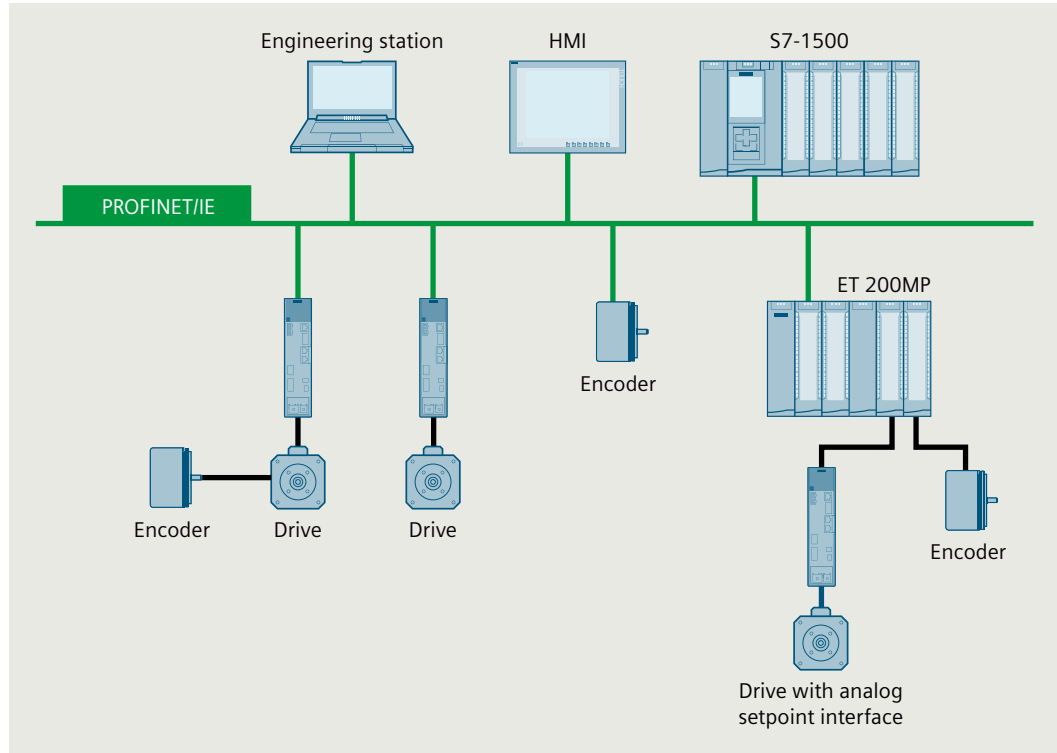
Figure 5-22 Example of a Motion Control configuration

SIMATIC S7-1500T CPUs

The Technology CPUs extend the Motion Control functions available in all SIMATIC S7-1500 controllers for demanding solutions to include gearing and camming and kinematics.

The S7-1500 T-CPUs are also suitable for safety applications, so that you only need one CPU for standard, safety and comprehensive Motion Control automation tasks.

Example: Quick and flexible packaging of luxury goods thanks to the CPU SIMATIC S7-1500T

Automation task:

Development of a modular, automatic packaging machine with a speed of up to 50 packages per minute.

Feature:

The packaging machine enables the outer packaging of individual products as well as containers at medium to high speeds (more than 40 products per minute). The possibility of quick changeover to new products is a condition. Scalability and cost efficiency is paramount in the automation solution.

Solution:

A SIMATIC S7-1500 TIME-CPU controls several axes in parallel with its technology functions gearing and camming.

The SINAMICS V90 drive communicates with the CPU via PROFINET IO with IRT. You assign parameters to the technology functions via technology objects with STEP 7.

Advantages

Motion Control with SIMATIC S7-1500T CPUs provide you with the following advantages:

- Rugged and stable motion control platform with easy extensibility to include additional axes
- Automatic alignment of the technological variables between controller and drive by means of technology objects; reduced engineering, commissioning and service times
- Simple setup and commissioning of the technology functions in the TIA Portal, no specialist knowledge required
- Inclusion in the integrated system diagnostics and trace function, thus reducing maintenance times and downtimes
- Numerous options for using synchronized axes in gearing with specification of the synchronous position, in camming and in velocity synchronous operation
- Configuration limits can be expanded through cross-PLC synchronous operation
- Graphical and tabular configuration and optimization and diagnostics of cams with integrated cam editor saves time and reduces the error rate
- Adaptation and calculation of the cam disks in the user program during operation, e.g. for quick product changeover
- Control of kinematics for handling tasks such as pick-and-place, assembly and palletizing

S7-1500 Motion Control KinPlus

The "S7-1500T Motion Control KinPlus" software extends the S7-1500T kinematics functions. The "S7-1500T Motion Control KinPlus" software enables control of kinematics with 5 or 6 interpolating axes.

More information

More information can be found in the function manuals S7-1500T Motion Control (https://support.industry.siemens.com/cs/ww/en/view/109751049)

5.8.2 PID Control

PID controllers are integrated as standard in all S7-1500 CPUs. PID controllers measure the actual value of a physical variable, for example, temperature or pressure, and compare the actual value with the setpoint. Based on the resulting system deviation, the controller calculates a manipulated variable that causes the actual value to reach the setpoint as quickly and stably as possible.

You can choose from three different PID technology objects:

PID technology object	Description
PID_Compact	The PID_Compact technology object provides a PID controller with integrated tuning for actuators with proportional action behavior. Different operating modes are possible with PID_Compact, such as: • Pretuning • Fine tuning • Automatic mode • Manual mode
PID_3Step	The PID_3Step technology object provides a PID controller with tuning for valves or actuators with integrating behavior. You can configure the following controllers: • Three-point stepping controller with position feedback • Three-point stepping controller without position feedback • Valve controller with analog output value
PID_Temp	The PID_Temp technology object provides a continuous PID controller with integrated tuning. PID_Temp is specially designed for temperature control and is suitable for heating or heating/cooling applications. Two outputs are available, one for heating and one for cooling. You can also use PID_Temp for other control tasks. PID_Temp can be cascaded. You can use PID_Temp in manual or automatic mode.

Example: PID Control optimizes the drying process

Automation task: Development of a temperature control for drying panes of glass in the production of mirrors**.**

Feature: The drying process is a critical phase in silvering mirrors. It is decisive for optimum product quality. During the silvering process, the glass panes are treated with chemical solutions and then dried in a pre-heated oven. Temperature control plays a key role in the drying process.

Solution: A PID controller controls the temperature in the drying oven. The filament of each infrared lamp in the oven is controlled separately and remotely. Control was previously only possible manually.

Benefits

The integrated controller PID Control of the SIMATIC S7-1500 CPUs offer you the following advantages:

• High-quality end product due to optimum control performance

• High flexibility in the drying oven

• Time savings thanks to automatic control parameter optimization for optimum control performance and simple commissioning

More information

A detailed description of PID Control in SIMATIC S7-1500 can be found in the Function Manual "SIMATIC S7-1200, S7-1500 PID Control" SIMATIC S7-1200, S7-1500 PID control (https://support.industry.siemens.com/cs/ww/en/view/108210036).

5.8.3 Technology functions of the compact CPUs

Technology functions are integrated into the SIMATIC S7-1500 compact CPUs.

Function	Value	Description
Six high-speed counters	Up to 100 kHz	For pulse and incremental encoders
Frequency measurement	0.04 Hz - 400 kHz	
Period duration measurement	2.5 µs - 25 s	
Velocity measurement		Dependent on measurement interval and signal evaluation Unit can be defined by user
Pulse width modulation (PWM output)	Max. 4 (up to 100 kHz)	Output of a signal with defined period duration and variable on-load factor at DQ
Pulse Train Output (PTO output)	Max. 4 (up to 100 kHz)	Output of position information, e. g. for activation of stepper motor drives or simulation of an incremental encoder
Frequency output	Up to 100 kHz	Precise assignment of a frequency value with high frequencies

Benefits

Compared with the other SIMATIC S7-1500 CPUs, the compact CPUs offer added value in a small space:

• The CPU with display and inputs/outputs in one enclosure

• Compact size with high performance

• Important technology functions such as counting, measuring and positioning are integrated

• Cost effective compared to modular systems with CPU and modules

• Space saving design

• Can be expanded by SIMATIC S7-1500 input and output modules

5.8.4 Technology modules for counting, measuring and position detection

For technological tasks, powerful technology modules are available that perform these tasks largely autonomously and reduce the load on the CPU. The table below shows the available technology modules for counting, measuring and position detection.

Short designation	TM Count 2x24V	TM PosInput 2
Article number	6ES7550-1AA01-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7550-1AA01-0AB0)	6ES7551-1AB01-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7551-1AB01-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/109783960)	↓ (https://support.industry.siemens.com/cs/ww/en/view/109813005)
Connectable encoders	Incremental encoder for signals, 24 V asymmetrical, Pulse encoders with/without direction signal, Pulse encoders up/down	Incremental encoder for signals to RS422 (5 V differential signal), Pulse encoders with/without direction signal, Pulse encoders up/down, Absolute encoders (SSI)
Max. count frequency	200 kHz 800 kHz with four-fold pulse	1 MHz 4 MHz with four-fold pulse
Integrated DI	3 DIs per counter channel for • Start • Stop • Capture • Synchronization	2 DIs per counter channel for • Start • Stop • Capture • Synchronization
Integrated DQ	2 DQs for comparators and limit values	2 DQs for comparators and limit values
Counting functions	Comparator Adjustable counting range, Incremental position detection	Comparator Adjustable counting range, Incremental and absolute position detection
Measuring functions	Frequency Period duration Velocity	Frequency Period duration Velocity
Diagnostic interrupt	X	X
Hardware interrupt	X	X
Isochronous mode	X	X

Benefits

Technology modules for counting, measuring and position detection offer you the following advantages:

- Fast and timely detection of events with fine resolution for high productivity and product quality
- Hardware-level signal processing for rapid counting, measurement and position detection for a variety of transducers
- Simple setup and commissioning of the technology functions in STEP 7
- Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system
- Quick response thanks to different hardware interrupts

5.8.5 Technology module for time-based IO

Time-based IO modules enable you to achieve maximum precision and speed - regardless of the performance of the controller and the fieldbus. The time-based IO modules output signals with a precisely defined response time. The I/O signals are processed on a time basis.

The table below shows the main features of the technology module for time-based IO. In conjunction with the "Output cam" and "Cam track" technology objects, the TM Timer DIDQ 16x24V ensures highly accurate cam output. In conjunction with the "Measuring input" technology object, the TM Timer DIDQ 16x24V ensures highly accurate detection of passing products.

Short designation	TM Timer DIDQ 16x24V
Article number	6ES7552-1AA00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7552-1AA00-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/95153313)
Connectable encoders	24 V incremental encoder with signals A and B 24 V pulse encoder with a signal
Max. count frequency	200 kHz with fourfold evaluation
Integrated DI	Up to 8 DIs with the following functions: • Up to 2 time stamps per cycle (resolution 1 µs) • 32x oversampling • Counting function up to 50 kHz • Incremental encoder acquisition with 2 phase-shifted tracks • Configurable input filter to suppress interference
Integrated DQ	Up to 16 DQs with the following functions: • Up to 2 time stamps per cycle (resolution 1 µs) • 32x oversampling • Pulse-width modulated output • Configurable substitute values per DQ
Diagnostic interrupt	X
Hardware interrupt	---
Isochronous mode	X (required for the time stamp and oversampling functions)

Benefits

The technology modules for time-based IO offers you the following advantages:

- Meets stringent requirements for precision and speed, independent of the CPU and fieldbus

- Signals are read in and output precisely, to within 1 microsecond

- Exact definition of response times, independent of the application cycle

- Typical use: cam control, length measurement, time measurement, as a probe, for dosing fluid quantities

5.8.6 Technology module for weighing technology

The technology modules SIWAREX WP521 and SIWAREX WP522 are used for the acquisition and processing of signals from weighing or force transducers. You can connect one scale (WP521) or two separate scales (WP522) respectively to the modules. The SIWAREX modules offer high accuracy.

The table below shows the main features of the technology modules for weighing technology.

Short designation	TM electronic weighing system SIWAREX WP 521 ST	TM electronic weighing system SIWAREX WP 522 ST
Article number	7MH4980-1AA01 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/7MH4-980-1AA01)	7MH4980-2AA01 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/7MH4-980-2AA01)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/109742780)	
Weighing channel	1 channel	2 channels
Interfaces	RS 485 with Modbus RTU or for connecting the remote display (per channel) Ethernet interface with SIWATOOL protocol and Modbus TCP/IP (1 for both channels)	
Integrated digital inputs	DI 3x24VDC	
Integrated digital outputs	DQ 4x24VDC	
Load cell connection	DMS load cells in 6- or 4-wire technology (per channel), 1 to 4 mV/V	
Functions	• Adjust the scale with weights or automatically • 3 limits • Tare • Set to zero • Trace • Commission with SIWATOOL (service tool for PC)	
Diagnostic interrupt	---	
Hardware interrupt	X (configurable)	

Benefits

The weighing modules SIWAREX for SIMATIC S7-1500 offer you the following advantages:

- Seamless integration of simple weighing applications such as platform and hopper scales in SIMATIC S7-1500
- Use for level monitoring, e.g. silos and bunkers
- Can be used centrally in SIMATIC S7-1500 and in ET 200MP distributed I/O system
- SIWAREX WP521 ST for the setup of one scale
- SIWAREX WP522 ST for the setup of two separate scales, with the same space requirements as WP521 ST
- Free sample application on the Internet for the quick implementation of customer or industry-specific solutions

5.8.7   Technology Module TM NPU

Technology Module TM NPU

Applications based on artificial intelligence can be implemented using the TM NPU technology module. The technology module TM NPU is used in the S7-1500 automation system / ET 200MP distributed I/O system.

The integrated AI processor (AI - Artificial Intelligence) enables the processing of large amounts of data from connected sensors, as well as data from the user program of the CPU. Connect the sensor technology via the integrated USB interface of the TM NPU, e.g.: Cameras or microphones. For TM NPU with V1.0.0, use the USB camera from Intel, type RealSense D435.

The supplied data is processed at high speed in the TM NPU over neural networks. The TM NPU transmits the processing result via the backplane bus to the CP. The CPU then evaluates the data in the user program.

Typical areas of application:

- Visual quality check in production plants
- Pick-and-place applications
- Image-guided robotic systems

Table 5-6 Technology Module TM NPU

Short designation	TM NPU
Article number	6ES7556-1AA00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7556-1AA00-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/109765877)
Interfaces	Ethernet (1 port) USB 3.1 (1 Port) SD card slot

Short designation	TM NPU
Interrupts/diagnostics/status information	
Status display	Yes
Interrupts	No
Diagnostic functions	Yes
Product function	
Artificial intelligence / Processing of neural networks	Yes

Benefits:

- Design of flexible and precise production processes
- Reduction of time required for configuration, programming and commissioning

5.8.8 Technology module TM MFP

Technology module TM MFP

The TM MFP (technology module multifunctional platform) is a module for IT applications that are not included in the control tasks of the CPU. The technology module processes, for example, the data of connected cameras or robot systems and the data from the user program of the CPU.

The Linux-based operating system SIMATIC Industrial OS (IndOS) has been pre-installed on the TM MFP. The Graphics Processing Unit (GPU) of the built-in processor is able to run and accelerate AI routines. This enables fast and efficient processing of large amounts of data and optimization of processes.

The technology module supports Docker software (not pre-installed by default) for loading software and algorithms, for example, into the TM MFP in the form of bins.

Typical areas of application:
- Edge computing for SIMATIC controllers
- Data processing of connected sensors, e.g. cameras
- Execution and acceleration of AI routines

Table 5-7 Technology module TM MFP

Short designation	TM MFP
Article number	6ES7558-1AA00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6E-S7558-1AA00-0AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/us/en/view/109820481)
Interfaces	2x Ethernet (1 port each) 2x USB 3.0 DisplayPort

Short designation	TM MFP
Interrupts/diagnostics/status information	
Status display	No
Interrupts	No
Diagnostic functions	No
Product function	
Execution of IT applications	Yes

Advantages

- Supports applications in high-level languages, e.g. C, C++ or Python
- Fast and efficient processing of large amounts of data

5.9 Power supply

The power supply of an automation system to be dimensioned according to plant size. The SIMATIC S7-1500 CPUs are supplied via a load power supply or a system power supply. A system power supply that supplies the backplane bus is integrated in the CPUs. Depending on the system configuration, you can expand the integrated system power supply with up to two additional system power supply modules. If your plant has high power requirements, e.g. I/O load groups, you can connect additional load power supplies.

The table below shows the main differences between the two power supplies for the SIMATIC S7-1500 automation system:

Power supply	Description
Load current supply (PM)	Supplies 24 V DC to the S7-1500 system components such as CPU, system power sup- ply (PS), input/output circuits of the I/O modules and any sensors and actuators. You can install the load power supply directly to the left of the CPU (without connection to the backplane bus). If you supply the voltage for the backplane bus via a system power supply, then the supply of the CPU or the interface module with DC 24 V is optional.
System power supply (PS)	Supplies only internally required system voltage. Supplies parts of the module electronics and the LEDs. Additionally the PS 60W 24/48/60V DC HF keeps the complete work memory of the CPU retentive.

Configuration example of a system with load power supply and system power supply

The following figure shows a system configuration with load power supply and additional system power supply.
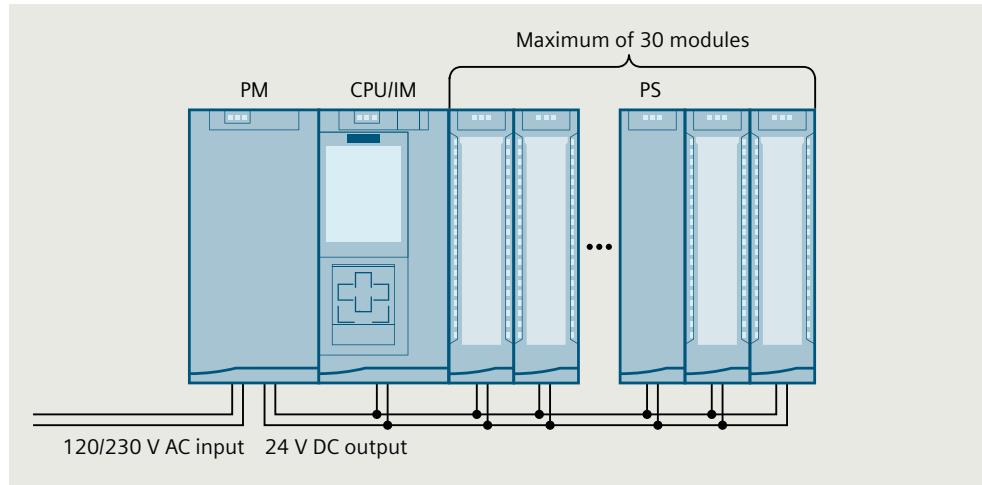

Figure 5-23 Overall configuration of power supply

In order to ensure the supply of the modules from the backplane bus, the incoming power is compared with the required power in the TIA Portal engineering system or in the TIA Selection Tool.

As early as in the planning stages, make sure that the power fed into the backplane bus is always greater than or equivalent to the power drawn.

System power supply modules

System power supplies supply the internal electronics of the S7-1500 modules with power via the backplane bus. The table below shows the available system power supply modules:

Short designation	PS 25 W 24 V DC	PS 60 W 24/48/60 V DC	PS 60 W 24/48/60 V DC HF	PS 60 W 120/230 V AC/DC
Article number	6ES7505-0KA01-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/-Product/6ES7505-0KA00-0AB0)	6ES7505-0RA00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/-Product/6ES7505-0RA00-0-AB0)	6ES7505-0RB00-0A-B0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6ES7505-0RB00-0AB0)	6ES7507-0RA00-0AB0 (https://mall.industry.siemens.com/mall/en/WW/Catalog/-Product/6ES7507-0RA00-0-AB0)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/5919-3552)	↓ (https://support.industry.siemens.com/cs/ww/en/view/5919-2919)	↓ (https://support.industry.siemens.com/cs/ww/en/view-/109746400)	↓ (https://support.industry.siemens.com/cs/ww/en/view/5919-3004)
Rated input voltage	24 V DC	24 VDC, 48 VDC, 60 VDC	24 VDC, 48 VDC, 60 VDC	120 V AC, 230 V AC 120 V DC, 230 V DC
Output power	25 W	60 W	60 W	60 W

Short designation	PS 25 W 24 V DC	PS 60 W 24/48/60 V DC	PS 60 W 24/48/60 V DC HF	PS 60 W 120/230 V AC/DC
Electrical isolation from the backplane bus	X	X	X	X
Diagnostic interrupt	X	X	X	X
Energy buffering for data backup in the CPU	---	---	Up to 20 MB retentive	---

Load power supply modules

The load power supply modules with automatic range selection of the input voltage are optimally adapted in design and functionality to the SIMATIC S7-1500 controller. The table below shows the available load power supply modules:

Short designation	PM 70 W 120/230 V AC	PM 190 W 120/230 V AC
Article number	6EP1332-4BA00 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6EP13-32-4BA00)	6EP1333-4BA00 (https://mall.industry.siemens.com/mall/en/WW/Catalog/Product/6EP13-33-4BA00)
Equipment Manual	↓ (https://support.industry.siemens.com/cs/ww/en/view/68036174)	↓ (https://support.industry.siemens.com/cs/ww/en/view/68022506)
Rated input voltage	120/230 V AC, with automatic switchover	120/230 V AC with automatic switchover
Output voltage	24 V DC	24 V DC
Rated output current	3 A	8 A
Power consumption	84 W	213 W

Using a SITOP power supply as an alternative to a load power supply

Alternatively, an external 24 V power supply from the SITOP range (https://mall.industry.siemens.com/mall/en/WW/Catalog/Products/10008864) (SITOP smart or SITOP modular) can be used:

- For higher output currents and 1-phase or 3-phase infeed
- With redundant installation (https://support.industry.siemens.com/cs/ww/de/view/109768676/en) of the 24 V power supply as protection against failure of a power supply unit
- With buffering of the 24 V power supply (e.g. with DC UPS) as protection against power failure
- With selective monitoring of 24 V loads as protection against overload or short-circuit

5.10   Connection elements and system cabling

Front connector and shield contact

The front connectors are used to wire the I/O modules. For modules with EMC-critical signals, such as analog modules and technology modules, the front connectors also need a shield contact.

The front connectors are available for 35 mm modules optionally with screw terminals and push-in terminals and for 25 mm modules with push-in terminals. The front connectors for 25 mm modules are included in the scope of delivery of the I/O modules.

24 V DC is supplied, for example, via a plug-in infeed element for analog modules.

The shield contact consists of shield bracket and shield terminal. Together with the shield terminal, the shield bracket allows the low-impedance, module-level connection of cable shields with minimum installation times. The shielding takes place without tools.

The components (infeed element, shielding bracket and shield clamp) are included in the scope of delivery of the modules.
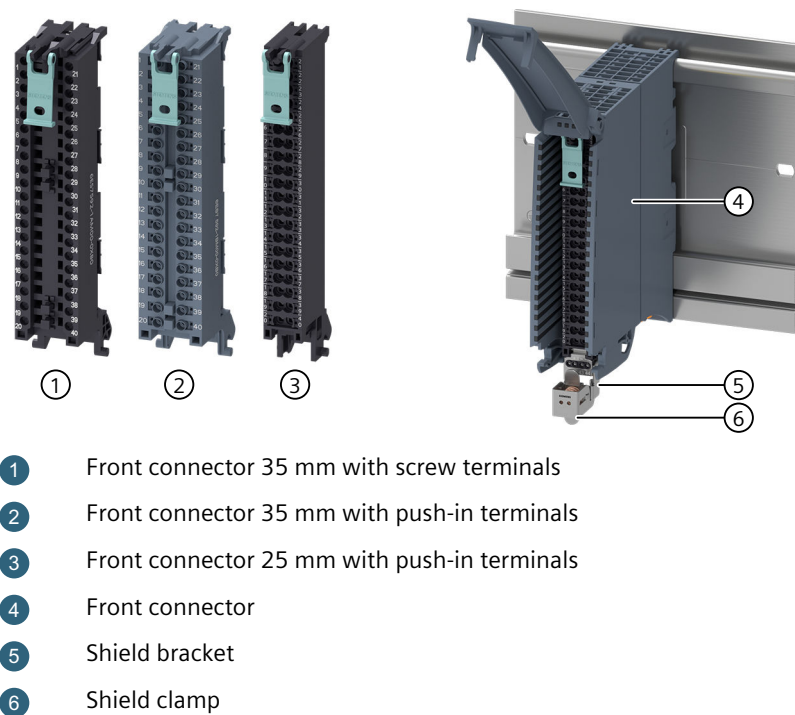

①	Front connector 35 mm with screw terminals
②	Front connector 35 mm with push-in terminals
③	Front connector 25 mm with push-in terminals
④	Front connector
⑤	Shield bracket
⑥	Shield clamp

Figure 5-24 Versions of the front connector with and without shield

U connector

The individual modules are connected to one another with the U connector. The U connector establishes the mechanical and electrical connection between the modules. The U connectors are included in the scope of delivery of the I/O modules.

System cabling SIMATIC TOP connect

Figure 5-25   Example: System cabling with SIMATIC TOP connect

For 35 mm modules, the system cabling SIMATIC TOP connect with prefabricated connection elements is available in two versions:

- Fully modular connection consisting of front connector module, connection cables and connection modules for connecting sensors and actuators from the field

- Flexible connection, consisting of front connector with single cores for wiring within the cabinet

You can find more information in the SIMATIC TOP connect for S7-1500 and ET 200MP (https://support.industry.siemens.com/cs/ww/en/view/95924607) manual.

5.11 Software

5.11.1 TIA Portal

The SIMATIC controllers are integrated into the Totally Integrated Automation Portal. Engineering with TIA Portal offers:

- Configuration and programming
- Shared data management
- A uniform operating concept for control, visualization and drives

The TIA Portal simplifies the integrated engineering in all configuration phases of a plant.
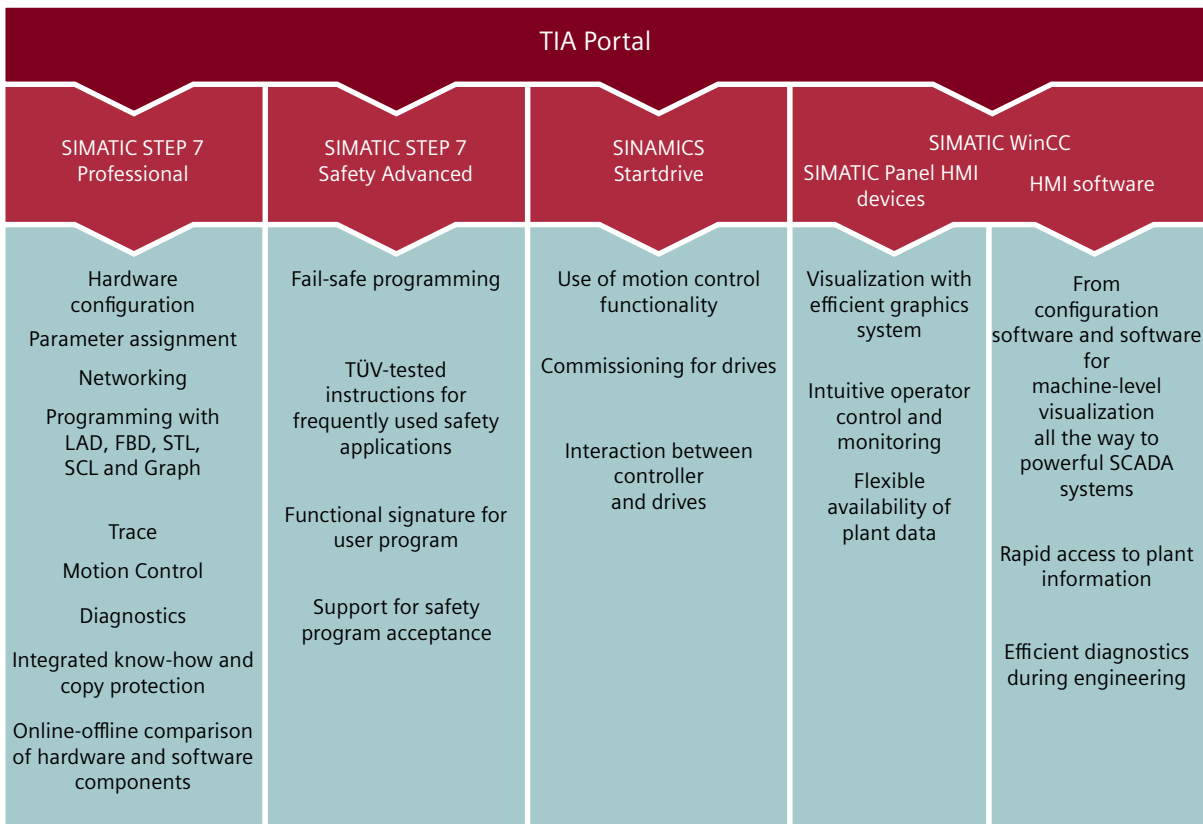

TIA Portal				
SIMATIC STEP 7 Professional	**SIMATIC STEP 7 Safety Advanced**	**SINAMICS Startdrive**	**SIMATIC Panel HMI devices**	**SIMATIC WinCC / HMI software**
Hardware configuration Parameter assignment Networking Programming with LAD, FBD, STL, SCL and Graph Trace Motion Control Diagnostics Integrated know-how and copy protection Online-offline comparison of hardware and software components	Fail-safe programming TÜV-tested instructions for frequently used safety applications Functional signature for user program Support for safety program acceptance	Use of motion control functionality Commissioning for drives Interaction between controller and drives	Visualization with efficient graphics system Intuitive operator control and monitoring Flexible availability of plant data	From configuration software and software for machine-level visualization all the way to powerful SCADA systems Rapid access to plant information Efficient diagnostics during engineering

Figure 5-26 TIA Portal overview

5.11.2 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 (https://new.siemens.com/global/en/products/automation/topic-areas/tia/tia-selection-tool.html).

5.11.3 SIMATIC Automation Tool

You use the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300) to perform commissioning and maintenance activities simultaneously on various SIMATIC S7 stations as a bulk operation independent of the TIA Portal. The SIMATIC Automation Tool provides you with a multitude of functions:

- Network browsing and creation of a table showing the accessible devices in the network.

- Flashing of device LEDs or HMI display to locate a device

- Downloading of addresses (IP, subnet, gateway) to a device

- Downloading the PROFINET name (station name) to a device

- Placing a CPU in RUN or STOP mode

- Setting the time in a CPU to the current time of your PG/PC

- Downloading a new program to a CPU or an HMI device

- Downloading from CPU, downloading to CPU or deleting recipe data from a CPU

- Downloading from CPU or deleting data log data from a CPU

- Backup/restore of data from/to a backup file for CPUs and HMI devices

- Downloading service data from a CPU

- Reading the diagnostics buffer of a CPU

- Performing a CPU memory reset

- Resetting devices to factory settings

- Downloading a firmware update to a device

- Documentation and backup of the configuration in

  – Standard .csv text file

  – Encrypted and password-protected .sat file

- Advanced functions:
  - Up to 10 concurrent connections
  - Scheduler for scheduling device operations at a time and frequency of your choosing
  - Ability to insert multiple devices in a single operation
  - Support for devices behind a NAT router
  - Archiving of SAT projects and related file data
  - Card browser for working with files and folders on SIMATIC Memory Cards in your CPUs

These functions can be executed as bulk operation, that is, simultaneously on various S7 stations and other devices.

The SIMATIC Automation Tool additionally has a Software Development Kit (SDK) version. With the SIMATIC Automation Tool SDK (Software Development Kit), you can create applications based on the SIMATIC Automation Tool API (Application Programming Interface). To deal with a large number of device automation tasks efficiently, these user-specific applications can be distributed to third parties including the API software. You do not need any license keys to use the user-specific applications.

5.11.4   SINETPLAN

SINETPLAN (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html), the Siemens Network Planner, supports you in planning automation systems and networks based on PROFINET. The tool facilitates professional and predictive dimensioning of your PROFINET installation as early as in the planning stage. In addition, SINETPLAN supports you during network optimization and helps you to exploit network resources optimally and to plan reserves. Thus, you prevent problems in commissioning or failures during productive operation even in advance of a planned operation. This increases the availability of the production plant and helps improve operational safety.

The advantages at a glance

- Network optimization thanks to port-specific calculation of the network load
- Increased production availability thanks to online scan and verification of existing systems
- Transparency before commissioning through import and simulation of existing STEP7 projects
- Efficiency through securing existing investment in the long term and optimal exploitation of resources

5.11.5 PRONETA

With SIEMENS PRONETA (PROFINET network analysis), you analyze the plant network during commissioning. PRONETA features two core functions:

- The topology overview independently scans PROFINET and all connected components.
- The IO check is a fast test of the wiring and the module configuration of a plant.

SIEMENS PRONETA (https://support.industry.siemens.com/cs/ww/en/view/67460624) is available for free on the Internet.

5.11.6 SIMATIC S7 app

With the SIMATIC S7 app (https://new.siemens.com/global/en/produkte/software/mobile-apps/simatic2go.html), you can establish a secure connection via WLAN to SIMATIC S7-1500 and ET 200SP with, for example, the following functions:

- Detect up to 50 networked CPUs via HTTPS and establish a connection
- Change CPU operating mode (RUN/STOP)
- Read out CPU diagnostics information and send via e-mail
- Monitor and modify variables and tags
- High security through encrypted communication and encrypted profile data; password to start app and establish the connection

Application planning

6

6.1 Hardware configuration

Introduction

The S7-1500 automation system/ET 200MP distributed I/O system consists of a single-row configuration in which all modules are installed on one mounting rail. The modules are connected by means of U connectors, and thus form a self-assembling backplane bus.

You can configure the S7-1500 automation system/ET 200MP distributed I/O system with fail-safe and non-fail-safe modules.

6.1.1 Hardware configuration of the S7-1500 automation system

Maximum configuration

- The integrated system power supply of the CPU supplies 10 W or 12 W (depending on CPU type) to the backplane bus. The power budget calculation determines the exact number of modules (without optional PS) that can be operated with the CPU. The operating principle is described in section Power balance calculation .

- A maximum of three system power supplies (PS) is possible. one system power supply (PS) can be inserted to the left of the CPU and two system power supplies (PS) can be inserted to the right of the CPU.

- If you use a system power supply (PS) left next to the CPU, a maximum configuration of 32 modules is possible. The modules occupy slots 0 to 31. If further system power supplies (PS) are required to the right of the CPU, they also occupy a slot.
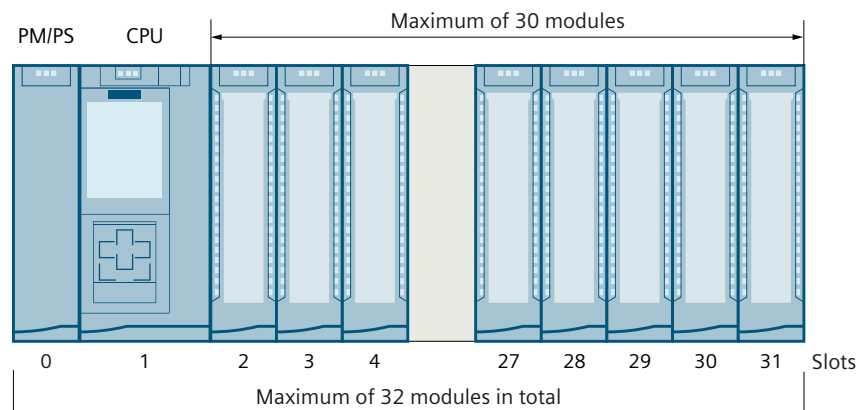

Figure 6-1 S7-1500 maximum configuration

Applicable modules

The following table shows which modules may be used in the various slots:

Table 6-1 Assignment of slot numbers

Module type	Permissible slots	Maximum number of modules
Load current supply (PM)*	0**	Unlimited / only 1 PM can be configured in STEP 7
System power supply (PS)	0; 2 - 31	3
PS 60W 24/48/60VDC HF system power supply	0	1***
CPU	1	1
Analog and digital I/O modules	2 - 31	30
Communication modules		
• Point-to-point	2 - 31	30
• PROFINET/Ethernet, PROFIBUS		
When using a CPU 1511-1(F) PN, CPU 1511C-1 PN, CPU 1511T(F)-1 PN	2 - 31	4
When using a CPU 1512C-1 PN	2 - 31	6
When using a CPU 1513(F)-1 PN	2 - 31	6
When using a CPU 1515(F)-2 PN, CPU 1515T(F)-2 PN	2 - 31	6
When using a CPU 1516(F)-3 PN/DP, CPU 1516T(F)-3 PN/DP, CPU 1516T(F)-3 PN	2 - 31	8
When using a CPU 1517(F)-3 PN/DP, CPU 1517(F)-3 PN, CPU 1517T(F)-3 PN/DP, CPU 1517T(F)-3 PN	2 - 31	8
When using a CPU 1518(F)-4 PN/DP, CPU 1518T(F)-4 PN/DP, CPU 1518(F)-4 PN/DP MFP, CPU 1518(F)-3 PN, CPU 1518T(F)-3 PN	2 - 31	8
Technology modules	2 - 31	30

* No connection to the backplane bus.

** When slot 0 is occupied by a load current supply (PM) in STEP 7, this slot can no longer be used for a system power supply (PS) in STEP 7. You do not have to configure a load current supply (PM) in STEP 7.

When you occupy slot "0" with the system power supply (PS), you can plug in a load current supply (PM) in the TIA Portal to the left of the PS in slot 100.

***The PS 60W 24/48/60VDC HF must only be inserted to the left of the CPU. Use a different system power supply (PS) for other power segments in the configuration to the right of the CPU.

6.1.2 Hardware configuration of the ET 200MP distributed I/O system with PROFINET interface module

Maximum configuration

- The integrated system power supply of the interface module feeds 14 W into the backplane bus. The power budget calculation determines the exact number of I/O modules that can be operated with the interface module (without optional PS). The operating principle is described in section Power balance calculation (Page 173).

- You use the integrated power supply for the IM 155-5 PN BA interface module. No 'additional system power supplies (PS) must be used. You can insert a maximum of 12 modules to the right of an interface module.

- The interface modules IM 155-5 MF HF and IM 155-5 PN HF also support the configuration with an active backplane bus. You can find information on the active backplane bus (e.g. installing, configuring, technical specifications) in the Active backplane bus (https://support.industry.siemens.com/cs/us/en/view/109778694) Equipment Manual.

- The following applies to the interface modules IM 155-5 PN ST and IM 155-5 PN HF: A maximum of three system power supplies (PS) is possible. You can insert one system power supply (PS) to the left of the interface module and two system power supplies (PS) to the right of the interface module.
If you insert a system power supply (PS) to the left of the interface module, this yields a possible maximum configuration of a total of 32 modules (up to 30 modules to the right of the interface module). If further system power supplies (PS) are required to the right of the interface module, they also occupy a slot.
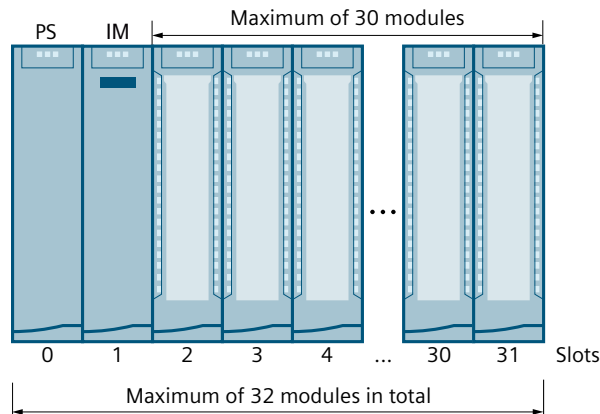

Figure 6-2 Maximum configuration ET 200MP with IM 155-5 PN ST or IM 155-5 PN HF

Applicable modules

The following table shows which modules may be used in the various slots:

Table 6-2 Assignment of slot numbers

Module type	Permissible slots IM 155-5 PN BA	Permissible slots IM 155-5 PN ST, IM 155-5 PN HF	Maximum number of modules
Load current supply (PM)*	-	0**	Unlimited / only 1 PM can be configured in STEP 7
System power supply (PS)	-	0; 2 - 31	3
PS 60W 24/48/60VDC HF system power supply	-	0	1***
Interface module	1	1	1
Analog and digital I/O modules	2 - 13	2 - 31	12 or 30
Communication modules			
• Point-to-point	2 - 13	2 - 31	12 or 30
Technology modules	2 - 13	2 - 31	12 or 30

* No connection to the backplane bus.

** When slot 0 is occupied by a load current supply (PM) in STEP 7, this slot can no longer be used for a system power supply (PS) in STEP 7. You do not have to configure a load current supply (PM) in STEP 7.

***The PS 60W 24/48/60VDC HF must only be inserted to the left of the interface module. Use a different system power supply (PS) for other power segments in the configuration to the right of the interface module.

6.1.3   Hardware configuration of the ET 200MP distributed I/O system with PROFIBUS interface module

Maximum configuration

The integrated system power supply of the interface module feeds 14 W into the backplane bus. You can insert a maximum of 12 modules to the right of an interface module. The power budget calculation determines the exact number of I/O modules that can be operated with the interface module. The operating principle is described in section Power balance calculation (Page 173).
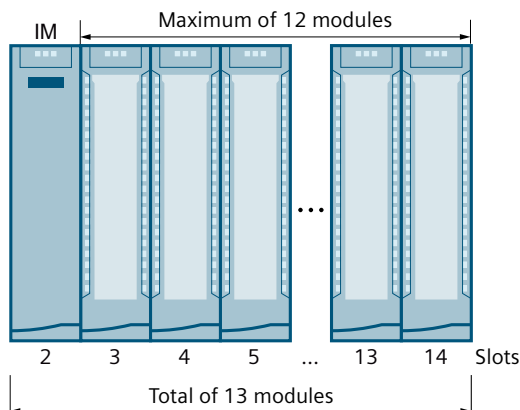

Figure 6-3 Maximum configuration ET 200MP with IM 155-5 DP

Applicable modules

The following table shows which modules may be used in the various slots:

Table 6-3 Assignment of slot numbers

Module type	Permissible slots	Maximum number of modules
Interface module	2	1
Analog and digital I/O modules	3 - 14	12
Communications modules		
Point-to-point	3 - 14	12
Technology modules	3 - 14	12

6.2   System and load power supply

Types of power supplies

The S7-1500 automation system/ET 200MP distributed I/O system distinguishes between two types of power supply:

- System power supply (PS)
- Load current supply (PM)

System power supply (PS)

The system power supply has a connection to the backplane bus (U connector) and supplies solely the internally required system voltage. This system voltage supplies parts of the module electronics and the LEDs. A system power supply can also supply CPUs or interface modules if these are not connected to a 24 VDC load current supply.

Load current supply (PM)

The load current supply feeds the input/output circuits of the modules, as well as the sensors and actuators of the plant, if installed. If you supply the voltage for the backplane bus via a system power supply, then the supply of the CPU/interface module with 24 V DC is optional.

Special characteristic of the load current supply

Load current supplies are mounted on the "S7-1500 mounting rail" and do not have a connection to the backplane bus.

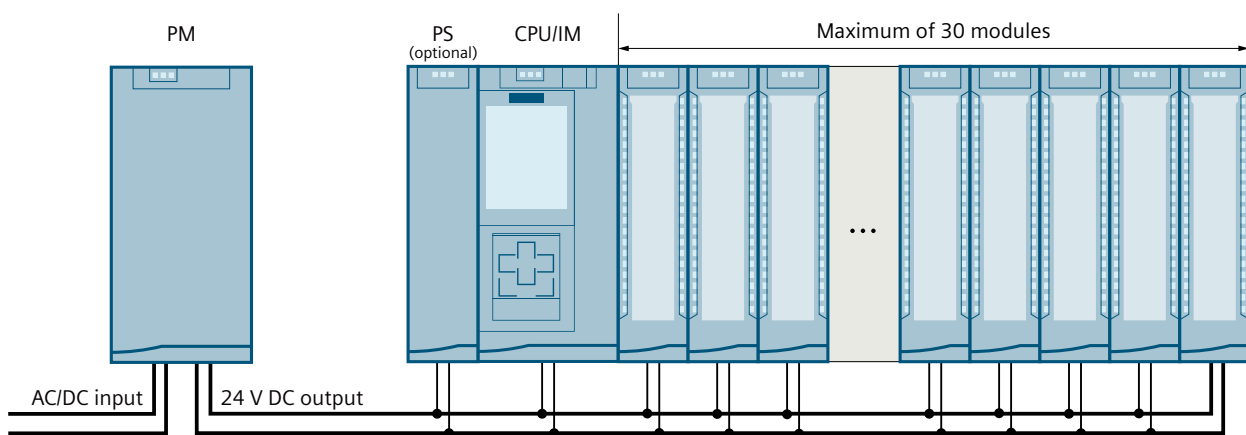## Total configuration with power supplies

Figure 6-4 Total configuration with load current supply (PM) and system power supply (PS)

Optionally, you can insert up to two system power supplies (PS) in the slots to the right of the CPU/interface module.

The number of load current supplies is unlimited.

Observe the installation rules and specified installation distances in the manuals of the load current supplies.

System power supplies

- PS 25W 24VDC: Supply voltage with 24 V DC and infeed power to the backplane bus of 25 W

- PS 60W 24/48/60VDC: Supply voltage with 24/48/60 V DC and infeed power to the backplane bus of 60 W

- PS 60W 24/48/60VDC HF:
  - Supply voltage with 24/48/60 V DC and infeed power to the backplane bus of 60 W
  - Extended retentive memory for CPUs as of FW V2.1.0 (see section Special requirements when using a system power supply PS 60W 24/48/60VDC HF (Page 169)).

- PS 60W 120/230V AC/DC: Supply voltage with 120/230 V AC and infeed power to the backplane bus of 60 W

Load current supplies

The load current supplies listed below have been technically adapted especially to the S7-1500 automation system/ET 200MP distributed I/O system. Use of the listed load current supplies is not imperative because you can use a SITOP module, for example, as an alternative.

- PM 70W 120/230VAC: Supply voltage with 120/230 V AC
- PM 190W 120/230VAC: Supply voltage with 120/230 V AC

Also note the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/96998532) in connection with load current supply units.

6.2.1 Use of system power supplies

Introduction

You can use system power supplies with the CPUs and the interface modules IM 155-5 PN ST and IM 155-5 PN HF.

If the power fed from the CPU/interface module into the backplane bus is not sufficient to supply all connected modules with power, system power supplies (PS) are required.

Whether or not you need a system power supply depends on the power consumption of the modules used. The power supplied by the CPU/interface module and the system power supplies must be greater than the power required by the I/O modules.

During configuration, STEP 7 compares the supplied power and the power required by the modules. If the required power is too high, you receive a corresponding message from STEP 7.

In addition, the system power supply PS 60W 24/48/60V DC HF buffers the power in the event of power failures and therefore enables the retentivity of the data of a CPU – without a battery and therefore maintenance-free.

Slots for system power supplies

The following slots may be used for system power supplies:

- A system power supply in slot 0 to the left of the CPU/interface module
- Up to 2 system power supplies in the slots to the right of the CPU/interface module (power segments) A power segment consists of a power supply module and the modules supplied by it.

NOTE

The system power supply PS 60W 24/48/60V DC HF can only be inserted in slot 0.

Power segment

The following applies for the CPUs and interface modules M 155-5 PN ST and IM 155-5 PN HF: If you are using system power supplies to the right of the CPU/interface module, divide the configuration into power segments.

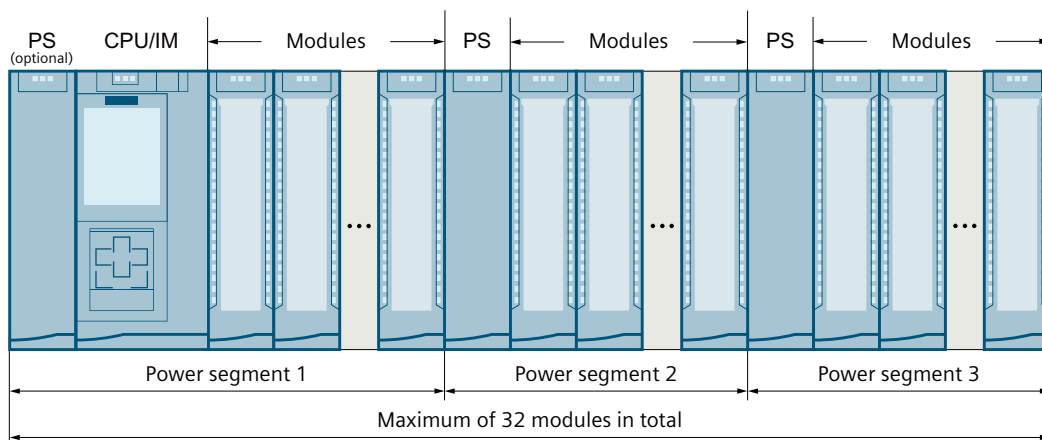**Configuration variant with power segments**

Figure 6-5   Configuration variants with 3 power segments

NOTE

When you configure with STEP 7, STEP 7 automatically checks configuration for consistency and tells you from which module you must open a new power segment.

Overload in the power segment

If an overload occurs in a power segment, the red SF LED flashes on the system power supply (PS). All I/O modules to the right of the PS in the power segment will be switched off.

Remedy:

1. Correct the configuration in the power segment of the overloaded PS.

2. Switch the supply voltage power off and on again via the on-off switch on the PS.

3. Switch the CPU from STOP to RUN mode.

Reference

Information about the required power is available in the section Power balance calculation (Page 173).

Additional information on the performance values (power feed, power consumption) of the CPU, interface module, system power supply, and I/O modules can be found in the manuals (https://support.automation.siemens.com/WW/view/en/57251228) of the respective modules.

6.2.2 Special considerations for the use of a system power supply in the first power segment

Infeed options

There are three options for the infeed of the required system voltage in the backplane bus:

- Infeed via CPU/interface module
- Infeed via CPU/interface module and system power supply
- Infeed only via system power supply in slot 0

Infeed via CPU/interface module

Infeed via the CPU/interface module generally suffices for small and medium hardware configurations. The power consumption of the connected modules must not exceed the power supplied by the CPU/interface module.

In this configuration variant, supply the CPU/interface module with 24 V DC from a load current supply.

Procedure

To set up the supply by means of the CPU/interface module, follow these steps:

1. Open the "Properties" tab of the CPU/interface module in STEP 7 and select the "System power supply" in the navigation.

2. Select the option "Connection to supply voltage L+".

General

General

⦿ Connection to supply voltage L+

◯ No connection to supply voltage L+
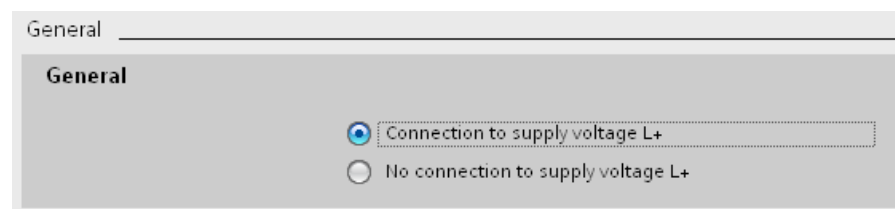
Figure 6-6 Supply voltage via CPU/interface module only

Infeed via CPU/interface module and system power supply

> For larger hardware configurations, infeed into the backplane bus by the CPU/interface module alone no longer suffices. If the modules consume more power in total than the power supplied by the CPU/interface module, you must insert an additional system power supply.
>
> Supply the system power supply with the permissible supply voltage and the CPU/interface module with 24 V DC.
>
> Both the system power supply and the CPU/interface module feed current into the backplane bus. The supplied power is summed.
>
> Power addition: "Infeed power of the system power supply" + "Infeed power of the CPU/interface module"

Procedure

> To set up the supply by means of the CPU/interface module and system power supply, follow these steps:
>
> 1. Open the "Properties" tab of the CPU/interface module in STEP 7 and select the "System power supply" in the navigation.
>
> 2. Select the option "Connection to supply voltage L+".
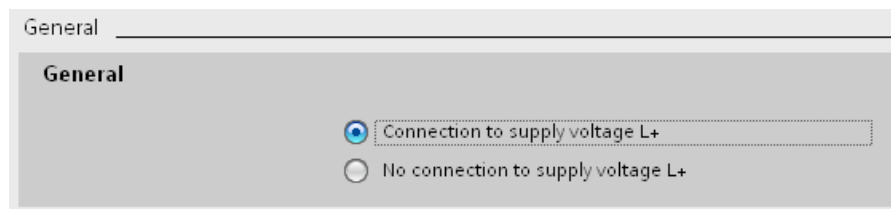
Figure 6-7 Supply voltage via the CPU/interface module and system power supply

Infeed via system power supply only

> As a further possibility you can supply the required power to the backplane bus using only a system power supply (in slot 0). In this case, the CPU/interface module is not supplied with 24 V DC, and draws its supply from the backplane bus. The system power supply must be inserted to the left of the CPU/interface module for this.
>
> In general, you can use system power supplies with AC or DC infeed for the configuration.
>
> If no supply voltage with 24 V DC is present (and e.g. only CMs/CPs are inserted next to the CPU), you can use a system power supply with 230 V AC because the CMs/CPs are supplied via the backplane bus.

Procedure

To set up infeed only via the system power supply, follow these steps:

1. Open the "Properties" tab of the CPU/interface module in STEP 7 and select the "System power supply" in the navigation.

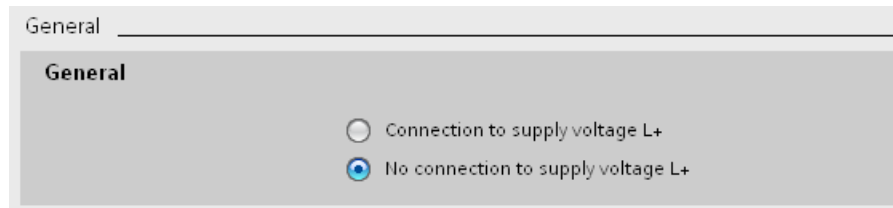2. Select the option "No connection to supply voltage L+".

Figure 6-8 No infeed into the backplane bus by means of the CPU/interface module

6.2.3 Special requirements when using the power supply PS 60W 24/48/60VDC HF

S7-1500 - Extended retentive memory for CPUs as of FW V2.1.0

When you use the PS 60W 24/48/60VDC HF system power supply, the entire data area can be used as retentive memory for CPUs as of firmware version V2.1.0 and higher.

The PS 60W 24/48/60VDC HF supplies enough energy in case of a POWER OFF that the CPU can save the entire data area retentively.

Requirements

• STEP 7 V14 SP1 or higher

• PS 60W 24/48/60VDC HF system power supply

• CPU with firmware version as of V2.1.0, see table below

Applicable CPUs

The size of the retentive memory depends on the size of the work memory for data of the CPU used. The table below shows the applicable CPUs with the required hardware function versions.

CPU with firmware version V2.1.0 or higher	Hardware function version	Article number	Max. retentive memory
CPU 1511-1 PN	FS01 or higher	6ES7511-1AK01-0AB0 6ES7511-1AK02-0AB0	1 MB
		6ES7511-1AL03-0AB0	1.5 MB
CPU 1511F-1 PN	FS01 or higher	6ES7511-1FK01-0AB0 6ES7511-1FK02-0AB0	1 MB
		6ES7511-1FL03-0AB0	1.5 MB
CPU 1511T-1 PN	FS01 or higher	6ES7511-1TK01-0AB0	1 MB
		6ES7511-1TL03-0AB0	1.5 MB
CPU 1511TF-1 PN	FS01 or higher	6ES7511-1UK01-0AB0	1 MB
		6ES7511-1UL03-0AB0	1.5 MB

CPU with firmware version V2.1.0 or higher	Hardware function version	Article number	Max. retentive memory
CPU 1511C-1 PN	FS01 or higher	6ES7511-1CK00-0AB0 6ES7511-1CK01-0AB0	1 MB
		6ES7511-1CL03-0AB0	1.5 MB
CPU 1512C-1 PN	FS01 or higher	6ES7512-1CK00-0AB0 6ES7512-1CK01-0AB0	1 MB
		6ES7512-1CM03-0AB0	2 MB
CPU 1513-1 PN	FS01 or higher	6ES7513-1AL01-0AB0 6ES7513-1AL02-0AB0	1.5 MB
		6ES7513-1AM03-0AB0	2.5 MB
CPU 1513F-1 PN	FS01 or higher	6ES7513-1FL01-0AB0 6ES7513-1FL02-0AB0	1.5 MB
		6ES7513-1FM03-0AB0	2.5 MB
CPU 1515-2 PN	FS01 or higher	6ES7515-2AM01-0AB0 6ES7515-2AM02-0AB0	3 MB
		6ES7515-2AN03-0AB0	4.5 MB
CPU 1515F-2 PN	FS01 or higher	6ES7515-2FM01-0AB0 6ES7515-2FM02-0AB0	3 MB
		6ES7515-2FN03-0AB0	4.5 MB
CPU 1515T-2 PN	FS01 or higher	6ES7515-2TM01-0AB0	3 MB
		6ES7515-2TN03-0AB0	4.5 MB
CPU 1515TF-2 PN	FS01 or higher	6ES7515-2UM01-0AB0	3 MB
		6ES7515-2UN03-0AB0	4.5 MB
CPU 1516-3 PN/DP	FS01 or higher	6ES7516-3AN01-0AB0 6ES7516-3AN02-0AB0	5 MB
		6ES7516-3AP03-0AB0	7.5 MB
CPU 1516F-3 PN/DP	FS01 or higher	6ES7516-3FN01-0AB0 6ES7516-3FN02-0AB0	5 MB
		6ES7516-3AP03-0AB0	7.5 MB
CPU 1516T-3 PN	FS01 or higher	6ES7516-3TP10-0AB0	15 MB
CPU 1516T-3 PN/DP	FS01 or higher	6ES7516-3TN00-0AB0	5 MB
CPU 1516TF-3 PN	FS01 or higher	6ES7516-3UP10-0AB0	15 MB
CPU 1516TF-3 PN/DP	FS01 or higher	6ES7516-3UN00-0AB0	5 MB
CPU 1517-3 PN	FS01 or higher	6ES7517-3AQ10-0AB0	50 MB
CPU 1517-3 PN/DP	FS03 or higher	6ES7517-3AP00-0AB0	8 MB
CPU 1517F-3 PN	FS01 or higher	6ES7517-3FQ10-0AB0	50 MB
CPU 1517F-3 PN/DP	FS03 or higher FS01 or higher	6ES7517-3FP00-0AB0 6ES7517-3FP01-0AB0	8 MB
CPU 1517T-3 PN	FS01 or higher	6ES7517-3TQ10-0AB0	50 MB
CPU 1517T-3 PN/DP	FS01 or higher	6ES7517-3TP00-0AB0	8 MB
CPU 1517TF-3 PN	FS01 or higher	6ES7517-3UQ10-0AB0	50 MB
CPU 1517TF-3 PN/DP	FS01 or higher	6ES7517-3UP00-0AB0	8 MB

CPU with firmware version V2.1.0 or higher	Hardware function version	Article number	Max. retentive memory
CPU 1518-3 PN	FS01 or higher	6ES7518-3AT10-0AB0	100 MB
CPU 1518F-3 PN	FS01 or higher	6ES7518-3FT10-0AB0	100 MB
CPU 1518T-3 PN	FS01 or higher	6ES7518-3TT10-0AB0	100 MB
CPU 1518TF-3 PN	FS01 or higher	6ES7 518-3UT10-0AB0	100 MB
CPU 1518-4 PN/DP	FS03 or higher	6ES7518-4AP00-0AB0	20 MB
CPU 1518F-4 PN/DP	FS03 or higher	6ES7518-4FP00-0AB0	20 MB
CPU 1518T-4 PN/DP	FS01 or higher	6ES7518-4TP00-0AB0	20 MB
CPU 1518TF-4 PN/DP	FS01 or higher	6ES7518-4UP00-0AB0	20 MB
CPU 1518-4 PN/DP MFP	FS01 or higher	6ES7518-4AX00-1AB0	20 MB
CPU 1518F-4 PN/DP MFP	FS01 or higher	6ES7518-4FX00-1AB0	20 MB

Connection, structure and configuration of an S7-1500 with PS 60W 24/48/60VDC HF

- You must insert the system power supply PS 60W 24/48/60VDC HF in slot 0.

Figure 6-9 Slot PS 60W 24/48/60VDC HF

- If you are using the PS 60W 24/48/60VDC HF, the 24 V supply of the CPU is not taken into account in the power budget calculation.

NOTE

You may only connect the 24 V DC supply voltage directly to the system power supply and not to the CPU.

You must set the "System power supply" parameter to the option "No connection to supply voltage L+" during configuration of the CPU. STEP 7 checks the setting when compiling the configuration.
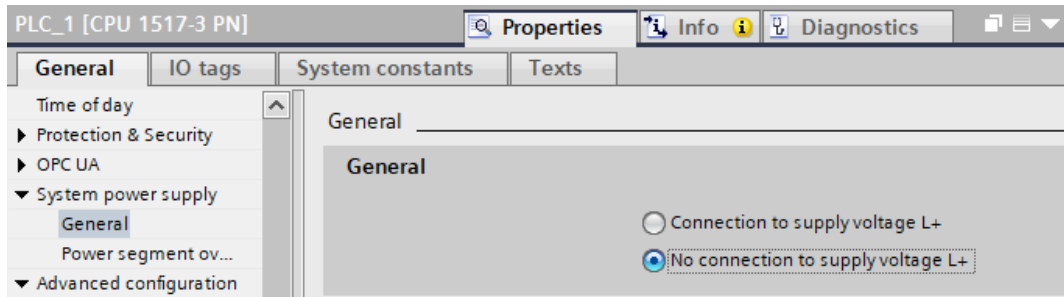
Figure 6-10 Connecting PS 60W 24/48/60VDC HF

- The parameter "Startup > Comparison preset to actual module" must be set to the value "Startup CPU only if compatible" during configuration of the PS 60W 24/48/60VDC HF. Reason: The retentivity of the entire CPU work memory (data) is only guaranteed when the PS 60W 24/48/60VDC HF is inserted.

  When you insert the PS 60W 24/48/60VDC HF, STEP 7 automatically sets the parameter.
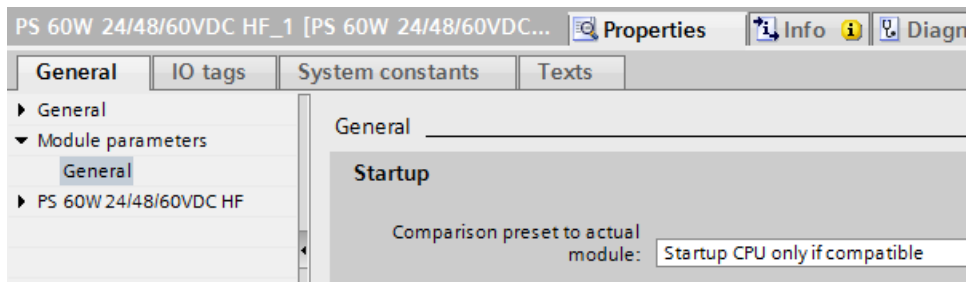
Figure 6-11 Startup of PS 60W 24/48/60VDC HF

NOTE

Other power segments in the configuration

The PS 60W 24/48/60VDC HF must only be inserted to the left of the CPU / interface module.

Use a different system power supply (PS) for other power segments in the configuration to the right of the CPU / interface module.

Missing diagnostics for the PS 60W 24/48/60VDC HF

In case of POWER OFF, saving the extended retentive data is most important. The CPU as of FW V2.1.0 and higher does **no longer** output the following diagnostics of the PS 60W 24/48/60VDC HF:

- Supply voltage fault
- Switch position Off

6.3 Power balance calculation

Principle of power balance calculation

In order to ensure the supply of the modules from the backplane bus, the power balance calculation compares the infed power with the required power for the modules. The supplied power of all system power supplies including the CPU/interface module must be greater than or equal to the power taken from the modules.

In order to operate the configuration with its used modules, the power balance must be positive for each power segment in use.

This means that the power fed into the power segment is greater than the power consumed by the modules.

Take care even during planning, that the power fed into the backplane bus is always greater than or equal to the power drawn. The TIA Selection Tool (https://new.siemens.com/global/en/products/automation/topic-areas/tia/tia-selection-tool.html) aids you during planning.

The power fed into the backplane bus by the CPU/interface module and system power supply is listed in the technical specifications of the CPU/interface module in the corresponding manuals.

The power consumed from the backplane bus by an I/O module or the CPU/interface module can be found in the technical specifications in the corresponding manuals.

The power balance calculation is performed:

- When configuring with STEP 7
- During operation by the CPU

Power balance calculation when configuring with STEP 7

STEP 7 checks compliance with the power balance during the configuration.

Proceed as follows to evaluate the power balance calculation:

1. Perform the configuration of the S7-1500/ET 200MP with all the required modules.

2. In the network view, select the CPU/interface module or the system power supply.

3. Open the "Properties" tab in the inspector window.

4. Select the "System power supply" entry in the area navigation.

5. Check the "Power segment overview" table, so see whether the power balance is positive. If the power balance is negative, STEP 7 marks the underpowered modules in red.

Figure 6-12 Example of a power balance calculation with STEP 7

Power balance calculation check for overload by the CPU/interface module

The CPU / the interface module monitors compliance with a positive power balance:

- At every POWER ON
- At every change of the installed hardware

Causes for overload

An overload can still occur despite a positive power balance during planning. The cause for overload can be a hardware configuration that does not correspond to the configuration in STEP 7, for example:

- More I/O modules inserted in the actual configuration than in the STEP 7 project.
- A supply voltage L+ (24 V DC) that is necessary for operation is not connected when system voltage infeed via the CPU/interface module is specified during parameter assignment (see section Special considerations for the use of a system power supply in the first power segment (Page 167)).
- A system power supply that is necessary for operation is not inserted.
- A system power supply that is necessary for operation is not switched on (power connection plug or on/off switch).
- A system power supply that is necessary for operation has no U connector inserted.

Response of the CPU to negative power balance or failure of system power supplies

As soon as the CPU detects a negative power balance/overload, the following actions are executed:

- The CPU stores the retentive data.
- The CPU enters the event in the diagnostics buffer.
- The CPU carries out a restart and repeats this until the cause of the negative power balance is resolved.

Response of the interface module to negative power balance or failure of system power supplies

As a result of the overload, the interface module switches off all power segments. The I/O controller or DP master can no longer access the I/O modules. The interface module provides diagnostic information and periodically checks the connection to the backplane bus and re-establishes the connection.

Exception: In the case of a voltage drop or a hardware fault in power segment 2 or 3, the corresponding system power supply module switches off its power segment (and possibly the following segments), and generates a diagnostic alarm, if possible.

More information on the behavior of the system power supply (PS) in the event of a fault can be found in the manuals for the system power supplies.

6.4 Use of load power supplies

Introduction

The load current supply (PM) supplies the system power (PS), central modules (CPU), interface module and input and output circuits of the I/O modules with DC 24 V.

Load current supplies can be mounted on the mounting rail but do not have a connection to the backplane bus.

Observe the installation rules and specified installation distances in the manuals of the load current supplies.

Use of multiple load current supplies

Several load current supplies (PM) can be used as follows for higher output currents:

Every load current supply feeds independent 24 V DC load lines.

Alternatively you can use an external 24 V power supply, e.g. from the SITOP line.
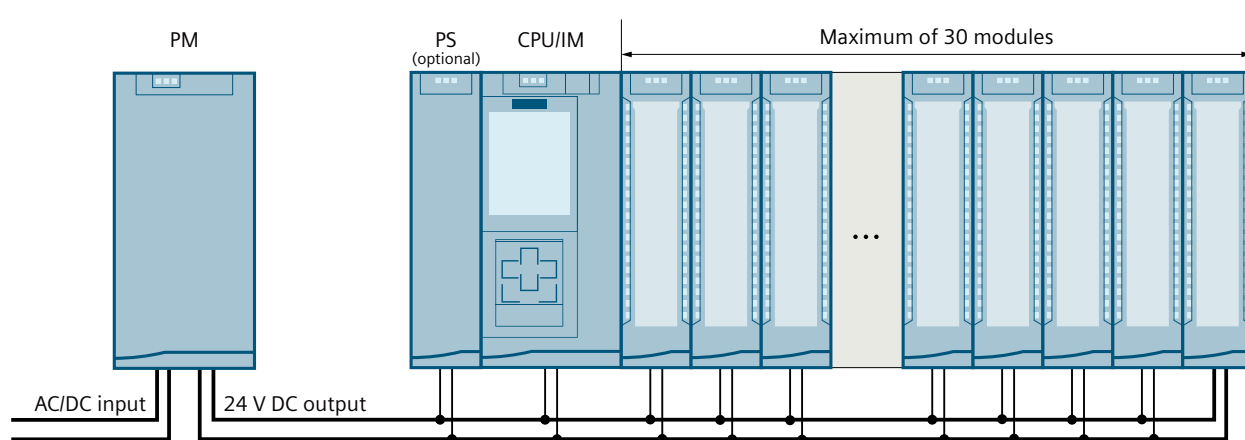
Figure 6-13 Supply of the modules from 24 V DC load current suppl

---

NOTE

Alternative 24 V supply of the modules from the control cabinet

If safe electrical separation (SELV/PELV according to IEC 61131-2 and IEC 61010-2-201) is guaranteed, you can alternatively supply the modules with 24 V DC from the control cabinet.

Reference

More information on load current supplies can be found on the Internet (https://mall.industry.siemens.com) in the online catalog and in the online ordering system.

Installation

7

7.1 Basics

Introduction

All modules of the S7-1500 automation system/ET 200MP distributed I/O system are open equipment. This means that you may only install this system in housings, cabinets or electrical operating rooms that are located indoors. The housings, cabinets and electrical operating rooms must guarantee protection against electric shock and spread of fire. The requirements for mechanical strength must also be met. The housings, cabinets, and electrical operating rooms must not be accessible without a key or tool. Personnel with access must have been trained or authorized.

Installation position

The S7-1500 automation system / ET 200MP distributed I/O system is designed for the following mounting positions:

- Horizontal mounting position for ambient temperatures up to 60 °C
- Vertical mounting position (CPU is down) for ambient temperatures up to 40 °C

More information can be found in chapter Mechanical and climatic ambient conditions (Page 414).

Mounting rail

You can mount the following components on the mounting rails alongside the S7-1500/ET 200MP modules:

- Modules from the S7-1200 and ET 200SP range
- Terminals
- Circuit breakers
- Small contactors
- Similar components

These components can influence the installation dimensions for the cable duct.

Modules can be mounted right to the outer edge of the mounting rail.

The mounting rails are available in various lengths. You order the mounting rails using the online catalog or the online ordering system. You can find the available lengths and article numbers in the section Accessories/spare parts (Page 425).

Minimum clearances

The modules can be mounted to the outer edge of the mounting rail. Maintain the following minimum clearances at the top and bottom when installing or removing the S7-1500 automation system / ET 200MP distributed I/O system:
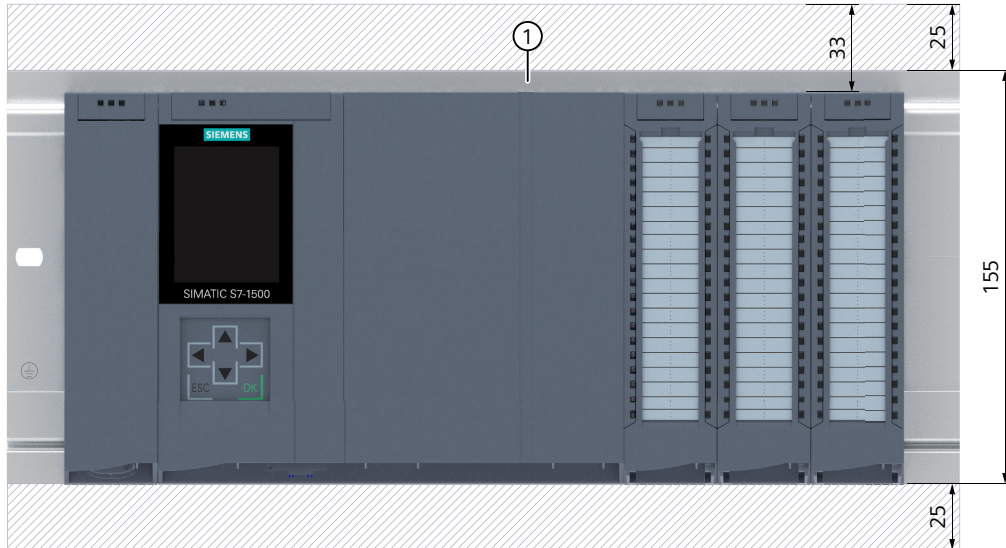
①   Upper edge of the mounting rail

Figure 7-1   Minimum clearances in the control cabinet

Installation rules

- The installation starts on the left with a CPU/interface module or a system power supply/load current supply.
- You connect the modules to each other with U connectors.
- Note that no U connector protrudes from the first and last module.

NOTE

Only remove and insert modules when the power to the system is switched off.

> ⚠️ **WARNING**
>
> **Protection from conductive contamination**
>
> Protect the devices against conductive contamination. At the same time, note the ambient conditions.
>
> Protection from conductive contamination can, for example, be achieved by installing the devices in a control cabinet with the appropriate degree of protection.

7.2 Installing the mounting rail

Lengths and drill holes

The mounting rails are delivered in six lengths:

- 160 mm
- 245 mm
- 482.6 mm (19 inches)
- 530 mm
- 830 mm
- 2 000 mm

You can find the article numbers in the appendix Accessories/spare parts (Page 425).

The mounting rails (from 160 to 830 mm) come with two drill holes for fixing screws. A set of screws for grounding the mounting rail is provided.

The 2 000 mm mounting rail is designed for assemblies with special lengths and does not have holes for fixing screws. No set of screws for grounding is enclosed with the mounting rail (can be ordered as Accessories/spare parts (Page 425)).

The specifications of the maximum offsets between two drill holes can be found in the table, "Dimensions for the drill holes".

Tools required

- Commercially available hacksaw
- Drill Ø 6.5 mm
- Screwdriver
- Size 10 adjustable screw-wrench or socket wrench for grounding cable connection
- Adjustable screw-wrench, matching the selected fixing screws
- Stripping tool and crimp tool for the grounding cable

Required accessories

Use the following screw types for fastening the mounting rails:

Table 7-1 Required accessories

For ...	you can use ...	Explanation
• Outer fixing screws • Additional fixing screws (for mounting rails > 482.6 mm)	M6 socket cap screw	Choose a suitable screw length for your assembly. You also need washers for cylinder head screws with an internal diameter of 6.4 mm and an external diameter of 11 mm.
	M6 hex screw	

Dimensions for the drill holes

Table 7-2 Dimensions for the drill holes

"Standard" mounting rails	"Longer" mounting rails

Length of the mounting rail	Distance a	Distance b
160 mm	10 mm	140 mm
245 mm	10 mm	225 mm
482.6 mm	8.3 mm	466 mm
530 mm	15 mm	500 mm
830 mm	15 mm	800 mm

Additional fixing screws (for mounting rails > 530 mm)

For mounting rails longer than 530 mm, we recommend using additional fixing screws at intervals of >482 mm on the identification groove.

Preparing the 2 000 mm mounting rail for installation

To prepare the 2 000 mm mounting rail for installation, proceed as follows:

1. Cut the 2 000 mm mounting rail to the required length.

2. Mark the holes. The necessary dimensions can be found in the table "Dimensions for the drill holes":

    – Two drill holes at the beginning and end of the mounting rail

    – Additional drill holes at equal intervals of 500 mm maximum, along the identification groove

3. Drill the marked holes according to the selected type of fastening.

4. Ensure that there are no burrs or shavings on the mounting rail.

NOTE

To ensure secure installation of the modules, make sure you position the drill holes centered on the identification groove and only use screws of the maximum size.

---
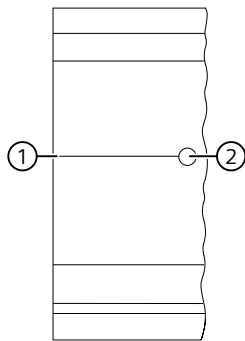
①   Identification groove for additional drill holes

②   Additional drill hole

Figure 7-2   Preparing the 2 000 mm mounting rail for installation

Installing the mounting rail

Place the mounting rail such that sufficient space remains for installation of and heat dissipation from the modules. Note the figure Minimum clearances in the control cabinet (Page 177-178).

Screw the rail onto the mounting surface.

Attaching the protective conductor

The S7-1500 automation system/ ET 200MP distributed I/O system has to be connected to the protective conductor system of the electrical system to ensure electrical safety.

Proceed as follows to connect the protective conductor:

1. Strip the ground conductor with a minimum diameter of 10 mm². Attach a ring cable lug for M6 bolts with the crimping pliers.

2. Slide the enclosed bolt into the T profile groove.

3. Insert the spacer, ring terminal with the grounding connector, flat washer, and lock washer onto the bolt (in that order). Thread on the hexagon nut. Fasten the components in place with the nut (tightening torque 4 Nm).

4. Connect the opposite end of the grounding cable to the central grounding point/protective conductor busbar (PE).
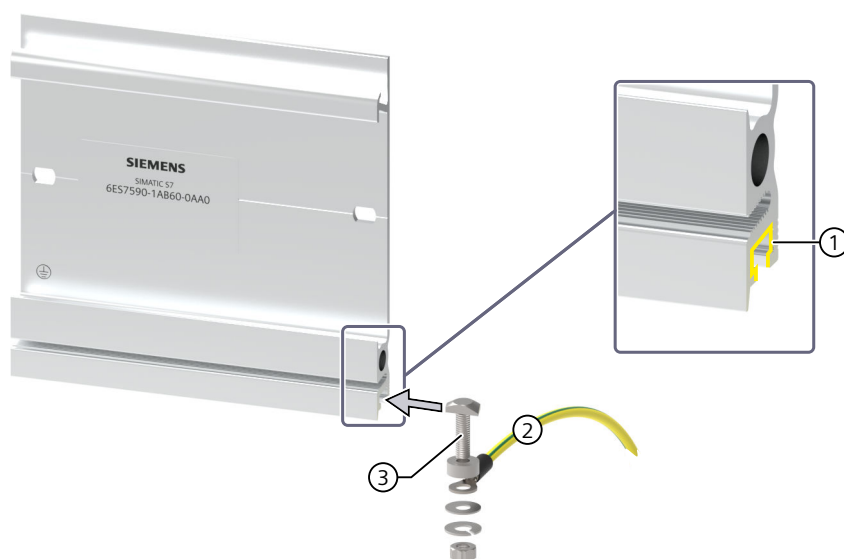
①   T-profile groove

②   Protective conductor (PE)

③   PE connection element for mounting rail

Figure 7-3   Attaching the protective conductor (protective earth)

NOTE

Alternative grounding of the mounting rail

Grounding with the grounding screw is not required if the following requirements are met:

The mounting rails must be permanently connected to the protective circuit using an equivalent fitting that complies with the applicable standards, for example by permanent attachment to a grounded control cabinet wall.

Note

You can find more information on the exact dimensions of the mounting rails in the appendix Dimension drawings of the mounting rails (Page 418).

7.3 Installing the standard rail adapter

Introduction

The DIN rail adapter allows you to mount the SIMATIC S7-1500/ET 200MP automation system on the standard 35 mm mounting rails.

You order the DIN rail adapter as separate accessories.

NOTE

Note the following reduced technical specifications regarding mechanical load when you install the S7-1500/ET 200MP modules on the 35 mm DIN rail using the DIN rail adapter:

Vibration test acc. to IEC 60068-2-6 (sinusoidal)

- 5 Hz ≤ f ≤ 8.4 Hz, constant amplitude **3.5 mm**
- 8.4 Hz ≤ f ≤ 150 Hz, constant acceleration **1 g**

Duration of vibration: 10 frequency sweeps per axis in each of three perpendicular axes

Shock, tested according to IEC 60068-2-27

- Type of shock: Half-sine
- Shock intensity: **150 m/s^2** peak value, **11 ms** duration
- Direction of shock: **3** shocks each in (+/-) direction, along each of the 3 mutually perpendicular axes

---

Article number

6ES7590-6AA00-0AA0

The scope of delivery consists of ten adapters, ten hexagon socket-head screws and ten washers.

View

The DIN rail adapter consists of a clamp, an adapter frame and a hexagon socket-head screw with washer.
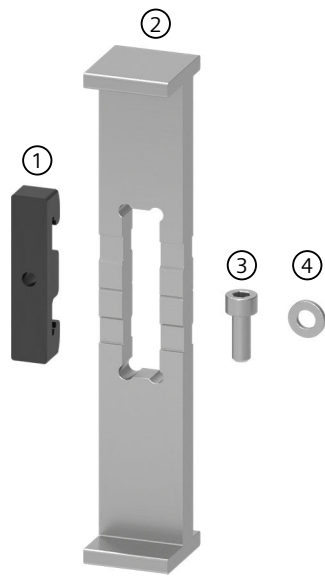
①   Clamp
②   Adapter frame
③   Hexagon socket-head screw
④   Washer

Figure 7-4 Parts of the DIN rail adapter

Dimensional drawing
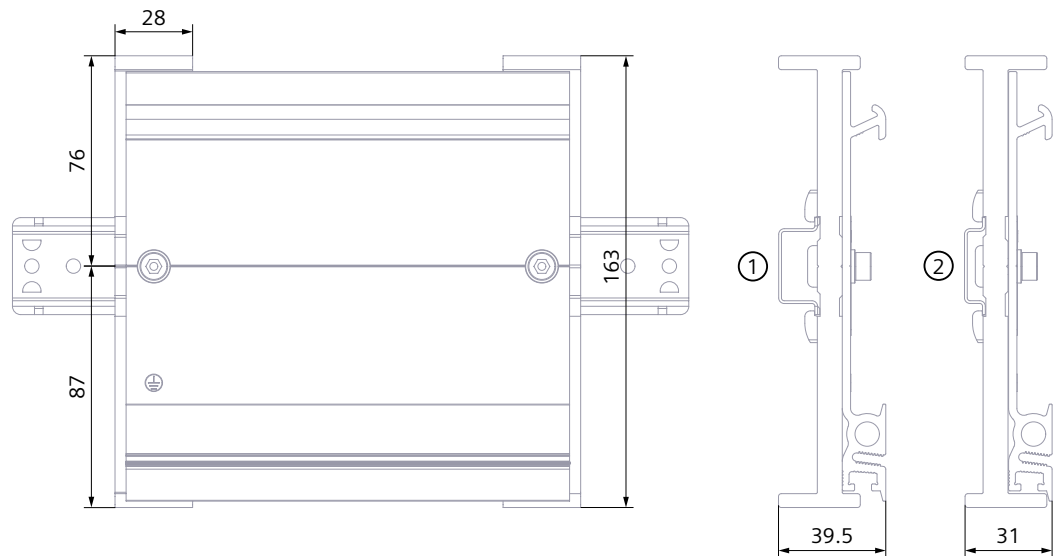
①   Position of the adapter frame during mounting to the standard DIN rail 35 mm x 7.5 mm

②   Position of the adapter frame during mounting to the standard DIN rail 35 mm x 15 mm

Figure 7-5   Dimensional drawing

Tools required

Wrench matching the hexagon socket head cap screw M6 according to EN ISO 4762 (DIN 912).

Properties

- The DIN rail adapter makes it possible to mount the S7-1500/ET 200MP mounting rail on standard 35 mm DIN rails.
- The DIN rail adapter allows the use of prefabricated control cabinet and terminal box systems.
- The total length of the S7-1500/ET 200MP mounting rail can be used again completely as before.
- To ensure optimal stability, the clearance between the two DIN rail adapters must be no more than 250 mm or less.
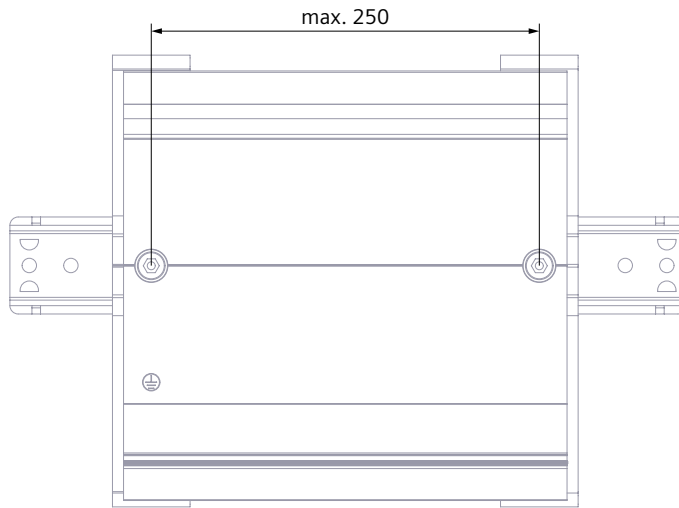
Figure 7-6 Distance between two DIN rail adapters

NOTE

Note that, depending on the mounting rail width, the mounting rail adapter can protrude up to 4 mm on each side due to the drill holes.
You can find an overview of the protrusion dimensions for the various DIN rails in the table below.

Table 7-3 Additional lateral space required

Mounting rail	Article number	Additional space required with adapter
• 160.0 mm (with drill holes)	6ES7590-1AB60-0AA0	4 mm
• 245.0 mm (with drill holes)	6ES7590-1AC40-0AA0	4 mm
• 482.6 mm (with drill holes)	6ES7590-1AE80-0AA0	8 mm
• 530.0 mm	6ES7590-1AF30-0AA0	0 mm
• 830.0 mm (with drill holes)	6ES7590-1AJ30-0AA0	0 mm
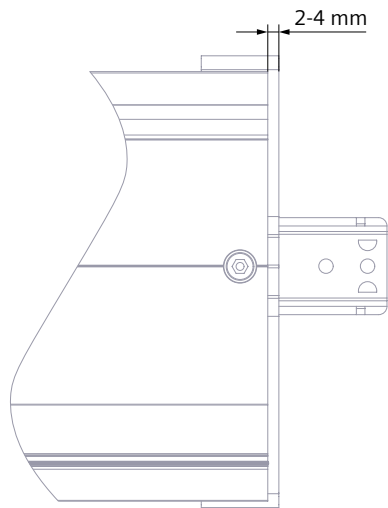
Figure 7-7 DIN rail adapter protrusion

Procedure

Mounting on the standard DIN rail 35 mm x 7.5 mm

To install DIN rail adapter on the standard DIN rail 35 mm x 7.5 mm, follow these steps:

1. Set the clamp onto the standard DIN rail.

2. The **shorter** transverse edge of the adapter frame points towards the cabinet or box wall (2).

3. Place the S7-1500/ET 200MP mounting rail on the adapter frame so that the groove in the S7-1500/ET 200MP mounting rail matches the groove in the adapter frame.
Place the S7-1500/ET 200MP mounting rail with the adapter frame on the clamp (4).

4. Use screws to fasten the S7-1500/ET 200MP mounting rail to the DIN rail adapter and the standard mounting rail (tightening torque 5 Nm to 6 Nm).
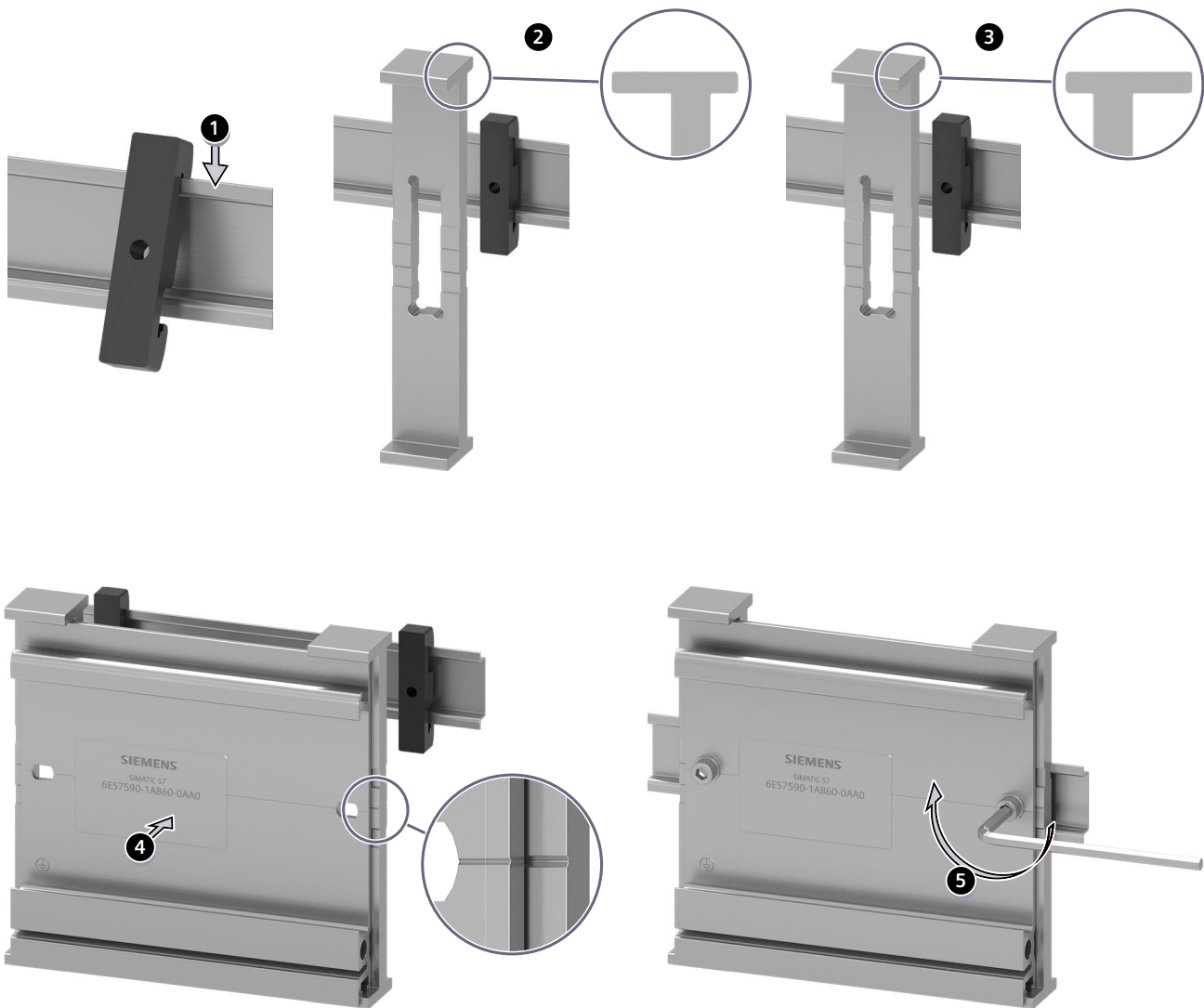
Figure 7-8   Mounting sequence of the DIN rail adapter to the DIN rail 35 mm x 7.5 mm or 35 mm x 15 mm

Mounting to the standard DIN rail 35 mm x 15 mm

To install DIN rail adapter on the standard DIN rail 35 mm x 15 mm, follow these steps:

1. Set the clamp onto the standard DIN rail.

2. The **longer** transverse edge of the adapter frame points toward the cabinet or box wall (3).

3. Place the S7-1500/ET 200MP mounting rail on the adapter frame so that the groove in the S7-1500/ET 200MP mounting rail fits into the groove in the adapter frame.
    Place the S7-1500/ET 200MP mounting rail with the adapter frame onto the clamp (4).

4. Use screws to fasten the S7-1500/ET 200MP mounting rail to the standard rail adapter and the standard mounting rail (tightening torque 5 Nm to 6 Nm).

7.4 Installing a system power supply

Introduction

The system power supply has a connection to the backplane bus and supplies the connected modules with the internal supply voltage.

Requirements

The mounting rail is installed.

Tools required

Screwdriver with 4.5 mm blade

Installing a system power supply

To install the system power supply, follow these steps:

1. Insert the U-connector into the back of the system power supply.

2. Hang the system power supply on the mounting rail.

3. Swivel the system power supply to the rear.
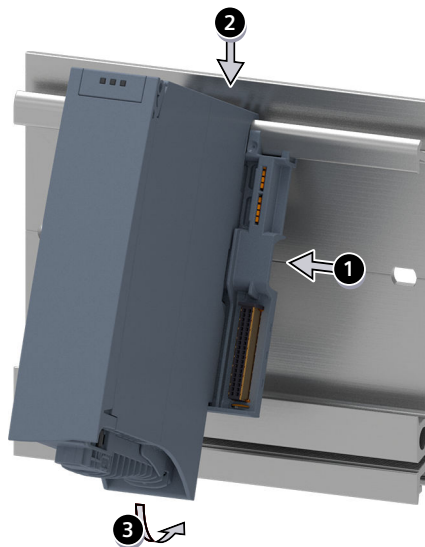
Figure 7-9   Installing a system power supply

4. Open the front cover.

5. Disconnect the power cable connector from the system power supply.

6. Screw the system power supply tight (tightening torque 1.5 Nm).

7. Insert the already wired-up power cable connector into the system power supply.

Information about wiring of the power cable connector is available in the section Connecting system power supply and load current supply (Page 218).

Uninstalling a system power supply

The system power supply is wired up.

To uninstall the system power supply, follow these steps:

1. Open the front cover.

2. Shut down the system power supply.

3. Switch off the supplied supply voltage.

4. Disconnect the power cable connector, and remove the connector from the system power supply.

5. Unscrew the fixing screw.

6. Swivel the system power supply out of the mounting rail.

Reference

Additional information can be found in the manuals for the system power supplies.

7.5 Installing a load current supply

Introduction

Load current supplies do not have a connection to the backplane bus of the S7-1500 automation systems/ET 200MP distributed I/O system and also do not occupy a slot on the backplane bus. The load current supply (PM) supplies the system power (PS), CPU, interface module and input and output circuits of the I/O modules with DC 24 V.

Requirements

The mounting rail is installed.

Tools required

Screwdriver with 4.5 mm blade

Installing a load current supply

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/78027451)

To install a load current supply, follow these steps:

1. Hook the load current supply on the mounting rail.
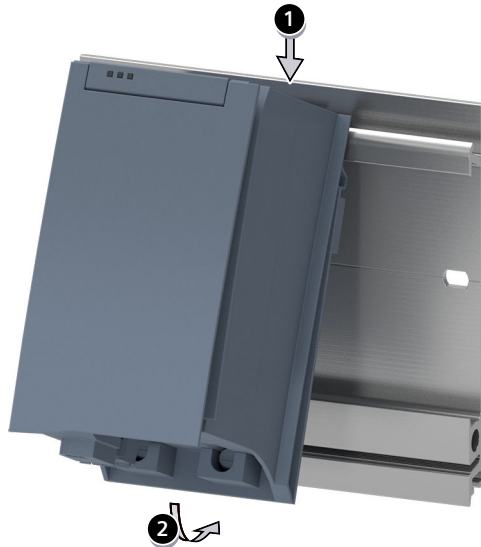
2. Swivel the load current supply to the rear.

Figure 7-10 Installing a load current supply

3. Open the front cover.

4. Disconnect the power cable connector from the load current supply.

5. Screw the load power supply tight (tightening torque 1.5 Nm).

6. Insert the already wired-up power cable connector into the load current supply.

For a description on how to wire the power cable connector, refer to the section Connecting system power supply and load current supply (Page 218).

NOTE

Load current supplies can only be mounted on the left or right side outside the S7-1500 automation system/ET 200MP distributed I/O system. If you mount a load current supply on the right of the configured setup, the heat development of the load current supply may make a gap to the configured setup necessary. For additional information, refer to the relevant manuals. The number of load current supplies that can be used is unlimited.

Uninstalling the load current supply

The load current supply is wired up.

To uninstall a load current supply, follow these steps:

1. Open the front cover.
2. Shut down the load current supply.
3. Turn off the feed supply voltage.
4. Disconnect the power cable connector, and remove the connector from the load current supply.
5. Unscrew the fixing screw.
6. Swivel the load current supply out of the mounting rail.

Reference

Additional information can be found in the manuals for the load current supplies.

7.6 Installing the CPU

Introduction

The CPU executes the user program and supplies the electronics of the modules with power via the backplane bus.

Requirements

The mounting rail is installed.

In a system power supply located on the left next to the CPU, a U connector is inserted on the back right.

NOTE

Protective film

Please note that the CPU is supplied with a removable protective film on the display. You can remove the protective film as required.

Tools required

Screwdriver with 4.5 mm blade

Installing the CPU

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/78027451)

To install a CPU, follow these steps:

1. Insert a U-connector into the back right on the CPU.

2. Install the CPU to the mounting rail. Also push the CPU to the left system power supply if necessary.

3. Ensure that the U-connector is inserted at the system power supply. Swivel the CPU in to the rear.

4. Screw the CPU tight (tightening torque 1.5 Nm).

Figure 7-11 Installing the CPU

Uninstalling the CPU

The CPU is wired, and is followed by additional modules.

To uninstall a CPU, follow these steps:

1. Open the front cover.

2. Switch the CPU into STOP mode.

3. Turn off the feed supply voltage.

4. Pull off the connector for the supply voltage.

5. Loosen the bus connectors for PROFIBUS/PROFINET with the screwdriver.

6. Disconnect the bus connector from the CPU.

7. Undo the CPU fixing screws.

8. Pivot the CPU out of the mounting rail.

Device damage caused by electrical fields or electrostatic discharge

Electrostatic sensitive devices (ESD) are individual components, integrated circuits, modules or devices that can be damaged by electrostatic fields or electrostatic discharge.

NOTICE
Device damage caused by electrical fields or electrostatic discharge
Electrical fields or electrostatic discharge can cause function failures that result from damaged individual components, integrated circuits, modules or devices.
• Pack, store, transport and send electronic components, modules or devices only in the original product packaging or in other suitable materials, e.g. conducting foam rubber or aluminum foil.
• Only touch components, modules and devices when you have grounded yourself with one of the following measures:
– Wear an ESD wrist strap
– Wear ESD shoes or ESD grounding strips in ESD areas with a conducting floor
• Place electronic components, modules and devices only on conducting surfaces (table with ESD coating, conducting ESD plastic foam, ESD packing bag, ESD transport container).

7.7 Installing the interface module

Introduction

The interface module connects the ET 200MP with the PROFINET IO/PROFIBUS DP.

The interface module exchanges data between the higher-level controller and the I/O modules.

Requirements

The mounting rail is installed.

For a system power supply located to the left of the interface module, a U connector is inserted on the back left.

Tools required

Screwdriver with 4.5 mm blade

Installing the interface module

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/67462859)

To install an interface module, proceed as follows:

1. Mount the U-connector on the back right-hand side of the interface module.

2. Hook the interface module on the rail.

3. Pivot the interface module towards the back.

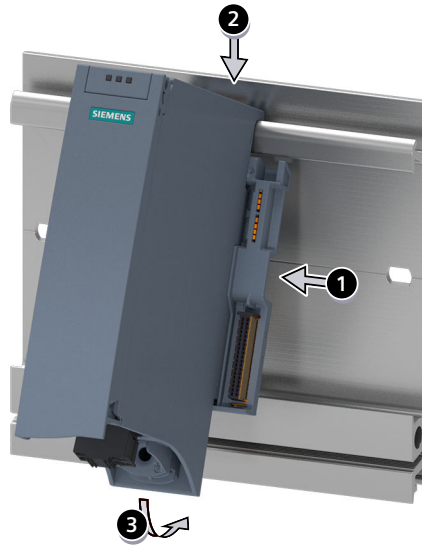4. Tighten the interface module (tightening torque 1.5 Nm).

Figure 7-12 Installing the interface module

Uninstalling the interface module

The interface module is wired and is followed by additional modules.

To uninstall the interface module, follow these steps:

1. Switch off the supply voltage for the interface module.

2. Open the front cover.

3. Loosen the bus connector and the connector for the supply voltage with the screwdriver.

4. Remove the plug from the interface module.

5. Loosen the fixing screw of the interface module.

6. Pivot the interface module out of the mounting rail.

7.8 Installing I/O modules

Introduction

The I/O modules are then mounted to the right of the CPU/interface module. I/O modules form the interface between the controller and the process. The controller detects the current process state via the connected sensors and actuators, and triggers the corresponding reactions.

Requirements

The mounting rail is installed.

The CPU/interface module is installed.

In the module/CPU/interface module located to the left of the I/O module, a U-connector is inserted on the back right.

Tools required

Screwdriver with 4.5 mm blade

Installing I/O modules

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/78027451)

Proceed as follows to install an I/O module:

1. Insert a U connector into the back right on the I/O module.
   Exception: the last I/O module in the assembly

2. Install the I/O module on the mounting rail. Push the I/O module up to the left module.

3. Pivot the I/O module towards the back.

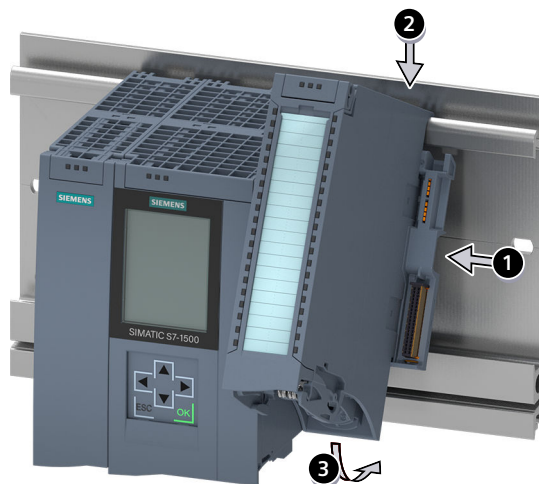4. Tighten the I/O module (tightening torque 1.5 Nm).

Figure 7-13 Installing I/O module

Uninstalling I/O modules

The I/O module is wired.

Proceed as follows to dismantle an I/O module:

1. Turn off all feed supply voltages.

2. Open the front cover.

3. For communications modules: Loosen and remove the connector from the module.

4. At I/O modules: Pull the front connector out of the I/O module using the unlocking strap. Swivel the front connector downward. Remove the front connector from the guide grooves.

5. Loosen the fixing screw of the I/O module.

6. Pivot the I/O module out of the mounting rail.

Wiring   8

8.1   Rules and regulations for operation

Introduction

The S7-1500 automation system / ET 200MP distributed I/O system is a component of plants or systems. Special rules and regulations must be adhered to in line with the area of application.

This section provides an overview of the most important rules that must be observed for the integration of the S7-1500 automation system/ ET 200MP distributed I/O system in a plant or system. Please follow these rules when connecting the S7-1500 automation system/ ET 200MP distributed I/O system.

Specific application

Observe the safety and accident prevention regulations that are applicable to specific applications (for example Machinery Directive).

EMERGENCY-STOP devices

EMERGENCY OFF equipment to IEC 60204 (corresponds to DIN VDE 0113) must remain effective in all operating modes of the plant or system.

Excluding hazardous plant states

Hazardous operating states must not occur when

- The plant restarts after a voltage dip or power failure.
- Bus communication is reestablished following a fault.

If a hazardous operating state occurs, force an EMERGENCY STOP.

After the EMERGENCY-STOP device has been unlocked, the S7-1500 automation system / ET 200MP distributed I/O system must not started uncontrolled or undefined.

External fuses/switches

Install the external fuses/switches in the proximity of the S7-1500 automation system/ET 200MP distributed I/O system.

Line voltage

The points to note for line voltage are set out below.

- For fixed plants or systems without multipole circuit breaker, a mains disconnection device (multipole) must be available in the building installation.

- For load current supplies, the configured rated voltage range must correspond to the local line voltage.

- For all power circuits of the S7-1500 automation system/ET 200MP distributed I/O system, the fluctuation/deviation of the line voltage from the rated value must be within the permitted tolerance.

You can find additional information in the section Information on insulation tests, protection class, degree of protection and rated voltage (Page 416).

24 V DC supply

The following describes what you must pay attention to in terms of the 24 V DC supply:

- Power supply units for the 24 V DC supply (SELV/PELV) must supply a safe extra-low voltage according to IEC 61131-2 or IEC 61010-2-201.

- To protect the S7-1500 automation system/ET 200MP distributed I/O system from lightning and overvoltages, use overvoltage arresters.

  Suitable components for the lightning and overvoltage protection are specified in the Defining interference-free controllers (https://support.automation.siemens.com/WW/view/en/59193566) function manual.

Requirements for power supplies in the event of voltage interruption

---

NOTE

To ensure adherence to IEC 61131-2, only use power packs/power supply units (e.g. 230/400 V AC → 24 V DC) with a mains buffering time of at least 10 ms. Observe the relevant requirements in your application (e.g. product standard for "burners" 30 ms according to EN 298 or 20 ms according to NAMUR recommendation NE 21) with respect to possible voltage interruptions. The latest up-to-date information on PS components is available on the Internet (https://mall.industry.siemens.com).

Of course, these requirements also apply to power packs/power supply units not constructed using S7-1500 or ET 200SP/S7-300-/S7-400 technology.

Protection against electrical shock

As protection against electric shock you must connect the mounting rail and if necessary, all other existing protective conductor connections of the S7-1500 automation system / ET 200MP distributed I/O system conductively with the protective conductor.

You may only use conductors in the colors yellow-green for connections to protective conductor connections.

Protection against external electrical influences

To protect against electrical effects or faults, observe the following rules:

• The system for discharging electromagnetic interference must be connected to a protective conductor with a sufficient cross-section for all plants with an S7-1500 automation system / ET 200MP distributed I/O system.

• You must ensure that all supply, signal and bus cables are correctly routed and installed.

• For signal and bus lines, a cable break, wire break or a cross circuit must not lead to undefined states in the plant or system.

Reference

Additional information can be found in the function manual, Designing interference-free controllers (https://support.automation.siemens.com/WW/view/en/59193566).

8.2 Additional rules and regulations for operation of the S7-1500/ET 200MP with fail-safe modules

8.2.1 Safety extra-low voltage (SELV, PELV) for failsafe modules

Key statement

> ⚠ **WARNING**
>
> The failsafe modules must be operated with safety extra-low voltage (SELV, PELV).
>
> You can find more information on safety extra-low voltage (SELV, PELV) in the data sheets of the applicable power supplies, for example.
>
> The fail-safe modules operate at a rated voltage of 24 V DC. The tolerance range is 19.2 V DC to 28.8 V DC.
>
> The fail-safe motor starters operate with the 24 V DC rated voltage. The tolerance range is 20.4 V DC to 28.8 V DC.
>
> Within the overvoltage range from 32 V DC to 36 V DC, the F-modules react in a fail-safe manner and the inputs and outputs are passivated. For overvoltages greater than 36 V DC, the F-modules are permanently de-energized.
>
> Use a power supply unit that does not exceed U_m = 36 V DC even in the event of a fault. For more on this, refer to the information in the data sheet on overvoltage protection in the case of an internal error. Or implement appropriate measures to limit the voltage, e.g., use of a surge protection device.
>
> All system components that can supply electrical energy in any form whatsoever must fulfill this condition.
>
> Each additional circuit (24 V DC) used in the system must have a safety extra low voltage (SELV, PELV). Refer to the relevant data sheets or contact the manufacturer.
>
> Sensors and actuators with an external power supply can also be connected to F-modules. Make sure that power is supplied to these components from safety extra-low voltage (SELV, PELV) as well. The process signal of a 24 V DC digital module must not exceed a fault voltage U_m in the event of a fault.

> ⚠ **WARNING**
>
> Even when a fault occurs, the permissible potential difference between the supply of the interface module (bus voltage) and the load voltage must not be exceeded.
>
> An external direct electrical connection is one way to meet this requirement. This also prevents potential differences from causing voltage additions at the individual voltage sources, which could cause the fault voltage U_m to be exceeded.

8.2.2 Requirements of sensors and actuators for fail-safe modules

General requirements for sensors and actuators

Note the following important warning regarding safety-related use of sensors and actuators:

> ⚠ **WARNING**
>
> Note that instrumentation with sensors and actuators bears a considerable **safety responsibility**. Also bear in mind that sensors and actuators generally do not have a service life of 20 years as defined in IEC 61508:2010 without considerable loss of safety.
>
> The probability of hazardous faults and the rate of hazardous faults of safety functions must comply with an SIL-defined high limit. A listing of values achieved by F-modules in the technical specifications of the F-modules is available under "Fail-safe performance characteristics".
>
> To achieve the respective safety class, suitably qualified sensors and actuators are necessary.

Additional sensor requirements

General rule: To achieve SIL3/Cat. 3/PLd, it is sufficient that a sensor has a single-channel connection. However, to achieve SIL3/Cat. 3/PLd with a single-channel connected sensor, the sensor itself must be SIL3/Cat. 3/PLd-capable. Otherwise, this safety level can only be achieved through two-channel connection of sensors.

To achieve Cat.4, sensors must be connected by two channels.

> ⚠ **WARNING**
>
> In the case of fail-safe input modules, a "0" value is output to the F-CPU after detection of faults. You therefore need to make sure that the sensors are implemented in such a way as to ensure the reliable reaction of the safety program when the sensor is in the "0" state.
>
> Example: In its safety program, an EMERGENCY-STOP sensor must achieve the shutdown of the respective actuator when it is in the "0" state (EMERGENCY-STOP button pressed).

Duration requirements for sensor signals

> ⚠ **WARNING**
>
> Observe the following requirements for sensor signals:
>
> - In order to ensure the correct detection of the sensor signals via fail-safe modules with inputs, you need to make sure that the sensor signals are output for a minimum duration.
> - In order for pulses to be detected with certainty, the time between two signal changes (pulse duration) must be greater than the PROFIsafe monitoring time.

Safe detection of inputs through F-modules

The minimum duration of sensor signals for fail-safe modules with inputs is dependent:

- On the parameters assigned for input delay
- On the parameters of the short-circuit test of sensor supplies.
- On the configured discrepancy behavior with 1oo2 (2v2) evaluation.

The duration of the signal must be greater than the maximum response time of the configured application. Information on calculating the maximum response time can be found in section "Response times" of the respective F-module.

The maximum permitted switching frequency of the sensor signals results from the minimum duration.

Additional requirements for actuators

The fail-safe output modules test the outputs at regular intervals. The F-module briefly switches off the activated outputs and, if necessary, briefly switches on the deactivated outputs. You can assign the maximum duration of the test pulses (dark and light period) with parameters.

High-speed actuators may briefly drop out or be activated during this test. If your process does not tolerate this, set the pulse duration of the light or dark test correspondingly or use actuators that have sufficient lag.

⚠️ **WARNING**

If the actuators switch voltages greater than 24 V DC (e.g. 230 V AC), the outputs of a fail-safe output module and the parts carrying a higher voltage must be electrically isolated (acc. to standard IEC 60664-1).

This is generally the case with relays and contactors and you must pay particular attention to this with semiconductor switching devices.

Technical specifications of sensors and actuators

Refer to the manuals of the fail-safe modules for technical specifications to assist you in selecting sensors and actuators.

8.2.3 Capacitive crosstalk of digital input/output signals

Readback errors may occur on the F-DQ modules if the fail-safe digital output signals and fail-safe digital input signals are routed through a single cable.

Cause: Capacitive crosstalk

During the bit pattern test of the outputs or the sensor supply of the inputs, the steep switching edge of the output drivers due to the coupling capacitance of the line may result in crosstalk to other non-activated output or input channels. This may then lead to a response of the readback circuit in these channels. The module detects a cross circuit/short circuit and performs a safety-related shutdown.

Solution:

- Separate cables for fail-safe DI modules and fail-safe DQ modules / non-fail-safe DQ modules
- Coupling relay or diodes in the outputs
- Disable the short-circuit test of the sensor supply if safety class requirements allow it.

Cause: magnetic crosstalk

Note that an inductive load connected to the F-DQ channels can induce coupling of a strong magnetic field.

Solution:

- Spatially disconnect the inductive loads or shield against the magnetic field.
- Configure the "Max. readback time dark test" to 50 ms or higher.

8.3 Operation on grounded infeed

Introduction

Information is provided below on the overall configuration of an S7-1500 automation system/ET 200MP distributed I/O system on a grounded infeed (TN-S system). The specific subjects discussed are:

- Shut-off devices, short circuit and overload protection in accordance with
  - IEC 60364, corresponds to DIN VDE 0100
  - IEC 60204, corresponds to DIN VDE 0113
- Load current supplies and load circuits

Grounded infeed

In the case of grounding incoming supplies (TN-S system) the neutral conductor (N) and the protective conductor (PE) are each grounded. Both conductors form a part of the overvoltage concept. When a plant is in operation, the current flows across the neutral conductor. When a fault occurs, for example a single ground fault between a live conductor and ground, the current flows through the protective conductor.

Safe electrical isolation (SELV in accordance with IEC 61131-2 or IEC 61010-2-201)

System power/load current supplies with 24 V DC output voltage feature safe electrical separation and a voltage limit (extra-low voltage). Load power supplies/system power supplies with a 24 V DC output voltage are not connected to the protective conductor. In accordance with IEC 61131-2 / IEC 61010-2-201, this protection is referred to as SELV (Safety Extra Low Voltage).

Either the wiring of SELV circuits must be safely isolated from the wiring of other circuits that are not SELV, or the insulation of all wires must be dimensioned for the higher voltage.

Protective extra-low voltage (PELV in accordance with IEC 61131-2 or IEC 61010-2-201)

Load current supplies with grounded 24 V DC output voltage require a safe connection to the protective conductor and a voltage limit (extra-low voltage).

In accordance with IEC 61131-2 / IEC 61010-2-201, this protection is referred to as PELV (Protective Extra Low Voltage).

Either the wiring of PELV circuits must be safely isolated from the wiring of other circuits that are not PELV, or the insulation of all wires must be dimensioned for the higher voltage.

Reference potential of the controller

The reference potential of the S7-1500 automation system/ ET 200MP distributed I/O system is connected with the mounting rail through a high-resistance RC combination in the CPU/interface module. In this way, high-frequency interference currents are conducted and electrostatic charges are avoided. Despite the grounded mounting rail, the reference potential of the S7-1500 automation system / ET 200MP distributed I/O system has to be considered as ungrounded due to the high-resistance connection.

If you want to configure the S7-1500 automation system/ET 200MP distributed I/O system with grounded reference potential, connect the M connection of the CPU/interface module galvanically with the protective conductor.

You can find a simplified representation of the potential relationships in section Electrical configuration (Page 208).

Short-circuit and overload protection

Various measures as protection against short-circuits and overloads are required for setting up a full installation. The nature of the components and the degree to which the required measures are binding depends on the IEC (DIN VDE) regulation applicable to your plant configuration. The table refers to the following figure and compares the IEC (DIN VDE) regulations.

Table 8-1 Components and required measures

	Reference to following figure	IEC 60364 (DIN VDE 0100)	IEC 60204 (DIN VDE 0113)
Shut-off device for control system, sensors, and actuators	①	Main switch	Disconnector
Short-circuit and overload protection: In groups for sensors and actuators	② ③	Single-pole protection of circuits	• With grounded secondary circuit: fuse **unipolar** • Otherwise: fuse **all poles**
Load power supply for AC load circuits with more than five items of electromagnetic equipment	④	Galvanic isolation by transformer **recommended**	Galvanic isolation by transformer **recommended**

S7-1500/ET 200MP in the overall configuration

The figure below shows the overall configuration of the S7-1500/ET 200MP (load current supply and grounding concept) with infeed from a TN-S system.

Own distribution/Zone B
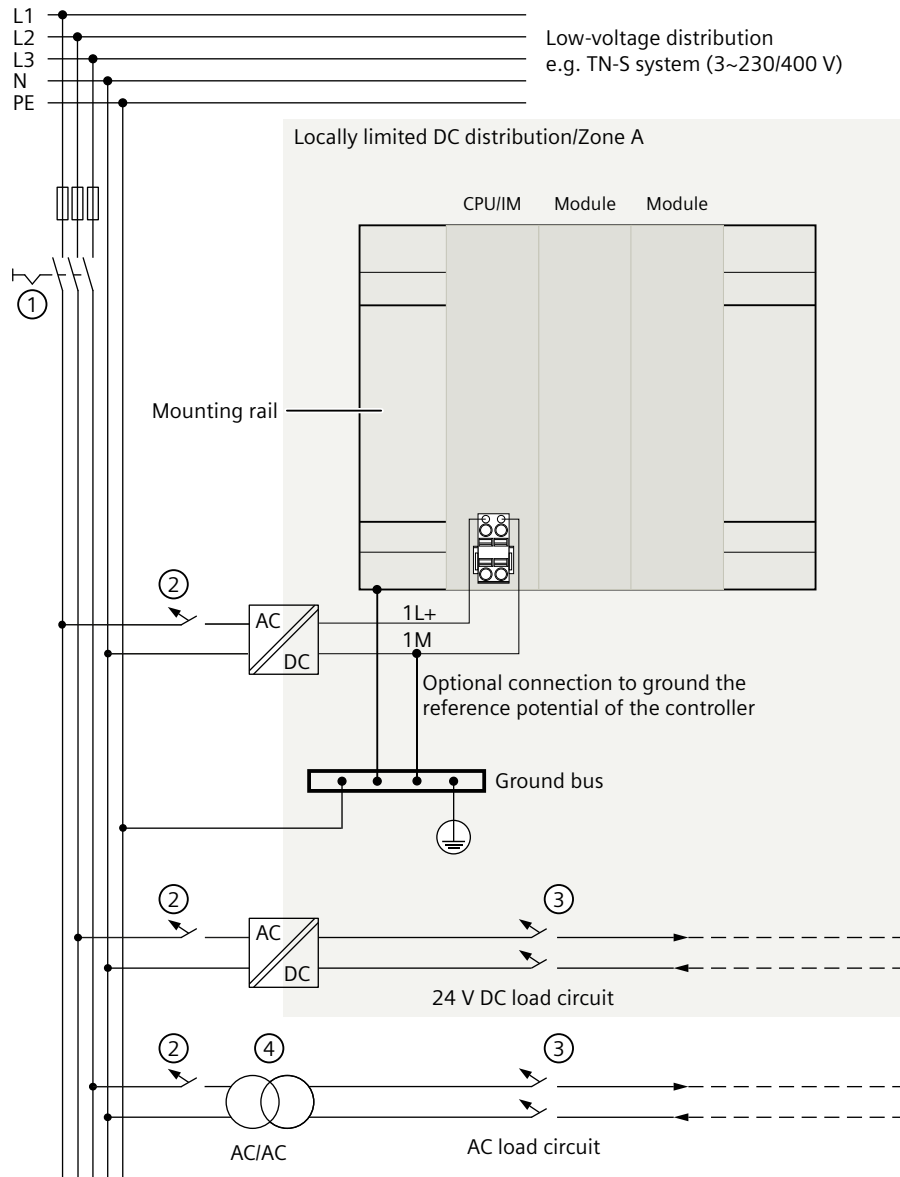
①   Main switch

②   Short-circuit and overload protection on the primary side

③   Short-circuit and overload protection on the secondary side

④   Optional for galvanic isolation

Figure 8-1   Operating the S7-1500/ET 200MP with grounded reference potential

---

NOTE

In general, you must connect all modules with DC supply of the automation system S7-1500/distributed I/O system ET 200MP to their own distribution (or batteries) by means of an upstream local power supply unit. If you connect the modules with DC supply directly to their own distribution, you need to provide additional protective measures against overvoltages.

8.4 Electrical configuration

Galvanic isolation

With the S7-1500 automation system/ET 200MP distributed I/O system, there is galvanic isolation between:

- The primary side of the system power supply (PS) and all other circuit components

- The (PROFIBUS/PROFINET) communication interfaces of the CPU/interface module and all other circuit components

- The load circuits/process electronics and all other circuit parts of the S7-1500/ET 200MP components

High-frequency interference currents are conducted and electrostatic charges are avoided through integrated RC combinations or integrated capacitors.

S7-1500 potential relationships

The following figure shows a simplified representation of the potential relationships of the S7-1500 automation system.
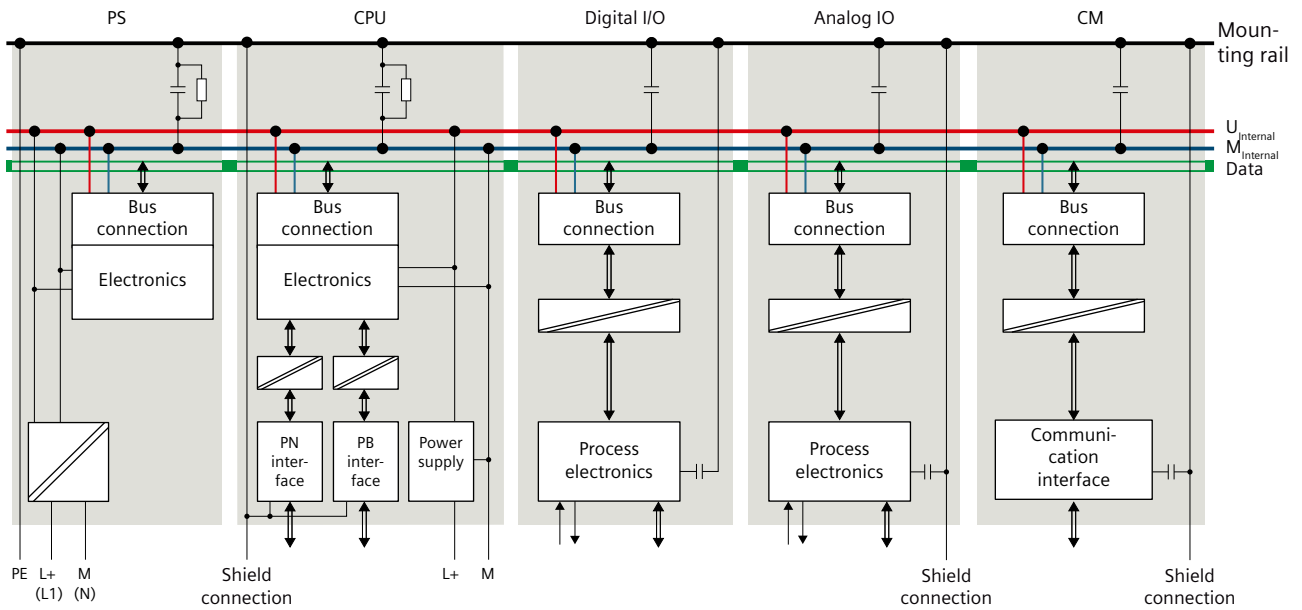
Figure 8-2 Potential relationships for S7-1500 using CPU 1516-3 PN/DP as an example

Potential relationships ET 200MP on PROFINET IO

The following figure shows a simplified representation of the potential relationships of the ET 200MP distributed I/O system on PROFINET IO.
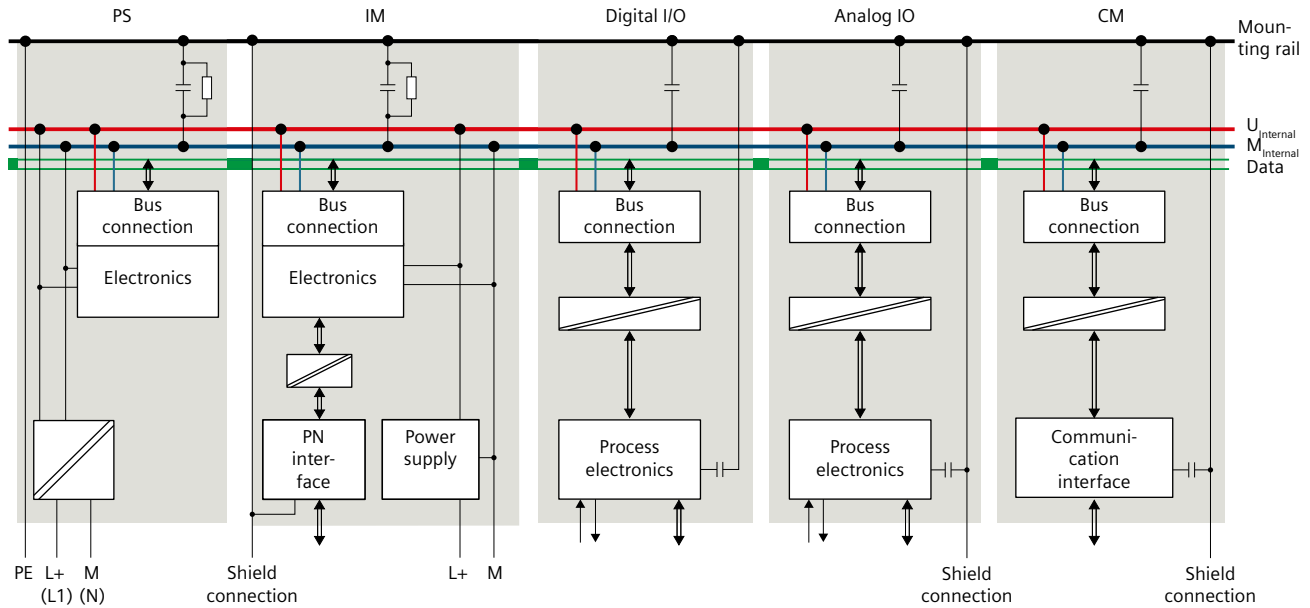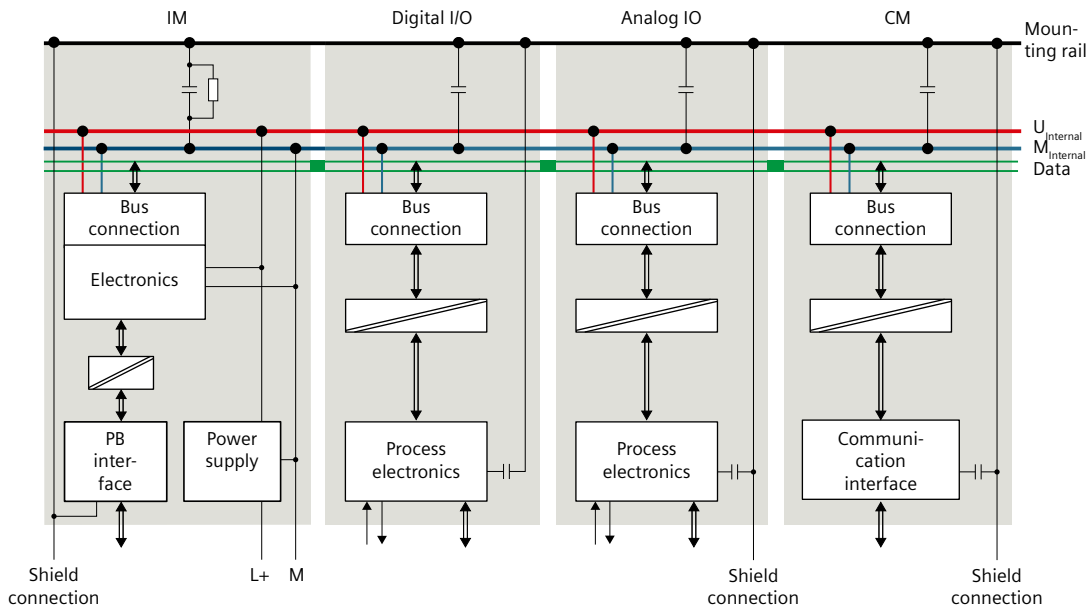

Figure 8-3 Potential relationships for ET 200MP using an IM 155-5 PN HF interface module as an example

Potential relationships ET 200MP on PROFIBUS DP

The following figure shows a simplified representation of the potential relationships of the ET 200MP distributed I/O system on PROFIBUS DP.

Figure 8-4 Potential relationships for ET 200MP using an IM 155-5 DP ST interface module as an example

8.5 Wiring rules

Introduction

Use suitable cables for connecting the S7-1500 automation system/ET 200MP distributed I/O system. Also select the cable insulation corresponding to the applied voltage. The following tables present the wiring rules for the CPU, interface module, system power supply, load current supply, front connector and power supply elements.

CPU, interface module, system power supply and load current supply

Table 8-2 Wiring rules for CPU, interface module, system power supply and load current supply

Wiring rules for ...		CPU/interface module	System power and load current supply
Permitted cable cross-sections of solid cables (Cu)		-	-
		-	-
Permitted cable cross-sections of flexible cables (Cu)	Without wire end sleeve	0.25 to 2.5 mm²	0.5 to 2.5 mm²
		AWG*: 24 to 14	AWG*: 20 to 14
	With end sleeve	0.25 to 1.5 mm²	0.5 to 1.5 mm²

* American Wire Gauge

Wiring rules for ...		CPU/interface module	System power and load current supply
Permitted cable cross-sections of flexible cables (Cu)	With end sleeve	AWG*: 24 to 16	AWG*: 20 to 16
Number of wires per connection		1	1
Stripped length of the wires		10 to 11 mm	7 to 8 mm
End sleeves according to DIN 46228	without plastic sleeve	Design A, 10 mm long	Design A, 7 mm long
	with plastic sleeve 0.25 to 1.5 mm²	Design E, 10 mm long	Design A, 7 mm long
Sheath diameter		-	8.5 mm
Tool		3 to 3.5 mm screwdriver, conic design	3 to 3.5 mm screwdriver, conic design
Connection system		Push-in terminal	Screw terminal
Tightening torque		-	from 0.5 Nm to 0.6 Nm

* American Wire Gauge
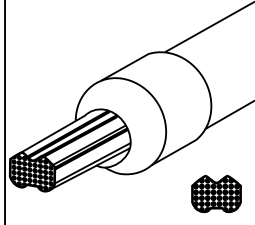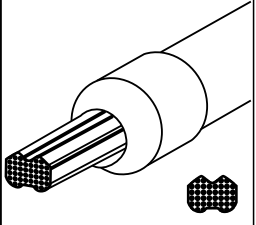
Front connectors

Table 8-3 Wiring rules for front connector

Wiring rules for ...		40-pin front connector (screw terminal, for 35 mm module)	40-pin front connector (push-in terminal, for 35 mm module)	40-pin front connector (push-in terminal, for 25 mm module)
Permitted cable cross-sections of solid cables (Cu)		up to 0.25 mm²	up to 0.25 mm²	up to 0.25 mm²
		AWG*: up to 24	AWG*: up to 24	AWG*: up to 24
Permitted cable cross-sections of flexible cables (Cu)	Without wire end sleeve	0.25 to 1.5 mm²	0.25 to 1.5 mm²	0.25 to 1.5 mm² (max. 40 x 0.75 mm²)
		AWG*: 24 to 16	AWG*: 24 to 16	AWG*: 24 to 16 mm² (max. 40 x 0.75 mm²)
	With end sleeve	0.25 to 1.5 mm²	0.25 to 1.5 mm²	0.25 to 1.5 mm² (max. 32 x 0.75 mm²; 8 x 1.5 mm²)
		AWG*: 24 to 16	AWG*: 24 to 16	AWG*: 24 to 16 (max. 32 x AWG 19; 8 x AWG 16)
Number of wires per connection		1 or combination of 2 wires up to 1.5 mm² (total) in the same end sleeve	1 or combination of 2 wires up to 1.5 mm² (total) in the same end sleeve	1 or combination of 2 wires up to 1.5 mm² (total) in the same end sleeve

* American Wire Gauge

** End sleeve

Wiring rules for ...		40-pin front connector (screw terminal, for 35 mm module)	40-pin front connector (push-in terminal, for 35 mm module)	40-pin front connector (push-in terminal, for 25 mm module)
Stripped length of the wires		8 mm up to max. 0.75 mm² (corresponding to length of end sleeve**: 8 mm) 10 to 12 mm for all cross-sections (corresponding to length of end sleeve**: 10 mm, 12 mm)	8 to 11 mm (corresponding to length of end sleeve**: 8 mm, 10 mm)	8 to 11 mm (corresponding to length of end sleeve**: 8 mm, 10 mm)
End sleeves according to DIN 46228	without plastic sleeve	Design A: 8 mm long up to max. 0.75 mm², 10 mm and 12 mm long for all cross-sections	Design A: 8 mm and 10 mm long	Design A: 8 mm and 10 mm long
	with plastic sleeve 0.25 to 1.5 mm²	Design E 8 mm long up to max. 0.75 mm², 10 mm and 12 mm long for all cross-sections	Design E 8 mm and 10 mm long	Design E 8 mm and 10 mm long
Sheath diameter		-	-	-
Tool		3 to 3.5 mm screwdriver, conic design	3 to 3.5 mm screwdriver, conic design	3 to 3.5 mm screwdriver, conic design
Connection system		Screw terminal	Push-in terminal	Push-in terminal
Tightening torque (screw terminal)		From 0.4 Nm to 0.7 Nm	-	-
Max. actuating force for complete opening of the push-in terminal		-	40 N	40 N
Recommended crimp shape for end sleeve		-	Corresponding to crimping tool PZ 6/5	Corresponding to crimping tool PZ 6/5

* American Wire Gauge

** End sleeve

NOTE

40-pin front connector (screw terminal, for 35 mm modules), article number 6ES7592-1AM00-0XB0

In case of a total current of more than 8 A, apply the supply voltage 24 V DC (terminals 19 and 39) and the ground (terminals 20 and 40) twice.
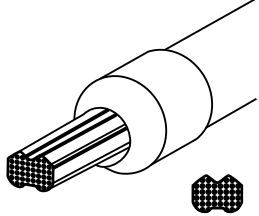

Power supply elements

Table 8-4 Wiring rules for power supply elements (component of shield set)

Wiring rules for ...		Power supply element (screw terminal, for 35 mm module)	Power supply element (push-in terminal, for 25 mm module)
Permitted cable cross-sections of solid cables (Cu)		-	-
		-	-
Permitted cable cross-sections of flexible cables (Cu)	Without wire end sleeve	0.25 to 1.5 mm^2	0.25 to 1.5 mm^2
		AWG*: 24 to 16	AWG*: 24 to 16
	With end sleeve	0.25 to 1.5 mm^2	0.25 to 1.5 mm^2
		AWG*: 24 to 16	AWG*: 24 to 16
Number of wires per connection		1 or combination of 2 wires up to 1.5 mm^2 (total) in the same end sleeve	1 or combination of 2 wires up to 1.5 mm^2 (total) in the same end sleeve
Stripped length of the wires		8 mm up to max. 0.75 mm^2(corresponding to length of end sleeve**: 8 mm) 10 to 12 mm for all cross-sections (corresponding to length of end sleeve**: 10 mm, 12 mm)	8 to 11 mm (corresponding to length of end sleeve**: 8 mm, 10 mm)
End sleeves according to DIN 46228	without plastic sleeve	Design A: 8 mm long up to max. 0.75 mm^2, 10 mm and 12 mm long for all cross-sections	Design A: 8 mm and10 mm long
	with plastic sleeve 0.25 to 1.5 mm^2	Design E 8 mm long up to max. 0.75 mm^2, 10 mm and 12 mm long for all cross-sections	Design E 8 mm and10 mm long
Sheath diameter		-	-
Tool		3 to 3.5 mm screwdriver, conic design	3 to 3.5 mm screwdriver, conic design
Connection system		Screw terminal	Push-in terminal

* American Wire Gauge

** End sleeve

Wiring rules for ...	Power supply element (screw terminal, for 35 mm module)	Power supply element (push-in terminal, for 25 mm module)
Tightening torque (screw terminal)	From 0.4 Nm to 0.7 Nm	-
Max. actuating force for complete opening of the push-in terminal	-	40 N
Recommended crimp shape for end sleeve	-	Corresponding to crimping tool PZ 6/5

* American Wire Gauge

** End sleeve

Permissible cable temperature

> **NOTE**
>
> **Permissible cable temperature**
>
> When choosing a cable, remember that the cable temperature in operation can be up to 30 °C higher than the ambient temperature of the S7-1500/ET 00MP system.
>
> Example: If you use the system in a switchgear cabinet at an ambient temperature of 30 °C, you must use a connecting conductor with a temperature range of at least 60 °C.
>
> With terminals that carry a current load of ≥ 8 A during operation, you must expect a cable temperature of up to 65 °C above the ambient temperature.
>
> You can determine the required cable temperature more precisely for each application. To do so, measure the cable temperature in the system at a load corresponding to the maximum possible power and ambient temperature values.
>
> You should specify other connection types and material requirements based on the electrical characteristics of the circuits you use and the installation environment.

8.6 Connecting the supply voltage

Introduction

The supply voltage of the CPU/interface module is supplied by means of a 4-pole connection plug, which is located on the front or below on the CPU / interface module.

Connection for supply voltage (X80)

The connections of the 4-pole connector have the following meaning:
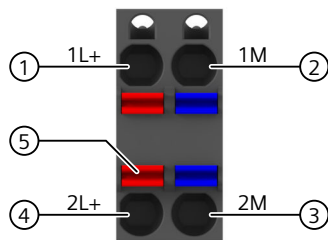
①	+24 V DC of the supply voltage (current limited to 10 A)
②	Ground of the supply voltage (current limited to 10 A)
③	Ground of the supply voltage for loop-through
④	+24 V DC of the supply voltage for loop-through
⑤	Spring opener (one spring opener per terminal)

Figure 8-5 Connection for supply voltage

The cable connector offers you the option of looping the supply voltage uninterrupted, even when it is unplugged.

For the maximum wire cross-sections, observe the information in the tables of the Wiring rules (Page 211).

Requirements

- Only wire the cable connector when the supply voltage is turned off.
- Observe the Wiring rules (Page 211).

Tools required

3 to 3.5 mm screwdriver

Tool-free connection of cables: multi-wire (stranded), with end sleeve or ultrasonic compressed

To connect a wire without tools, follow these steps:

1. Strip 8 to 11 mm of the wires.

2. Seal or crimp the wire with end sleeves.

3. Insert the wire into the push-in terminal as far as it will go.

4. Push the wired connector into the socket of the CPU/interface module.

Connection of wires: multi-wire (stranded), without end sleeve, unprocessed

To connect a wire without end sleeve, follow these steps:

1. Strip 8 to 11 mm of the wires.

2. Using a screwdriver, press the spring release and insert the wire into the push-in terminal as far as it will go.

3. Pull the screwdriver out of the spring release.

4. Push the wired connector into the socket of the CPU/interface module.

Loosening a wire

Push with the screwdriver as far as it will go into the spring release. Remove the wire from the push-in terminal.

Uninstalling the connection plug

To uninstall the connection plug, you need a screwdriver. With the screwdriver, pry the connection plug out of the CPU/interface module.

8.7 Connecting system power supply and load current supply

Introduction

In the delivery condition of the system power supplies/load current supplies, power connectors are inserted. The modules and the associated power connectors are coded. There are two parts to the coding element. One coding element is located in the module, and the other in the power connector. The system power supplies/load current supplies use identical power connectors for the voltage connection.

The coding element prevents the insertion of a power connector into a different type of system power supply/load current supply.

Tools required

3 to 3.5 mm screwdriver

Connecting the supply voltage to a system power supply/load current supply

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/78027451)

To connect the supply voltage, follow these steps:

1. Swing the front cover of the module up until the front cover latches.

2. Press down the unlocking button of the power cable connector (Figure 1). Remove the power cable connector from the front of the module.

3. Loosen the screw on the front of the connector. This loosens the housing latch and the cable relief. With a tightened screw the connector's cover can't be removed (Figure 2).

4. Pry off the connector cover using a suitable tool (Figure 3).

Figure 8-6 Connecting the supply voltage to a system power supply/load current supply (1)

5. Strip the cable jacket to a length of 35 mm and the conductors to a length of 7 to 8 mm. Attach the end sleeves.

6. Connect the wires in the connector according to the connection diagram (Figure 4).

7. Close the cover (Figure 5).

8. Retighten the screw (Figure 6). This effects a strain relief on the lines.
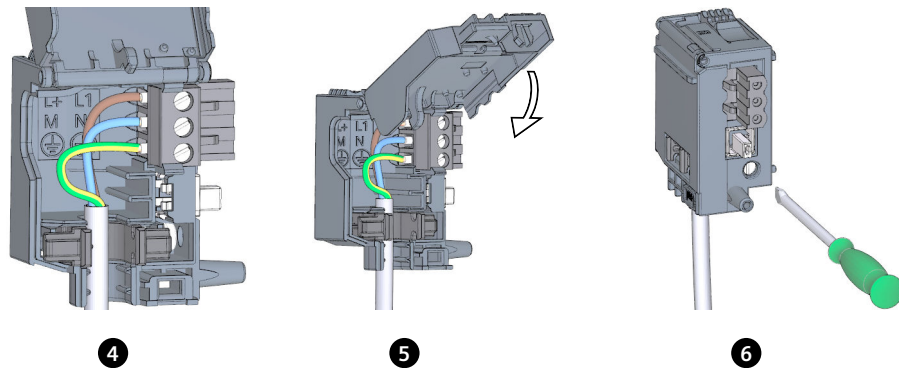
Figure 8-7 Connecting the supply voltage to a system power supply/load current supply (2)

9. Insert the power connector into the module, until the latch engages.

Reference

You can find more information on connecting the 24 V DC output voltage of the load power supply (PM) in the manuals for the relevant modules.

8.8 Connecting the CPU/interface module to the load current supply

Introduction

The load current supply is fitted with a plug-in 24 V DC output terminal (behind the front cover at the bottom). You connect the cables for the supply voltage to the CPU/interface module at this terminal.

Requirements

- Only wire the connection plug when the supply voltage is turned off.
- The connection plug for connecting the supply voltage to the CPU/interface module is already mounted.

You can find additional information in the section Connecting the supply voltage (Page 216).

Tools required

3 to 3.5 mm screwdriver

Connecting the CPU/interface module to a load current supply

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/78027451)

To connect the supply voltage, follow these steps:

1. Open the front cover of the load power supply. Pull the 24 V DC output terminal downwards.

2. Connect the 24 V DC output terminal to the wires of the 4-pole connection plug of the CPU/interface module.
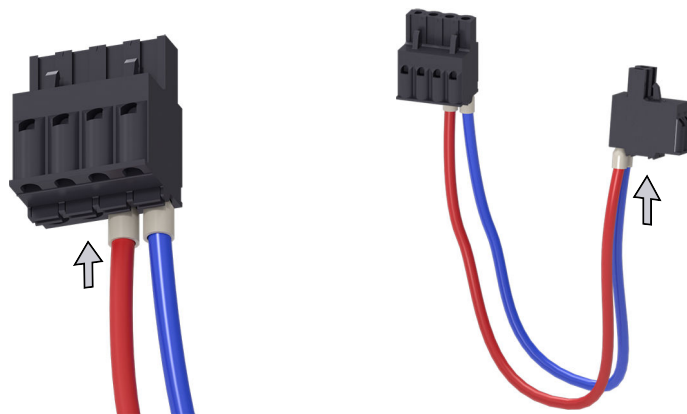
3. Connecting the load current supply to the CPU/interface module.
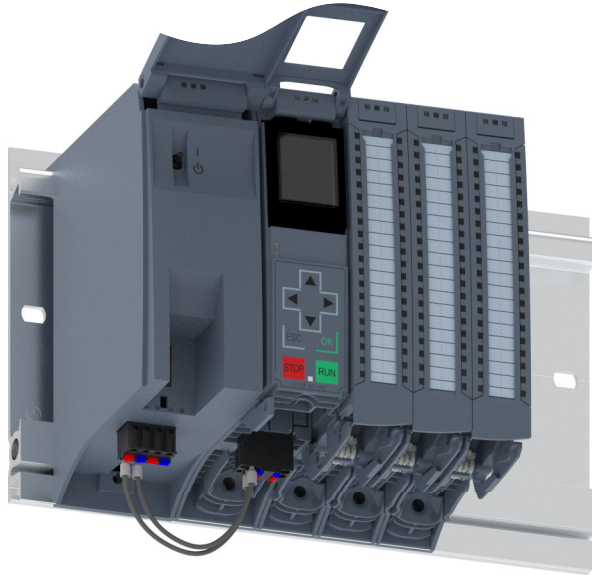
NOTE

Position of the connection socket at the CPU

The connection socket for the 4-pole connection plug is located on the underside of the device for the following CPUs/interface modules:

– Standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0

– Interface modules IM 155-5 PN BA as of article number 6ES7155-5AA00-0AA0 and IM 155-5 PN ST as of article number 6ES7155-5AA01-0AB0

In the case of all CPUs with older article numbers, the connection socket is located on the front of the device under the front flap.

Additional information can be found in the associated manuals for the CPUs/interface modules.

8.9 Connecting interfaces for communication

Connecting interfaces for communication

Connect the communication interfaces of the CPU/interface module using standardized plug connectors.

Use prefabricated connecting cables for the connection. If you want to prepare communication cables yourself, the interface assignment is specified in the manuals of the corresponding modules. Observe the mounting instructions for the connectors.

Special consideration: Unlock connectors Industrial Ethernet FastConnect RJ45 plug 180 2x 2 or Industrial Ethernet FastConnect RJ45 plug 180 4x 2 and disconnect from PROFINET interface of CPU/IM

Tools required

- Industrial Ethernet FastConnect RJ45 Plug 180 2x 2 (6K1901-1BB10-2Ax0): **2.5 mm screwdriver**

- Industrial Ethernet FastConnect RJ45 Plug 180 4x 2 (6GK1901-1BB12-2Ax0): **3.0 mm screwdriver**

Procedure

1. Press the screwdriver parallel to the connector into the unlocking.

2. Disconnect the connector from the PROFINET interface.

NOTE

Do not unlock the connector under tension!
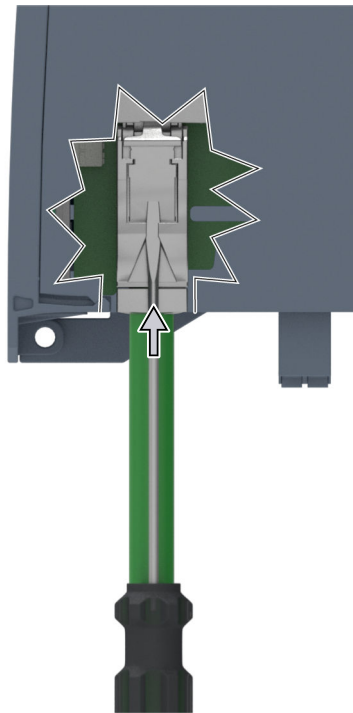
Figure 8-8 Unlocking the FastConnect connector

8.10 Front connector for the I/O modules

Introduction

The sensors and actuators of your plant are connected to the automation system by means of front connectors. Wire the sensors and actuators to the front connector. Plug the front connector with the wired sensors and actuators onto the I/O module.

You can wire the front connector as follows:

- In the "pre-wiring position", which allows a convenient wiring
- Completely, before you insert it into the I/O module.

You can remove the front connector easily from the I/O module with the wiring attached. This means it is not necessary to loosen the wiring when you replace the module.

Device versions of the front connector
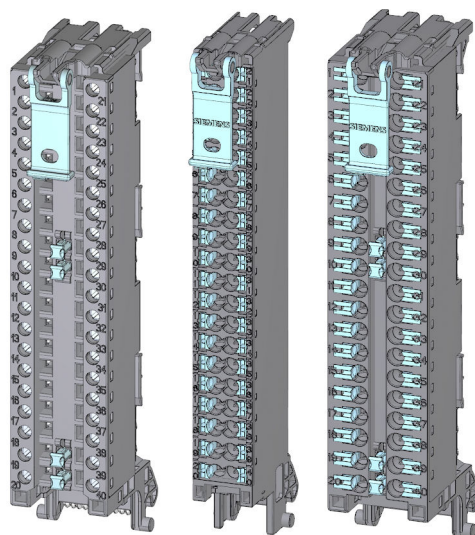
①	Front connector 35 mm with screw terminals
②	Front connector 25 mm with push-in terminals
③	Front connector 35 mm with push-in terminals

Figure 8-9 Device versions of the front connector

Properties of the front connectors

The three different front connectors are characterized as follows:

- 40 clamping points each

- Connection system: Screw terminal (for 35 mm modules only) or push-in terminal

- Module width: 35 mm or 25 mm

- If you want to supply load groups with the same potential (non-isolated), use the potential bridges supplied for the front connector (with 35 mm width) for digital I/O modules. The bridges are used to connect the terminals 9 and 29, 10 and 30, 19 and 39 as well as 20 and 40 facing each other. Advantage: Reduction of the wiring effort.

NOTE

Use of potential bridges

The use of potential bridges depends on the relevant module used.

It is not permitted to use potential bridges for 230 V modules. Use the potential bridges only with a maximum supply voltage of 24 V DC. The current capacity per potential bridge is 8 A maximum.

Because of the different assignment, you may not use the potential bridges with analog I/O modules.

The front connectors for 25 mm modules have no potential bridges.

Observe the instructions and wiring rules in the product manual of the respective I/O module when using potential bridges.

- In the delivery state a coding element is located in the module. When the front connector is first inserted into the I/O module, a part of the coding element clips onto the front connector. When the front connector is removed from the I/O module, one part of the coding element remains in the front connector, and the other part remains in the I/O module. The insertion of a front connector that is not suited to the module is thereby mechanically prevented. This ensures, for example, that the front connector with the coding element for a digital module cannot be inserted into an analog module.

Properties of the front connectors on fail-safe modules

In as-delivered condition, a fail-safe module not only has a mechanical coding element but also an electronic coding element. The electronic coding key is a rewritable memory for the PROFIsafe address. When the front connector is inserted in the F-module, the electronic coding element engages completely in the front connector. If you remove the front connector from the F-module, the memory with the PROFIsafe address of the fail-safe module remains in the front connector (see section Replacing a front connector (Page 373)).

Reference

You can find additional information on the coding element in the section Coding element on the I/O module and on the front connector (Page 369).

Additional information on the use of the potential bridges can be found in the product manual for the respective I/O module.

8.10.1   Wiring front connectors for I/O modules without shield contact element

Requirements

- The I/O modules are installed on the mounting rail.
- The supply voltages are turned off.
- The cables are prepared according to the clamping technology used; take the Wiring rules (Page 211) into account for this purpose.

Tools required

- Stripping tool
- 3 to 3.5 mm screwdriver

Preparing and wiring front connectors for I/O modules without shield contact element

Proceed as follows to wire the front connector:

1. Shut down the load current supply.

2. Place the included cable strain relief (cable tie) for the cable harness into the front connector (Figure 1).

3. Swing the front cover of the wired I/O module up until the front cover latches (Figure 2). Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/67462859)

4. Bring the front connector into the pre-wiring position. To do this, hook the front connector into the bottom of the I/O module and swivel the front connector upward until the front connector latches (Figure 3).

   Result: In this position, the front connector still protrudes from the I/O module (Figure 4). However, front connector and I/O module are not yet electrically connected. By means of the pre-wiring position, you can easily wire the front connector.

❶   ❷
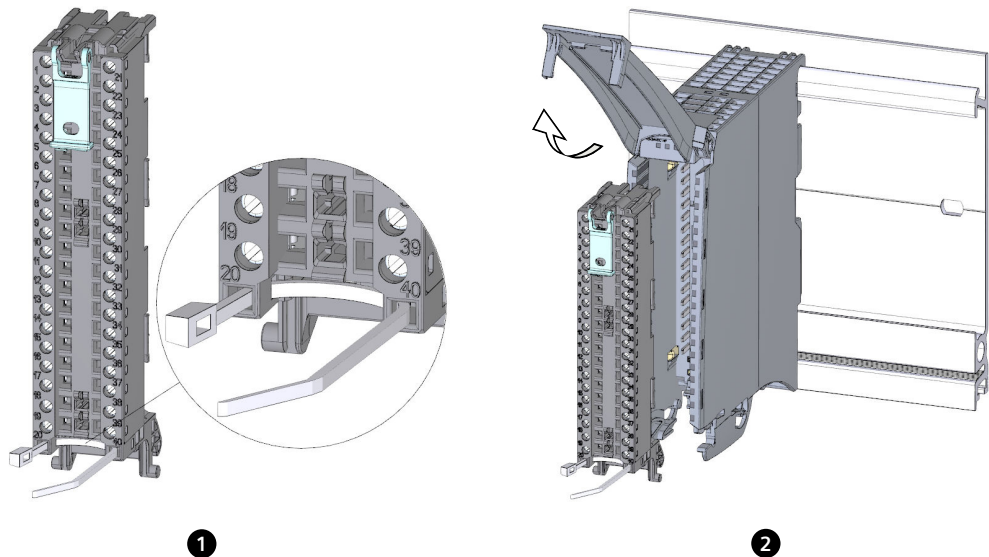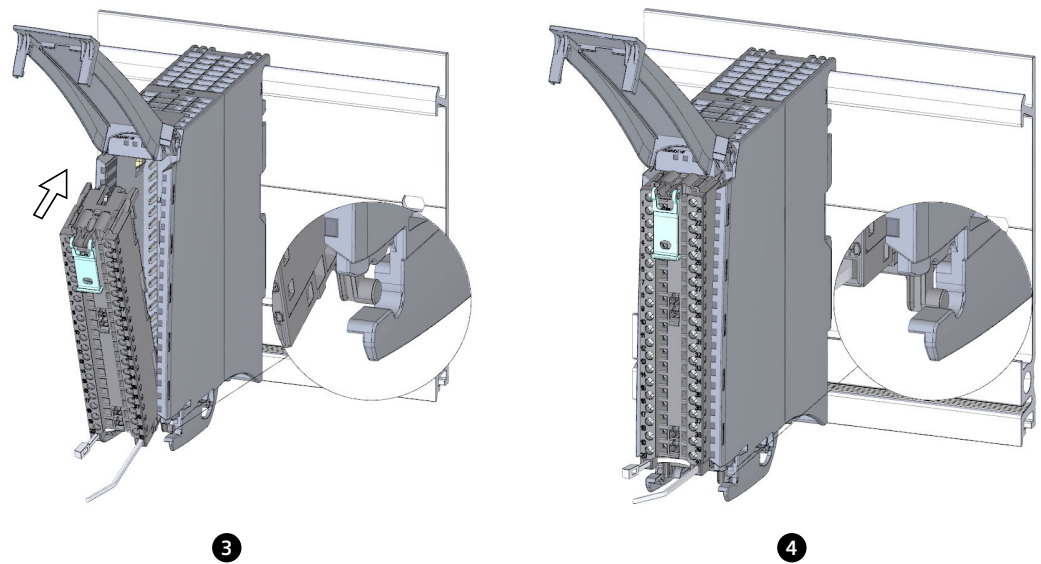
Figure 8-10 Wiring front connectors for I/O modules without shield contact element

5. Begin to completely wire the front connector.

6. Put the strain relief around the cable harness, and pull the strain relief for the cable harness tight.

Use of the potential bridges on 35 mm digital modules

With the delivered potential bridges, for digital modules with a maximum rated voltage of 24 V DC, you can bridge the terminals for the voltage supply and thus reduce the wiring effort. The bridges are used to connect the following pairs of opposing terminals: 9 and 29, 10 and 30, 19 and 39 as well as 20 and 40.

Reference

Additional information on wiring the inputs and outputs can be found in the manuals for the I/O modules.

8.10.2   Wiring front connectors for I/O modules with shield contact element

Requirements

- The I/O modules are installed on the mounting rail.
- The supply voltages are turned off.
- The wires are prepared according to the clamping technology used. To do this, follow the Wiring rules (Page 211).

Tools required

- Stripping tool
- 3 to 3.5 mm screwdriver
- Flat pliers

Details view

The shielding bracket, the power supply element, and the shielding clamp are included in the scope of delivery for the analog and technology modules.

The following figure shows the details view of a front connector with shield connection element:
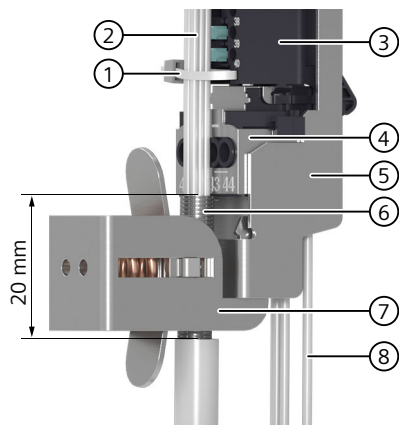
①	Shield clamp	⑥	Power supply element
②	Cable sheathing removed (approx. 20 mm)	⑦	Shielding bracket
③	Strain relief (cable tie)	⑧	Supply lines
④	Signal cables	①+⑦	Shield contact
⑤	Front connectors		

Figure 8-11 Details view for front connectors with shield connection elements

Preparing front connectors for I/O modules with shield contact element

Watch video sequence (https://support.industry.siemens.com/cs/ww/en/view/67462859)

To prepare the front connector for wiring, follow these steps:

1. Remove the connection separator from the lower part of the connector (Figure 1).

2. Insert the power supply element (Figure 2).

3. Insert the shielding bracket from below into the guiding groove of the front connector until the shielding bracket latches into place (Figure 3).

4. Place the included cable strain relief (cable tie) for the cable harness into the front connector (Figure 4).

Figure 8-12 Preparing front connectors for I/O modules with shield contact element (1)

5. Swing the front cover up until the front cover latches (Figure 5).

6. Bring the front connector into the pre-wiring position. To do this, hook the front connector into the bottom of the I/O module and swivel it upwards until the front connector latches (Figure 6).

Result: In this position, the front connector still protrudes from the I/O module (Figure 7). However, front connector and I/O module are not yet electrically connected.

Figure 8-13 Preparing front connectors for I/O modules with shield contact element (2)

7. Wire the power supply element (Figure 8).
   Terminals 41/42 and 43/44 are galvanically connected to each other. If you connect the supply voltage to 41 (L+) and 44 (M), you can then loop-through the potential to the next module (max. 8 A) with terminals 42 (L+) and 43 (M).
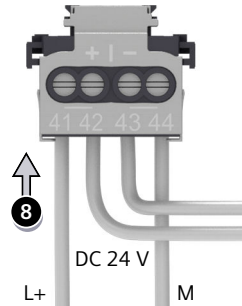
Figure 8-14 Preparing front connectors for I/O modules with shield connection element (3)

Wiring front connectors for I/O modules with shield contact element

To wire a front connector, follow these steps:

1. Strip the cable shielding.

2. Begin to completely wire the front connector (Figure 1).
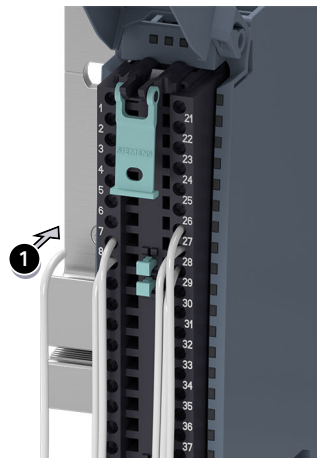
Figure 8-15 Wiring front connectors for I/O modules with shield connection element (1)

3. Put the strain relief (cable tie) around the cable harness, and pull the strain relief for the cable harness tight (Figure 2).
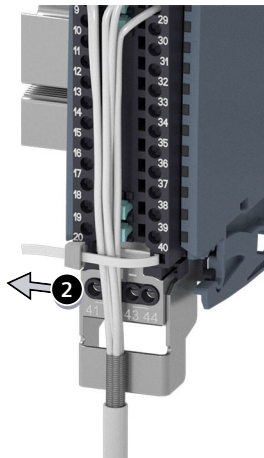
Figure 8-16 Wiring front connectors for I/O modules with shield connection element (2)

4. Insert the shield clamp from below into the shielding bracket in order to connect the cable shielding (Figure 3).
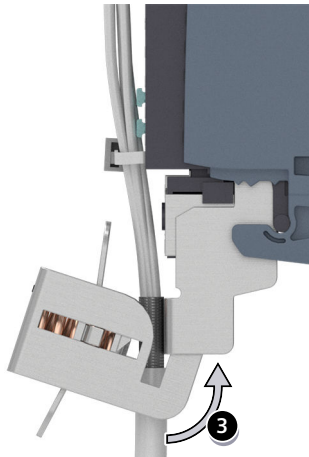

Figure 8-17 Wiring front connectors for I/O modules with shield connection element (3)

Functions of the shield contact

The shield contact:

- Is needed to apply cable shields (e.g., for analog modules)

- Interference currents on cable shields are diverted from the shield connection to ground via the mounting rail. The shielding connection is not required at cable entry into the switchboard.

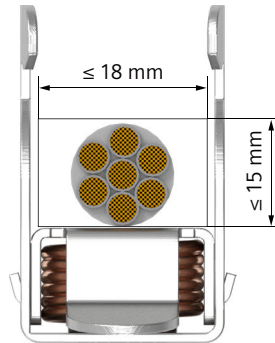- The shield support has a cable storage area of 18 mm x 15 mm.

Figure 8-18 Shield clamp

Reference

Additional information on wiring the inputs and outputs can be found in the manuals for the I/O modules.

8.10.3   Bringing the front connector into final position

Bring the front connector from the pre-wiring position into final position

Proceed as follows to bring the front connector from the pre-wiring position into final position:

1. Grip the front connector by the unlocking strap.

2. Pull on the strap until the front connector is released from its latched position.

3. Tilt the top section of the front connector and raise it slightly. The front connector slides over the guide channel into its final position.
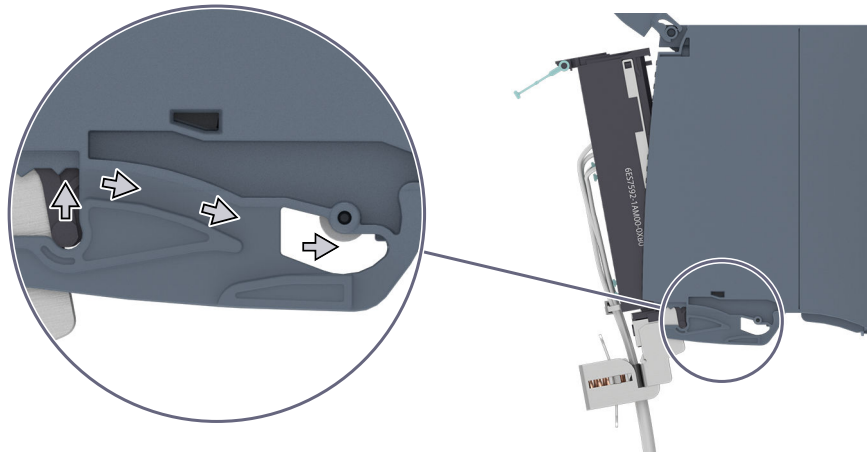

Figure 8-19 Bring the front connector from the pre-wiring position into final position

4. Push the front connector back into the I/O module until it latches. The front connector is now electrically connected with the I/O module.

5. Swivel the front cover down into place. Various latch positions are possible depending on the space requirement of the cable harness so that the required cable storage space can grow as needed.

Bringing the front connector directly into final position

Proceed as follows to bring the front connector directly into final position:

1. Grip the front connector by the unlocking strap.

2. Push the guide pin of the front connector into the guide channel that has been displaced downwards. The front connector slides over the guide channel into its final position.
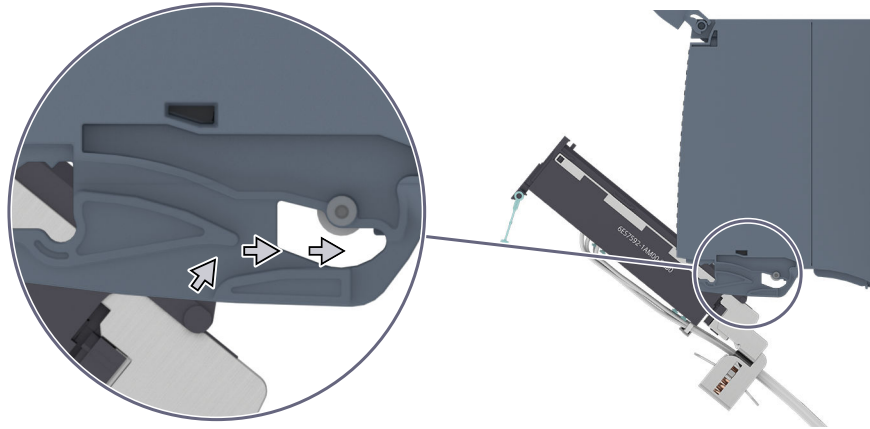

Figure 8-20   Bringing the front connector directly into final position

3. Tilt the front connector and press it into the I/O module until it latches. The front connector is now electrically connected with the I/O module.

4. Swivel the front cover down into place. Various latch positions are possible depending on the space requirement of the cable harness so that the required cable storage space can grow as needed.

8.11 Marking the I/O modules

8.11.1 Labeling strips

Introduction

Mark the pin assignment of the I/O modules using labeling strips. You can label the labeling strips as desired and slide them into the outside of the front cover.

The labeling strips are available in the following models:

- Pre-prepared strips that are included with the I/O module as delivered.
- DIN A4 sheets, pre-perforated strips for machine printing; see section Accessories/spare parts (Page 425)

Preparing and installing the labeling strip

Proceed as follows to prepare and install the labeling strips:

1. Label the labeling strip.

   You can print labeling strips for the modules in your project with STEP 7. The labeling strips are exported to Microsoft Word DOCX files and printed from the text editing program. You can find more information in the online help.

2. With a pre-perforated strip: Separate the labeling strip from the sheet.

3. Slide the labeling strip into the outside of the front cover.
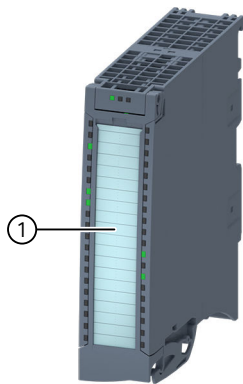
①   Labeling strips

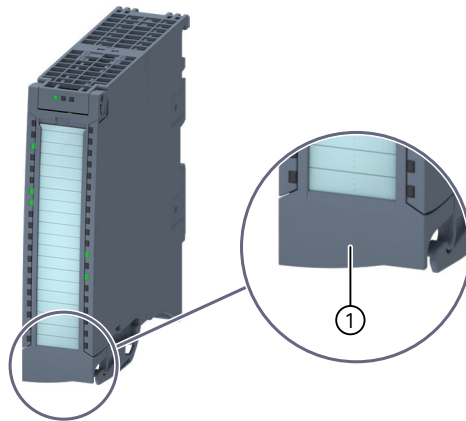Figure 8-21 Marking with labeling strips

8.11.2 Optional marking

Introduction

The I/O modules have a free area on the front cover. You can label or mark the free area yourself.

Optional marking

The front cover provides about 30 mm x 10 mm of space in its lower part for an optional identifier label.

①   Free space, for example for equipment identifiers

Figure 8-22 Optional marking

Configuring 9

Introduction

By configuring the individual hardware components, assigning their parameters, and connecting them, you communicate to the S7-1500 automation system/ET 200MP distributed I/O system its preset configuration and operating principle. You perform the work needed for this in the device and network views in STEP 7.

"**Configuring**" is understood to mean the arranging, setup and networking of devices and modules within the device view or network view of STEP 7. STEP 7 graphically represents modules and racks. Just like "real" module racks, the device view allows the insertion of a defined number of modules.

When the modules are inserted, STEP 7 automatically assigns the addresses and a unique hardware identifier (HW identifier). You can change the addresses later. The HW identifiers cannot be changed.

At startup, the system components compare the configured preset configuration with the actual configuration of the system. By means of parameter assignment, you can specify the response of the CPU to errors in the hardware configuration.

"**Assigning parameters**" is understood to mean setting the properties of the components used (CPU, modules).

STEP 7 compiles the hardware configuration (the result of "configuring" and "assigning parameters") and downloads it to the CPU. The CPU then connects to the configured components and transfers their configuration and parameters. Modules can be replaced very easily because when a new module is inserted, STEP 7 transfers its configuration and parameters again.

9.1   Configuring the CPU

Requirements for configuration of the CPU

Configuration software	Installation information
STEP 7 as of V12.0 [1]	STEP 7 online help

[1] The following CPUs can be configured as of V12: CPU 1511-1 PN, CPU 1513-1 PN, CPU 1516-3 PN/DP
Note that all other CPUs can be configured only as of a later version (e.g. V12 SP1). Refer to the manual for the CPU to find out whether the version of the CPU you are using is configurable in STEP 7.

Project compatibility of CPUs with firmware version V3.1

In order to download older projects to CPUs with firmware version V3.1, you must upgrade your project to CPUs with at least firmware version 1.8.

Spare parts compatibility for CPUs with article numbers ≥ 6ES751x-xxx03-0AB0

The following applies to the CPUs as of article number 6ES751x-xxx**10**-0AB0:
The CPUs have 2 ports at the PROFINET interface X2, but do not have a PROFIBUS DP interface. Therefore, these CPUs are not compatible with the CPUs with article numbers 6ES751x-xxx**0**x-0AB0 with regard to spare parts.

The following applies to the CPUs as of the article numbers 6ES751x-xxx0**3**-0AB0:
The CPUs are compatible for use with CPUs with article numbers ≥ 6ES751x-xxx0**1**-0AB0 with regard to spare parts.

You cannot download STEP 7 projects that have a hardware configuration with CPU article number 6ES751x-xxx0**0**-0AB0 to a CPU with article number 6ES751x-xxx0**3**-0AB0.

Solution: When replacing a CPU 6ES751x-xxx0**0**-0AB0 with a successor type 6ES751x-xxx0**3**-0AB0, you must upgrade the STEP 7 project to ≥ 6ES751x-xxx01-0AB0. For the upgrade, use STEP 7 ≥ V13 SP1 Update 3.

Replace CPUs with article numbers ≥ 6ES751x-xxx10-0AB0 in STEP 7

S7-1500 CPUs as of article numbers 6ES751x-xxx10-0AB0 have 2 ports at the PROFINET interface X2, but do not have a PROFIBUS DP interface. If, for example, you replace a CPU 1517-3 PN/DP by a CPU 1517-3 PN (article number: 6ES7517-3AQ**10**-0AB0), use the function "Change device" for the exchange in STEP 7. More information on this function is available in the STEP 7 online help.

Configuring CPUs with article numbers < 6ES751x-xxx03-0AB0 in older STEP 7 versions

CPUs with article numbers < 6ES751x-xxx0**3**-0AB0 are compatible with their predecessor version in terms of spare parts. Manipulation protection, particularly with respect to the SIMATIC Memory Card and RUN/STOP function, is retained.

When replacing a CPU (e.g. 6ES7515-2AM01-0AB0) with a compatible successor type (e.g. 6ES7515-2AM02-0AB0), the STEP 7 project does not have to be changed, nor is it necessary to upgrade the STEP 7 project.

You can still configure modules with new article numbers in STEP 7 as the predecessor version (e.g. 6ES7515-2AM01-0AB0). Because the new article number (e g 6ES7515-2AN03-0AB0) is not yet contained in previous STEP 7 versions, you can also configure the CPU as a predecessor version, i.e. with the predecessor article number (e.g. 6ES7515-2AM01-0AB0).

References

- If you want to configure new CPUs whose article numbers are not yet included in the hardware catalog of STEP 7, please refer to the following FAQ in the Internet (https://support.industry.siemens.com/cs/ww/en/view/109760846).

- If you want to load project data, but the firmware version installed in the CPU cannot be selected in STEP 7, refer to the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109744163).

- If the supplied module has an article number different to the one which was ordered, refer to the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/de/view/109763472).

- If you are searching for the successor product for a totally discontinued module and information on its compatibility, take the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/de/view/109826566/en) into account.

- You can find an overview of the most important documents and links to STEP 7 in the following FAQ on the Internet (https://support.industry.siemens.com/cs/de/de/view/65601780/en).

## 9.1.1   Reading out the configuration

Introduction

When there is a connection to an existing CPU that is being installed, you can load the configuration of this CPU, including centrally present modules, from the device into your project using the "Hardware detection" function. You do not need to manually configure the CPU and the centrally present modules, as the physical configuration is read out automatically.

If you have already configured a CPU and the centrally present modules and you want to load the current configuration and parameters in a new project, it is advisable to use the "Upload device as new station" function. For additional information about this function, refer to section Backing up and restoring the CPU configuration (Page 341).

Procedure for reading out an existing configuration

1. Create a new project and configure an "Unspecified CPU 1500".
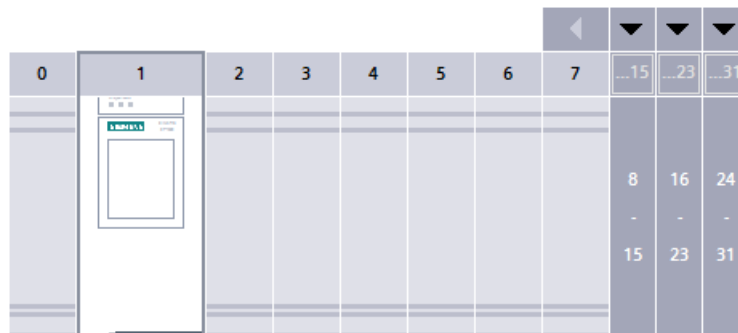
Figure 9-1 Unspecified S7-1500 CPU in the device view

NOTE

To open the "Hardware detection for PLC_x" dialog, click the "Detect" link. An example can be found in the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/de/view/41885693/en).

An alternative procedure is described in step 2 and step 3.

---

2. In the device view (or network view), select the "Hardware detection" command in the "Online" menu.
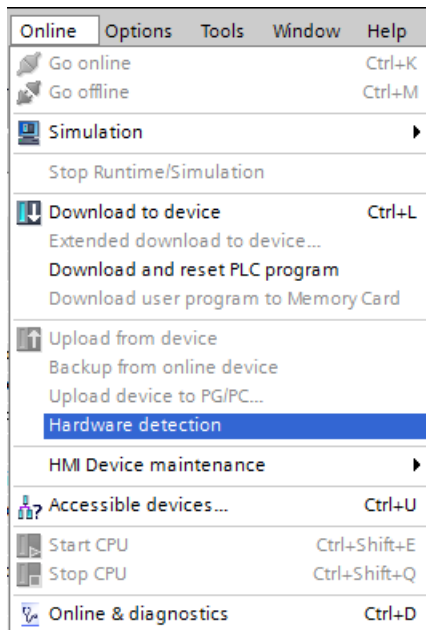

Figure 9-2 Hardware detection in the Online menu

STEP 7 opens the "Hardware detection for PLC_x" dialog box.

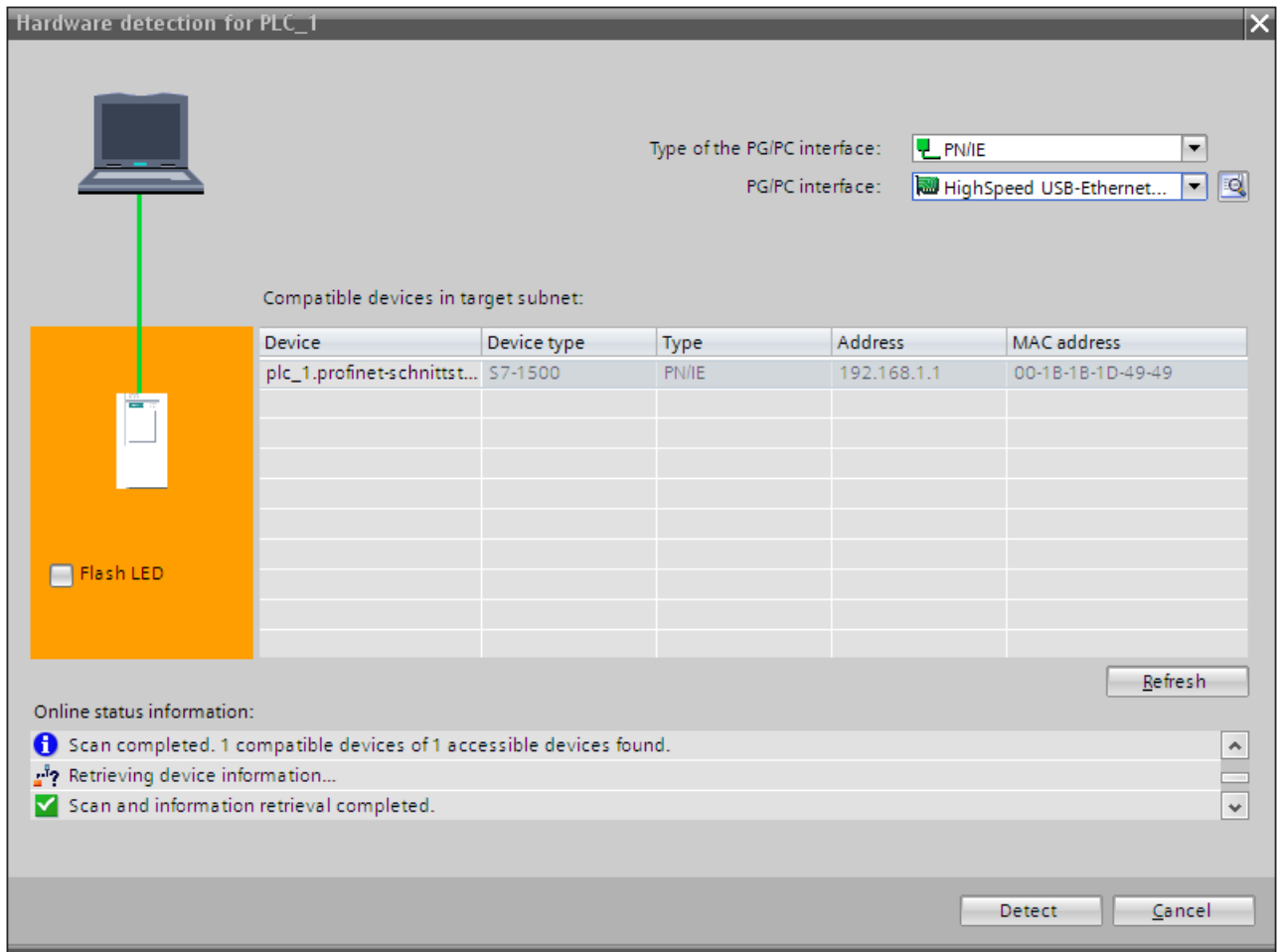3. In the "Hardware detection for PLC_x" dialog, click "Refresh". Then, select the CPU and click "Detect".

Figure 9-3 Hardware detection dialog box

Result of the hardware detection

STEP 7 has read out the hardware configuration and the modules and transferred them to your project. STEP 7 assigns a valid default parameter assignments for all modules. You can change the parameter assignment subsequently.
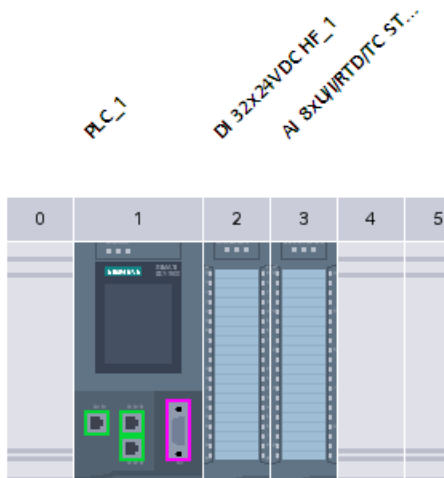

Figure 9-4 Result of the hardware detection in the device view

---

NOTE

If you want to go online after the hardware detection, you have to first download the detected configuration to the CPU; otherwise, an error may occur due to inconsistent configurations.

You can find an example of downloading a project to the CPU with STEP 7 in the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/de/view/42637263/en).

Properties of the CPUs

The properties of the CPUs have special significance for system behavior. For a CPU you can make the following settings in STEP 7, for example:

- Startup characteristics
- Parameter assignment of the interfaces, for example, IP address, subnet mask
- Web server, e.g., activation, user administration, and languages
- OPC UA server
- Global Security Certificate Manager
- Cycle times, e.g., maximum cycle time
- Properties for the operation of the display
- System and clock memory

- Protection level for access protection with assigned password parameter
- Time and day settings (daylight saving/standard). For additional information, refer to the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/de/view/43566349/en).

The properties that can be set and the corresponding value ranges are specified by STEP 7. Fields that cannot be edited are grayed out.

Reference

Information about the individual settings can be found in the STEP 7 online help and in the manuals of the relevant CPUs.

9.1.2 Address assignment

9.1.2.1 Addressing - overview

Introduction

In order to address the automation components or modules, they must have unique addresses. The following section explains the various address areas.

I/O address

I/O addresses (input/output addresses) are required in the user program to read inputs and set outputs.

STEP 7 automatically assigns input and output addresses when modules are configured. Each module uses a continuous range of input and/or output addresses corresponding to its volume of input and output data.

Module	Rack	Slot	I address	Q address	Type	Article no.
	0	100				
PS 25W 24VDC_1	0	0			PS 25W 24VDC	6ES7 505-0KA00-0AB0
▸ PLC_1	0	1			CPU 1518-4 PN/DP	6ES7 518-4AP00-0AB0
DI 32x24VDC HF_1	0	2	0...3		DI 32x24VDC HF	6ES7 521-1BL00-0AB0
DQ 8x230VAC/5A ST_1	0	3		0	DQ 8x230VAC/5A ST	6ES7 522-5HF00-0AB0
AI 8xU/I/RTD/TC ST_1	0	4	4...19		AI 8xU/I/RTD/TC ST	6ES7 531-7KF00-0AB0
AQ 4xU/I ST_1	0	5		1...8	AQ 4xU/I ST	6ES7 532-5HD00-0AB0

Figure 9-5 Example with input / output addresses from STEP 7

STEP 7 assigns the address areas of the modules by default to the process image partition 0 ("Automatic updating"). This process image partition is updated in the main cycle of the CPU.
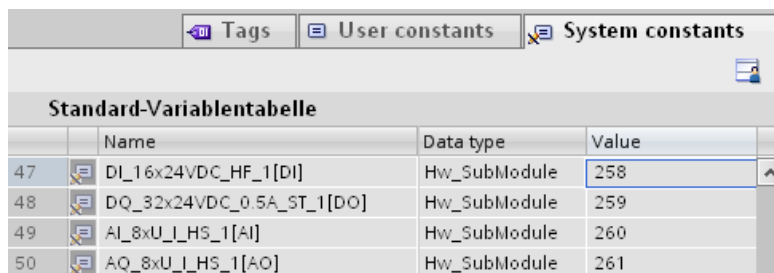
Device address (e.g., Ethernet address)

Device addresses are addresses of modules with interfaces to a subnet (e.g., IP address or PROFIBUS address). They are required to address the various devices on a subnet, for example, to download a user program.

Hardware identifier

STEP 7 automatically assigns a hardware identifier (HW identifier) for identification and addressing of modules and submodules. The HW identifier is used, for example, for diagnostics alarms or for instructions, to identify the faulty module or the addressed module.

The "System constants" tab contains all hardware identifiers and their symbolic names (of HW identifier) for the selected module.

The HW identifiers and names of all modules of a device are also available in the default tag table on the "System constants" tab.

		Name	Data type	Value	
47		DI_16x24VDC_HF_1[DI]	Hw_SubModule	258	^
48		DQ_32x24VDC_0.5A_ST_1[DO]	Hw_SubModule	259	
49		AI_8xU_I_HS_1[AI]	Hw_SubModule	260	
50		AQ_8xU_I_HS_1[AO]	Hw_SubModule	261	

Figure 9-6 Example of a default tag table from STEP 7

9.1.2.2   Addressing digital modules

Introduction

The following section describes the addressing of the digital modules. In your user program, you require the addresses of the channels of the digital module.

Digital module addresses

The address of a digital module's input or output is composed of the byte address and the bit address. The channels of the digital module are assigned bit addresses.

Example: **I 1.2**

The example consists of:

I   Input   -

1   Byte address   The byte address depends on the module start address

2   Bit address   You read the bit address from the module

When you insert a digital module into a free slot, STEP 7 assigns a default address. You can change the proposed default address in STEP 7.

Example for the assignment of channel addresses (digital module)

The following figure shows how the addresses of the individual channels of the digital input module are determined.
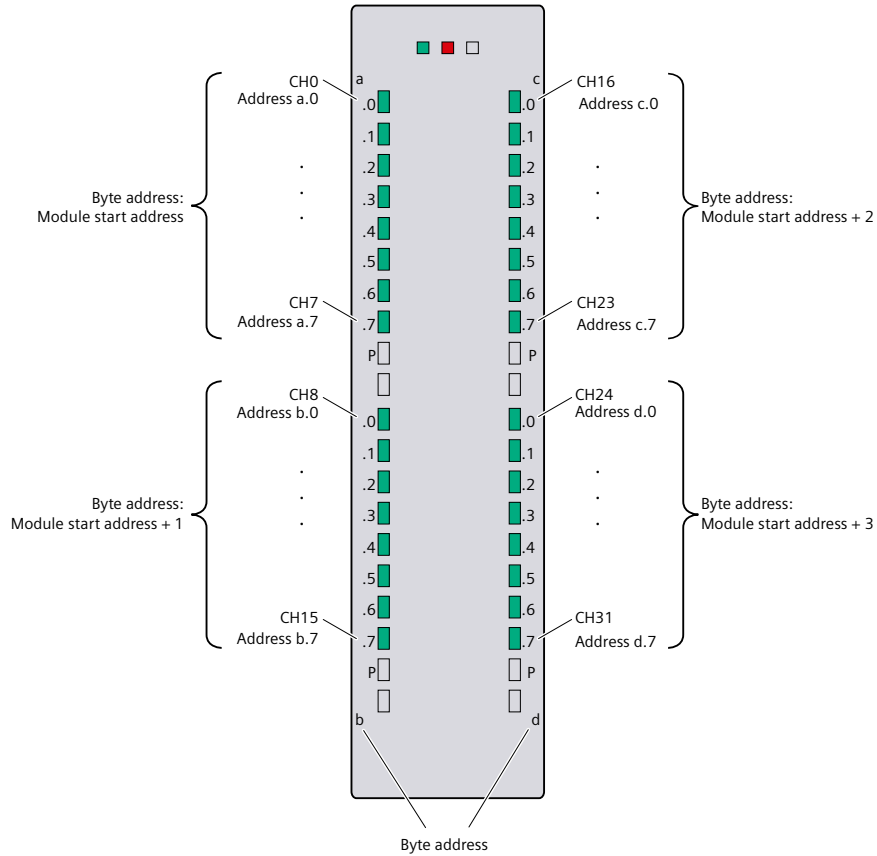

Figure 9-7 Example for the assignment of channel addresses (digital module)

NOTE

You can assign symbolic names to the addresses at the following locations in STEP 7:

- PLC tag table
- Properties of the module in the "IO Tags" tab.

Value status

The value status is additional binary information of a digital input or output signal. It is entered simultaneously with the process signal in the process image input and provides information about the validity of the input or output signal.

The value status of a module informs you whether the value of the corresponding channel can be read or output. You can respond to this information with simple binary operations in the user program without having to evaluate the diagnostics information of the module for this. Configured diagnostics in STEP 7 is not necessary for output of the value status.

If you enable the value status for a digital module, then additional bytes are allocated in the input address area. Each bit in the value status is assigned to a channel and provides information about the validity of the process value. You can find the assignment in the product manual for the respective I/O module.

The value status is influenced by all diagnostics that might falsify the process value, e.g. wire break, short-circuit.

- 1_B: A valid process value is being output or read for the channel.
- 0_B: A substitute value is being output for the channel, or the channel is deactivated, faulty or inaccessible.

You can find more information on evaluation and processing of the value status for fail-safe digital modules in the SIMATIC Safety – Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126) manual.

Reference

More information on addressing and address allocation with value status can be found in the manuals of the digital modules, and in the online help for STEP 7. An example of the evaluation of the value status in the user program is available in the function manual Diagnostics (https://support.automation.siemens.com/WW/view/en/59192926).

9.1.2.3   Addressing analog modules

Introduction

The following section describes the addressing of the analog modules. In your user program, you require the addresses of the channels of the analog module.

Analog module addresses

The address of an analog channel is always a word address. The channel address depends on the module start address. STEP 7 automatically assigns the channel addresses during configuration. Based on the module start addresses, STEP 7 assigns the channel addresses in increasing sequence (in the following figure, the module start address is 256).

When you insert an analog module into a free slot, STEP 7 assigns a default address. You can change the assigned default address in STEP 7.

Example for the assignment of channel addresses (analog module)

The following figure shows how the addresses of the individual channels of an analog input module are determined when the module has the start address 256.
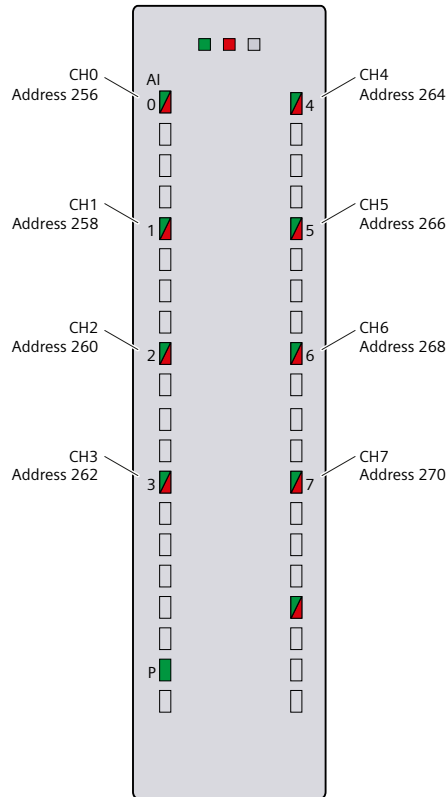

Figure 9-8 Example for the assignment of channel addresses (analog module)

NOTE

You can assign symbolic names to the addresses at the following locations in STEP 7:

- PLC tag table
- Properties of the module in the "IO Tags" tab.

Value status

The value status is additional binary information of an analog input or output value. It is entered simultaneously with the process value in the process image input and provides information about the validity of the analog value.

The value status of a module informs you whether the value of the corresponding channel can be read or output. You can respond to this information with simple binary operations in the user program without having to evaluate the diagnostics information of the module for this. Configured diagnostics in STEP 7 is not necessary for output of the value status.

If you enable the value status for an analog module, then additional bytes are allocated in the input address area. Each bit in the value status is assigned to a channel and provides

information about the validity of the process value. You can find the assignment in the product manual for the respective I/O module.

The value status is influenced by all diagnostics that might falsify the process value, e.g. wire break, short-circuit.

- 1_B: A valid process value is being output or read for the channel.

- 0_B: A substitute value is being output for the channel, or the channel is deactivated, faulty or inaccessible.

Reference

More information on addressing and address allocation with value status can be found in the manuals of the analog modules, and in the online help for STEP 7. A detailed description of the value status for analog modules is available in the function manual Analog value processing (https://support.automation.siemens.com/WW/view/en/67989094). An example of the evaluation of the value status in the user program is available in the function manual Diagnostics (https://support.automation.siemens.com/WW/view/en/59192926).

9.1.3 Process images and process image partitions

9.1.3.1 Process image - overview

Process image of the inputs and outputs

The process image of the inputs and outputs is an image of the signal states. The CPU transfers the values from the input and output modules to the process image in this memory area. At the start of the cyclic program, the CPU transfers the process image output as a signal state to the output modules. The CPU then transfers the signal states of the input modules to the process image inputs.

Advantages of the process image

A process image accesses a consistent image of the process signals during cyclic program execution. If a signal state at an input module changes during program processing, the signal state is retained in the process image. The CPU does not update the process image until the next cycle.

Consistency of the process image

When the process image is updated, the S7-1500 accesses the data of each submodule as consistent data. The maximum data width that is accessed as consistent data for each submodule is dependent on the IO system. For PROFINET IO, for example, this data width is 1024 bytes.

32 process image partitions

By means of process image partitions, the CPU synchronizes the updated inputs/outputs of particular modules with defined user program sections.

In the S7-1500 automation system, the overall process image is subdivided into up to 32 process image partitions (PIP).

The CPU automatically updates PIP 0 (automatic update) in each program cycle and assigns it to OB 1.

You can assign the process image partitions PIP 1 to PIP 31 to the other OBs during configuration of the input/output modules.

The CPU always reads the process image partition of the inputs (PIPI) before processing the associated OB. The CPU outputs the process image of the outputs (PIPQ) at the end of the OB.

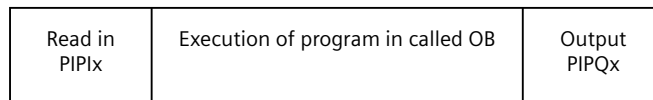The figure below illustrates the updating of a process image partition.

Read in PIPIx	Execution of program in called OB	Output PIPQx

Figure 9-9 process image

9.1.3.2 Update process image partitions in the user program

Requirements

Alternatively, you can also use the following instructions to update process images:

- Instruction "UPDAT_PI"

- Instruction "UPDAT_PO"

You will find the instructions in STEP 7 in the "Instructions" task card under "Extended instructions". The instructions can be called from any point in the program.

Requirements for updating process image partitions with the "UPDAT_PI" and "UPDAT_PO" instructions:

- The process image partitions must not be assigned to any OB. This means the process image partitions are not automatically updated.

NOTE

Update of PPI 0

PIP 0 (automatic update) cannot be updated with the "UPDAT_PI" and "UPDAT_PO" instructions.

UPDAT_PI: Update process image partition of the inputs

With this instruction you read the signal states from the input modules into the process image partition of the inputs (PIPI).

UPDAT_PO: Update process image partition of the outputs

With this instruction you transmit the process image partition of the outputs to the output modules.

Isochronous mode interrupt OBs

In the isochronous mode interrupt OBs you use the instructions "SYNC_PI" and "SYNC_PO" to update the process image partitions. Additional information on isochronous mode interrupt OBs is available in the STEP 7 online help.

Direct I/O access to the inputs and outputs of the module

You also have direct read and write access to the I/O, as an alternative to access via the process image, should direct access be required for programming reasons. A direct (write) I/O access also writes the process image. This prevents the situation where a subsequent output of the process image overwrites the value written via direct access again.

Reference

Additional information on process image partitions is available found in the function manual, Cycle and response times (https://support.automation.siemens.com/WW/view/en/59193558).

9.2 Configuring ET 200MP distributed I/O system

Introduction

You configure and assign parameters to the ET 200MP (interface module and I/O modules) with STEP 7 or in the configuration software of another manufacturer.

Requirements

Table 9-1 Requirements for installation

Configuration software	Requirements	Installation information
STEP 7 as of V13 [1]	• IM 155-5 PN ST and IM 155-5 DP ST: as of firmware version V2.0.0 • IM 155-5 PN HF: as of firmware version V1.0.0	• The TIA Portal supports the following GSDML specifications: – TIA Portal V11: V2.3 – TIA Portal V12SP1: V2.31 – TIA Portal V14: V2.32 – TIA Portal V15: V2.34 • The GSDML versions are largely downwards compatible.

Configuration software	Requirements	Installation information
STEP 7 as of V13 [1]	• PROFINET: PROFINET GSD files (https://support.industry.siemens.com/cs/ww/de/view/68189683/en?d-l=en) • PROFIBUS: PROFIBUS GSD files (https://support.industry.siemens.com/cs/de/de/view/80206700/en?dl-=en)	• The ET 200MP is already delivered with a GSD file based on specification V2.3. The GSD file can be installed and used in the TIA Portal.
		STEP 7 online help
STEP 7 V5.5 SP4 HF1 or higher	• PROFINET: PROFINET GSD files (https://support.automation.siemens.com/WW/view/en/19698639/13000-0) • PROFIBUS: PROFIBUS GSD files (https://support.automation.siemens.com/WW/view/en/10805317/13330-0)	STEP 7 online help
Software of another manufacturer		Manufacturer documentation

[1] STEP 7 does not support all the PROFINET features contained in the GSDML specifications. Non-supported features cannot be used with GSD devices.

Reference

You can find an overview of the most important documents and links to STEP 7 in the following FAQ on the Internet (https://support.industry.siemens.com/cs/de/de/view/65601780/en).

Configuring operation on PROFIBUS DP using a GSD file

If you want to configure the operation on the PROFIBUS DP with GSD file, you need to note the following additional requirements:

Table 9-2 Requirements for PROFIBUS DP with GSD file

I/O modules	Required firmware version IM 155-5 DP ST as of ...	Required firmware version I/O modules as of ...
Input/output modules 35 mm	V1.0.0	V2.0
Input/output modules 25 mm	V2.0.0	V1.0
Technology modules (TM)	V2.0.0	V1.1
Communications modules CM PtP	V1.0.0	V1.0.1

9.3 Assigning PROFIsafe address to fail-safe modules with SIMATIC Safety

The PROFIsafe address is saved permanently on the electronic coding element of the S7-1500/ET 200MP fail-safe modules. You can find additional information on the electronic coding element in the section Replacing the coding element at the power connector of the system power supply and load current supply (Page 375).

NOTE

The supply voltage L+ must be applied to the F-module during the assignment of the PROFIsafe address (F-destination address together with F-source address).

For additional information on assigning the PROFIsafe address (F-destination address together with the F-source address), refer to the SIMATIC Safety - Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126) programming and operating manual and the online help.

Basics of program execution

10

10.1 Events and OBs

Triggers

The table below gives an overview of the possible event sources for start events and their OBs.

Table 10-1 Triggers

Event sources	Possible priorities (default priority)	Possible OB numbers	Default system reaction [1]	Number of OBs
Startup [2]	1	100, ≥ 123	Ignore	0 to 100
Cyclic program [2]	1	1, ≥ 123	Ignore	0 to 100
Time-of-day interrupt [2]	2 to 24 (2)	10 to 17, ≥ 123	Not applicable	0 to 20
Time-delay interrupt [2]	2 to 24 (3)	20 to 23, ≥ 123	Not applicable	0 to 20
Cyclic interrupt [2]	2 to 24 (8 to 17, frequency dependent)	30 to 38, ≥ 123	Not applicable	0 to 20
Hardware interrupt [2]	2 to 26 (16)	40 to 47, ≥ 123	Ignore	0 to 50
Status interrupt	2 to 24 (4)	55	Ignore	0 or 1
Update interrupt	2 to 24 (4)	56	Ignore	0 or 1
Manufacturer-specific or profile-specific interrupt	2 to 24 (4)	57	Ignore	0 or 1
Isochronous mode interrupt	16 to 26 (21)	61 to 64, ≥ 123	Ignore	0 to 2
Time error [3]	22	80	Ignore	0 or 1
Maximum cycle time exceeded once			STOP	
Diagnostic interrupt	2 to 26 (5)	82	Ignore	0 or 1
Removal/insertion of modules	2 to 26 (6)	83	Ignore	0 or 1
Rack error	2 to 26 (6)	86	Ignore	0 or 1
MC servo [4]	17 to 26 (26)	91	Not applicable	0 or 1
MC pre-servo [4]	corresponds to priority of the MC-Servo	67	Not applicable	0 or 1

[1] If you have not configured the OB.

[2] For these event sources, apart from the permanently assigned OB numbers (see column: possible OB numbers), you can also assign OB numbers from the range ≥ 123 in STEP 7.

[3] If the maximum cycle time has been exceeded twice within a cycle, the CPU always switches to STOP regardless of whether you have configured OB80.

[4] You will find more information on these event sources and the starting behavior in the S7-1500/S7-1500T Motion Control function manual.

Event sources	Possible priorities (default priority)	Possible OB numbers	Default system reaction [1]	Number of OBs
MC post-servo [4]	corresponds to priority of the MC-Servo	95	Not applicable	0 or 1
MC interpolator [4]	16 to 26 (24)	92	Not applicable	0 or 1
MC pre-interpolator [4]	corresponds to priority of the MC interpolator	68	Not applicable	0 or 1
MC-LookAhead [4]	15 to 16 (15)	97	Not applicable	0 or 1
MC-Transformation [4]	17 to 25 (25)	98	Not applicable	0 or 1
Programming error (only for global error handling)	2 to 26 (7)	121	STOP	0 or 1
I/O access error (only for global error handling)	2 to 26 (7)	122	Ignore	0 or 1

[1] If you have not configured the OB.

[2] For these event sources, apart from the permanently assigned OB numbers (see column: possible OB numbers), you can also assign OB numbers from the range ≥ 123 in STEP 7.

[3] If the maximum cycle time has been exceeded twice within a cycle, the CPU always switches to STOP regardless of whether you have configured OB80.

[4] You will find more information on these event sources and the starting behavior in the S7-1500/S7-1500T Motion Control function manual.

Response to start events

The occurrence of a start event results in the following reaction:

- If the event comes from an event source to which you have assigned an OB, this event triggers the execution of the assigned OB. The event enters the queue according to its priority.

- If the event comes from an event source to which you have not assigned an OB, the CPU executes the default system reaction.

NOTE

Some event sources, such as startup, pull/plug, exist even if you do not configure them.

Assignment between event source and OBs

The type of OB determines where you assign OB to event source:

- For hardware interrupts and isochronous mode interrupts: The assignment is made during the configuration of the hardware or when the OB is created.

- For MC-servo, MC-PreServo, MC-PostServo, MC-Interpolator and MC-PreInterpolator: automatic assignment of OBs 91/92 by STEP 7 as soon as you add a technology object.

- For all other OB types: Assignment when the OB is created, where applicable after you have configured the event source.

For hardware interrupts, you can change an assignment which has already been made during runtime with the instructions ATTACH and DETACH. In this case, only the actually effective

assignment changes, and not the configured assignment. The configured assignment takes effect after loading, and upon each startup.

The CPU ignores hardware interrupts to which you did not assign an OB in your configuration or which occur after the DETACH instruction. The CPU does not check whether an OB is assigned to this event when an event arrives, but only prior to the actual processing of the hardware interrupt.

OB priority and runtime behavior

If you have assigned an OB to the event, the OB has the priority of the event. S7-1500 CPUs support the priority classes 1 (lowest) to 26 (highest). The following items are essential to the execution of an event:

- Call and execution of the assigned OB
- The update of the process image partition of the assigned OB

The user program processes the OBs exclusively on a priority basis. This means the program processes the OB with the highest priority first when multiple OB requests occur at the same time. If an event occurs that has a higher priority than the currently active OB, this OB is interrupted. The user program processes events of the same priority in order of occurrence.

NOTE

Communication

The communication (e.g. test functions with the PG) always works with priority 15. To avoid unnecessarily prolonging the program runtime in the case of time-critical applications, make sure that these OBs are not interrupted by communication. Assign a priority > 15 for these OBs.

Programming guideline and programming style guide

The programming guideline contains many recommendations and tips for optimal programming of the S7-1500 automation system.

The programming guidelines described in the programming style guide help you to create a uniform program code. You can better maintain and reuse the uniform program code. This allows you to detect or avoid errors early on, for example, through compilers.

You can find the programming guideline and programming style guide on the Internet (https://support.industry.siemens.com/cs/us/en/view/81318674).

Reference

More information on organization blocks is available in the STEP 7 online help.

10.2 Asynchronous instructions

Introduction

Program execution makes a distinction between synchronous and asynchronous instructions.

The "synchronous" and "asynchronous" properties relate to the temporal relationship between the call and execution of the instruction.

The following applies to synchronous instructions: When the call of a synchronous instruction is complete, execution of the instruction is also complete.

This is different in the case of asynchronous instructions: When the call of an asynchronous instruction is complete, execution of the asynchronous instruction is not necessarily complete yet. This means the execution of an asynchronous instruction can extend over multiple calls. The CPU processes asynchronous instructions in parallel with the cyclic user program. Asynchronous instructions generate jobs in the CPU for their processing.

Asynchronous instructions are usually instructions for transferring data, for example, data records for modules, communication data, diagnostics data.

Difference between synchronous/asynchronous instructions

The figure below shows the difference between the processing of an asynchronous instruction and a synchronous instruction. In this figure the CPU calls the asynchronous instruction five times before its execution is complete, e.g. a data record has been completely transferred.

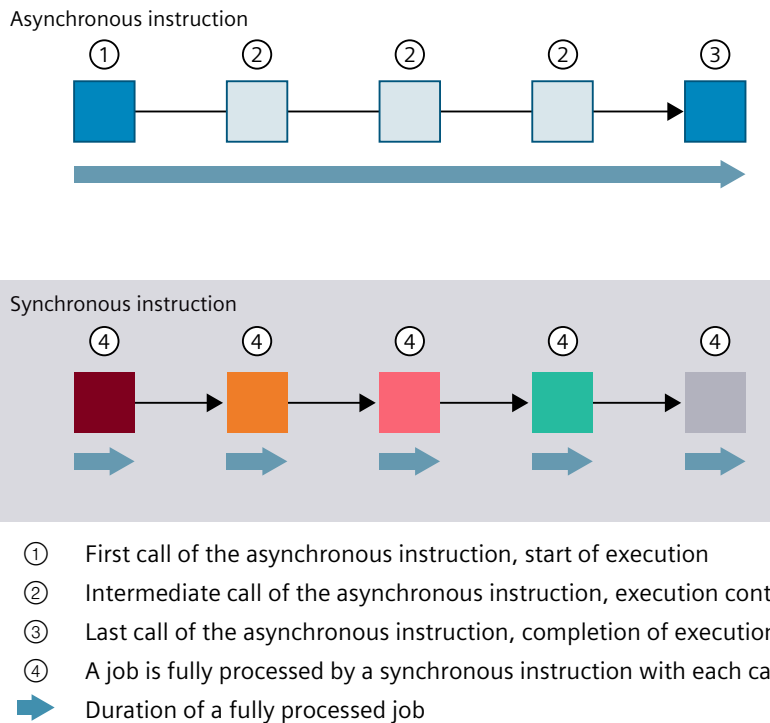In the case of a synchronous instruction, this is completely executed with each call.

①	First call of the asynchronous instruction, start of execution
②	Intermediate call of the asynchronous instruction, execution continues
③	Last call of the asynchronous instruction, completion of execution
④	A job is fully processed by a synchronous instruction with each call.
➡	Duration of a fully processed job

Figure 10-1 Difference between asynchronous and synchronous instructions

Parallel processing of asynchronous instruction jobs

A CPU can process several asynchronous instruction jobs in parallel. The CPU processes the jobs in parallel under the following conditions:

- Jobs for an asynchronous instruction are started while other jobs for that instruction are still running.
- The maximum number of simultaneously running jobs for the instruction is not exceeded.

The figure below shows the parallel processing of two jobs of the WRREC instruction. The two instructions are executed simultaneously for a certain duration.
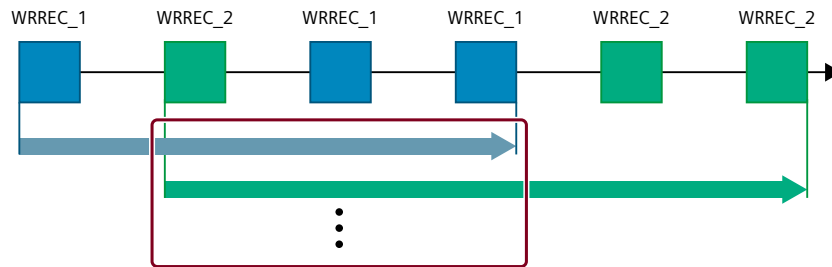
Figure 10-2 Parallel processing of the asynchronous instruction WRREC

NOTE

Dependencies between asynchronous instructions

The call order in the user program may differ from the order of execution of the asynchronous instructions. This may lead to problems with dependencies between asynchronous instructions.

Solution: To ensure the correct chronological execution, use the status outputs of the asynchronous instructions in a sequencer. The next asynchronous instruction should only when an asynchronous instruction is completed, and this is acknowledged via the parameter DONE.

Example: With the recipe phases RecipeImport and RecipeExport you need a CSV file for the recipe data. If you use the same CSV file for import and export, then the two asynchronous instructions are interdependent. In a sequencer, link the status of the DONE parameter of the RecipeImport instruction in the transition to the next step where the RecipeExport is executed. The link thus ensures the correct execution.

Assigning calls of an instruction to a job

To execute an instruction over multiple calls, the CPU must be able to uniquely relate a subsequent call to a running job of the instruction.

To relate a call to a job, the CPU uses one of the following two mechanisms, depending on the type of the instruction:

- Using the instance data block of the instruction (for "SFB" type)
- Using job-identifying input parameters of the instruction. These input parameters must match in each call during processing of the asynchronous instruction.
  Example: A job of the "Create_DB" instruction is identified by input parameters LOW_LIMIT, UP_LIMIT, COUNT, ATTRIB and SRCBLK.

The following table shows which input parameters you use to identify which instruction.

Table 10-2 Identifying input parameters for asynchronous instructions

Instruction	Job is identified by
DPSYC_FR	LADDR, GROUP, MODE
D_ACT_DP	LADDR
DPNRM_DG	LADDR
WR_DPARM	LADDR, RECNUM
WR_REC	LADDR, RECNUM
RD_REC	LADDR, RECNUM
CREATE_DB	LOW_LIMIT, UP_LIMIT, COUNT, ATTRIB, SRCBLK
READ_DBL	SRCBLK, DSTBLK
WRIT_DBL	SRCBLK, DSTBLK
RD_DPARA	LADDR, RECNUM
DP_TOPOL	DP_ID

Status of an asynchronous instruction

An asynchronous instruction shows its status via the block parameters STATUS/RET_VAL and BUSY. Many asynchronous instructions also use the block parameters DONE and ERROR.

The figure below shows the two asynchronous instructions WRREC and CREATE_DB.
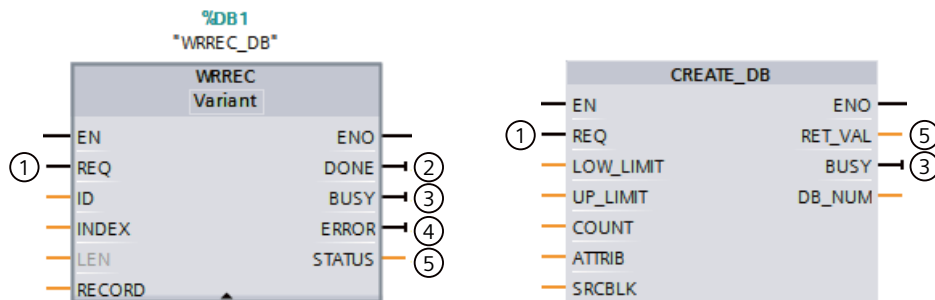
① The input parameter REQ starts the job to execute the asynchronous instruction.

② The output parameter DONE indicates that the job was completed without error.

③ The output parameter BUSY indicates whether the job is currently being executed. When BUSY =1, a resource is allocated for the asynchronous instruction. When BUSY = 0, the resource is free.

④ The output parameter ERROR indicates that an error has occurred.

⑤ The output parameter STATUS/RET_VAL provides information on the status of the job execution. The output parameter STATUS/RET_VAL receives the error information after the occurrence of an error.

Figure 10-3 Block parameters of asynchronous instructions using the instructions WRREC and CREATE_DB as examples.

Summary

The table below provides you with an overview of the relationships described above. It shows in particular the possible values of the output parameters if execution of the instruction is not complete after a call.

NOTE

You must evaluate the relevant output parameters in your program after each call

---

Table 10-3 Relationship between REQ, STATUS/RET_VAL, BUSY and DONE during a "running" job.

Seq. no. of the call	Type of call	REQ	STATUS/RET_VAL	BUSY	DONE	ERROR
-	Idle	0	W#16#7000	0	0	0
1	First call	1	W#16#7001	1	0	0
			Error code (e.g. W#16#80C3 for lack of resources)	0	0	1
2 to (n - 1)	Intermediate call	Not relevant	W#16#7002	1	0	0
n	Last call	Not relevant	W#16#0000, if no errors have occurred.	0	1	0
			Error code if errors occurred.	0	0	1

Use of resources

Asynchronous instructions use resources in the CPU during their execution. The resources are limited depending on the type of CPU and instruction. The CPU can simultaneously process only a maximum number of asynchronous instruction jobs. The resources are available again after a job has been processed successfully or with errors.

Example: For the RDREC instruction, an S7-1500 CPU can process up to 20 jobs in parallel.

If the maximum number of concurrent jobs for an instruction is exceeded, the following occurs:

- The instruction returns the error code 80C3 (lack of resources) in the block parameter STATUS.

- The CPU stops execution of the job until a resource becomes free again.

NOTE

Lower-level asynchronous instructions

Some asynchronous instructions use one or more lower-level asynchronous instructions for their processing. This dependence is shown in the tables below.

Please note that each lower-level instruction typically occupies one resource in the instruction's resource pool.

Extended instructions: maximum number of simultaneously running jobs

Table 10-4 Maximum number of simultaneous jobs for asynchronous extended instructions and lower-level instructions used

Extended instructions	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)	1507S(F) 1512C 1513(F)	1515(F) 1515T(F)	1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
Distributed I/O							
RDREC	20						
RD_REC	10						
WRREC	20						
WR_REC	10						
D_ACT_DP	8						
ReconfigIOSystem	uses RDREC, WRREC, D_ACT_DP,						
DPSYC_FR	2						
DPNRM_DG	8						
DP_TOPOL	1						
ASI_CTRL	uses RDREC, WRREC						
PROFIenergy							
PE_START_END	uses RDREC, WRREC						
PE_CMD	uses RDREC, WRREC						
PE_DS3_Write_ET200S	uses RDREC, WRREC						
PE_WOL	uses RDREC, WRREC, TUSEND, TURCV, TCON, TDISCON						
Module parameter assignment							
RD_DPAR	10						
RD_DPARA	10						
RD_DPARM	10						
WR_DPARM	10						
Diagnostics							
Get_IM_Data	10						
GetStationInfo	10						
Recipes and data logging							
RecipeExport	10						
RecipeImport	10						
DataLogCreate	10						
DataLogOpen	10						
DataLogWrite	10						
DataLogClear	10						
DataLogClose	10						
DataLogDelete	10						
DataLogNewFile	10						

Extended instructions	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)	1507S(F) 1512C 1513(F)	1515(F) 1515T(F)	1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
Data block functions							
CREATE_DB				10			
READ_DBL				10			
WRIT_DBL				10			
DELETE_DB				10			
File handling							
FileReadC				10			
FileWriteC				10			
Reference information							
ResolveSymbols				10			
GetSymbolForReference				10			

Basic instructions: maximum number of simultaneously running jobs

Table 10-5 Lower-level instructions used for asynchronous basic instructions

Basic instructions	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)	1507S(F) 1512C 1513(F)	1515(F) 1515T(F)	1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
Array DB							
ReadFromArrayDBL	uses READ_DBL (see Extended instructions)						
WriteToArrayDBL	uses READ_DBL, WRIT_DBL (see Extended instructions)						

Communication: maximum number of simultaneously running jobs

Table 10-6 Maximum number of simultaneous jobs for asynchronous instructions and lower-level instructions used for Open User Communication

Open User Communication	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)		1507S(F) 1512C 1513(F)	1515(F) 1515T(F)		1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
		Up to V2.9x	V3.0 and higher		Up to V2.9x	V3.0 and higher			
TSEND TUSEND	88	96	128	128	192	256	256	320	384
TRCV TURCV	88	96	128	128	192	256	256	320	384
TCON	88	96	128	128	192	256	256	320	384
TCONSettings	88	96	128	128	192	256	256	320	384
TDISCON	88	96	128	128	192	256	256	320	384

Open User Communication	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)		1507S(F) 1512C 1513(F)	1515(F) 1515T(F)		1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F)
		Up to V2.9x	V3.0 and higher		Up to V2.9x	V3.0 and higher			MFP
T_RESET	88	96	128	128	192	256	256	320	384
T_DIAG	88	96	128	128	192	256	256	320	384
T_CONFIG	1								
TSEND_C	Uses TSEND, TUSEND, TRCV, TCON, TDISCON								
TRCV_C	Uses TSEND, TUSEND, TRCV, TURCV, TCON, TDISCON								
TMAIL_C	Uses TSEND, TUSEND, TRCV, TURCV, TCON, TDISCON								

Table 10-7 Lower-level instructions used for asynchronous instructions for MODBUS TCP

MODBUS TCP	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)	1507S(F) 1512C 1513(F)	1515(F) 1515T(F)	1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
MB_CLIENT	uses TSEND, TUSEND, TRCV, TURCV, TCON, TDISCON						
MB_SERVER	uses TSEND, TUSEND, TRCV, TURCV, TCON, TDISCON						

Table 10-8 Maximum number of simultaneously running jobs for asynchronous instructions for S7 communication. The S7 communication instructions use a common pool of resources

S7 communication	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)		1507S(F) 1512C 1513(F)	1515(F) 1515T(F)		1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F)
		Up to V2.9x	V3.0 and higher		Up to V2.9x	V3.0 and higher			MFP
PUT GET USEND URCV BSEND BRCV	264	288	384	384	576	768	768	960	1 152

Table 10-9 Lower-level instructions used for asynchronous instructions for communication processors

Communications processors	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)	1507S(F) 1512C 1513(F)	1515(F) 1515T(F)	1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
PtP communication							
Port_Config	uses RDDEC, WRREC						
Send_Config	uses RDDEC, WRREC						
Receive_Config	uses RDDEC, WRREC						
Send_P2P	uses RDDEC, WRREC						
Receive_P2P	uses RDDEC, WRREC						

Communications processors	1505SP (F) 1505SP T(F)	1511(F) 1511C 1511T(F)	1507S(F) 1512C 1513(F)	1515(F) 1515T(F)	1516(F) 1516T(F)	1517(F) 1517T(F)	1518(F) 1518T(F) 1518(F) MFP
Receive_Reset	uses RDDEC, WRREC						
Signal_Get	uses RDDEC, WRREC						
Signal_Set	uses RDDEC, WRREC						
Get_Features	uses RDDEC, WRREC						
Set_Features	uses RDDEC, WRREC						
USS communication							
USS_Port_Scan	uses RDDEC, WRREC						
MODBUS (RTU)							
Modbus_Comm_Load	uses RDDEC, WRREC						
ET 200S serial interface							
S_USSI	uses CREATE_DB						
SIMATIC NET CP							
FTP_CMD	uses TSEND, TRCV, TCON, TDISCON						

Table 10-10 Maximum number of simultaneously running jobs for asynchronous instructions for OPC UA.

OPC UA instruction	1511(C/F/T/TF) 1512C 1513(F)	1505(S/SP/SP F/SP T/SP TF) 1515(F/T/TF) 1515 SP PC (F/T/T-F) 1516(F/T/TF)	1507S(F) 1517(F/T/TF) 1518 (F/T/TF//MFP)	1517(F/T) V4.0 or higher	1518(F/T) V4.0 or higher
OPC_UA_Connect	4	10	40	40	40
OPC_UA_NamespaceGet-IndexList	4*	10*	40*	40*	40*
OPC_UA_NodeGetH-andleList	4*	10*	40*	40*	40*
OPC_UA_MethodGetH-andleList	4*	10*	40*	40*	40*
OPC_UA_TranslatePathList	4*	10*	40*	40*	40*
OPC_UA_ReadList	20 in total (max. 5 per connection, see OPC_UA_Connect)	50 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)
OPC_UA_WriteList	20 in total (max. 5 per connection, see OPC_UA_Connect)	50 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)
OPC_UA_MethodCall	20 in total (max. 5 per connection, see OPC_UA_Connect)	50 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)	200 in total (max. 5 per connection, see OPC_UA_Connect)

* maximum 1 per connection

** Valid for Version V1.1 of the Methods instructions (OPC_UA_ServerMethodPre, OPC_UA_ServerMethodPost)

OPC UA instruction	1511(C/F/T/TF) 1512C 1513(F)	1505(S/SP/SP F/SP T/SP TF) 1515(F/T/TF) 1515 SP PC (F/T/T-F) 1516(F/T/TF)	1507S(F) 1517(F/T/TF) 1518 (F/T/TF//MFP)	1517(F/T) V4.0 or higher	1518(F/T) V4.0 or higher
OPC_UA_NodeRelease-HandleList	4*	10*	40*	40*	40*
OPC_UA_MethodRelease-HandleList	4*	10*	40*	40*	40*
OPC_UA_Disconnect	4*	10*	40*	40*	40*
OPC_UA_ConnectionGet-Status	4*	10*	40*	40*	40*
OPC UA server instructions					
OPC_UA_ServerMethodPre	20	20	20	100**	200**
OPC_UA_ServerMethod-Post	20	20	20	100**	200**

* maximum 1 per connection

** Valid for Version V1.1 of the Methods instructions (OPC_UA_ServerMethodPre, OPC_UA_ServerMethodPost)

Technology: maximum number of simultaneously running jobs

Table 10-11 Maximum number of simultaneously running jobs for asynchronous instructions for technology. The instructions for technology use a common pool of resources.

Technology	1511(F) 1511C 1512C 1513(F)	1511T	1505SP (F) 1515(F) 1516(F)	1515T 1505SP T (F) 1516T(F)	1507S (F)	1517 (F)	1517T (F)	1518(F) 1518(F) MFP	1518T (F)
S7-1500 Motion Control									
MC_Power MC_Reset MC_Home MC_Halt MC_MoveAbsolute MC_MoveRelative MC_MoveVelocity MC_MoveJog MC_MoveSuperimposed MC_Stop MC_WriteParameter MC_SetAxisSTW MC_SaveAbsoluteEncoderData MC_MeasuringInput MC_MeasuringInputCyclic MC_AbortMeasuringInput MC_OutputCam MC_CamTrack MC_GearIn MC_HaltSuperimposed MC_TorqueLimiting	300		1 500		3 000	4 800		6 400	

Technology	1511(F) 1511C 1512C 1513(F)	1511T	1505SP (F) 1515(F) 1516(F)	1515T 1505SP T (F) 1516T(F)	1507S (F)	1517 (F)	1517T (F)	1518(F) 1518(F) MFP	1518T (F)
MC_TorqueAdditive MC_TorqueRange									
MC_SetSensor MC_GearInVelocity MC_GearInPos MC_PhasingRelative MC_PhasingAbsolute MC_OffsetRelative MC_OffsetAbsolute MC_CamIn MC_SynchronizedMotionSimulation MC_GearOut MC_CamOut MC_LeadingValueAdditive MC_InterpolateCam MC_GetCamFollowingValue MC_GetCamLeadingValue MC_CopyCamData MC_MotionInVelocity MC_MotionInPosition MC_MotionSuperimposed MC_GroupInterrupt MC_GroupContinue MC_GroupStop MC_MoveLinearAbsolute MC_MoveLinearRelative MC_MoveCircularAbsolute MC_MoveCircularRelative MC_MoveDirectAbsolute MC_MoveDirectRelative MC_TrackConveyorBelt MC_KinematicsMotionSimulation MC_DefineWorkspaceZone MC_DefineKinematicsZone MC_SetWorkspaceZoneActive MC_SetWorkspaceZoneInactive MC_SetKinematicsZoneActive MC_SetKinematicsZoneInactive MC_DefineTool MC_SetTool MC_SetOcsFrame MC_KinematicsTransformation MC_InverseKinematicsTransformation	-	300	-	1 500	-	-	4 800	-	6 400

Reference

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

Protection 11

11.1 Overview of the protection functions

Advantages and customer benefits of protection functions

The protection functions listed protect your investments from unauthorized access and manipulation, helping to secure plant availability.

Protection functions

To set up secure networks, the SIMATIC S7-1500 automation system offers an integrated security concept:

Table 11-1 Overview of protection functions

Protection function	Description	S7-1500	ET 200MP
Integrity protection	The CPUs come with an integrity protection function as standard. This helps detect any manipulations: • In the engineering data on the SIMATIC Memory Card; see also information on the integrity protection of the SIMATIC Memory Card as of CPU FW version V3.1 in the next section • In the engineering data during data transfer between TIA Portal and CPU • At the engineering data during data transfer between HMI system and CPU • At the encrypted firmware	✔	---
Protection of confidential configuration data	Protection of confidential CPU configuration data	✔	---
Central user administration (as of firmware version 4.0)	Connection of a central server (UMC server) that is responsible for the administration and authentication of users. The central user management UMC (User Management Component) allows management of user groups and users independently of TIA Portal for extensive automation solutions.	✔	---
Local user management (as of FW version V3.1)	Improved management of users, roles, and CPU function rights (User Management & Access Control, UMAC). You can use the local user management in the editor to manage all project users along with their rights (e. g. access rights) for project users and roles in the TIA Portal.	✔	---
Access protection (up to FW version V3.0)	Protection against unauthorized configuration changes using authorization levels	✔	---

Protection function	Description	S7-1500	ET 200MP
Know-how protection	Protection against unauthorized access and modifications to algorithms with password protection	✔	---
Copy protection	Protection against duplication of programs by linking individual blocks to the serial number of the original memory card on the SIMATIC Memory Card	✔	---
Protection by locking the CPU/interface module	Protection against unauthorized access by locking the front cover with a seal or a lock	✔	✔

You can find more information about security mechanisms of the SIMATIC automation systems in the Security with SIMATIC S7 controllers (https://support.industry.siemens.com/cs/ww/en/view/77431846) document and in the Communication (https://support.industry.siemens.com/cs/us/en/view/59192925) Function Manual.

Integrity protection of the SIMATIC Memory Card, as of CPU FW version V3.1 or higher

With CPUs as of FW version V3.1, the integrity protection of the SIMATIC Memory Card depends on the password for protecting confidential configuration data that you assigned during the configuration of the CPU. This results in the following changes when using SIMATIC Memory Cards:

- To transfer a CPU to a card reader/USB memory device via drag and drop:
  For CPUs as of FW version V3.1, you need to enter the password of the CPU you want to use with the SIMATIC Memory Card. If you enter an incorrect password, the CPU will not start up after power on and will report the contents of the SIMATIC Memory Card as faulty.

- To insert a CPU from a card reader/USB memory device:
  In order to be able to verify the integrity of the included configuration in STEP 7, you must enter the password of the CPU from which the project was loaded. In this case, STEP 7 checks the data on the SIMATIC Memory Card and reports potential damage.
  Entering the password is optional. If you do not want to use the integrity check, you do not need to enter the password (restore project).

Secure communication

There is an increasing need to transfer data to external computers in encrypted form via Intranet or public networks.

SIMATIC S7-1500 CPUs and ET 200 CPUs with firmware version 2.0 or higher support the Internet PKI (RFC 5280) with STEP 7 as of V14. This makes the configuration and the operation of Secure Communication possible, for example:

- Hypertext Transfer Protocol Secure (HTTPS)

- Secure Open User Communication

- Secure communication with OPC UA

A public key infrastructure (PKI) can issue, distribute and check digital certificates. For S7-1500 CPUs, you create certificates for various applications in the CPU properties in STEP 7,

for example: TLS certificates for Secure Open User Communication, web server certificates, OPC UA certificates.

SIMATIC S7-1500 CPUs and ET 200 CPUs from firmware version 2.9 support with STEP 7 and WinCC as of Version 17 innovated and standardized secure PG/PC and HMI communication – referred to as Secure PG/HMI communication for short.

Further measures for protecting the CPU

The following measures additionally increase the protection against unauthorized access to functions and data of the S7-1500 CPU from external sources and via the network:

- Deactivation of the Web server
- Disabling the OPC UA server (you can find more information on the security mechanisms for OPC UA server in the Communication (https://support.industry.siemens.com/cs/us/en/view/59192925) Function Manual)
- Deactivation of the time synchronization via an NTP Server
- Deactivation of the PUT/GET communication
- Deactivation of SNMP

When you use the Web server, protect your S7-1500 automation system against unauthorized access:

- By setting password-protected access rights for specific users in the user administration.
- By using the pre-set option "Permit access only via HTTPS".
  The option allows access to the web server only with the secure hypertext transmission protocol HTTPS.

When you use the OPC UA server, protect your S7-1500 automation system against unauthorized access:

- By not setting up OPC UA server access for the "Anonymous" user.
- By disabling the "Automatically accept client certificates during runtime" option.

Security functions in communications processors

Communications processors support security functions, such as access protection using a firewall, protection against data manipulation using VPN, FTPS, HTTPS, SNMPv3, and secure NTP.

More information

You can find more information on the protection functions described in the STEP 7 online help.

Siemens products and solutions are only one element of a comprehensive industrial security concept. Observe the additional information on Industrial Security (http://www.siemens.com/industrialsecurity).

11.2 Protection of confidential configuration data

As of STEP 7 V17, you have the option of assigning a password for protecting confidential configuration data of the respective CPU. This refers to data such as private keys that are required for the proper functioning of certificate-based protocols.

You can find detailed information on protecting confidential configuration data in the Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) function manual.

11.3 Local user management

11.3.1 Useful information on the local user administration and access control

As of TIA Portal version V19 and CPU firmware version V3.1, S7-1500 CPUs feature improved management of users, roles, and CPU function rights (User Management & Access Control, UMAC).

For HMI devices, authentication is not possible via either local or central users (TIA Portal V19/V20).

From the versions mentioned above onwards, you manage all project users along with their rights (for example, access rights) for all CPUs in the project in the editor for users and roles of the project in the TIA Portal:

- To manage users along with their rights, for example to control access rights, navigate to the "Security settings > Users and roles" area in the project tree.

TIA Portal saves the assignment of the function rights of a CPU to user-defined roles and the assignment of these roles to users for each CPU. There are no system-defined roles with predefined function rights for CPUs.

After loading the configuration, the user management becomes effective in the respective CPUs. After loading, every CPU "knows" who may access which service and execute certain functions.

This new feature is also called "local user management and access control" below.

NOTE

Support of central users and groups for CPU function rights

UMC (User Management Component) can also be used to manage users centrally in TIA Portal. With this component, you can manage central users and groups on connected UMC servers, e.g. by connecting an MS Active Directory. The authentication is then implemented via UMC. The central user management for CPU-specific function rights via UMC is supported as of TIA Portal V20 and CPU FW version V4.0 (see Useful information on central user management and access control (Page 282)).

User management as a component of your security strategy

Carefully designed user management increases the security of your automation solution - however, only if you ensure the confidentiality of the user-relevant information.

In addition, the rules for industrial cybersecurity must be observed, for example regarding the "Defense in Depth" security concept, in particular the remarks on plant security and hardening measures.

You can find detailed information in the Industrial cybersecurity (Page 40) section.

Users, roles and function rights

Users and roles were already being managed in the predecessor version by TIA Portal under "Security settings > Users and roles". In addition to the existing user management options, e.g. for HMI devices, you can also manage all CPU function rights in this editor starting from TIA Portal Version V19.

The CPU function rights are valid during runtime. Therefore, these rights are located in the "Runtime rights" tab in the editor for users and roles. For each CPU in the project, there is a section with all CPU function rights to choose from – listed according to CPU services such as PG/HMI communication (engineering access, access levels), web server, and OPC UA.

Besides the user management for projects, additional user management possibilities were available for the web server and OPC UA server in the CPU properties (static user management for CPUs up to FW version V3.0):

• Users for the OPC UA server (authentication)

• User for the web server (authentication and access control)

These additional user management options have been integrated in the local user management in the project tree as of TIA Portal V19 and CPU FW version V3.1.

Introduction to the local user management and access control

For S7-1500 CPUs up to firmware version V3.0, users were managed under the respective CPU properties, separated according to services such as "Web server" and "OPC UA". Web server users were managed in the "Web server" area, OPC UA users in the "OPC UA" area.

To restrict the PG/HMI access to the CPU at different levels, you configured passwords for the corresponding access levels. With this approach, for example, HMI access could be permitted without restriction, but write access could be made dependent on the knowledge of a password. You assigned the passwords for the different access levels in the "Protection & Security" area of the CPU properties. The access protection therefore always related to groups that have the appropriate passwords - not to individual users.

With the introduction of local user management and access control in TIA Portal version V19, you use the "Security settings > Users and roles" area in the project tree in TIA Portal to manage all users, together with their roles and function rights, of a CPU. The same holds for the access protection for engineering/HMI access, which as of TIA Portal version V19 no longer relies on access levels with password protection by default but instead on the user management.

More information on the new access protection is available here (Page 278).

As already introduced, e.g. for engineering rights, you use role assignments for combining individual function rights. In a further step, you assign the roles to individual users. All the

function rights which were assigned to a user via roles and which the user can exercise for the corresponding CPU are listed In the "Assigned rights" tab.

The following figure shows an example of the available and activated function rights of a CPU. At least one user must have full access to the CPU. Otherwise, the configuration cannot be compiled. A role with full access to the CPU must be created for this.
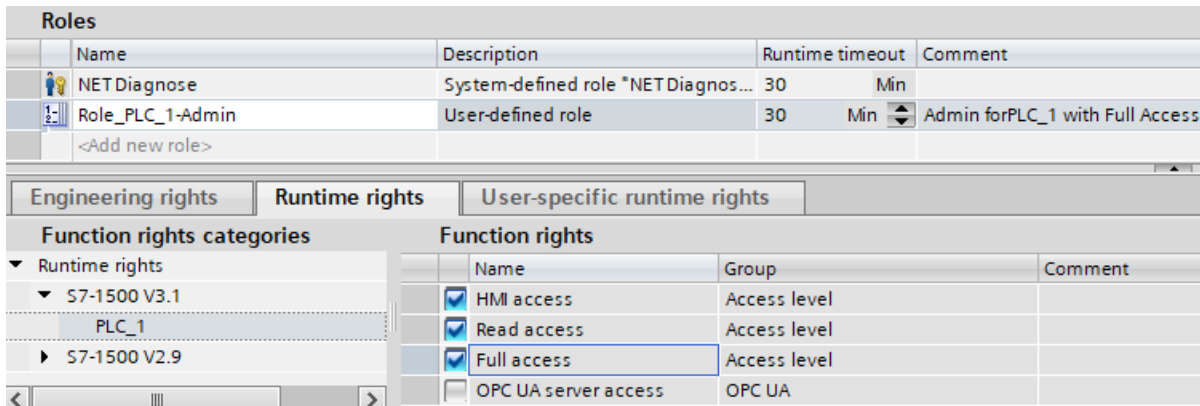
Figure 11-1 Assigning function rights of a CPU to a role

The following figure shows the assignment of the role with full access to a user ("Admin").
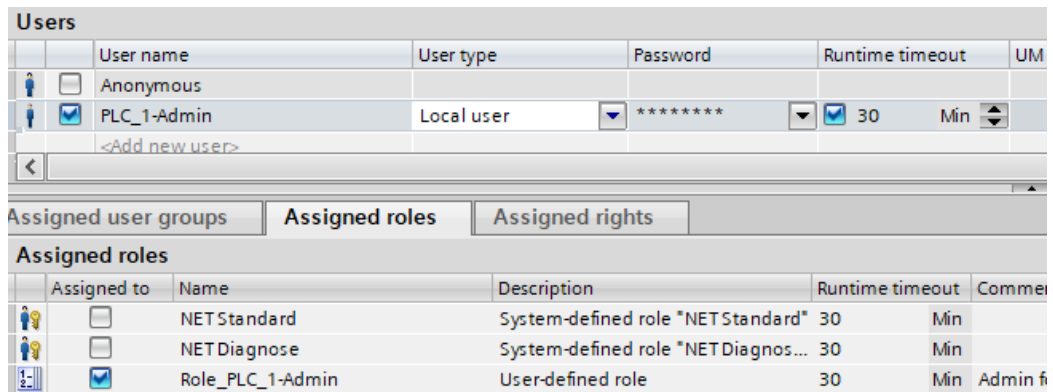
Figure 11-2 Assigning a role to a user

Requirement

CPU parameterization: To make use of users, roles and function rights for a CPU, the "Enable access control" option must be selected in the "Protection & Security > Access control" area.

In the "Configuration of user management" area, the "Local user management" option is preset, whereby the users are loaded to the CPU.

If you select the "Central user management" option, you have to add additional parameters such as the UMC server address and server ID (see Useful information on central user management and access control (Page 282)).

No project protection is required for user management.

Default characteristics

The "Activate access control" option is preset for the access control. Users can be configured with their assigned passwords and their roles and function rights.

Downloading to device

If you want to download changes to the user configuration in RUN mode, the hardware configuration in the CPU and in the STEP 7 project must be unchanged. Otherwise, a transition to STOP is required to download the user configuration together with the changed hardware configuration.

Save your STEP 7 project and then configure only the desired changes in the user configuration. Load your project into the CPU.

Changes to the access rights for the "Anonymous" user can only be loaded in STOP mode.

A fail-safe S7-1500 CPU may only load a user to whom the runtime right "Full access including fail-safe" is assigned. Otherwise, STEP 7 displays an error message when loading the configuration.

Explanations of the options for the user management download (Load preview):

- If you select the option "Keep online user management data", the local user management is not downloaded to the CPU.

- If you select the option "Download all user management data (reset to project)", all passwords changed online via WebAPI are deleted. After the download, the configured local user data is valid.

- If you select the option "Update user management data, but keep online passwords" and have not changed existing user names, the passwords changed online via WebAPI are retained. Only changes to function rights and/or roles take effect. Newly configured users are downloaded with their settings and deleted users are no longer available after the download to the CPU.
  If you have changed a user name in the project and assigned a password to this user in the project, this setting becomes valid after the download. The previously valid user name with the password changed online is deleted during the download.

Runtime timeout

You can set a runtime timeout for both the role and the user in 'Security Settings > Users and Roles'.

For an S7-1500 CPU, these settings are taken into account by the various services as follows:

- By means of the Web API you can, for example, create a web page or application that takes the settings for the runtime timeout into account. Standard web pages do not take the settings for runtime timeout into account and use the default value.

- The other services (PG/HMI communication and OPC UA server) do not use the runtime timeout; the logged-in user is not logged out after the set time.

11.3.2 Advantages of the local user administration and access control

The advantages of the new local user management for S7-1500 CPUs and the changes associated with it are described in the following.

Quick activation/deactivation of local user management

The options for user administration are located in the "Protection & Security > Access control" tab:

- Access control deactivated: Every user has full access to all functions with the exception of the GDS Push function for the online transfer of certificates.

> ⚠️ **DANGER**
>
> **Disabled access control carries the risk of unauthorized access and thus the risk of personal injury and property damage.**
>
> Only use this setting in a protected environment, such as during commissioning.

- Access control enabled: The configured users with their assigned roles and concomitant linked function rights become effective after loading.

Access protection for PG/HMI accesses, now with user authentication

While it was possible to assign passwords for access levels for S7-1500 CPUs with firmware versions <V3.1, you can configure users with corresponding function rights for the current CPUs. This means that the authentication options for PG/HMI access correspond to the options offered by OPC UA or web server accesses.

All in one place

Irrespective of the service for which you configure users, roles and rights for a CPU: You have to manage the data at the same location.

All users, no matter if you manage their engineering rights for the project or their local runtime rights for each CPU in the project, can be found in the editor for users and roles in the project tree.

Powerful password functions

- Support for compliance with complexity rules for password creation:
  Already at the password creation stage, you can have the TIA Portal check for compliance with complexity rules, such as rules on password length, uppercase/lowercase letters (project tree, "Security settings > Settings" area).
  The complexity rules are also saved in the CPU when the user management is loaded. When the password is changed online, the CPU determines and considers these rules. This prevents a user from overriding the complexity rules set by the configuration engineer and assigning a non-secure password.

- The period of validity of passwords is adjustable:
  To ensure that a user does not have access to the CPU with a compromised password for an unlimited time, you can parameterize a period of validity. Before the period of validity expires, the remaining time is then displayed on login so that each user has the possibility to change their password in time.

Loading the user management during operation

As of firmware version V3.1, certain security-relevant configuration data can be loaded in both STOP and RUN system state. This means that loading the hardware configuration does not necessarily lead to a CPU STOP.

You can load the following changes in STOP, RUN-Solo or Run-Redundant system state (Download to device > Hardware configuration):

- Local user management extended/changed

- TIA Portal-configured certificates modified

- Syslog configuration changed

If you made additional changes to the hardware configuration (for example, modules added, parameters reassigned, etc.), then the CPU automatically requests the STOP state before loading the configuration.

So if you, for example, load just one user with modified roles/function rights to the CPU, this process does not require the CPU to be in STOP state.

The preview dialog for loading contains a security area so that you can determine when loading how the CPU should deal with user data that has changed in the meantime (not when loading for the first time). This allows changes to user data (e.g. password changes during runtime) to be retained.

Loading the device as a new station - with user data

If you load a previously configured CPU into a new project, for example, because you do not have the original project, the user data is also loaded into the project and is available for further editing of the CPU settings.

Changing of passwords during operation

You can use the web server API to write an application with which each user can change their password at runtime, provided that the original password was entered correctly and the new password corresponds to the set password guideline.

Requirement: You have enabled access control for the CPU.

A user can change their own password at any time, even if the password has expired. If the password has expired, the user must change the password. Login will not be possible with an expired password.

API methods used:

- Api.ChangePassword
- Api.GetPasswordPolicy

You can find more information about the API methods in the Web server Function Manual (https://support.industry.siemens.com/cs/de/en/view/59193560).

NOTE

Passwords changed at runtime take priority over loaded passwords

If you have changed your password during running operation and subsequently load your project, the password assigned during runtime takes precedence over the password set in the project (default setting).

If you want to overwrite the passwords changed during runtime by loading the project, you have to select the option "Load all user management data (reset to project data)". In this case, **all** passwords changed during runtime will be lost.

11.3.3 From the access level to the function right of users

The following section shows how to implement access protection with the new local user management for CPUs.

Access levels as function rights

With S7-1500 CPUs up to FW version V3.0, access could only be controlled via passwords. With CPUs as of FW version V3.1, you can create the appropriate users and roles with the necessary function rights for access control. The assignment between access level and the associated function right results from the already known access levels:

- Users who are to have full access must have a role with the function right "Full access", or "Full access incl. failsafe" for F-CPUs.

  A CPU configuration can only be compiled and loaded if at least one user has the function right "Full access" or "Full access incl. failsafe".

- Users who are to have read access must have a role with the function right "Read access".

- Users who are to have HMI access must have a role with the function right "HMI access".

If a user does not have any of these specified function rights, that user also has no access to the CPU.

The hierarchical organization of the access levels also remains the same for the corresponding function rights:

- A user with full access also has the function rights "Read access" and "HMI access".

- A user with read access also has the function right "HMI access".

NOTE

Compatibility of the "ENDIS_PW" instruction

The "ENDIS_PW" instruction can only be used to disable or enable passwords for access levels. The "ENDIS_PW" instruction has no effect on assigned rights for users or roles.

Continuing to use access levels

Even though the new local user management replaces the usual access protection via corresponding function rights of individual users, there is still the possibility to continue to use this familiar access protection. This is required, for example, for HMI devices which only support access levels and which do not benefit yet from possibilities of the new user management.

If you require the configuration of an access level, for example, to ensure an HMI device access even without user or password access, you have to activate the "Use legacy access control via access levels" option in the CPU properties.

NOTE

User for OPC UA and for the web server

Independent of the access protection, you always have to configure the users for the web server and OPC UA server in the project tree ("Security settings > Users and roles" area).

Restrictions on continued use of the access levels

When using the "Legacy access control" option, you cannot select the access level directly in the table for setting the access levels. This selection can only be set for the new local user management in one way: Via the access protection function rights of the "Anonymous" user.

The local user "Anonymous" is created in a project by the system by default. With the help of this user, you determine the behavior of the CPUs in the project for someone who logs in without a user name and password. For security reasons, the anonymous user is deactivated and needs to be activated before use.

The area where you set the access levels leads you via a link to the editor for the required settings for the "Anonymous" user.

Examples:

- If the "Anonymous" user is deactivated or if the "Anonymous" user is activated and no function rights have been assigned to that user, then nobody can log in without a user name and password (corresponds to the access level "No access (complete protection)").

- If the "Anonymous" user is activated and the "Full access" function right for a CPU is assigned to that user via a corresponding role, the result of this setting is "No protection". You can achieve the same effect with regard to access protection by setting "No access protection" in the "Protection & Security" area of the CPU properties.

Procedure

To activate the "Legacy access control" and set the required access level, follow these steps:

1. In the CPU properties, go to "Protection & Security > Access control".

2. Select the option "Activate access control" and, in addition, select the check box "Use legacy access control via access levels" check box.

   The access level selection cannot be used in this setting. You have to set the access level via the "Anonymous" user of the CPU.

   The "Anonymous" user is deactivated by default. This means that the resulting access level for users without a password is "No access (complete protection)" (default setting).

3. Go to "Security Settings > Users and roles" in the project tree.

4. Activate the "Anonymous" user, if you want to set a different access level than "No access (complete protection)". You can assign a role with function rights that grants access to the CPU without password input, only to the activated "Anonymous" user.

5. You cannot assign function rights for a CPU directly to a user. You must first assign a role: Therefore switch to the "Roles" tab and add a new role. Assign a meaningful name, e.g. "PLC1-Read-Access-Role". If you assign this role to a user, this user should have read access to PLC1 during operation.

6. Assign the required function right for the access to the CPU with the name "PLC1" to the role "PLC1-Read-Access-Role" - in this case "Read access".

7. Switch to the "User" tab and assign the "PLC1-Read-Access-Role" role to the activated "Anonymous" user.

   Result: The "Anonymous" user has read access for PLC1. This means that the access level tables of the CPU "PLC1" in the project are preset to "Read access" (cannot be changed) and users who are not logged in only have read access.

   For full access, or full access including fail-safe, you have to configure a password for the full access in the table for the access protection. Users who need full access to the CPU during runtime via an action, e.g. because a project is to be loaded onto the CPU, must legitimize themselves for this action with this password.

Tip

> To make the user rights transparent, use meaningful names for the respective roles. You create users and roles for the entire project; you must select the function rights of a role individually for each CPU in the project. With a descriptive name you can, for example, immediately see which CPUs have read access and which CPUs are fully protected.

11.3.4 Information about compatibility

> In the following sections, you will find information on the behavior of the CPUs with the local user administration, e.g. when replacing modules in STEP 7 and for further use of projects and programs without local user administration.

Replacement part scenario

> If you replace a CPU with a firmware version < V3.1 with a CPU with a firmware version V3.1 or higher, the program stored on the memory card runs like the original CPU. The behavior with regard to the configured access levels, the users for the OPC UA server and the web server corresponds to the behavior of the previous CPU.
>
> In this case, the "Change password function" via the web server API is not accepted by the CPU because the CPU has been configured for firmware version < V3.1 and has no local user administration.

Replace CPU (upgrade)

> If you replace a CPU (FW < V3.1) with a current CPU (FW V3.1 or higher) in the TIA Portal, this has the following effects on the configured user data:
>
> • The user data from the OPC UA server and web server is transferred to the "Users and roles" editor in the project navigation.

> | NOTICE |
> | --- |
> | **Passwords are lost when replacing the CPU** |
> | Before replacing the CPU, make sure that the passwords are available. They must be entered again in the "Users and roles" editor. Otherwise, you have to assign new passwords and inform the users. |

> • A corresponding role is created for each web server user in the "Users and roles" editor; the name of the role contains the CPU name, the "Web" string and the already configured web server user name. In this way, by assigning these roles in the "Users and roles" editor, you can easily restore the original rights for each CPU.
>
> • The "OPC UA server access" role is created for each OPC UA server user.
>
> • OPC UA guest access and the web server "Everybody" are migrated to the "Anonymous" user.
>
> • Each OPC UA user and each web server user is listed in the "User" column in the editor for users and roles. If the names are the same (web server and OPC UA user), only one user is created.

- With a protected project, you can select which action the CPU performs:
    - Migrate user (requirement: You are logged in as a user with the right to manage users and roles and the right to edit the project/configuration)
    - Remove user
    - Cancel
- The "Legacy access control via access levels" option is set for access protection.

Replace CPU (downgrade)

If you replace a CPU (as of FW V3.1) with a previous CPU (< FW V3.1) in the TIA Portal, this has the following effects on the configured user data:

- The local user administration is no longer available.
- Users with function rights for the web server are not transferred.
- Users of the OPC UA server remain with their user rights in the "Users and roles" editor. No users are moved to the "OPC UA" area of the CPU parameters.
- It is no longer possible for users to change passwords during runtime (via web server API).

11.4 Central user management

11.4.1 Useful information on central user management and access control

As of TIA Portal version V20 and CPU firmware version V4.0, S7-1500 CPUs have a feature whereby authentication of users can be left to a central UMC server.

As of the versions specified above, you manage users centrally and combine multiple users with the same roles/function rights into one group.

The central authentication service is performed in this case by the UMC (User Management Component).

You set up linking between user/group and assigned roles and function rights in the editor "Users and roles" in TIA Portal - as with the local user management.

For HMI devices, the authentication is not possible via either local or central users (TIA Portal V19/V20).

User management as a component of your security strategy

Carefully designed user management increases the security of your automation solution - however, only if you ensure the confidentiality of the user-relevant information.

In addition, the rules for industrial cybersecurity must be observed, for example regarding the "Defense in Depth" security concept, in particular the remarks on plant security and hardening measures.

You can find detailed information in the Industrial cybersecurity (Page 40) section.

Advantages of central user management

Central user management allows management of users and user groups independently of TIA Portal. This enables the user management to be scaled from a few users and CPUs in a single project (local user management) up to extensive automation solutions with multiple projects, users and user groups (central user management) – without increased workload.

If you use the central user management (UMC), you can, for example, configure user groups on the UMC server set up for this purpose. The users of a group then have the same roles and function rights on the CPU.

During operation, users can be added to or removed from a group or passwords can be changed on the UMC server. The CPU configurations do not need to be changed and reloaded.

> ⚠ **WARNING**
>
> **Decoupling the user management from the CPU involves risks**
>
> When central user management is used, the CPU or TIA Project has no way, for example, of checking the plausibility of changes to the group assignment of individual users. UMC administrators must carefully check the effect of their changes with regard to modified roles and function rights.

Requirements

The configuration in the editor for users and roles (TIA Portal) provides you with a wide scope of usage scenarios in connection with UMC:

- Programming device with TIA Portal is connected to a UMC domain. In this case, the users and groups can be synchronized in the editor for users and roles.

- Programming device with TIA Portal is not connected to a UMC domain but the names of the user groups/central users used in operation are known and can be added without contact to the UMC server.

  The names of the user groups/central users can also be entered without connection to the UMC domain and synchronized with the UMC domain later.

  The synchronization is not necessary for authentication of CPU users via a UMC server. The group names or user names only have to match to make use of the authentication service.

A CPU which needs to authenticate the querying users (e.g. via web, PG/HMI communication, or OPC UA) for diverse online functions requires the following information for accessing the authentication service:

- The UMC server address

  Example: https://central.umc.testnet:443/ra

  (443 = Port for https, ra = remote authentication)

- A server ID (fingerprint of the server certificate).

  You can determine the fingerprint of a certificate through Windows (open the certificate, "Details" tab, "Fingerprint" field).

As an alternative to the server ID, you can configure a list of CA certificates. These certificates are used by the CPU to verify the certificate returned by the UMC server when a connection is established. In order for the verification to be successful, the entire certificate chain down to

the root certificate must have been loaded. The verification does not work for end-entity certificates or for intermediate certificates without a certificate chain to the root certificate.

Further requirements for operation (Runtime):

• User groups and users have been set up on the UMC server.

• A connection can be established between the CPU and UMC server via the configured UMC server address.

• CPU time is current

NOTE

No logon possible if the UMC server is not available or the CPU time is reset

– If you use only UMC users and UMC user groups to access the CPU during operation and the UMC server becomes unreachable, e.g. due to connection abort, then no one can log on anymore.

  – To enable access to the CPU in this case, configure at least one local user with the required roles/function rights.

– If you use UMC user groups or UMC users to access the CPU during operation, the CPU time must be up-to-ate.

  If the CPU time has been reset, e.g. by restoring the factory settings, and no NTP time synchronization has been configured, it is also not possible to log on via the central user management. Authentication of the UMC server using certificates requires an up-to-date CPU time.

  – To enable access to the CPU in this case, configure at least one local user with the required roles/function rights to set the time (e.g. from the "Web server – Maintenance" group).

  – Alternatively, you can synchronize the CPU time using NTP servers (for information on configuration; see section Time synchronization (Page 345)).

Basic procedure for using the User Management Component (UMC)

The following basic steps are required to use the User Management Component (UMC):

1. Installation of UMC on one or more computers in the system.

2. Assigning a corresponding UMC version as a UMC ring server or UMC server. This creates a UMC system consisting of one or multiple UMC computers.

3. Creating users and user groups in UMC. These can exist only in UMC or can be imported from a Microsoft Active Directory.

4. Connection of the UMC agent that is installed on the computer with the TIA Portal installation. The connection can be established with the TIA Administrator or with the Windows command line.

5. Use of UMC users and UMC user groups, for example, in the context of the TIA Portal project creation.

6. Authentication of UMC users after logging on via UMC.

NOTE

Enabled "Anonymous" user is always loaded

An enabled "Anonymous" user with its configured roles/function rights is loaded even if you only enabled the central user management. Local user management does not have to be additionally enabled for the "Anonymous" user to take effect.

Additional information on the UMC server

More information on setting up (installing, configuring) a UMC server as well as creating central users and groups can be found here (https://support.industry.siemens.com/cs/us/en/view/109780337).

11.4.2 Configuring central user management in the editor for users and roles

The procedure for configuring the central user management in TIA Portal version V20 with an S7-1500 CPU is described below (firmware version as of V4.0).

We distinguish between the following use cases:

• The project is configured in the environment that has access to the UMC server.

• The project is created in an environment that has no access to the UMC server.

  This is, for example, the case for a machine that is configured independently of the later place of installation and environment. The parameters for the user management must still be modified at the installation location.

Requirements - TIA Portal has access to the UMC server

• TIA Portal, editor for users and roles: The needed roles have been configured and the required function rights for these roles have been assigned.

• There is an online connection to the UMC server.

Procedure - Creating a new user group

To create a new user group, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).

2. Select the "User groups" tab.

3. Click the "Add new UMC user group" button.

4. Log on to the UMC server as the admin user.

5. In the dialog for selecting the user groups, select the user groups to be imported into the editor.

6. Assign the desired roles to the groups.

Procedure - Creating a new central user

To create a new central user, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).

2. Select the "User" tab.

3. Click "Add user".

4. Log on to the UMC server as the admin user.

5. In the dialog for selecting the central users, select the users to be imported into the editor.

6. Assign the desired roles to the users.

Requirements - TIA Portal has no access to the UMC server

- TIA Portal, editor for users and roles: The needed roles have been configured and the required function rights for these roles have been assigned.

- There is no online connection to the UMC server at the time in which user management is configured.

NOTE

Case sensitivity of user name

Although the UMC server does not differentiate between upper and lower case of the user name/group name when logging on, deviations in case prevent the user from logging on for users/groups configured offline or unsynchronized in the TIA Portal.

Recommendation:

- Before login, synchronize users and user groups in the TIA Portal and download this configuration to the CPU. In this case, the case of the user name is not relevant during logon.

- If possible, import users/groups as described above.

Procedure - Creating a new user group

To create a new user group, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).

2. Select the "User groups" tab.

3. Click in the <Add new user group> field in the "Name" column.

   The TIA Portal enters a default name.

4. Modify the default name - this name will be used in the target environment of UMC.

   The name can also be modified in the target environment during commissioning.

Result: The groups are set up but not synchronized, i.e. no UM domain ID is assigned.

When a connection to the UMC server exists in the target environment, the following process takes place when a central user logs on:

- The CPU forwards the authentication request to the UMC server.

- After a successful check, the UMC server returns a list of groups to which the logged-on user belongs.

- The CPU determines the assigned roles and function rights for the user based on the group names.

Procedure - Creating a new central user

To create a new central user, follow these steps:

1. Open the editor for users and roles (project tree: Security settings > Users and roles).

2. Click in the <Add new user> field in the "User name" column.

   The user type "Local user" is preset.

3. Modify the default user name - this name will be used in the target environment of UMC.

4. In the column "User type" change the entry to "Central user".

Result: The central user has been set up but not yet synchronized, meaning that no UM domain ID is assigned.

In the target environment with a connection to a UMC server, you can still adjust the provisional group and central user names using the TIA Portal.

Changing the user type - Effects

- When you change the user type (central user > local user), the data for the connection to the UMC server is lost (UM domains ID).

- When the user type is changed from local user to a central user, the configured password and the comment are lost.

11.4.3 Configuring central user management for an S7-1500 CPU

The procedure for configuring the S7-1500 CPU is described below (firmware version as of V4.0).

Procedure - CPU configuration for central user management
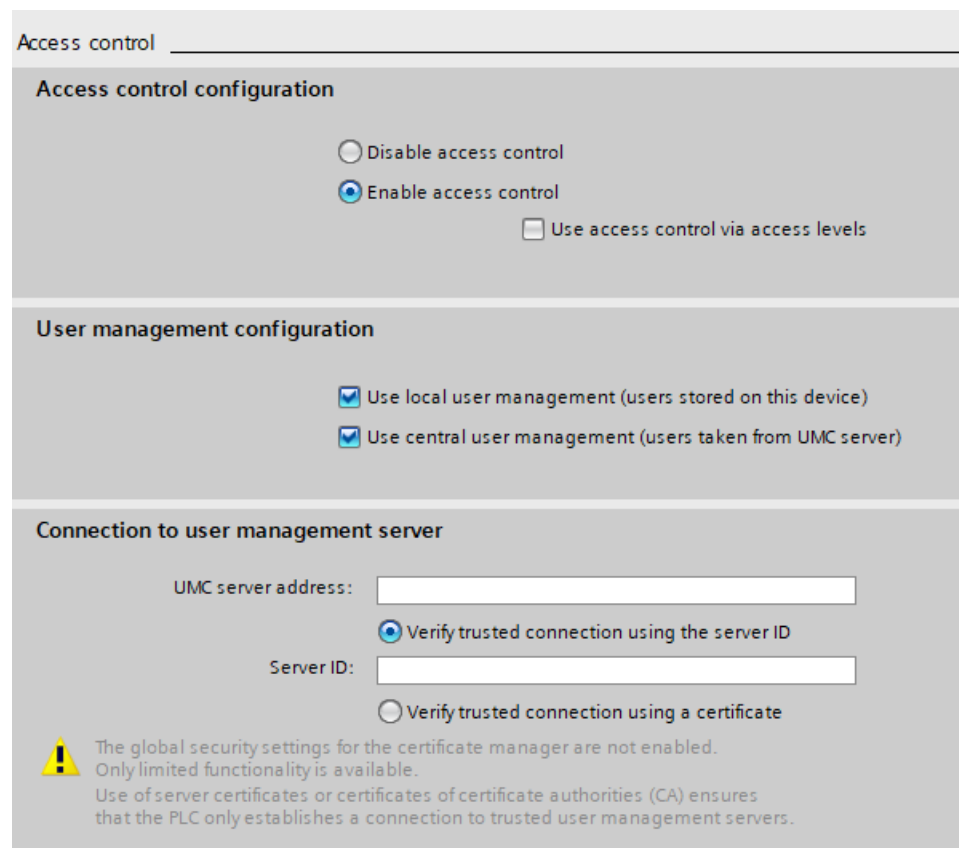
To configure the central user management for an S7-1500 CPU, follow these steps:

1. Place the CPU and navigate to the area "Protection & Security > Access control".
2. Ensure that access control has been enabled (access control via protection levels may be enabled or disabled).
3. Activate the option "Use central user management (users taken from UMC server)".

   In addition, the local user management can also be activated in order to still be able to access the CPU if the connection to the UMC server fails, for example.

4. Add the specifications to the UMC server address and server ID for authentication of the UMC server.

   As an alternative to the server ID, you can also add the CA certificate or intermediate certificate for authentication. The CPU must have the entire certificate chain for verification of the server certificate including root certificate.

Changing the connection data for the UMC server

A user with a role that grants full access to the CPU can download modified connection data (UMC server address and server ID) in both STOP and RUN modes of the CPU.

11.4.4   Logon of central users

The processes for the logon of central users are described below from the perspective of different applications.

Requirements

- A UMC server is connected to the CPU (firmware version V4.0 or higher) and is accessible.
- The required central users and groups have been set up for the UMC server.
- The CPUs are configured accordingly for the central user management (roles and function rights) and the configuration is loaded.

Logging onto a protected CPU

If you access a CPU online and the operation requires function rights from users, a dialog appears, as with the local user management, which queries the user type. As of TIA Portal version V20, you can log on as a central user.

Causes of a failed logon of a central user

Besides known causes, such as a wrong user name (not configured) or wrong password, the logon may, for example, fail due to network problems (UMC server not reachable) or an oversized response frame.

Tip

To handle such cases, set up a local user who can read the diagnostic buffer in the event of a failed logon and determine the exact cause. You can find additional information on these diagnostic buffer entries in: Product information on S7-1500/ET 200MP, S7-1500R/H documentation (https://support.industry.siemens.com/cs/ww/en/view/68052815).

Logging on as an OPC UA client or as a web client

When an OPC UA client logs on to the OPC UA server of the S7-1500 CPU, the user name and password are transferred via the UserNameIdentityToken.

The user name and password are also queried for web clients if you want to use the full functionality of the web server of the S7-1500 CPU. See also the Web server function manual, section "Authentication". The following process applies to OPC UA clients and web clients:

• For central users, the CPU forwards the authentication query to the UMC server.

• If the authentication is successful, the UMC server returns the assigned groups to which the user belongs.

• The CPU generates the corresponding session context and grants the authorizations (function rights from the determined roles).

• The client can then execute the access in the context of the session in accordance with the granted function rights.

How does the CPU (OPC UA server or the website of the web server) detect whether the user is a local or central user?

You have the freedom to configure a user both as a local user and as a central user. This results in an ambiguity about which service is responsible for the authentication and which user ultimately gains access. Since access permission for the user depends solely on the password in this case, you should use strong passwords, e.g. created by a password generator.

The following rules apply to ensure unambiguousness for the responsible authentication service (local or central user management):

• For logon of a local user, add the prefix "L:" (uppercase or lowercase) in front of the user name.
  Example: L:username

  If you do not use a prefix for the user names, central user management is automatically responsible (when central and local user management are used at the same time). If you use only one type of user management, access is unambiguous even without a prefix.

• A user name must not begin with the string "L:" (uppercase or lowercase).

11.5 Configuring access protection for the CPU

Introduction

The following section describes how to use the various access levels of the CPUs. The description applies to S7-1500 CPUs up to firmware version V3.0.

In later firmware versions, use the local user management in the editor for users and roles in the project tree. The access levels are represented there by function rights of the same name which you assign to individual users via roles.

The CPU provides you with various access levels to limit access to specific functions.

By setting up access levels and passwords, you limit the functions and memory areas that are accessible without a password. The individual access levels as well as their associated passwords are specified in the object properties of the CPU.

Rules for passwords

Ensure that passwords are sufficiently secure. Passwords must not follow a machine-recognizable pattern.

Apply the following rules:

- Assign a password that is at least 8 characters long.

- Use different cases and characters: uppercase/lowercase, numbers and special characters.

Access levels of the CPU

Table 11-2 Access levels and access restrictions

Access levels	Access restrictions
Full access including fail-safe (no protection)	Users of STEP 7 and HMI applications have access to all standard and fail-safe functions. A password is not required.
Complete access (no protection)	Users of STEP 7 have access to standard functions. HMI applications can access all functions (fail-safe and standard). **Required password:** For additional access to the fail-safe functions, the user must enter the password for "Full access incl. fail-safe" in STEP 7.
Read access	In this access level, only read access to the hardware configuration and the blocks is possible without a password. HMI access and access to diagnostics data is also possible. Neither blocks nor the hardware configuration can be downloaded to the CPUs without the password. Additionally, the following is not possible without the password: Writing test functions and firmware update (online).
HMI access	The access restrictions that apply to read access also apply to HMI access. Additionally, the following is **not** possible without the password: Test functions, changing the operating mode (RUN/STOP), firmware update and display of online/offline comparison status.
No access (complete protection)	When the CPU has complete protection, no read or write access to the hardware configuration and the blocks is possible (without access authorization in the form of a password). HMI access is also not possible. The server function for PUT/GET communication is disabled in this access level (cannot be changed). Authentication with the password will again provide you full access to the CPU.

Reference

An enumeration of which functions are available in the different access levels is available in the "Setting options for the protection" entry in the STEP 7 online help.

Properties of the access levels

Each access level allows unrestricted access to certain functions without entering a password, e.g. identification using the "Accessible devices" function.

The default of the CPUs is "No access (complete protection)". In the default access level, the user may neither read nor change the hardware configuration and the blocks. To obtain access to the CPUs, use an alternative parameter assignment in the properties of the CPU:

*   A password for the protection level "No access (complete protection)"

*   A different protection level, e.g. "Full access (no protection)"

Communication between the CPUs (via the communication functions in the blocks) is not restricted by the access level of the CPU, unless PUT/GET communication is deactivated in the "No access" (complete protection) access level.

Entry of the right password allows access to all the functions that are allowed in the corresponding level.

NOTE

Configuring an access level does not replace know-how protection

Configuring access levels offers a high degree of protection against unauthorized changes on the CPU via network access. Access levels are used to restrict the rights to download the hardware and software configuration to the CPU. However, blocks on the SIMATIC Memory Card are not write-protected or read-protected. Use know-how protection to protect the code of blocks on the SIMATIC Memory Card.

Behavior of functions with different access levels

The STEP 7 online help contains a tabular list of the online functions that are possible in the various access levels.

Configuring access levels

To configure the access levels for an S7-1500 CPU up to FW version V3.0, follow these steps:

1. Open the properties of the S7-1500 CPU in the Inspector window.

2. Open the "Protection & Security" entry in the area navigation.

   A table with the possible access levels appears in the Inspector window.

Figure 11-3 Possible access levels of an S7-1500 CPU up to FW version V3.0

3. Activate the desired protection level in the first column of the table. The green check marks in the columns to the right of the respective access level show you which operations are still available without entering the password. In the example (Figure: Possible access levels), access is not possible without a password.

4. In the "Enter password" column, specify a password for the access level "Full access" in the first row. In the "Confirm password" column, enter the selected password again to guard against incorrect entries.

5. Assign additional passwords as required for other access levels.

6. Download the hardware configuration for the access level to take effect.

The CPU logs the following actions with an entry in the diagnostic buffer:

- Input of the correct or, possibly, wrong password

- Changes to access level configuration

Behavior of a password-protected CPU during operation

Protection of an S7-1500 CPU up to FW version V3.0 takes effect for an online connection after you have downloaded the settings to the CPU. If you set a higher access level and download it to the CPU, all other online connections will be interrupted. You must then establish a new online connection.

Before an online function is executed, STEP 7 checks the necessary permission and, if necessary, prompts the user to enter a password. The functions protected by a password can only be executed by one programming device/PC at any one time. Another programming device/PC cannot log on.

Logon authorization to the protected data applies for the duration of the online connection or for as long as you have STEP 7 open. The menu command "Online > Delete access rights" cancels the access authorization.

You can limit access to a password-protected CPU in RUN locally on the display. This prevents access even with the password.

Access level for F-CPUs

For the fail-safe CPUs up to FW version V3.0, there is an additional access level in addition to the four described access levels. For more information on this access level, refer to the description of the fail-safe system SIMATIC Safety Programming and Operating Manual SIMATIC Safety - Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126).

11.6 Using the display to set additional password protection

Blocking access to a password-protected CPU

On the display of an S7-1500 CPU, you can block access to a password-protected CPU (local block of the password). If the mode selector is set to RUN, the block is effective.
The access block requires a configured protection level in STEP 7 and works independently of the password protection. This means that even if someone accesses the CPU via a connected programming device and has entered the correct password, access to the CPU remains disabled.
The access block can be set separately for each access level on the display. Then, for example, the read access is allowed locally, but the writing access is not allowed locally.

Procedure

If you want to block access to the CPU via the display, you need to configure an access level with a password in STEP 7.

When you set the local access protection for an S7-1500 CPU on the display, proceed as follows:

1. On the display, select Settings > Protection menu.

2. Confirm the selection using "OK", and configure for each access level, whether access at the RUN mode selector switch is allowed or not:

   – Allow: Access to the CPU is possible with the corresponding password in STEP 7.

   – Deactivated in RUN: If the mode selector is set to RUN, no additional logon to the CPU is possible with the rights of this access level. Access is denied despite the fact that the user knows the password. Access with the password is enabled again in the STOP operating state.

Access protection for the display

Configure a password for the display in STEP 7 in the properties of the CPU. This protects local access protection with a local password.

11.7 Using the user program to set additional access protection

Access protection by means of the user program

In addition to access protection via the display, you have another option. You can also restrict access to a password-protected CPU using the ENDIS_PW instruction in STEP 7.

You can find more information on this instruction in the STEP 7 online help under "ENDIS_PW: Limit and enable password legitimation ".

11.8   Know-how protection

Application

You can use know-how protection to protect one or more OB, FB or FC blocks as well as global data blocks in your program from unauthorized access. Enter a password to restrict access to a block. The password offers high-level protection against unauthorized reading or manipulation of the block. Know-how protection does not involve the CPU (offline access in STEP 7).

Password provider

As an alternative to manual password input, you can assign a password provider to STEP 7. When using a password provider, you select a password from a list of available passwords. When a protected block is opened, STEP 7 connects to the password provider and retrieves the corresponding password.

To connect a password provider you have to install and activate it. A settings file in which you define the use of a password provider is also required.

A password provider offers you the following advantages:

*   The password provider defines and manages the passwords. When know-how protected blocks are opened, you work with symbolic names for passwords. For example, a password is marked with the symbolic name "Machine_1" n the password provider. The actual password behind "Machine1" remains hidden from you.
    A password provider therefore offers optimum block protection as the users do not know the password themselves.

*   STEP 7 automatically opens know-how protected blocks without the direct entry of a password. This saves you time.

You can find more information on connecting a password provider in the STEP 7 online help.

Readable data

If a block is know-how protected, only the following data is readable without the correct password:

*   Block title, comments and block properties

*   Block parameters (INPUT, OUTPUT, IN, OUT, RETURN)

*   Call structure of the program

*   Global tags without information on the point of use

Further actions

Further actions that can be carried out with a know-how protected block:

- Copying and deleting
- Calling within a program
- Online/offline comparison
- Load

Global data blocks and array data blocks

You protect global data blocks (global DBs) from unauthorized access with know-how protection. If you do not have the valid password, you can read the global data block but not change it.

Know-how protection is not available for array data blocks (array DBs).

Setting up block know-how protection

To set up block know-how protection, follow these steps:

1. Open the properties of the respective block.
2. Select the "Protection" option under "General".
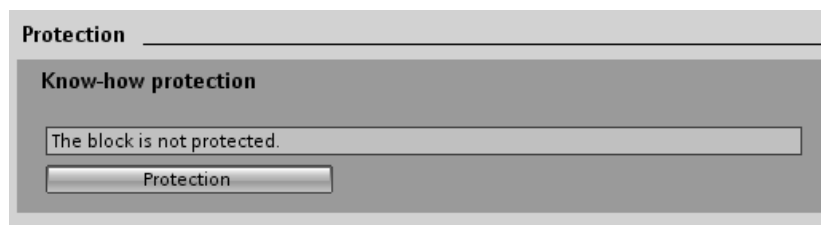
Figure 11-4 Setting up block know-how protection (1)

3. Click the "Protection" button to display the "Define protection" dialog.
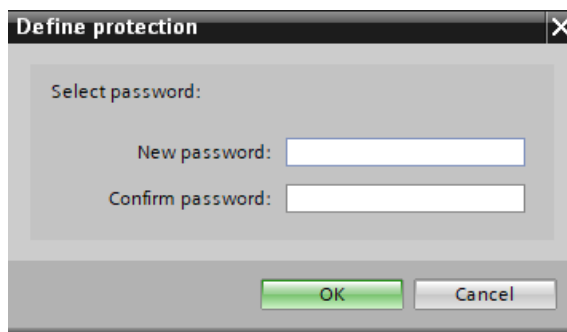
Figure 11-5 Setting up block know-how protection (2)

4. Enter the new password in the "New password" field. Enter the same password in the "Confirm password" field.
5. Click "OK" to confirm your entry.
6. Close the "Know-how protection" dialog by clicking "OK".

Result: The blocks selected will be know-how-protected. Know-how protected blocks are marked with a lock symbol in the project tree. The password entered applies to all blocks selected.

NOTE
Password provider
Alternatively, you can set up know-how protection for blocks with a password provider.

Opening know-how protected blocks

To open a know-how protected block, follow these steps:

1. Double-click the block to open the "Access protection" dialog.

2. Enter the password for the know-how protected block.

3. Click "OK" to confirm your entry.

Result: The know-how-protected blockopens.

Once you have opened the block, you can edit the program code and the block interface of the block for as long as the block or STEP 7 is open. You need to enter the password again the next time you open the block. If you close the "Access protection" dialog with "Cancel", the block will open but the block code will not be displayed. You will not be able to edit the block.

If you copy the block or add it to a library, for example, this does not cancel the know-how protection of the block. The copies will also be know-how-protected.

Changing know-how protection for blocks

To change the know-how protection for blocks, follow these steps:

1. Select the block for which you want to change the know-how protection. The protected block must not be open in the program editor.

2. To open the "Change protection" dialog, select the "Know-how protection" command in the "Edit" menu.

3. To change the password for the know-how protection, enter the current password under "Old password".

4. Then enter a new password under "New password" and confirm the password under "Confirm password".

5. Click "OK" to confirm your entry.

Result: The password for the know-how protection of the selected block has been changed.

Removing know-how protection for blocks

To remove block know-how protection, follow these steps:

1. Select the block from which you want to remove know-how protection. The protected block must not be open in the program editor.

2. Select the "Know-how protection" command in the "Edit" menu.
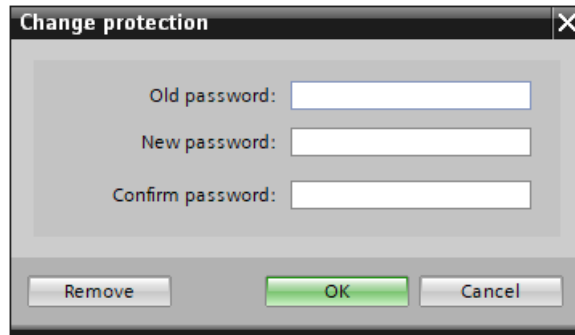
Figure 11-6 Removing know-how protection for blocks

3. To remove the block protection, enter the current password under "Old password". Leave the fields for the new password empty.

4. Click "Remove" to confirm your entry.

Result: Know-how protection for the selected block has been canceled.

11.9 Copy protection

Application

The copy protection allows you to protect your program against unauthorized duplication. With copy protection you associate the blocks with a specific SIMATIC memory card or CPU. The link to the serial number means that you can only use the block in conjunction with the corresponding SIMATIC memory card or CPU.

Copy and know-how protection

Recommendation: To prevent an unauthorized reset of the copy protection, provide a copy-protected block with additional know-how protection. First set up the copy protection for the block and after this the know-how protection. You can find additional information on setting up know-how protection in the section Know-how protection (Page 296).

Setting up copy protection

To set up copy protection, follow these steps:

1. Open the properties of the respective block.

2. Select the "Protection" option under "General".

3. In the "Copy protection" area, select either the "Bind to serial number of the CPU" entry or the "Bind to serial number of the memory card" entry from the drop-down list.
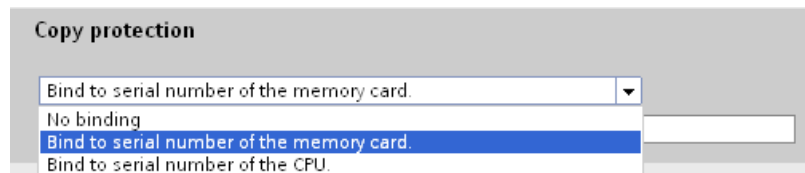
Figure 11-7 Setting up copy protection

4. Activate the option "Serial number is inserted when downloading to a device or a memory card" if STEP 7 is to automatically insert the serial number during the uploading process (dynamic binding). Assign a password using the "Define password" button to link the use of a block additionally to the input of a password.
If you want to manually bind the serial number of the CPU or the SIMATIC memory card to a block (static binding), activate the "Enter serial number" option.

5. You can now set up the know-how protection for the block in the "Know-how protection" area.

NOTE

If you download a copy-protected block to a device that does not match the specified serial number, the entire download operation is not possible. This means that you also cannot download blocks without copy protection.

Removing copy protection

To remove copy protection, follow these steps:

1. Remove the Know-how protection (Page 296), if it is set.

2. Open the properties of the respective block.

3. Select the "Protection" option under "General".

4. In the "Copy protection" area, select the "No binding" entry from the drop-down list.

Figure 11-8 Removing copy protection

11.10 Protection by locking the CPU/interface module

Locking options

Provide additional protection for your CPU/Ihr interface module from unauthorized access (for example to the SIMATIC memory card) by using a secure front cover.

You have e.g. the following options:

- Attach a seal
- Secure the front cover with a lock (shackle diameter: 3 mm)
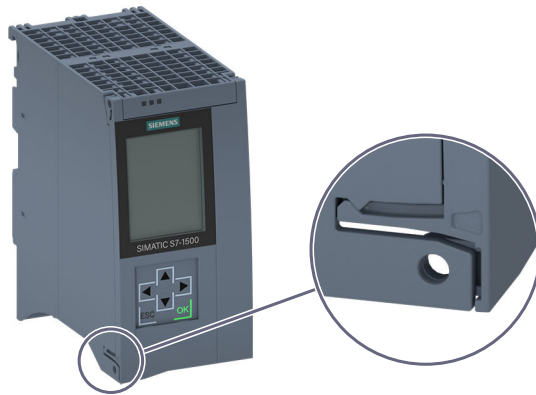
Figure 11-9 Locking latch on a CPU

Flexible automation concepts

12

12.1 Standard machine projects

Introduction

Standard machine projects are STEP 7 projects that use a set of innovative functions allowing simple configuration and commissioning of flexible automation solutions for standard machines or for machines with a modular structure.

A hardware configuration consisting of an S7-1500 CPU as the IO controller and any connected IO devices represents a "PROFINET IO system master". This master is configured with a maximum configuration based on which various options can be derived for different standard machines, for example with different configuration variants of the IO system.

Greater flexibility at all levels

Standard machine projects have the following central characteristics:

- From one project (IO system master) with an engineered maximum configuration, different variants of a standard machine can be loaded (IO system options). The standard machine project covers all variants (options) of the IO system.

- An IO system option can be integrated in an existing network locally using simple tools.

Flexibility is provided in more ways than one:

- With suitable configuration, adaptation of the IP address parameters of the IO controller is possible locally using simple tools. This allows a standard machine to be integrated in different plants with little effort or to be included in a network several times.
  IO systems with this property are known as **multiple use IO systems**.

- With suitable configuration and programming, different setups of IO system options can be operated locally that differ in terms of the selection of IO devices used or in terms of the arrangement of the IO devices.
  Since the specific configuration of the IO system is controlled by the user program, this is known as **configuration control for IO systems**.

- Independently of the functions described above, with suitable configuration and programming, you can use different station options of central devices or distributed I/O devices in one project. The devices can be different in terms of the selection and arrangement of the modules.
  Since the concrete configuration of the station is controlled by the user program, this is also known as **configuration control**.

Additional information

You can find additional information on configuration control in the section Configuration control (option handling) .

You can find additional information on multiple-use IO systems and on configuration control for IO systems in the PROFINET with STEP 7 (https://support.automation.siemens.com/WW/view/en/49948856) function manual.

12.2 Configuration control (option handling)

Introduction

With configuration control (option handling), you handle various standard machine configuration levels in one project. You do not need to change the hardware configuration or the user program.

Operating principle of configuration control

Configuration control enables you to operate different configuration levels of a standard machine with a single configuration of the S7-1500 automation system/ET 200MP distributed I/O system.

- A station master (maximum configuration) is configured in a project. The station master comprises all modules needed for all possible equipment components of a modular standard machine.

- Provision is made in the user program of the project for various station options for the different configuration levels of the standard machine and for selection of a station option. A station option uses, for example, only some of the modules of the station master and these modules are not inserted in the configured order.

- Manufacturers of standard machines select a station option for a configuration level of the standard machine and does not have to change the project or load a changed configuration.

You use a control data record you have programmed to notify the CPU/interface module as to which modules are missing or located on different slots in a station option as compared to the station master. The configuration control has no effect on the parameter assignment of the modules.

The configuration control allows you to flexibly vary the centralized/distributed configuration. As a precondition for this, the station option must be able to be derived from the station master.

The following figure shows three configuration levels of a standard machine with the corresponding station options of the S7-1500 automation system.

Configuration level 1: Baking

Station option 1

Configuration level 2:
Baking and packaging

Station option 2

Configuration level 3:
Baking, decorating and packaging

Station master
(maximum configuration)
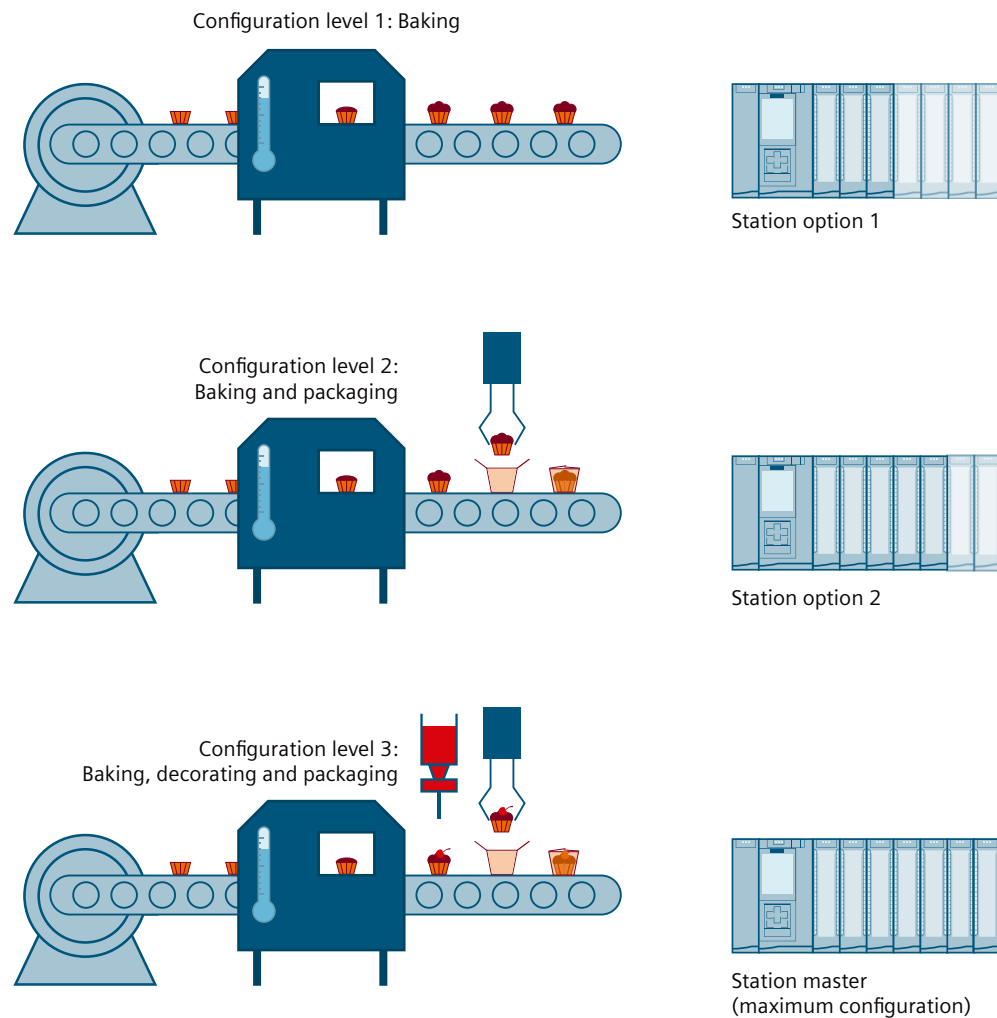
Figure 12-1 Various configuration levels of a standard machine with the corresponding station options of the S7-1500 automation system

Benefits

- Easy project handling and commissioning through use of a single STEP 7 project for all station options.
- Easy handling during maintenance, versioning and upgrades.
- Hardware savings: I/O modules are installed that are necessary for the current station option of the machine.
- Potential savings when building, commissioning and creating documentation for standard machines.

Procedure

To set up the configuration control, proceed as follows:

Table 12-1 Procedure for commissioning the SIMATIC S7-1500

Step	Procedure	See...
1	Enable configuration control in STEP 7	Section Configuring (Page 305)
2	Create control data record	Section Creating the control data record (Page 307)
3	Transfer control data record	Section Transferring the control data record in the startup program of the CPU (Page 316)

Library for configuration control

A library for configuration control is available for download (https://support.industry.siemens.com/cs/ww/en/view/29430270) on the internet. The library contains data types with the structure of the control data records for the S7-1500/ET 200MP automation system. You can implement the configuration control for your flexible automation solution economically using these data types.

12.2.1 Configuring

Requirements

In the case of the S7-1500, configuration control is possible both with centrally inserted modules and with the ET 200MP distributed I/O system via PROFINET IO.

For S7-1500 automation system:

- STEP 7 Professional as of Version V13

- CPU S7-15XX as of firmware version V1.5

- The startup parameter "Comparison preset to actual configuration" is set to "Startup CPU even if mismatch" (default setting).
  You can find the "Comparison preset to actual configuration" parameter in the Inspector window of the CPU properties under "General">"Startup".

For ET 200MP distributed I/O system:

- STEP 7 Professional as of Version V13

- IM 155-5 PN ST/HF

- You have assigned the interface module to an IO controller/DP master in STEP 7

- The startup parameter "Comparison preset to actual module" is set to "Startup CPU even if mismatch" (default setting).
  You can find the "Comparison preset to actual module" parameter in the Inspector window of the interface module properties in the "Startup" field under "General">"Module parameters".

Required steps

Enable the "Allow to reconfigure the device via the user program" parameter when configuring the CPU/interface module.

- For an S7-1500 CPU, you can find the "Allow to reconfigure the device via the user program" parameter in the "Configuration control" area.

- For an IM 155-5 PN interface module, you can find the "Allow to reconfigure the device via the user program" parameter in the "Configuration control" field under "General">"Module parameters".
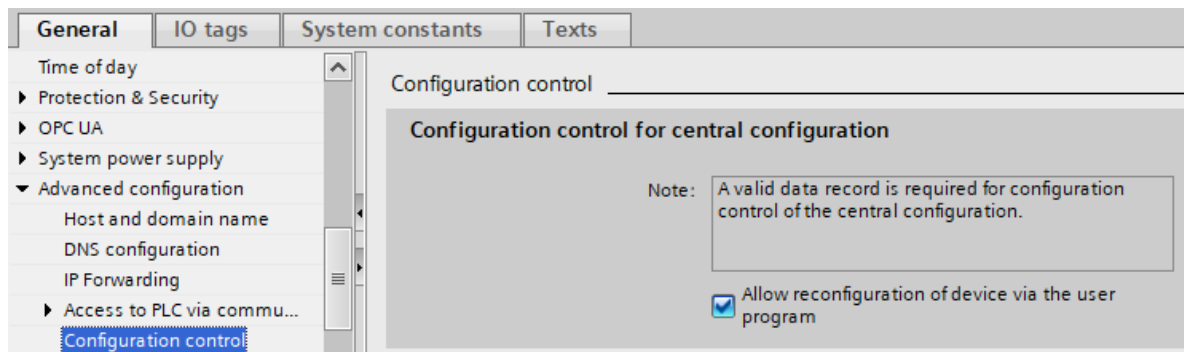
Figure 12-2 Enabling configuration control using an S7-1500 CPU as an example

12.2.2 Creating the control data record

Required steps

To create a control data record for the configuration control, follow these steps:

1. Create a PLC data type that contains the structure of the control data record.

   You can find the structure of the control data record:

   – For the S7-1500 automation system in section Control data record for the S7-1500 Automation System (Page 309).

   – For the ET 200MP distributed I/O system in section Control data record for the ET 200MP distributed I/O system (Page 310).

Figure 12-3 Creating control data record 196 using an S7-1500 CPU as an example

2. Create a global data block.

3. Create an array of the data type of the above created PLC data type in the data block.

   The following figure shows a data block containing three control data records for an S7-1500 CPU.

Figure 12-4 Data block for configuration control

4. In the "Start value" column of the control data records, enter which module is located at which slot.

		Name	Data type	Start value	R..	A...	W...	V...	Comment
1	▼	Static			☐	☐	☐	☐	
2	▪	Option	Int	0	☑	☑	☑	☑	selection of record
3	▪ ▼	ConfigControl	Array[0..2] of "CTR_REC"		☐	☑	☑	☑	
4	▪ ▼	ConfigControl[0]	"CTR_REC"		☐	☑	☑	☑	
5	▪	Block_Lenght	USInt	36	☐	☑	☑	☑	4+number of slots
6	▪	Block_ID	USInt	196	☐	☑	☑	☑	
7	▪	Version	USInt	4	☐	☑	☑	☑	S7-1500
8	▪	Subversion	USInt	0	☐	☑	☑	☑	
9	▪	Slot 0	USInt	0	☐	☑	☑	☑	Slot 0 Power module
10	▪	Slot 1	USInt	1	☐	☑	☑	☑	Slot 1 CPU
11	▪	Slot 2	USInt	255	☐	☑	☑	☑	assigned "real" slot
12	▪	Slot 3	USInt	2	☐	☑	☑	☑	assigned "real" slot
13	▪	Slot 4	USInt	3	☐	☑	☑	☑	assigned "real" slot
14	▪	Slot 5	USInt	5	☐	☑	☑	☑	assigned "real" slot

Figure 12-5 Assigning slots

Rules

Observe the following rules:

- The CPU/interface module ignores slot entries in the control data record outside the station master.

- The control data record must contain the entries up to the last slot of the station option.

- Each slot of a station option may only be present once in the control data record.

- Each slot of a station option may only be assigned to one slot in the station master.

- System power supplies (PS) can also be subject to configuration control.

NOTE

Configuration control for system power supplies

In the case of a configuration (station option) loaded using a data record, STEP 7 does not automatically check compliance with the power budget.

Ensure that the power supplied in each power segment of the station option is greater than or equal to the power drawn.

You can find more information in the section Power balance calculation (Page 173).

Using communication modules

- Point-to-point communication modules:
Point-to-point communication modules can be used without any restrictions for the configuration control.

- PROFINET/Ethernet and PROFIBUS communication modules:
CPUs as of firmware version V1.7 support configuration control when using PROFINET/Ethernet or PROFIBUS communication modules. If communication modules for PROFINET/Ethernet or PROFIBUS, such as a CM 1542-5 (DP master or DP slave), are inserted in the central configuration, these communication modules cannot be influenced by the configuration control. You must therefore leave these modules in the slots preassigned in the station master and enter the slot numbers from the station master in the control data record ("Station option slot = Station master slot"). In a station option, all slots up to the communication module furthest from the CPU must be present in the control data record. Maximum flexibility is achieved by inserting the communication modules directly to the right of the CPU.

12.2.2.1 Control data record for the S7-1500 Automation System

Slot assignment

The following table shows the slot assignment of the modules for the S7-1500 automation system:

Table 12-2 Slot assignment

Slot	Modules	Comment
0	System power supply (optional)	Upstream of CPU
1	CPU	Slot 1 is always the CPU
2 - 31	I/O modules/system power supplies, depending on the station option	Downstream of CPU

Control data record

For configuration control of the S7-1500 automation system, you define a control data record 196 V4.0, which contains a slot assignment. The table below shows the structure of a control data record with explanations of the individual elements.

Table 12-3 Configuration control: Structure of control data record 196

Byte	Element	Code	Explanation
0	Block length	4 + number of slots	Header
1	Block ID	196	
2	Version	4	
3	Version	0	
4	Slot 0 of the station master	Slot assignment in the station option	**Control element**

Byte	Element	Code	Explanation
5	Slot 1 of the station master	Slot assignment 1 in the station option (always 1, because the CPU is always in slot 1)	Contains information on which module is inserted in which slot. The following rule determines which value you must enter in the respective byte:
6	Slot 2 of the station master	Slot assignment in the station option	• If the module is included in the station option, enter the slot number of the module.
7	Slot 3 of the station master	Slot assignment in the station option	• If the module is not included in the station option, enter 255.
:	:	:	
4 + (max. slot number)	Maximum slot of the station master	Slot assignment in the station option	

12.2.2.2 Control data record for the ET 200MP distributed I/O system

Slot assignment

The following table shows the slot assignment of the modules for the ET 200MP distributed I/O system:

Table 12-4 Slot assignment

Slot	Modules	Comment
0	System power supply (optional)	Upstream from interface module
1	Interface module	Interface module (slot 1) is not an element of the configuration control, but instead controls the configuration control.
2 - 31	I/O modules/system power supplies, depending on the station option	Downstream from the interface module

Control data record

For configuration control of the ET 200MP distributed I/O system, you define a control data record 196 V3.0, which contains a slot assignment. The table below shows the structure of a control data record with explanations of the individual elements.

Table 12-5 Configuration control: Structure of control data record 196

Byte	Element	Code	Explanation
0	Block length	4 + number of slots	Header
1	Block ID	196	
2	Version	3	
3	Version	0	
4	Slot 0 of the station master	Slot assignment in the station option	**Control element**

Byte	Element	Code	Explanation
5	Slot 2 of the station master	Slot assignment in the station option	Contains information on which module is inserted in which slot. The following rule determines which value you must enter in the respective byte: • If the module is included in the station option, enter the slot number of the module. • If the module is not included in the station option, enter 127.
6	Slot 3 of the station master	Slot assignment in the station option	
:	:	:	
4 + (max. slot no. - 1)	Maximum slot of the station master	Slot assignment in the station option	

12.2.2.3 Feedback data record of the ET 200MP distributed I/O system

Operating principle

The feedback data record informs you about the accuracy of the module assignment and gives you the option of detecting assignment errors in the control data record. The feedback data record is mapped via a separate data record 197 V2.0.

Slot assignment

The feedback data record exists only when configuration control is configured and always refers to the maximum quantity framework **without interface module**, i.e., 31 slots.

The following table shows the slot assignment of the modules:

Table 12-6 Slot assignment

Slot	Modules	Comment
0	System power supply (optional)	Upstream from interface module
2 - 31	I/O modules/system power supplies, depending on the station option	Downstream from the interface module

Partial reading of the feedback data record is possible.

Feedback data record

Table 12-7 Feedback data record

Byte	Element	Code	Explanation
0	Block length	66	Header
1	Block ID	197	
2	Version	2	
3		0	
4	Status slot 0	0/1	Status = 1:

* Not possible if the slot is marked as not available.

Byte	Element	Code	Explanation
5	Reserved	0	• Module from station master is inserted in the station option
6	Status slot 2	0/1	• Slot is marked as not available in the control data record
7	Reserved	0	
:	:	:	Status = 0:
64	Slot n status	Maximum slot	• Module pulled
65	Reserved	0	• Incorrect module inserted in the station option*

* Not possible if the slot is marked as not available.

NOTE

The data in the feedback data record is always mapped for all modules. In a Shared Device configuration, it is therefore irrelevant which IO controller the respective modules are assigned to.

As long as no control data record was sent, a one-to-one module assignment is assumed for the compilation of data record 197 (station master → station option).

Error messages

In the case of an error when reading the feedback data record, the RDREC instruction returns the following error messages via the STATUS block parameter:

Table 12-8 Error messages

Error code	Meaning
80B1$_H$	Invalid length; the length information in data record 197 is not correct.
80B5$_H$	Configuration control not configured
80B8$_H$	Parameter error The following events cause a parameter error: • Incorrect block ID in the header (not equal to 197) • Invalid version identifier in the header • A reserved bit was set • Multiple slots in the station master are assigned to the same slot in the station option

12.2.2.4   Examples of configuration control

A station master consisting of a system power supply, CPU, and three I/O modules is configured in STEP 7 in the following section.

The module at slot 3 is not present in the station option 1 and is "hidden" by the configuration control.

In station option 2, the order of the modules in slots 3 and 4 is interchanged. The modified order of the modules is made known to the CPU by a modified control data record.

Station option 1 with module that is not present

The module that is located in slot 3 in the station master is not present in the station option 1. Slot 3 must be designated in the control data record accordingly with 255 (= not present).
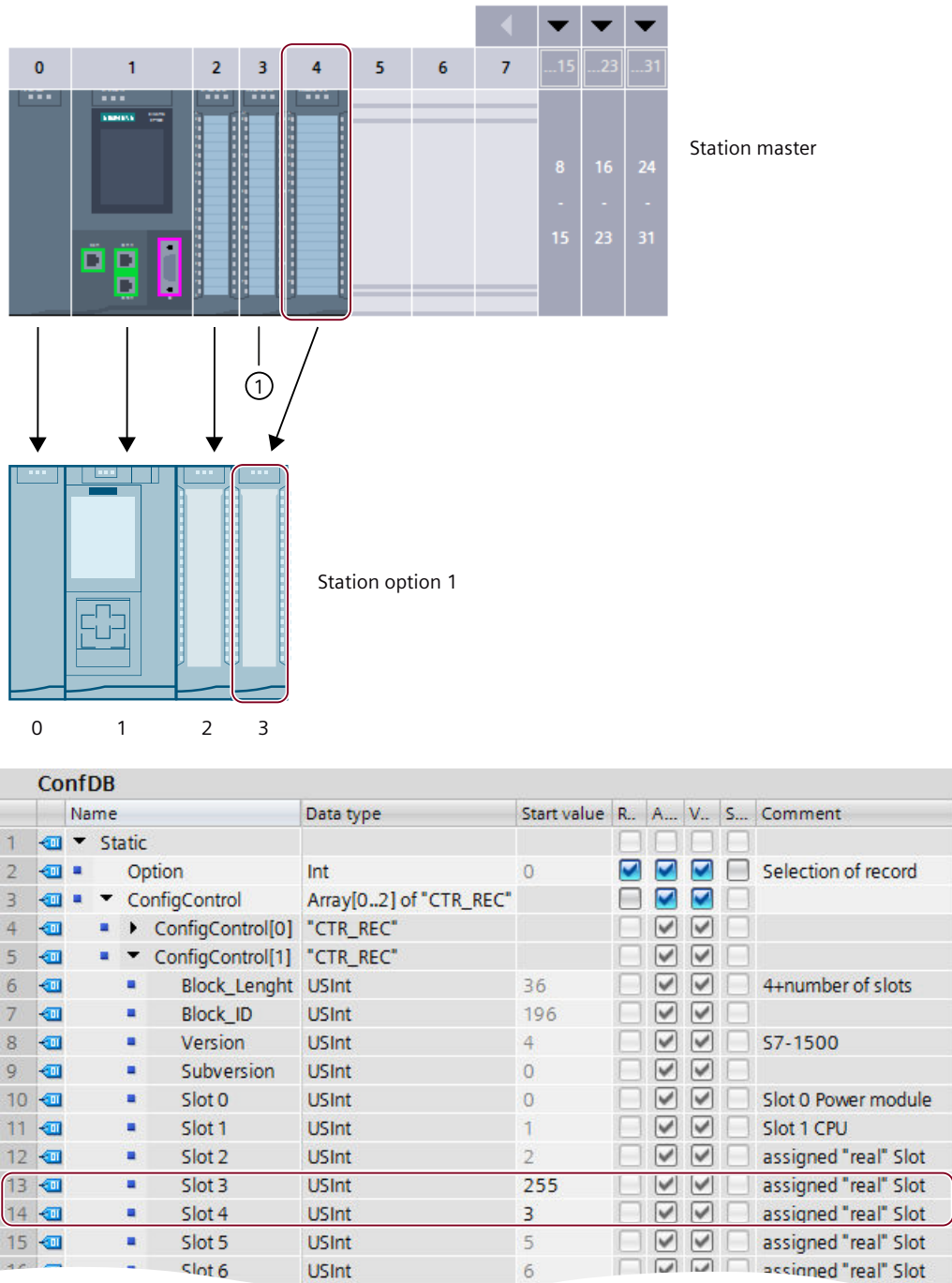
① Module is not present in the station option 1.

Figure 12-6 Example: Hardware configuration of station option 1 with the associated control data record in STEP 7

Station option 2 with modified order of modules

The order of the modules in slot 3 and 4 is interchanged.

Figure 12-7 Example: Hardware configuration of station option 2 with the associated control data record in STEP 7

Detailed application example

You can find a detailed application example for the configuration control in S7-1500 in here (https://support.industry.siemens.com/cs/ww/en/view/29430270) under **"**Application example for ET 200SP (PROFINET) and S7-1500 by using the library".

12.2.3   Transferring the control data record in the startup program of the CPU

Required steps

Transfer the created control data record 196 to the CPU/interface module using the WRREC (Write data record) instruction.

Parameters of the WRREC instruction

Below, you will find explanations of individual parameters of the WRREC instruction which you must supply with specific values in the configuration control context. You can find additional information on the WRREC instruction in the STEP 7 online help.

ID	Hardware identifier
	• For configuration control for centrally arranged modules, use the HW identifier for the CPU. If you have selected the CPU in the network view or device view, you can find the HW identifier on the **System constants** tab of the Inspector window. Use the value of the system constant "Local Configuration". • For configuration control for distributed I/O, use the HW identifier of the interface module. If you have selected the interface module in the network view or device view, you can find the HW identifier on the **System constants** tab of the Inspector window. Use the value of the system constant "<Name_of_interface_module> Head".
INDEX	Data record number: 196 (decimal)
RECORD	Control data record to be transferred. For the structure of the control data record, see section Creating the control data record (Page 307).

Error messages

In case of error, the WRREC instruction returns the following error messages via the STATUS block parameter:

Table 12-9 Error messages

Error code	Meaning
80B1$_H$	Invalid length; the length information in data record 196 is not correct.
80B5$_H$	Configuration control parameters not assigned.
80E2$_H$	Data record was transferred in the wrong OB context. The data record must be transferred in the startup program.
80B8$_H$	Parameter error Reasons for a parameter error are: • Incorrect block ID in the header (not equal to 196) • Invalid version identifier in the header • A reserved bit was set • A station master slot was assigned an invalid slot in the station option • Multiple slots in the station master are assigned to the same slot in the station option • For shared device on submodule level: violation of defined restrictions

Special requirements relating to the transfer of the control data record to the CPU

- If you have enabled configuration control, the CPU is not ready for operation without a control data record. The CPU returns from startup to STOP if a valid control data record is not transferred in the startup OB (for example, OB 100). The central I/O is not initialized in this case. The cause for STOP mode is entered in the diagnostics buffer.

NOTE

If an incorrect control data record is transferred to the CPU in the startup OB, the startup of the CPU may be prevented.

In this case, perform a reset to factory settings of the CPU and then transfer a correct control data record.

- The CPU processes the WRREC instruction for transferring the control data record asynchronously. For this reason, you must call WRREC in the startup OB (for example, OB 100) repeatedly in a loop until the output parameters "BUSY" and "DONE" indicate that the data record has been transferred.

  – Tip: To program the loop, use the SCL programming language with the REPEAT ... UNTIL instruction.

```
REPEAT
  "WRREC_DB"(REQ := "start_config_control",
             ID := "Local Configuration",
             INDEX := 196,
```

```
                 LEN := "conf_LEN",
                 DONE => "conf_DONE",
                 BUSY => "conf_BUSY",
                 RECORD := "ConfDB".ConfigControl["ConfDB".Option],
//Selection of control data record*
                 ERROR => "conf_ERROR",
                 STATUS => "conf_STATUS");
UNTIL NOT "conf_BUSY"
END_REPEAT;
```

*Selection of the station option in the user program: In order for the CPU to know which station option you want to operate, you must set up a possibility to select between the various control data records in the user program. You can implement the selection, for example, via an Int tag that references an array element. Please note that the variable used to select the control data record must be stored in the retentive memory area. If the tag is not retentive, it will be initialized during startup of the CPU and will thus be unavailable for selection of the station option.

– In the graphical programming languages, you implement the loop using instructions for program control.

Example in FBD: Use the LABEL (jump label) and JMP (jump at RLO=1) instructions to program a loop.
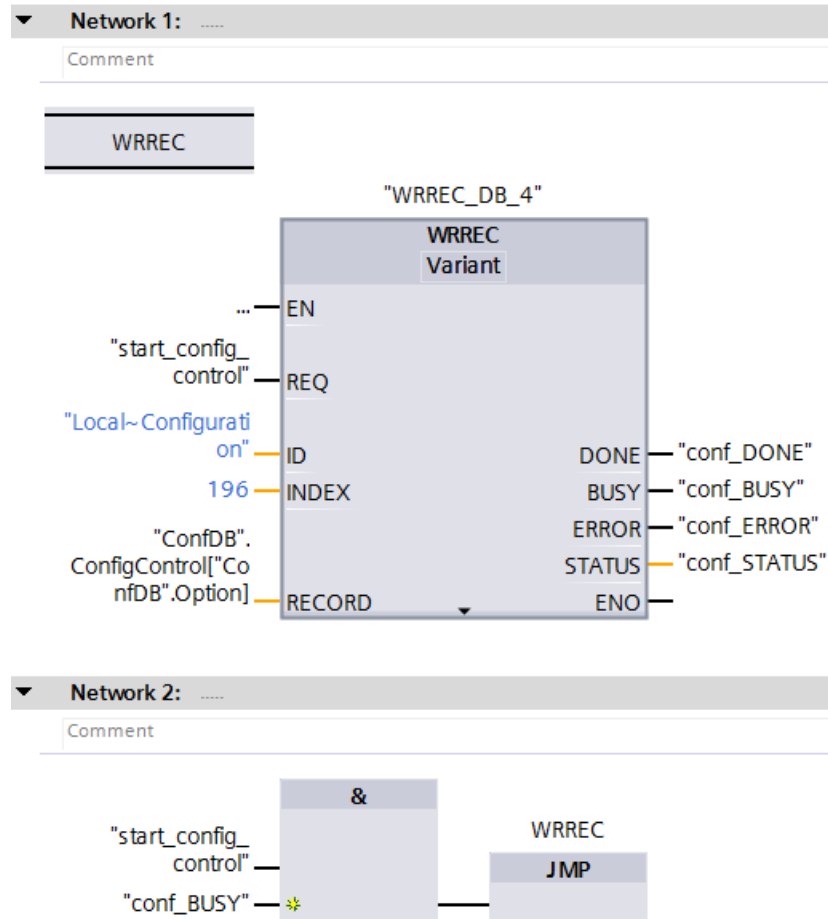

Figure 12-8   WRREC

• The control data record is stored retentively in the CPU. Note:

– The retentivity of the control data record is independent of the retentivity settings in the STEP 7-memory area. The memory area in which the control data record is configured does then not have to be configured as retentive for this purpose.

– If you write a control data record with modified configuration, the original data record 196 is deleted and the new data record 196 is saved retentively. The CPU will then restart with the modified configuration.

Special requirements relating to the transfer of the control data record to the interface module

- If you have enabled configuration control, the ET 200MP station is not ready for operation without a control data record. As long as no valid control data record has been transferred, the I/O modules are considered as failed by the CPU and exhibit substitute value behavior. The interface module continues to exchange data.

- The control data record is stored retentively in the interface module. Note:

    – If the configuration is unchanged, you do not have to rewrite the control data record 196 during restart.

    – If you write a control data record with modified configuration, this will result in a station failure in the distributed I/O system. The original data record196 is deleted and the new data record 196 is saved retentively. The station will then restart with the modified configuration.

12.2.4 Behavior during operation

Effect of discrepancy between station master and station option

For the online display and for the display in the diagnostics buffer (module OK or module faulty), the station master is always used and not the differing station option.

Example: A module outputs diagnostics data. This module is configured in slot 4 in the station master, but is inserted in slot 3 in the station option (missing module; see example in the next section). The online view (station master) shows an incorrect module in slot 4. In the real configuration, the module in slot 3 indicates an error via an LED display.

Response to modules that are not present

If modules are entered as not present in the control data record, the automation system behaves as follows:

- Modules designated as not present in the control data record do not supply diagnostics and their status is always OK. The value status is OK.

- Direct writing access to the outputs that are not present or writing access to the process image of outputs that are not present: Remains without effect; no access error is signaled.

- Direct reading access to the inputs that are not present or reading access to the process image of inputs that are not present: Value "0" is supplied; no access error is signaled.

- Write data record to module that is not present: Remains without effect; no error is signaled.

- Read data record from module that is not present: The output parameter STATUS of the instruction RDREC supplies the value 80A3$_H$ "General CM error".

Commissioning 13

13.1 Overview

Introduction

This section includes information on the following topics:

- Check before powering on for the first time
- Procedure for commissioning the S7-1500 automation system
  - Removing/inserting the SIMATIC memory card
  - First power-on of the CPU
- Procedure for commissioning the S7-1500 distributed I/O system
  - First power-on of the ET 200MP on PROFINET IO
  - First power-on of the ET 200MP on PROFIBUS DP
- Operating modes of the CPU STARTUP, STOP, RUN and operating mode transitions
- CPU memory reset: Automatic and manual
- Backing up and restoring the CPU configuration
- Time synchronization
- Identification and maintenance data
- Shared commissioning of projects

Commissioning requirements

NOTE

Performing tests

You must ensure the safety of your plant. You therefore need to perform a complete functional test and the necessary safety checks before the final commissioning of a plant.

Also allow for any possible foreseeable errors in the tests. This avoids endangering persons or equipment during operation.

NOTE

Check coding element in the I/O module

Make sure that the coding element is present in the I/O module before you plug in the front connector for the first time. This reduces the risk of plugging a wired front connector into the wrong type of module when replacing a module.

Software tools for commissioning

The following software tools support you during commissioning:

- SIEMENS PRONETA in commissioning PROFINET systems.
- SIMATIC automation tool in commissioning the S7-1500 automation system / ET 200MP distributed I/O system.

You can find more information on SIEMENS PRONETA and the SIMATIC Automation Tool in the section Software (Page 155).

13.2 Check before powering on for the first time

Before the first power-on, check the installation and the wiring of the S7-1500 automation system/ET 200MP distributed I/O system.

Questions for the check

The following questions provide instructions for checking your system in the form of a checklist.

Racks

- Are the mounting rails firmly installed on the wall, in the framework, or in the cabinet?
- Are the cable ducts correctly installed?
- Have the minimum clearances been observed?

Grounding and chassis concept

- Is the mounting rail connected to the protective conductor?
- If applicable, are all further protective conductor connection points on the S7-1500 automation system / ET 200MP distributed I/O system connected to the protective conductor? Has the protective conductor been tested?
- Has the connection between reference ground and ground been correctly made on all mounting rails?
- Are the required equipotential bonding cables connected with low impedance to the affected plant units?

Module installation and wiring

- Are all the modules inserted / installed in accordance with the mounting plan and corresponding to the configuration with STEP 7 and screwed firmly to the mounting rail?
- Are the coding elements present in the I/O modules?
- Are all the front connectors wired according to the circuit diagram, in the final position, and inserted on the correct module?
- Are the correct modules installed and connected to each other with U connectors?
- Are U connectors projecting either at the left-hand or right-hand over the outer modules on the S7-1500 automation system/ET 200MP distributed I/O system?

System power supply or load current supply

- Are all system power supplies and load current supplies switched off?

- Is the power cable connector correctly wired?

- Has the connection to line voltage been made?

13.3 Procedure for commissioning the S7-1500 automation system

Requirements

- The CPU is in the "Factory settings" state or has been reset to factory settings. You can find more information in the section Resetting the CPU to factory settings (Page 383).

- The SIMATIC memory card is as delivered or has been formatted.

Commissioning procedure

For the first commissioning of an S7-1500 automation system, we recommend the following procedure:

Table 13-1 Procedure for commissioning the SIMATIC S7-1500

Step	Procedure	See...
1	Configure hardware in STEP 7 and perform power balance calculation (see also "Requirements: CPU as bus device")	Section Power balance calculation (Page 173)
2	Create user program	STEP 7 online help
3	Insert required modules	Section Installation (Page 177)
4	Wiring and checking the assembly (system power supplies, front connectors, etc.)	Section Wiring (Page 198)
5	Insert SIMATIC memory card in the CPU	Section Removing/inserting a SIMATIC memory card on the CPU (Page 324)
6	Switch on the CPU and system power supply	Section First power-on of the CPU (Page 327)
7	Check LEDs	The meaning of the LEDs can be found in the manuals of the modules.
8	Evaluate information on the CPU's display	Section CPU display (Page 357)
9	Load hardware configuration and user program to the CPU	Online and diagnostics functions in STEP 7
10	Test inputs and outputs	The following functions are helpful: Monitoring and modifying tags, testing with program status, forcing, modifying the outputs in STOP mode. Section Test and service functions (Page 393)

Requirements: CPU as bus device

Note the following requirements for operation of a CPU as bus device:

- PROFIBUS interface

  – The integrated PROFIBUS interface of the CPU is configured using STEP 7 (device address and bus parameters configured).

  – The CPU is connected to the subnet.

  – The terminating resistors at the segment boundaries are switched on.

  You can find more information in the PROFIBUS function manual (https://support.industry.siemens.com/cs/ww/en/view/59193579)

- PROFINET interface

  – The integrated PROFINET interface of the CPU is configured using STEP 7 (IP address and device name configured).

  – The CPU is connected to the subnet.

  You can find more information in the PROFINET function manual (https://support.automation.siemens.com/WW/view/en/49948856)

Procedure for commissioning a SIMATIC Safety F-system

The procedure for commissioning an F-system is essentially the same as for commissioning a standard system. You use the Safety Administration Editor to commission SIMATIC Safety and activate the safety mode. The Safety Administration Editor is assigned to the fail-safe CPU in the STEP 7 project tree.

You can find more information on commissioning a SIMATIC Safety F-system and the Safety Administration Editor in the programming and operating manual SIMATIC Safety – Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126).

13.3.1 Removing/inserting a SIMATIC memory card on the CPU

Requirements

The CPU only supports pre-formatted SIMATIC memory cards. If applicable, delete all previously stored data before using the SIMATIC memory card. More information about deleting the contents of the SIMATIC memory card can be found in the Function Manual Structure and use of the CPU memory (https://support.industry.siemens.com/cs/ww/en/view/59193101).

In order to work with the SIMATIC memory card, first ensure that the SIMATIC memory card is not write-protected. For this purpose, slide the slider on the SIMATIC memory card out of the lock position.

If the inserted SIMATIC memory card is write-protected, the CPU display outputs the symbol ⚠ in the menu "Memory card" > "Overview". In addition, the display shows a message in the lower level of the menu.

Inserting the SIMATIC memory card

To insert a SIMATIC memory card, follow these steps:

1. Open the front cover of the CPU.

2. Ensure that the CPU is either switched off, or in the STOP mode.

3. Insert the SIMATIC memory card, as depicted on the CPU, into the slot for the SIMATIC memory card.
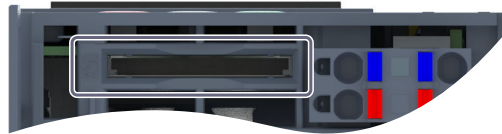
①   Standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0: The slot for the SIMATIC memory card is located on the bottom of the CPU.

Figure 13-1 Slot for the SIMATIC memory card

4. Insert the SIMATIC memory card with light pressure into the CPU, until the SIMATIC memory card latches.

Removing the SIMATIC memory card

To remove a SIMATIC memory card, follow these steps:

1. Open the front cover.

2. Switch the CPU into STOP mode.

3. Press the SIMATIC memory card into the CPU with light pressure. Once it has clicked into place, remove the SIMATIC memory card.

Only remove the SIMATIC Memory Card in POWER OFF or STOP mode of the CPU. Ensure that:

- No writing functions are active in STOP . Writing functions are online functions with the PG/PC, for example loading/deleting a block and test functions.

- No writing functions were active before POWER OFF.

If you remove the SIMATIC memory card during a write process, the following problems can occur:

- The data content of a file is incomplete.

- The file is no longer readable, or no longer exists.

- The entire content of the card is corrupted.

Please also note the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/59457183) for removal of the SIMATIC memory card.

Reactions after removing/inserting the SIMATIC memory card

Inserting and removing the SIMATIC memory card in STOP mode triggers a re-evaluation of the SIMATIC memory card. The CPU hereby compares the content of the configuration on the SIMATIC memory card with the backed-up retentive data. If the backed-up retentive data matches the data of the configuration on the SIMATIC memory card, the retentive data is retained. If the data differs, the CPU automatically performs a memory reset. The retentive data is deleted and CPU then goes to STOP.

The CPU evaluates the SIMATIC memory card and indicates this by flashing the RUN/STOP LED.

NOTE

Using the SIMATIC memory card as a firmware update card

If you use the SIMATIC memory card as a firmware update card, removing and inserting the card will not result in the loss of retentive data.

Reference

You can find more information on the SIMATIC memory card in the Function Manual Structure and use of the CPU memory (https://support.industry.siemens.com/cs/ww/en/view/59193101).

13.3.2 First power-on of the CPU

Requirements

- An S7-1500 automation system has been installed.
- The system has been wired.
- The SIMATIC Memory Card is inserted in the CPU.

Procedure

Proceed as follows to commission the CPU:

- Switch on the system power supply and load current supply.

Result:

- The CPU executes a flash test:
  - All LEDs flash at 2 Hz
  - RUN/STOP LED flashes alternately yellow/green
  - ERROR LED flashes red
  - MAINT LED flashes yellow
- The CPU performs the system initialization and evaluates the SIMATIC Memory Card:
  - RUN/STOP LED flashes yellow at 2 Hz
- After the system initialization has been completed, the CPU goes to STOP mode:
  - The RUN/STOP LED lights up yellow

13.4 Procedure for commissioning the ET 200MP distributed I/O system

13.4.1 Commissioning the ET 200MP for PROFINET IO

Introduction

The commissioning of your automation system depends on the plant configuration.

Commissioning procedure

To commission the ET 200MP as IO device for PROFINET IO, proceed as follows:

Table 13-2 Procedure for commissioning the ET 200MP as an IO device for PROFINET IO

Step	Procedure	See...
1	Install ET 200MP	Section Installation (Page 177)
2	Connect ET 200MP • Supply voltages • PROFINET IO • Sensors and actuators	Section Wiring (Page 198)
4	Configure IO controller	CPU manual or documentation of the IO controller
5	Switch on supply voltages for the IO controller	CPU manual or documentation of the IO controller
6	Switch on supply voltages for IO devices	Interface module (https://support.automation.siemens.com/WW/view/en/67295970/1-33300) manual
7	Download configuration to the IO controller	STEP 7 online help
8	Switch IO controller to RUN mode	CPU manual or documentation of the IO controller
9	Check LEDs	Interface module (https://support.automation.siemens.com/WW/view/en/67295970/1-33300) manual
10	Test inputs and outputs	The following functions are helpful: Monitoring and modifying tags, testing with program status, forcing, modifying the outputs. See section Test and service functions (Page 393)

NOTE

The operating mode transitions for the IO controller from RUN to STOP or from STOP to RUN can take several milliseconds, until the mode transition for the inputs and outputs of all I/O modules for the ET 200MP station is completed. This delay also applies to isochronous mode.

13.4.2 Commissioning the ET 200MP for PROFIBUS DP

Introduction

The commissioning of your automation system depends on the plant configuration.

Commissioning procedure

To commission the ET 200MP as a DP device on PROFIBUS DP, follow these steps:

Step	Procedure	See...
1	Install the ET 200MP (with IM 155-5 DP ST)	Section Installation (Page 177)
2	Set the PROFIBUS address on the interface module	Manual for the interface module (https://support.automation.siemens.com/WW/view/en/77910801/133300)
3	Connect the ET 200MP • Supply voltages • PROFIBUS DP • Sensors and actuators	Section Wiring (Page 198)
4	Configure DP master (including PROFIBUS address)	Documentation of the DP master
5	Switch on supply voltages for DP master	Documentation of the DP master
6	Switch on supply voltages for DP devices	Interface module (https://support.automation.siemens.com/WW/view/en/77910801/133300) manual
7	Download configuration to the DP master	STEP 7 online help
8	Switch DP master to RUN	Documentation of the DP master
9	Check LEDs	Interface module (https://support.automation.siemens.com/WW/view/en/77910801/133300) manual
10	Test inputs and outputs	The following functions are helpful: Monitoring and modifying tags, testing with program status, forcing, modifying the outputs. Section Test and service functions (Page 393)

NOTE

During operating mode transitions of the DP master from RUN to STOP or from STOP to RUN, it can take several milliseconds until the mode transition is complete for the inputs and outputs of all the I/O modules of the ET 200MP.

13.5 Operating modes

Introduction

Operating states describe the behavior of the CPU at a specific time. The following operating states are possible via the mode selector:

- STARTUP
- RUN
- STOP

In these operating modes, the CPU can communicate, for example, via the PROFINET IO interface (X1).

The status LEDs on the front side of the CPU indicate the current operating mode.

13.5.1 STARTUP mode

Response

Before the CPU starts to execute the cyclic user program, a start-up routine is executed.

By suitably programming startup OBs, you can specify initialization tags for your cyclic program in the start-up routine. That is, you can set up one or several startup OBs in your program, or none at all.

Points to note

- The CPU resets the process image input.
- All outputs are disabled or react according to the parameter settings for the respective module: They provide a substitute value as set in the parameters or retain the last value output and bring the controlled process to a safe operating mode.
- Before processing the start-up routine, the CPU transfers the I/O inputs to the process image input.
- After processing the start-up routine, the CPU releases the peripheral outputs.

NOTE

To read the current state of inputs during STARTUP, you can access inputs via the process image or via direct I/O access.
To initialize outputs during STARTUP, you can write values via the process image or via direct I/O access. The values are output at the outputs during the transition to the RUN mode.

- The CPU always starts up in a warm restart.
  - The non-retentive bit memories, timers and counters are initialized.
  - The non-retentive tags in data blocks are initialized.
- During startup, no cycle time monitoring is running yet.

- The CPU processes the startup OBs in the order of the startup OB numbers. The CPU processes all programmed startup OBs, regardless of the selected startup mode (figure "Setting the startup behavior").

- If a corresponding event occurs, the CPU can start the following OBs in startup:
  - OB 82: Diagnostics interrupt
  - OB 83: Removal/insertion of modules
  - OB 86: Rack error
  - OB 121: Programming error (only for global error handling)
  - OB 122: Time-out (for global error handling only)
    You can find a description of how to use global and local error handling in the STEP 7 online help.

The CPU does not start all other OBs until the transition to RUN mode.

Response when expected and actual configurations do not match

The configuration downloaded to the CPU represents the expected configuration. The actual configuration is the actual configuration of the automation system. If the expected configuration and actual configuration deviate from one another, the CPU's behavior is specified by the setting of the hardware compatibility. For more information about the hardware compatibility, see section Operating mode transitions (Page 336).

Cancellation of the startup

If errors occur during startup, the CPU cancels the startup and returns to STOP mode.

The CPU does not perform startup or interrupts the startup under the following conditions:

- You have not inserted a SIMATIC memory card or an invalid one is inserted.
- You have not downloaded a hardware configuration to the CPU.

Configuring startup behavior

You configure the behavior of the CPU in the Startup group of the CPU properties.

Setting the startup behavior

To set the startup behavior, follow these steps:

1. Select the CPU in the device view of the STEP 7 hardware network editor.

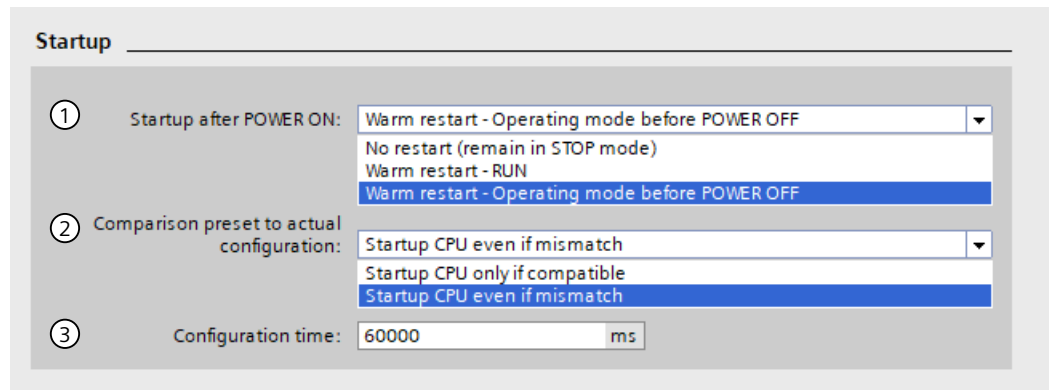2. In the properties under "General" select the "Startup" area.

Figure 13-2 Setting the startup behavior

① Sets the startup type after POWER ON

② Defines the startup behavior for the case where a module in a slot does not correspond to the configured module. This parameter applies to the CPU and to all the modules for which no other setting was selected.

- Startup CPU only if compatible: In this setting a module on a configured slot has to be compatible with the configured module. Compatible means that the module matches the number of inputs and output and must match with respect to its electrical and functional properties.

- Startup CPU even if mismatch: At this setting the CPU starts up irrespective of the type of module plugged.

For locally used modules you can configure the hardware compatibility in the parameter "Comparison preset to actual module" individually for each slot. When you change the setting of the hardware compatibility for a module, the setting made at the CPU does not apply for this module.

③ Specifies a maximum period (default: 60000 ms) in which the central and distributed I/O must be ready for operation. The communications modules (CM/CP) are supplied with voltage and communication parameters during the CPU startup. This parameter assignment time grants a period within which the I/O modules connected to the communication module (CM/CP) must be operationally ready.
The CPU goes into RUN mode when the central and the distributed I/O is operationally ready within the parameter assignment time.

If the central and distributed I/O is not ready for operation within the configuration time, the startup characteristics of the CPU depends on the setting of the hardware compatibility.

Example for the "Comparison preset to actual configuration" parameter

"Startup CPU only if compatible"

The DI 32x24VDC HF input module with 32 digital inputs can be a compatible replacement for a DI 16x24VDC HF input module with 16 digital inputs. The pin assignment and all electrical and functional properties are identical.

"Startup CPU even if mismatch"

Instead of a configured digital input module, you insert an analog output module or no module is present in this slot and thus in all subsequent slots. Although the configured inputs cannot be accessed, the CPU starts up.

Note that the user program cannot function correctly in this case. Therefore, take appropriate measures!

13.5.2 STOP mode

Response

The CPU does not execute the user program in STOP mode.

All outputs are disabled or react according to the parameter settings for the respective module: They provide a substitute value as set in the parameters or retain the last value output and thus hold the controlled process in a safe operating mode.

13.5.3 RUN mode

Response

In "RUN" mode the cyclic, time-driven, and interrupt-driven program execution is performed. Addresses that are in the "Automatic Update" process image are automatically updated in each program cycle. For more information, see section Process images and process image partitions (Page 250).

Execution of the user program

Once the CPU has written the outputs and read the inputs, it runs through the cyclic program from the first instruction to the last instruction. Events with higher priority, such as hardware interrupts, diagnostic interrupts and communication, can interrupt the cyclic program flow and prolong the cycle time.

If you have configured a minimum cycle time, the CPU will not end the cycle until this minimum cycle time has expired, even if the user program is completed sooner.

The operating system monitors the execution time of the cyclic program for a configurable upper limit known as the maximum cycle time. You can restart this time monitoring at any point in your program by calling the RE_TRIGR instruction.

If the cyclic program exceeds the maximum cycle time, the operating system starts the time error OB (OB 80). If the OB is not available, the CPU goes to STOP mode. If the cycle monitoring time is exceeded a second time, e.g. while the time error OB is being processed, the CPU goes to STOP mode.

Causes for loss of RUN mode

The following table provides a summary of causes that result in a loss of the RUN mode.

Cause	Reason	Comments
Triggering the STOP mode	Time error without calling OB 80	Maximum cycle time was exceeded.
	Time error when calling OB 80	The cycle time was exceeded twice in the same cycle.
	Programming error (without OB 121)	-
	Programming error in OB 121	-
	For motion control: Overflow of events	MC_Interpolator (OB 92)
		MC_Servo (OB 91)
	For motion control: Temperature monitor tripped	After a warning, the system switches to STOP mode
	For F-CPUs: Error responses occurred	75D1 / 75DC: Safety program: Internal CPU error
		75D2: Safety program: Maximum cycle time exceeded
		75D6: Safety program: Data corruption before output to F-I/O
		75D7: Safety program: Data corruption before output to partner F-CPU/other F-runtime group
		75D9: Safety program: Permissible time in deactivated safety mode exceeded
		75DF: Safety program: Data corruption before output to OPC UA SafetyConsumer instance
		75E6: Safety program: Inconsistent
		75EE: Safety program: Modifying jobs on F-I/O not completed
	Central module for S7-1500 unplugged/plugged	-
	Switched to STOP mode	Via STP instruction, mode selector switch/button, display, STEP 7, HMI, web server or SAT tool
CPU failure	CPU defective	-
	Power supply failed	-
	Negative power segment overview occurred	-
	SIMATIC Memory Card unplugged	-
Interrupting the RUN mode	Set breakpoint reached	-

Reference

More information about cycle and response times is available in the Function Manual Cycle and response times (https://support.automation.siemens.com/WW/view/en/59193558).

13.5.4 Operating mode transitions

Operating modes and operating mode transitions

The following figure shows the operating modes and the operating mode transitions:
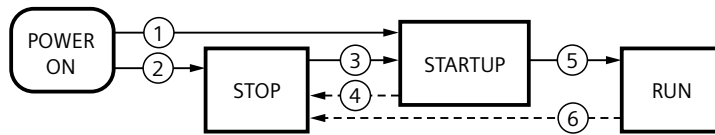

Figure 13-3 Operating modes and operating mode transitions

The table below shows the effects of the operating mode transitions:

Table 13-3 Operating mode transitions

No.	Operating mode transitions		Effects
①	POWER ON → STARTUP	After switching on, the CPU switches to "STARTUP" mode if: • The hardware configuration and program blocks are consistent. • The preceding "POWER OFF" was triggered by an interruption in the power supply. • Startup type "Warm restart - RUN" is set. or • Startup type "Warm restart mode before POWER OFF" is set and the CPU was in RUN mode before POWER OFF.	The CPU clears the non-retentive memory, and resets the content of non-retentive DBs to the start values of the load memory. Retentive memory and retentive DB contents are retained. The 500 newest entries in the diagnostics buffer are retained.
②	POWER ON → STOP	After switching on, the CPU goes to "STOP" mode if: • The hardware configuration and program blocks are inconsistent. or • Startup type "No restart" is set. or • Startup type "Warm restart mode before POWER OFF" is set and the CPU was in STOP mode before POWER OFF.	The CPU clears the non-retentive memory, and resets the content of non-retentive DBs to the start values of the load memory. Retentive memory and retentive DB contents are retained. The 500 newest entries in the diagnostics buffer are retained.
③	STOP → STARTUP	The CPU switches to "STARTUP" mode if: • The hardware configuration and program blocks are consistent. • You set the CPU to "RUN" mode via the programming device or the display and the mode switch in is RUN position. or • You set the mode selector from STOP to RUN or press the operating mode button RUN.[1]	The CPU clears the non-retentive memory, and resets the content of non-retentive DBs to the start values of the load memory. Retentive memory and retentive DB contents are retained. The 500 newest entries in the diagnostics buffer are retained.
④	STARTUP → STOP	In the following cases the CPU returns from "STARTUP" to "STOP" mode when: • The CPU detects an error during startup. • You set the CPU to "STOP" via the programming device, display or mode selector switch / keys.[1] • The CPU executes a STOP command in the Startup OB.	These operating mode transitions have no effect on data.

[1] Standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0: You switch the mode using keys (RUN and STOP).

No.	Operating mode transitions		Effects
⑤	STARTUP → RUN	In the following cases, the CPU goes from "STARTUP" to "RUN" mode when: • The CPU has initialized the PLC tags. • The CPU has executed the startup blocks successfully.	These operating mode transitions have no effect on data.
⑥	RUN → STOP	In the following cases, the CPU goes from "RUN" mode back to "STOP" mode: • The CPU detects an error that prevents it from continuing to operate. • You have inserted CMs/CPs that have not yet been configured. • The CPU processes a STOP command in the user program. • You set the CPU to "STOP" via the programming device, display or mode selector switch / operating mode button.[1]	

[1] Standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0: You switch the mode using keys (RUN and STOP).

NOTE

RUN → STOP in configurations with centrally inserted communication modules (CM) and/or communications processors (CPs)

Centrally inserted communications modules (CMs) and/or communications processors (CPs) that have not yet been configured and downloaded to the CPU can cause a transition from "RUN" mode back to "STOP" mode.

Remove unconfigured CMs/CPs or configure and download the configuration of these CMs to the CPU before you set the CPU to "RUN" mode.

13.6 CPU memory reset

Basics of a memory reset

The CPU must be in STOP mode for a memory reset.

A memory reset returns the CPU to its "initial state".

Memory reset means:

- An existing online connection between your programming device/PC and the CPU is terminated.

- The content of the work memory and the retentive and non-retentive data are deleted (with manual memory reset).

- The diagnostics buffer, time of day, and IP address are retained.

- Subsequently the CPU is initialized with the loaded project data (hardware configuration, code and data blocks, force jobs). The CPU copies this data from the load memory to the work memory.

    Result:

    – If you set an IP address in the hardware configuration ("Set IP address in the project" option) and a SIMATIC memory card with the project is in the CPU, this IP address is valid after the memory reset.

    – Data blocks no longer have current values but rather their configured start values.

    – Force jobs remain active.

Detecting a CPU memory reset

The RUN/STOP LED flashes yellow at 2 Hz. After completion, the CPU switches to STOP. The RUN/STOP LED is on (constant yellow light).

Result after memory reset

The following table provides an overview of the contents of the memory objects after memory reset.

Table 13-4 Memory objects after memory reset

Memory object	Contents
Actual values of the data blocks, instance data blocks	Initialized
Bit memories, timers and counters	Initialized
Retentive tags of technology objects (e.g. adjustment values of absolute encoders)	Retained
Diagnostics buffer entries	Retained
IP address	Retained
Device name	Retained
Counter readings of the runtime meters	Retained
Time of day	Retained
CPU operating state: RUN/STOP	The CPUs retain the STOP state.

> **NOTE**
>
> **Password for protection of confidential configuration data**
>
> The password for protection of confidential configuration data is retained after a memory reset of the CPU. The password is only deleted when the "Delete password for protection of confidential PLC configuration data" option is set.
>
> You can find more information on the password for protection of confidential configuration data in the Communication (https://support.industry.siemens.com/cs/ww/de/view/59192925/en) Function Manual.

13.6.1 Automatic memory reset

Possible causes of automatic memory reset

The CPU executes an automatic memory reset if an error occurs that prevents normal further processing.

Examples of such errors:

- User program is too large and cannot be loaded to the work memory in full.

- The project data on the SIMATIC memory card are damaged, for example because a file was deleted.

- You remove or insert the SIMATIC memory card. The backed-up retentive data differs in structure from the data in the configuration on the SIMATIC memory card.

13.6.2 Manual memory reset

Reason for manual memory reset

Memory reset is required to reset the CPU to the "original state".

CPU memory reset

Three options are available for performing a CPU memory reset:

- Via the operating mode keys/mode switches

- Using the display

- Using STEP 7

Procedure via the mode selector keys (standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0)

NOTE

Memory reset ↔ Reset to factory settings

The procedure described below also corresponds to the procedure for resetting to factory settings:

- Key operation with inserted SIMATIC memory card: CPU executes a memory reset

- Key operation without inserted SIMATIC memory card: CPU executes reset to factory settings

---

To perform a memory reset of the CPU using the mode selector keys, follow these steps:

1. Press the STOP mode selector key.

   Result: The STOP ACTIVE and RUN/STOP LED light up yellow.

2. Press the STOP operating mode button until the RUN/STOP LED lights up for the 2nd time and remains continuously lit after 3 seconds. After this, release the button.

3. Press the STOP mode button again within the next 3 seconds.

Result: The CPU executes memory reset.

For information on resetting the CPU to factory settings, refer to the section Resetting the CPU to factory settings .

Procedure using the mode selector

NOTE

Memory reset ↔ Reset to factory settings

The procedure described below also corresponds to the procedure for resetting to factory settings:

- Selector operation with inserted SIMATIC memory card: CPU executes a memory reset
- Selector operation without inserted SIMATIC memory card: CPU executes reset to factory settings

---

To perform a memory reset of the CPU using the mode selector, follow these steps:

1. Set the mode selector to the STOP position.

   Result: The RUN/STOP LED lights up yellow.

2. Set the mode selector to the MRES position. Hold the switch in this position until the RUN/STOP LED lights up for the second time and remains continuously lit after three seconds. After this, release the selector.

3. Within the next three seconds, switch the mode selector back to the MRES position, and then back to STOP again.

Result: The CPU executes memory reset.

For information on resetting the CPU to factory settings, refer to the section Resetting the CPU to factory settings .

Procedure using the display

To navigate to the desired "Memory reset" menu command, select the following sequence of menu commands and confirm after each selection with "OK".

- Settings → Reset → Memory reset

Result: The CPU executes memory reset.

Procedure using STEP 7

To perform a memory reset of the CPU via STEP 7, follow these steps:

1. Open the "Online Tools" task card of the CPU.

2. Click the "MRES" button in the "CPU control panel" pane.

3. Click "OK" in response to the confirmation prompt.

Result: The CPU is set to STOP mode and performs memory reset.

13.7 Backing up and restoring the CPU configuration

Backup from online device

You may make changes in the operation of your plant. For example, you may add new devices, replace existing ones or adapt the user program. If these changes result in undesirable behavior, you can restore the plant to an earlier state. Before you download a changed configuration to the CPU, first use the option "Backup from online device" to create a complete backup of the current device state. If you have assigned a password to protect confidential PLC configuration data, then this password is not saved. You can find more information on passwords in the section Protection of confidential configuration data (Page 272).

Upload from device (software)

With the option "Upload from device (software)", you load the software project data from the CPU to an existing CPU in the project.

Upload device as new station

If you are operating a new PG/PC in the plant, the STEP 7 project that was used to create the plant configuration might not be available. In this case, you can use the option "Upload device as new station" to load the data to a project in your PG/PC.

Snapshot of the monitor values

To allow you to restore the actual values at a later date, back up the actual values of the data blocks using the option "Snapshot of the observed values".

Overview of backup types

The table below shows the backup of CPU data depending on the selected type of backup and its specific characteristics:

Table 13-5 Types of backup

	Backup from online device	Upload from device (software)	Upload device as new station	Snapshot of the monitor values
Current values of all DBs (global and instance data blocks) [1]	✓	✓	✓	✓
Blocks of the type OB, FC, FB and DB	✓	✓	✓	--
PLC tags (tag names and constant names)	✓	✓	✓	--

[1] Only the values of the tags that are set as retentive are saved.

[2] Contents of the DataLogs, Recipes and UserFiles folders

	Backup from online device	Upload from device (software)	Upload device as new station	Snapshot of the monitor values
Technology objects	✔	✔	✔	--
Hardware configuration	✔	--	✔	--
Actual values (bit memories, timers and counters)[1]	✔	--	--	--
Content of the SIMATIC memory card	✔	--	✔[2]	--
Archives, recipes	✔	--	--	--
Entries in the diagnostics buffer	--	--	--	--
Current time	--	--	--	--
Properties of the type of backup				
Backup possible for fail-safe CPUs	✔	✔	✔	✔
Backup can be edited	--	✔	✔	✔
Backup possible in operating mode	STOP	RUN, STOP	RUN, STOP	RUN, STOP

[1] Only the values of the tags that are set as retentive are saved.

[2] Contents of the DataLogs, Recipes and UserFiles folders

Example: Backup from online device

The following example shows how to carry out a complete backup of the current device state of the CPU in STEP 7. The S7-1500 automation system is in RUN mode. Before the backup, the CPU goes into STOP mode.

To start the backup, proceed as follows:

1. Right-click to select the CPU in the project tree.

2. Select the "Backup from online device" command from the shortcut menu.
   The "Upload preview" dialog window sets out the key information on the backup process to be run. For a backup you have to switch the CPU to the STOP mode.

3. In the "Action" column, select the "Stop module" command from the drop-down menu.

4. Click "Upload from device". The CPU changes to STOP mode. The backup of the CPU data starts. The backup is saved in the project tree in the folder of the CPU under "Online backups".

Example: Restoring a backup of an online device

If you have saved the CPU data beforehand, you can transfer the backup back to the device. The saved backup is then restored to the CPU.

The S7-1500 automation system is in RUN mode. Before the restoration, the CPU goes into STOP mode.

To start the backup restore, proceed as follows:

1. Open the CPU's folder in the project navigator. The lower-level objects are displayed.

2. Open the "Online backups" folder.

3. Select the backup you want to restore.

4. In the "Online" menu, select the "Download to device" command.

5. The "Load preview" dialog window sets out the key information on the restore process to be run. For a restoration you have to switch the CPU to the STOP mode.

6. In the "Action" column, select the "Overwrite" command from the drop-down menu.

7. Click "Download". The CPU changes to STOP mode. The backup is transferred to the CPU and restored. The "Load results" dialog then opens. In this dialog, you can check whether or not the loading operation was successful and take any further action that may be necessary (no action, start modules).

8. Click "Finish".

Reference

You can find additional information on the different backup methods in the STEP 7 online help.

Emergency address (Emergency IP)

The emergency address (emergency IP address) of a CPU is intended for diagnostic and download functions, e.g. when the CPU is no longer accessible via the IP protocol after a wrong project is downloaded. For information on the emergency address, please refer to the Communication (https://support.industry.siemens.com/cs/ww/de/view/59192925/en) function manual.

Storage of multilingual project texts

When you configure a CPU, texts of different categories result, e.g.

- Object names (names of blocks, modules, tags, etc.)

- Comments (for blocks, networks, watch tables, etc.)

- Messages and diagnostic texts

Texts are provided by the system, for example texts in the diagnostics buffer, or they are created during configuration, for example, messages.

Texts exist in the project in one language or, after a translation process, in multiple languages. You can maintain project texts in all languages available to you in the project tree

(Languages & resources > Project texts). The texts produced when configuring can be downloaded to the CPU.

The following texts are downloaded in the selected languages with the project data to the CPU and are also used by the Web server/CPU display:

- Diagnostics buffer texts (cannot be changed)
- Status texts for the module status (cannot be changed)
- Message texts with associated text lists
- Tag comments and step comments for S7 GRAPH and PLC Code Viewer
- Comments in watch tables

The following texts are also downloaded in the selected languages with the project languages to the CPU but are not used by the Web server/CPU display:

- Comments in tag tables (for tags and constants)
- Comments in global data blocks
- Comments of elements in block interfaces of FBs, FCs, DBs and UDTs
- Network titles in blocks written in LAD, FBD or STL
- Block comments
- Network comments
- Comments of LAD and FBD elements

The S7-1500 CPUs support the storage of multilingual project texts in up to three different project languages. If the project texts for a project language nevertheless exceed the memory space reserved for them, the project cannot be downloaded to the CPU. The download is aborted with a notice that not enough memory space is available. In such a case, take measures to reduce the required storage space, for example by shortening comments.

You will find information on parameterization of multilingual project texts in STEP 7 in the STEP 7 online help.

Size of files and size of the SIMATIC memory card

NOTE

SIMATIC memory card

Make sure that there is enough available storage space on your SIMATIC memory card for downloading projects.

To download and back up projects, the project size and the size of the files on the SIMATIC memory card must be less than 2 GB.

Do not manipulate any contents in the OMSSTORE directory on the SIMATIC memory card.

You can find information on reading out the memory usage of the CPU and the SIMATIC memory card in the Structure and Use of the CPU Memory (https://support.industry.siemens.com/cs/de/de/view/59193101/en) Function Manual.

13.8 Time synchronization

Introduction

All CPUs are equipped with an internal clock. The clock shows:

- The time of day with a resolution of 1 millisecond
- The date and the day of the week

The CPU take into account the time change caused by daylight saving time.

You can synchronize the time of the CPUs with an NTP server in NTP mode.

Principle of operation

In NTP mode, the device sends time queries at regular intervals (in client mode) to the NTP server in the subnet (LAN). Based on the replies from the server, the most reliable and most accurate time is calculated and the time of day on the CPU is synchronized. The advantage of this mode is that it allows the time to be synchronized across subnets. You can synchronize the time of day of up to a maximum of four NTP servers. You address a communications processor or an HMI device, for example, as sources for time synchronization via the IP addresses.

The update interval defines the interval between the time queries (in seconds). The value of the interval ranges between 10 seconds and one day. In NTP mode, it is generally UTC (Universal Time Coordinated) that is transferred. UTC corresponds to GMT (Greenwich Mean Time).

NTP server for the CPU S7-1500

You can assign up to 4 NTP servers to a CPU S7-1500.

You have the following options to reset the IP addresses of the NTP servers:

- Configure IP addresses of the NTP servers in STEP 7.
- Set IP addresses of the NTP servers with the "T_CONFIG" instruction.
- Obtain IP addresses of the NTP servers via DHCP.
  As of firmware version V2.9, the CPU can also obtain the NTP servers via DHCP. You can find more information on the procedure and the DHCP communication protocol in the Communication (https://support.industry.siemens.com/cs/ww/de/view/59192925/en) function manual.

Configuring IP addresses of the NTP servers in STEP 7

To configure the IP addresses of the NTP servers in STEP 7, follow these steps:

1. Select the S7-1500 CPU in STEP 7.
2. Configure the time synchronization in the "Properties > General > Time" parameter group.
3. Set the "Set NTP server in the project" value at the "Time synchronization" parameter.
4. Enter the IP addresses of up to four NTP servers for "NTP Server 1" to "NTP Server 4".
5. Set the time interval of time queries for "Update interval". Set the update interval to between 10 s and 86400 s.

Setting the IP addresses of the NTP servers with the "T_CONFIG" instruction

Requirement:

- You selected the option "Set NTP server directly on the device (e.g. PLC program, display)" in the "Time synchronization" drop-down list in STEP 7.

Proceed as follows to set the IP addresses of the NTP servers with the T_CONFIG instruction:

1. Enter the IP addresses of up to four NTP servers in a tag of the data type IF_CONF_NTP.
2. Connect the tag of the data type IF_CONF_NTP to the block parameter CONF_DATA of the instruction T_CONFIG.
3. Call the T_CONFIG instruction in the user program.

Result: The CPU adopts the addresses of the NTP servers from the T_CONFIG instruction.

If necessary, you can change the addresses of the NTP servers several times with T_CONFIG.

Reference

For more information on time-of-day synchronization - time synchronization in automation, refer to the following FAQ on the Internet (https://support.industry.siemens.com/cs/de/en/view/86535497).

13.8.1 Example: Configuring the IP address of the NTP server in STEP 7 or setting it in the user program

Automation task

You are using your own NTP server in your network with the IP address 192.168.1.15. Your own server provides you with the following advantages:

- Protection against unauthorized accesses from outside
- Every device that you synchronize with your own NTP server uses the same time.

You want to synchronize the S7-1500 CPU with this NTP server.

The following sections describe how to configure the IP address of the NTP server in STEP 7 or set it in the user program.

Configuring the IP address of the NTP server in STEP 7

Procedure

1. Select the S7-1500 CPU in STEP 7.

2. Configure the time synchronization in the "Properties > General > Time" parameter group.

3. Set the "Set NTP server in the project" value at the "Time synchronization" parameter.

4. For "NTP Server 1", enter the IP address of the NTP server: 192.168.1.15.

5. Download the hardware configuration to the CPU.

Result

The S7-1500 synchronizes the time with the NTP server 192.168.1.15.

Set IP addresses of the NTP server with the "T_CONFIG" instruction

Requirement:

- You selected the option "Set NTP server directly on the device (e.g. PLC program, display)" in the "Time synchronization" drop-down list in STEP 7.

To set the IP address for the NTP server, use the following block parameters of the "T_CONFIG" instruction:

- Req: A positive edge at the block parameter "Req" starts a job of the "T_CONFIG" instruction.

- Interface: Enter the HW ID of the PROFINET interface 1 of the CPU at the block parameter "Interface". In this example, the HW ID is "64".

- Conf_Data: Area in which you save the IP addresses of the NTP server. Use the data type "IF_CONF_NTP" for this purpose.

Procedure

Proceed as follows to set the IP address of the NTP server in the user program to
"192.168.1.15":

1. Create a global data block in the project tree under "Program blocks > Add new block".
   Name the global data block "NTP".

2. Create an "NTP_Server" tag of the data type "IF_CONF_NTP" in the global data block "NTP".

		Name	Data type	Start value	Comment
	NTP				
1		▼ Static			
2		▼ NTP_Server	IF_CONF_NTP		
3		Id	UInt	17	
4		Length	UInt	22	
5		Mode	UInt	0	
6		▼ NTP_IP	Array[1..4] of IP_V4		
7		▼ NTP_IP[1]	IP_V4		
8		▼ ADDR	Array[1..4] of Byte		IPv4 address
9		ADDR[1]	Byte	192	IPv4 address
10		ADDR[2]	Byte	168	IPv4 address
11		ADDR[3]	Byte	1	IPv4 address
12		ADDR[4]	Byte	10	IPv4 address
13		▶ NTP_IP[2]	IP_V4		
14		▶ NTP_IP[3]	IP_V4		
15		▶ NTP_IP[4]	IP_V4		
16		change_NTP-Server	Bool	false	
17		done	Bool	false	
18		busy	Bool	false	
19		error	Bool	false	
20		status	DWord	16#0	
21		err_loc	DWord	16#0	

Figure 13-4 Example data block with IF_CONF_NTP

3. Create a "T_CONFIG" instruction in the user program.

4. Connect the "T_CONFIG" instruction as follows.
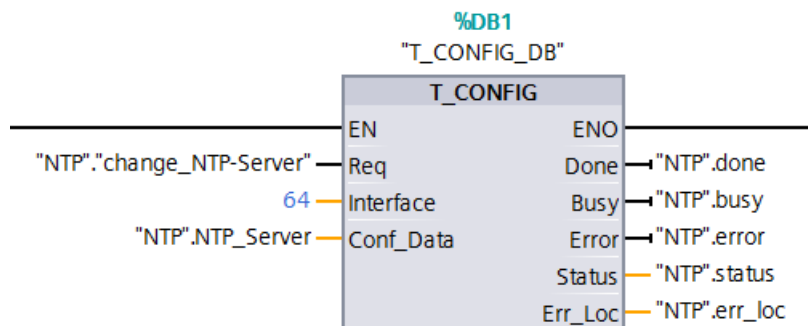
Figure 13-5 Example T_CONFIG: Setting the NTP server

5. In the user program, assign the IP address 192.168.1.15 to the data type "IF_CONF_NTP":

   ```
   "NTP".NTP_Server.NTP_IP[1].ADDR[1] := 192;
   "NTP".NTP_Server.NTP_IP[1].ADDR[2] := 168;
   "NTP".NTP_Server.NTP_IP[1].ADDR[3] := 1;
   "NTP".NTP_Server.NTP_IP[1].ADDR[4] := 15;
   ```

6. Generate a positive edge for the tag "change_NTP-Server" in the user program:

   ```
   "NTP"."change_NTP-Server" := true;
   ```

Result

The S7-1500 synchronizes the time with the NTP server 192.168.1.15.

13.9 Identification and maintenance data

13.9.1 Reading out and entering I&M data

I&M data

Identification and maintenance data (I&M data) is information saved on the module. The data is:

- Read-only (I data) or
- Readable/writable (M data)

Identification data (I&M0): Manufacturer information about the module that can only be read. Some identification data is also printed on the housing of the module, for example article number and serial number.
Maintenance data (I&M1, 2, 3): Plant-specific information, for example installation location. Maintenance data for the S7-1500/ET 200MP is created during configuration and downloaded to the automation system/distributed I/O system.

All modules of the S7-1500/ET 200MP support identification data I&M0 through I&M3.

The I&M identification data supports you in the following activities:

- Checking the plant configuration
- Locating hardware changes in a plant
- Correcting errors in a plant

Modules can be clearly identified online using the I&M identification data.

Maintenance data (I&M4): Storage of a CRC test value for IM 155-5 MF HF interface modules to ensure data integrity of data used by the interface module.

Options for reading out I&M data

- Via the user program
- Using the display of the CPU
- Via STEP 7 or HMI devices
- Via the CPU web server

Reading I&M data via the user program

You have the following options for reading module I&M data in the user program:

- Using the RDREC instruction

  The data record structure for centrally inserted modules as well as for distributed modules that are accessible via PROFINET IO/PROFIBUS DP is described in the section Record structure for I&M data (Page 351).

- Using the Get_IM_Data instruction

Reference

The description of the instructions can be found in the STEP 7 online help.

Reading I&M data from displays

To read the I&M data "Plant designation" or "Location identifier" of the CPU via the display, follow these steps:

1. Navigate to the "Overview/PLC" menu on the display of the CPU.

2. Select "Plant designation" or "Location identifier" and confirm with "OK".

To read the I&M data "Plant designation" or "Location identifier" of a centrally used module, follow these steps:

1. Navigate to the "Modules" menu on the display of the CPU.

2. Select the menu command "Local modules" and confirm with "OK".

3. Select the slot of the module (e.g., slot 3: DI 32 x 24VDC HF) and confirm with "OK".

4. Select the "Status" and confirm with OK.

5. Select "Plant designation" or "Location identifier" and confirm with "OK".

To read the I&M data "Plant designation" or "Location identifier" of a module used in distributed mode, follow these steps:

1. Navigate to the "Modules" menu on the display of the CPU.

2. Select the corresponding distributed I/O system (for example PROFINET IO system) and confirm with "OK".

3. Select the corresponding device (for example ET 200SP-Station_1) and confirm with "OK".

4. Select the slot of the module (e.g., slot 1: DI 16 x DC24V ST_1) and confirm with "OK".

5. Select the "Status" and confirm with OK.

6. Select "Plant designation" or "Location identifier" and confirm with "OK".

Reading I&M data via STEP 7

Requirement: There must be an online connection to the CPU/interface module.

To read I&M data using STEP 7, follow these steps:

1. In the project tree, select the CPU/the interface module.

2. Go to "Online & diagnostics".

3. In the "Diagnostics" folder, select the "General" area.

Enter maintenance data via STEP 7

STEP 7 assigns a default module name. You can enter the following information:

- Plant designation (I&M 1)

- Location identifier (I&M 1)

- Installation date (I&M 2)

- Additional information (I&M 3)

To enter maintenance data via STEP 7, follow these steps:

1. In the device view of STEP 7, select the CPU/interface module or a module.

2. Go to properties, "General", and select the "Identification & Maintenance" area

3. Enter the data.

During the loading of the hardware configuration, the maintenance data (I&M 1, 2, 3) are also loaded.

Procedure for reading I&M data via the Web server

The procedure is described in detail in the Web server Function Manual (https://support.automation.siemens.com/WW/view/en/59193560).

13.9.2 Record structure for I&M data

Reading I&M records via user program (centrally and distributed via PROFINET IO)

Use **Read data record** ("RDREC" instruction) to access specific identification data. Under the associated record index you obtain the corresponding part of the identification data.

The records are structured as follows:

Table 13-6 Basic structure of data records with I&M identification data

Contents	Length (bytes)	Coding (hex)
Header information		
BlockType	2	I&M0: 0020_H I&M1: 0021_H I&M2: 0022_H I&M3: 0023_H I&M4: 0024_H

Contents	Length (bytes)	Coding (hex)
BlockLength	2	I&M0: 0038_H I&M1: 0038_H I&M2: 0012_H I&M3: 0038_H I&M4: 0038_H
BlockVersionHigh	1	01
BlockVersionLow	1	00
Identification data		
Identification data (see table below)	I&M0/Index $AFF0_H$: 54 I&M1/Index $AFF1_H$: 54 I&M2/Index $AFF2_H$: 16 I&M3/Index $AFF3_H$: 54 I&M4/Index $AFF4_H$: 54	- - - - -

Table 13-7 Record structure for I&M identification data

Identification data	Access	Default setting	Explanation
Identification data 0: (record index $AFF0_H$)			
VendorIDHigh	read (1 bytes)	00_H	Name of the manufacturer
VendorIDLow	read (1 bytes)	$2A_H$	(42_D = Siemens AG)
Order_ID	read (20 bytes)	6ES7155-5MU00-0CN0	Article number of module (e.g. IM 155-5 MF HF)
IM_SERIAL_NUMBER	read (16 bytes)	-	Serial number (device-specific)
IM_HARDWARE_REVISION	read (2 bytes)	1	Corresponding to hardware version
IM_SOFTWARE_REVISION	read	Firmware version	Provides information about the firmware version of the module
• SWRevisionPrefix	(1 byte)	V	
• IM_SWRevision_Functional_Enhancement	(1 byte)	00_H - FF_H	
• IM_SWRevision_Bug_Fix	(1 byte)	00_H - FF_H	
• IM_SWRevision_Internal_Change	(1 byte)	00_H - FF_H	
IM_REVISION_COUNTER	read (2 bytes)	0000_H	Provides information about parameter changes on the module (not used)
IM_PROFILE_ID	read (2 bytes)	0000_H	Generic Device
IM_PROFILE_SPECIFIC_TYPE	read (2 bytes)	0001_H	CPU
		0003_H	I/O modules
IM_VERSION	read	0101_H	Provides information on the ID data version
• IM_Version_Major	(1 byte)		(0101_H = Version 1.1)
• IM_Version_Minor	(1 byte)		
IM_SUPPORTED	read (2 bytes)	$000E_H$	Provides information about the available identification data and maintenance data (I&M1 to I&M3)

* A value of 0 indicates that the IM firmware does not yet support the CRC calculation of the assigned modules.
If the value is ≠ 0, the IM supports this function, regardless of whether the associated modules support I&M4 data.

Identification data	Access	Default setting	Explanation
Maintenance data 1: (Record index AFF1$_H$)			
IM_TAG_FUNCTION	read/write (32 bytes)	-	Enter an identifier for the module here, that is unique plant-wide.
IM_TAG_LOCATION	read/write (22 bytes)	-	Enter the installation location of the module here.
Maintenance data 2: (Record index AFF2$_H$)			
IM_DATE	read/write (16 bytes)	YYYY-MM-DD HH:MM	Enter the installation date of the module here.
Maintenance data 3: (Record index AFF3$_H$)			
IM_DESCRIPTOR	read/write (54 bytes)	-	Enter a comment about the module here.
Maintenance data 4: (Record index AFF4$_H$)			
USI	Read (4 bytes)	0x63726331	UserstructureIdentifier: Internal, fixed value
CHK_OVERALL	Read (4 bytes)	-	Overall CRC via all individual CRCs
CHK_OVERALL_SUBS	Read (4 bytes)	0 or value*	Overall CRC via all assigned modules of the IM
CHK_STATIC_LOCAL	Read (4 bytes)	-	CRC via static data of the IM
CHK_STATIC_SUBS	Read (4 bytes)	0 or value*	CRC via all static data of the modules of the IM
CHK_OVERALL_SETUP	Read (4 bytes)	-	Overall CRC via all setup data of the IM and modules of the IM
CHK_REMANENT_LOCAL	Read (4 bytes)	-	CRC via retentive data of the IM
CHK_REMANENT_SUBS	Read (4 bytes)	0 or value*	CRC via all retentive data of the modules of the IM
CHK_WORKING_LOCAL	Read (4 bytes)	-	CRC via the parameters in STEP 7 for the IM
CHK_WORKING_SUBS	Read (4 bytes)	0 or value*	CRC via all parameters in STEP 7 for the modules of the IM
NOT USED	Read (14 bytes)	0	14 reserved bytes

* A value of 0 indicates that the IM firmware does not yet support the CRC calculation of the assigned modules.
If the value is ≠ 0, the IM supports this function, regardless of whether the associated modules support I&M4 data.

Reading I&M records with record 255 (distributed configuration via PROFIBUS)

Use **Read data record** ("RDREC" instruction) to access specific identification data.

The modules support standardized access to identification data using DR 255 (index 65000 to 65003). For more information on the DR 255 data structure, refer to the specifications of the Profile Guidelines Part 1: Identification & Maintenance Functions - Order no.: 3.502, Version 1.2, October 2009.

The specifications are available, for example, on the PROFIBUS & PROFINET International (PI) website on the Internet (https://www.profibus.com/).

13.9.3 Example: Read out firmware version of the CPU with Get_IM_Data

Automation task

You want to check whether the modules in your automation system have the current firmware. The firmware version of the modules can be found in the I&M0 data. The I&M0 data is the basic information for a device. The I&M0 data contains information, for example:

- Manufacturer ID
- Article number and serial number
- Hardware and firmware version.

To read out the I&M0 data, use the "Get_IM_Data" instruction. You read the I&M0 data of all modules in the user program of the CPU with "Get_IM_Data" instructions and store the I&M data in a data block.

Conditions and parameters

To read out the I&M data of the CPU, use the following block parameters of the "Get_IM_Data" instruction:

- LADDR: Enter the HW ID of the module at the block parameter "LADDR".
- IM_TYPE: Enter the I&M data number (e.g. "0" for I&M 0 data) at the block parameter "IM_TYPE".
- DATA: Area for storing the read I&M data (for example. in a global data block). Store the I&M 0 data in an area of the data type "IM0_Data".

This example shows how to read out the I&M 0 data of a CPU 1511-1 PN. To read out the I&M 0 data of a different module, simply use the HW ID of the module at the parameter LADDR.

Solution

To read out the I&M 0 data of the CPU, follow these steps:

1. Create a global data block to store the I&M 0 data.

2. Create a structure of the data type "IM0_Data" in the global data block. You can assign any name to the structure ("imData") in this case.

		Name	Data type	Start value
		SLI_gDB_Get_IM_Data		
1		▼ Static		
2		▶ imData	IM0_Data	
3		done	Bool	false
4		busy	Bool	false
5		error	Bool	false
6		status	Word	16#0

Figure 13-6 Example: Data block for I&M data

3. Create the Insert the "Get_IM_Data" instruction in the user program, e.g. in OB 1.

4. Connect the "Get_IM_Data" instruction as follows:

#GET_IM_DATA_
Instance

Get_IM_Data

EN   ENO

49 — LADDR   DONE — "SLI_gDB_Get_IM_Data".done

0 — IM_TYPE

"SLI_gDB_Get_IM_Data".imData — DATA   BUSY — "SLI_gDB_Get_IM_Data".busy

ERROR — "SLI_gDB_Get_IM_Data".error

STATUS — "SLI_gDB_Get_IM_Data".status
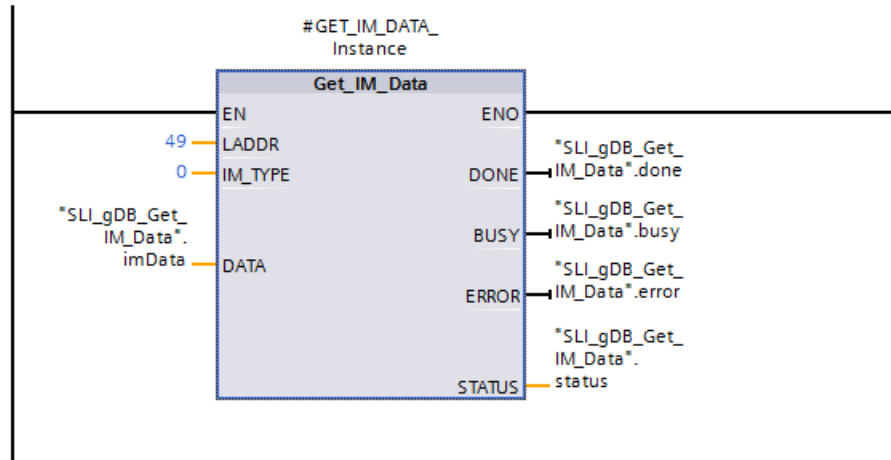
Figure 13-7 Example: Reading out I&M0 data

5. Call the "Get_IM_Data" instruction in the user program.

Result

The "Get_IM_Data" instruction has stored the I&M0 data in the data block.

You can view the I&M0-Daten online in STEP 7, for example, in the data block with the "Monitor all" button. The CPU in the example is a CPU 1511-1 PN (6ES7511-...) with firmware version V1.5.

		Name	Data type	Start value	Monitor value
		SLI_gDB_Get_IM_Data			
1		▼ Static			
2		▼ imData	IM0_Data		
3		Manufacturer_ID	UInt	0	42
4		Order_ID	String[20]	''	'6ES7 511-...'
5		Serial_Number	String[16]	''	'S C-DOS710132013'
6		Hardware_Revision	UInt	0	3
7		▼ Software_Revision	IM0_Version		
8		Type	Char	' '	'V'
9		Functional	USInt	0	1
10		Bugfix	USInt	0	5
11		Internal	USInt	0	0
12		Revision_Counter	UInt	0	0
13		Profile_ID	UInt	0	0
14		Profile_Specific_Ty...	UInt	0	0
15		IM_Version	Word	16#0	16#0101
16		IM_Supported	Word	16#0	16#001E
17		done	Bool	false	TRUE
18		busy	Bool	false	FALSE
19		error	Bool	false	FALSE
20		status	Word	16#0	16#0000

Figure 13-8 Example: I&M0 data of an S7-1500 CPU

13.10 Shared commissioning of projects

Team Engineering

In Team Engineering, several users from various engineering systems work on a project at the same time and access one S7-1500 CPU.

The users can edit separate parts of a master project independently of one another at the same time. The CPU show the changes of the other editors in a synchronization dialog during the loading of the configuration into the CPU and synchronizes the changes automatically, if possible.

Certain online functions can also be executed in parallel from several engineering systems on a shared CPU, such as:

- Monitoring blocks on the CPU
- Modifying blocks on the CPU
- Trace functions

You can find detailed information on the topic of Team Engineering in the STEP 7 online help.

CPU display

14

Introduction

The section below gives an overview of the mode of operation of the CPU display. Detailed information on the individual options, a training course and a simulation of the selectable menu items is available in the SIMATIC S7-1500 Display Simulator (https://support.industry.siemens.com/cs/ww/en/view/109761758).

Display

The S7-1500 CPU has a display and operating keys. The display of the CPU shows you the control and status information in different menus. You use operating keys to navigate through the menus and make a variety of settings in the process.

Advantages

The display of the CPU offers the following advantages:

- Reduced downtimes through diagnostic messages in plain text
- Time savings during commissioning, maintenance and downtime of the plant by changing the interface settings (e.g. IP address) of CPU and connected CMs/CPs. No programming device is required.
- Shorter downtimes due to read/write access to force tables and read/write access to watch tables.
  This allows the current values of the individual tags of a user program or a CPU to be monitored and changed by the monitoring and force tables. You can find more information on the watch and force tables in section Test functions and fault correction (Page 393) and in the STEP 7 online help.
- On site, an image (backup copy) of the functioning plant can be
  - Backed up on the SIMATIC Memory Card of the CPU
  - Restored from the SIMATIC Memory Card of the CPU

You do not require an additional PG/PC.

- For F-CPUs: Overview of status of safety mode and of F-parameters of F-CPU and F-I/O.

Password protection for the display

In the properties of the CPU, configure a password in STEP 7 for the display operation. Local access protection is thus protected via a local password.

Operating temperature for the display

To increase the service life of the display, the display switches off when the permitted operating temperature is exceeded. When the display has cooled down again, it switches on automatically again. When the display is switched off, the LEDs continue to show the status of the CPU.

Information about the temperatures at which the display switches off and back on again is available in the technical data of the manuals of the CPUs.

NOTE

The S7-1500 CPU has no internal temperature measurement. Reading out the internal temperature of the S7-1500 CPU is not supported.

Display

The following figures show an example of a CPU with large display (left: for example, CPU 1516-3 PN/DP) and a CPU with small display (right: for example, CPU 1511-1 PN).
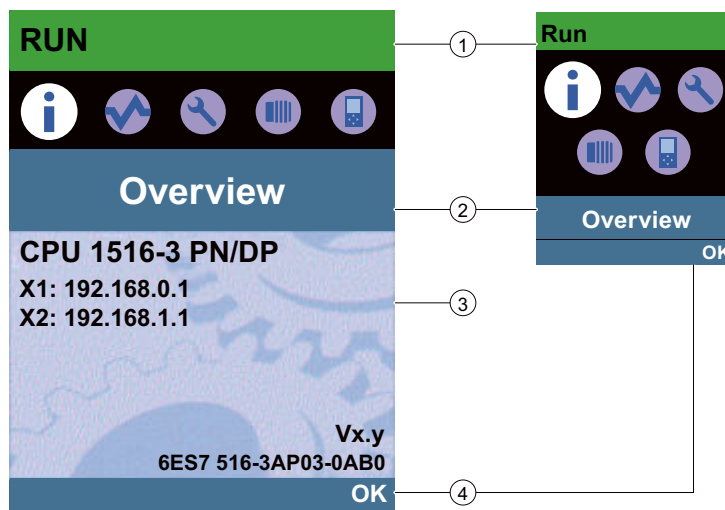
①	CPU status information
②	Names of the menus
③	Data display field
④	Navigation aid, e.g. OK/ESC or the page number

Figure 14-1 Example views of the displays

Regarding ①: CPU status information

The following table shows the CPU status information that can be retrieved via the display.

Table 14-1 CPU status information

Color and icons for the status data	Meaning
Green	RUN
Orange	• STOP • STOP - firmware update
Red	FAULT
White	• Connection established between CPU and display.
🔒	• Access protection configured. • Incorrectly displayed with the following configuration: You have not configured access control and the "Anonymous" user does not have full access rights (e.g. read-only access) to the CPU.
⚠️	• At least one interrupt is active in the CPU. • No SIMATIC Memory Card inserted in the CPU. • The serial number to which a know-how-protected block is bound does not match the serial number of the CPU or the SIMATIC Memory Card. • No user program loaded.
F	Force job is active in the CPU.
🔴	F-capability activated. Safety operation active (for fail-safe CPUs) The symbol is grayed out when safety mode is deactivated.
▬	Fail-safe CPU (for fail-safe CPUs).

Regarding ②: Names of the menus

The following table shows the available menus of the display.

Table 14-2 Names of the menus

Main menu items	Meaning	Description
ℹ️	Overview	The "Overview" menu contains information about: • The properties of the CPU • The properties of the inserted SIMATIC Memory Card • Whether a know-how protection or a linking of the serial number exists. The following information is displayed for F-CPUs: • The status of the safety mode • The collective signature • The date of the last changes
〰️	Diagnostics	The "Diagnostics" menu includes: • The display of diagnostic messages. • Read/write access to force and watch tables. • Display of cycle time. • Display of CPU memory utilization. • Display of interrupts.

Main menu items	Meaning	Description
	Settings	In the "Settings" menu you: • Assign the IP addresses and the PROFINET device name of the CPU. • Set the network properties of each CPU interface. • Set the date, time, time zones, operating modes (RUN/STOP) and protection levels. • Disable/enable display with display password • Perform a CPU memory reset. • Perform a reset to factory settings. • Format the SIMATIC Memory Card. • Delete the user program. • Back up/restore the CPU configuration to/from the SIMATIC Memory Card. • View the status of the firmware update. • Convert the SIMATIC Memory Card to a program card
	Modules	The "Modules" menu contains information about the central and distributed modules that are used in your configuration. Peripherally deployed modules are connected to the CPU via PROFINET and/or PROFIBUS. You can set the IP addresses for the CPU or a CP/CM here. Fail-safe parameters are displayed for F-modules.
	Display	In the "Display" menu you can configure settings related to the display, such as language setting, brightness and energy-saving mode. The energy-saving mode dims the display. The standby mode selectors the display off.

Menu icons

The following table shows the icons that are displayed in the menus.

Table 14-3 Menu icons

Icon	Meaning
	Editable menu item.
	Select the desired language here.
	A message is available in the next lower level page.
	There is an error in the next lower level page.
	The marked module is not accessible.
	Navigate to the next lower level page.
	In edit mode you make the selection using two arrow keys: • Down/up: jumps to the selection or is used to select the desired digits/options.
	In edit mode you make the selection using four arrow keys: • Down/up: jumps to the selection or is used to select the desired digits. • Left/right: jumps one spot forward or backward.
	The alarm is not yet acknowledged.
	The alarm is acknowledged.

Control keys

You operate the display using the following keys:

- Four arrow keys: "up", "down", "left", "right"
  If you press and hold an arrow key for 2 seconds, this generates an automatic scroll function.
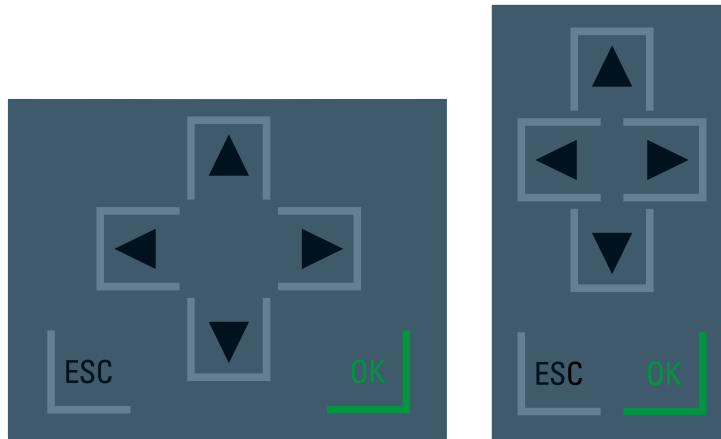
- One ESC key

- One OK key

Figure 14-2 Control keys

NOTE

If the display is in energy-saving mode or in standby mode, you can exit this mode by pressing any key.

Functions of the "OK" and "ESC" keys

- For menu commands in which an entry can be made:
  - OK → valid access to the menu command, confirmation of input, and exit from the edit mode
  - ESC → Restore original content (changes are not saved) and exit edit mode
- For menu commands in which no entry can be made:
  - OK → to next submenu command
  - ESC → back to previous menu command

Hold ESC for about 3 seconds on any screen of the display. Result: You automatically return to the home page.

Tooltips

Some of the values shown on the display can exceed the available display width. The values in question include:

- Station name
- Plant designation
- Location identifier
- PROFINET device name

The available display width is frequently exceeded on CPUs with small displays.

If you focus on the relevant value on the display and press the "Left" arrow key, a tooltip appears. The tooltip shows the name of the value in complete length. To hide the tooltip again, press the "Left" arrow key again or the "ESC" key.
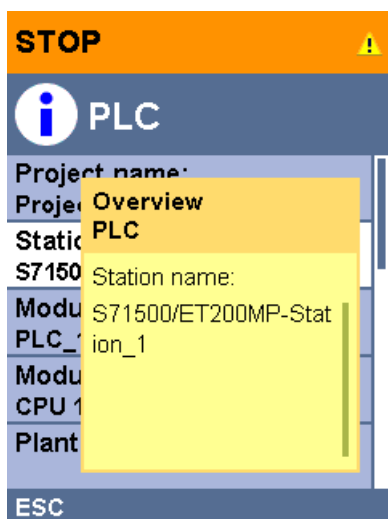
Figure 14-3 Tooltip function

Uploading image to the display via STEP 7

In the STEP 7 device view, you download an image from your file system to the CPU display with the "Display > User-defined logo" function.
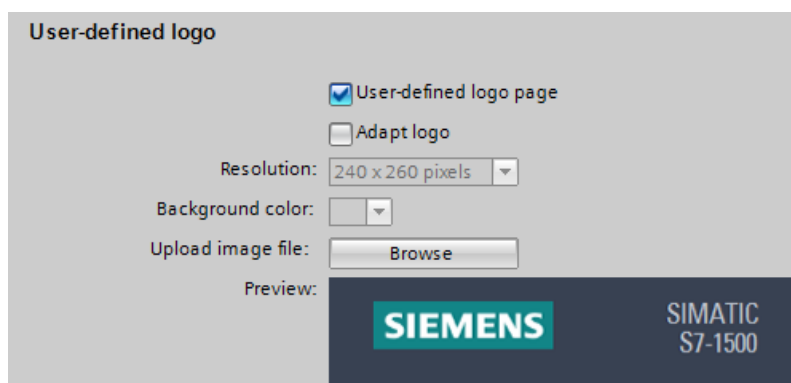
Figure 14-4 Uploading image to CPU

To display the uploaded image in the correct aspect ratio, use images with the following dimensions depending on the CPU.

Table 14-4 Dimensions

CPU	Dimensions	Supported formats
CPU 1511(F)-1 PN CPU 1511C-1 PN CPU 1511T(F)-1 PN	128 x 120 pixels	Bitmap, JPEG, GIF, PNG
CPU 1512C-1 PN	128 x 120 pixels	Bitmap, JPEG, GIF, PNG
CPU 1513(F)-1 PN	128 x 120 pixels	Bitmap, JPEG, GIF, PNG
CPU 1515(F)-2 PN CPU 1515T(F)-2 PN	240 x 260 pixels	Bitmap, JPEG, GIF, PNG
CPU 1516T(F)-3 PN CPU 1516(F)-3 PN/DP CPU 1516T(F)-3 PN/DP	240 x 260 pixels	Bitmap, JPEG, GIF, PNG
CPU 1517(F)-3 PN CPU 1517(F)-3 PN/DP CPU 1517T(F)-3 PN CPU 1517T(F)-3 PN/DP	240 x 260 pixels	Bitmap, JPEG, GIF, PNG
CPU 1518(F)-3 PN CPU 1518(F)-4 PN/DP CPU 1518T(F)-3 PN CPU 1518T(F)-4 PN/DP CPU 1518(F)-4 PN/DP MFP	240 x 260 pixels	Bitmap, JPEG, GIF, PNG

If the uploaded image exceeds the specified dimensions, the display shows only part of the image. The "Adapt logo" option in STEP 7 allows you to reduce the image to the specified dimensions. However, note that the original aspect ratio of the image is not retained in such cases.

Displaying image on the display

To display the uploaded image on the display of the CPU, press the ESC key in the main screen of the display. When you upload an image and are in the main screen, the display automatically shows the image after 60 seconds. To hide the image again, press any key on the display.

Available language settings

You can set the following languages separately for menu and message texts:

- Chinese
- German
- English
- French
- Italian
- Japanese
- Korean

- Portuguese (Brazil)

- Russian

- Spanish

- Turkish

You select the required language directly on the display in the "Display" menu or in STEP 7 in the hardware configuration of the CPU under "User interface languages".

To display message texts on the display, follow these steps:

1. Download the message texts to the CPU as a software component.

   – To do so, select the "Consistent download" option under "Text libraries" in the "Load preview" dialog.

2. You set the project language you would like to be displayed as the interface language by means of parameter assignment.

   – To do so, select a CPU and navigate to the "Multiple languages" area ("Properties > General > Multilingual support") in the Inspector window.

   – Assign the required project languages to the interface languages.

Reference

Important information/special requirements for the display of F-CPUs can be found in Product Information F-CPUs S7-1500 (https://support.industry.siemens.com/cs/ww/de/view/109478599/en)

Maintenance

<div style="text-align: right; font-size: 2em;">**15**</div>

15.1 Removing and inserting I/O modules

Requirement

Remove or insert front connectors and I/O modules only when the voltage is switched off.

NOTICE
Physical damage can occur
If you install or uninstall front connectors and/or I/O modules with switched-on voltage, this can lead to undefined conditions in your plant.
The S7-1500 automation system/ET 200MP distributed I/O system may be damaged as a result.
Therefore only install/uninstall front connectors and/or I/O modules with switched-off voltage.
Therefore during the planning of a plant always make sure to comply with the necessary, pertinent standards and safety guidelines.

Replacement part scenario

Replacing the CPU in a replacement part scenario has an impact on the password for protection of confidential configuration data. When you replace the CPU, observe the rules for the replacement part scenario in the Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

If you replace an existing CPU with a higher-grade CPU, you must also make the change in your STEP 7 project accordingly. You can only replace CPUs with CPUs of the same family. Then load the customized STEP 7 project into the CPU.

15.2 Replacing the display/front cover

Replacing display (Standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0)

The display is pluggable. You can remove or replace the display during operation (RUN). Removing or replacing of the display does not have any influence on the running CPU.

To remove the display from the CPU, follow these steps:

1. Flip the front cover up.

2. Press with a 3.5 mm screwdriver from the front into the unlatching mechanism of the display. This is found in the middle directly above the display.

3. Press the screwdriver lightly from above and lever out the display from the support.

4. Remove the display in an upward direction.

5. You have removed the display.

6. Place the new display in the CPU and press the display firmly in the top area until it audibly engages.

7. Flip the front cover down into place.

The figure below shows an example of the operation at the CPU 1511-1 PN.
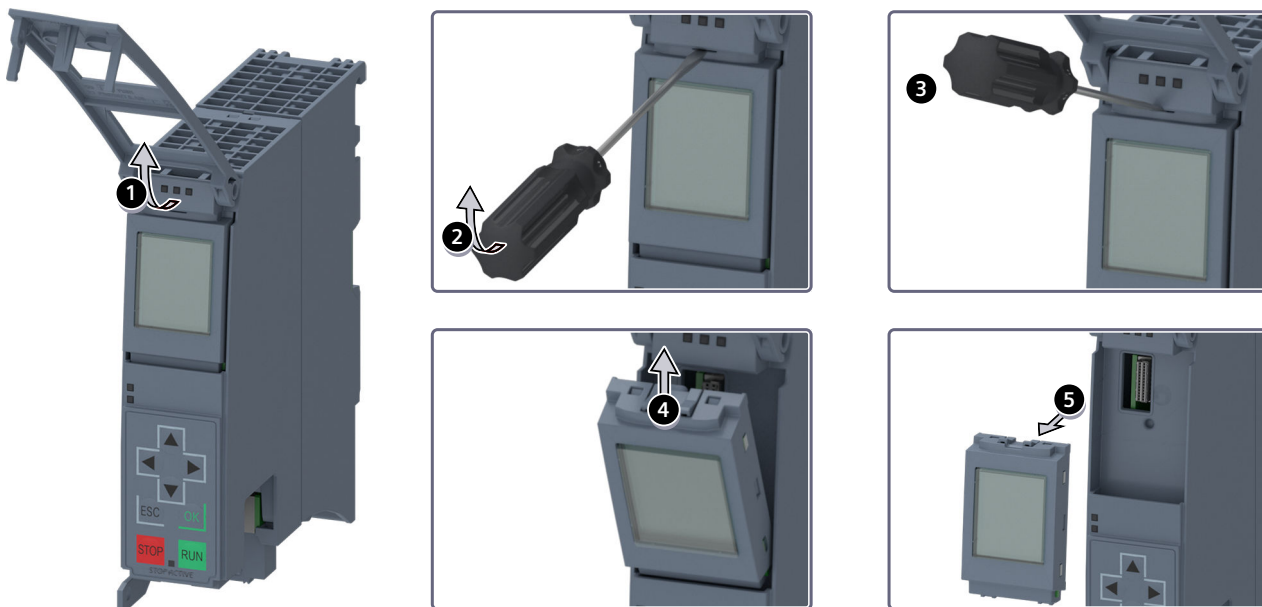
Figure 15-1 Remove display

> ⚠ **WARNING**
>
> **Personal injury or material damage can occur in zone 2 hazardous areas**
>
> In Zone 2 hazardous areas, personal injury or damage to property can occur if you pull or plug the display of an S7-1500 automation system during operation.
>
> Before you remove or fit the display, always switch off the power supply to the S7-1500 automation system in hazardous area zone 2.

Exchanging the front cover

The front cover is pluggable. If necessary, you can take off the front cover or replace the front cover during runtime (RUN). Removing or replacing the front cover does not affect the CPU in operation.

To remove the front cover from the CPU, follow these steps:

1. Flip up the front cover until the front cover stands at a 90° angle to the front of the module.

2. In the top section of the front cover, press on the anchor(s). At the same time, pull the front cover toward you and off.

3. Insert the new front panel (at a 90° angle to the module) from the front into the anchor(s) until they audibly engage.

4. Flip the front cover down into place.

The figure below shows an exemplary view of the CPU 1516-3 PN/DP.
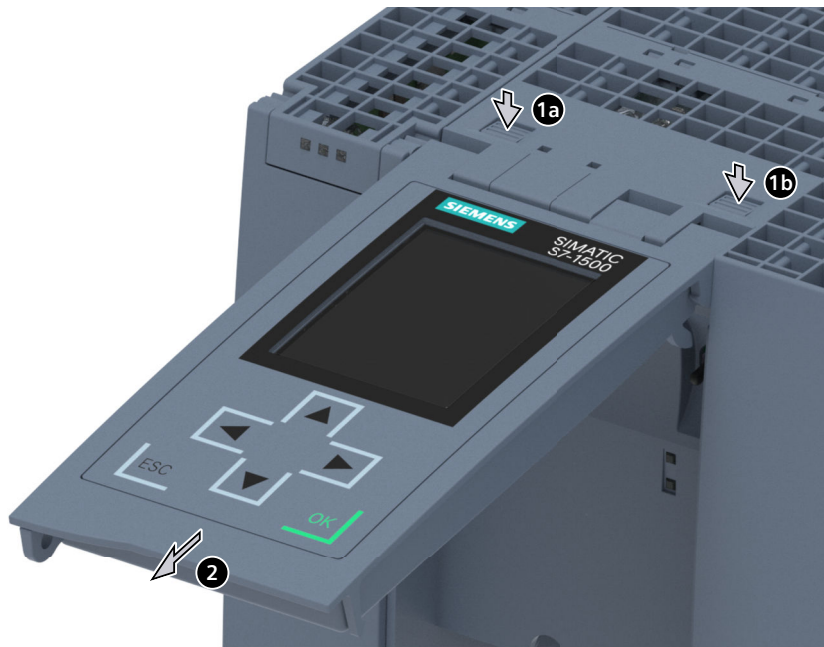
①   Fasteners for removing and fitting the front panel

②   Pull the front cover off towards the front

Figure 15-2 Removing and fitting the front panel

> ⚠ **WARNING**
>
> **Personal injury or material damage can occur in zone 2 hazardous areas**
>
> If you pull or plug the front panel of an S7-1500 automation system during operation, personal injury or damage to property can occur in zone 2 hazardous areas.
>
> Before you remove or fit the front panel, always switch off the power supply to the S7-1500 automation system in hazardous area zone 2.

15.3 Replacement of I/O modules and front connectors

15.3.1 Coding element on the I/O module and on the front connector

Function

All front connectors for the I/O modules of the S7-1500 automation system/ET 200MP distributed I/O system are identical. The coding element prevents a front connector from being inserted on a module with a different electrical pin assignment.

Delivery state of the I/O module

In the delivery state, the coding element is located in the I/O module.
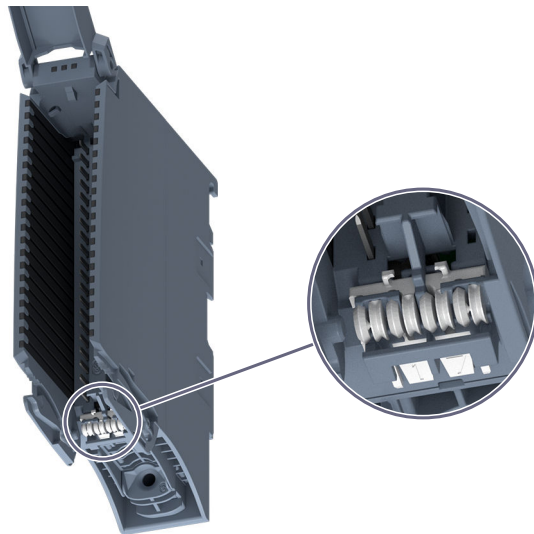
Figure 15-3 Coding element in the I/O module (delivery condition)

Coding element in the front connector

When the front connector is inserted into the I/O module for the first time, one half of the coding element latches into the front connector. When you remove the front connector from the I/O module, this half of the coding element remains in the front connector, while the other half remains in the I/O module.
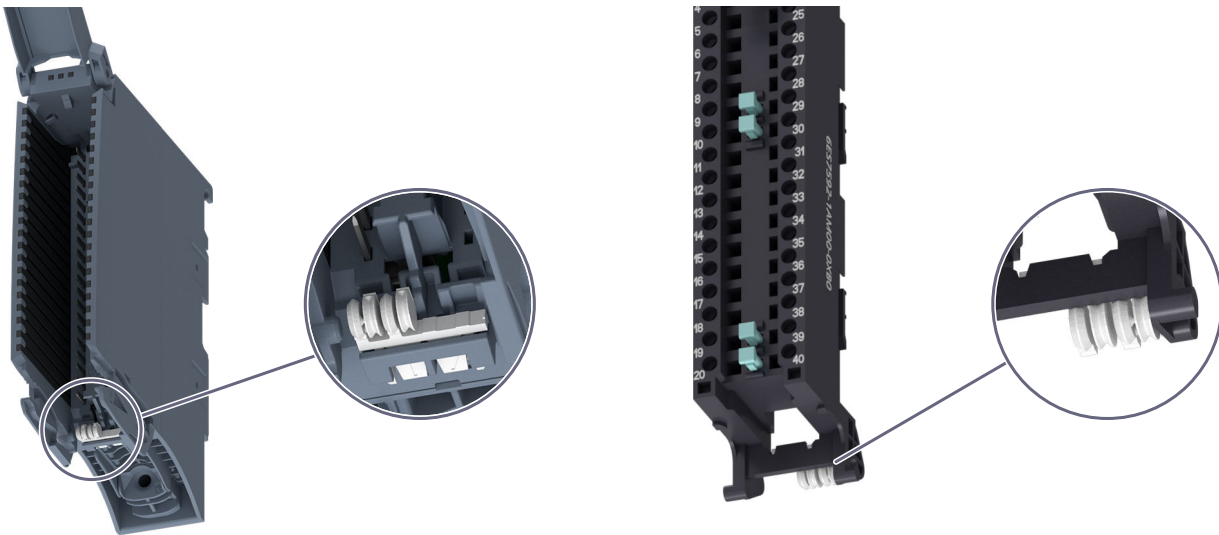
Figure 15-4 Coding element in the I/O module/front connector

You can insert a coded front connector on modules with the same electrical pin assignment.

Refer to section Application planning (Page 159).

NOTICE
Physical damage can occur
If the coding element is changed or removed, it will be possible to insert the front connector on modules in which the electrical connection is not properly wired.
This can destroy the module and/or the connected sensors and actuators. Even hazardous plant states are possible.
Do not change the coding element unless you want to use the front connector on a different module and you change the process wiring accordingly.

Use cases for replacing the coding element

- Replacing an I/O module, for example, due to a defect or incorrect configuration
- Replacing a front connector

Additional electronic coding element for fail-safe modules

In as-delivered condition, a fail-safe module not only has a mechanical coding element but also an electronic rewritable memory for the PROFIsafe address.
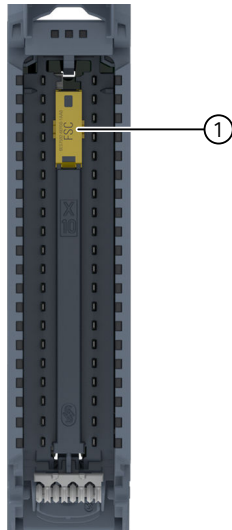
①   Electronic coding element

Figure 15-5   F-module with electronic coding element (as delivered)

When the front connector is inserted in the F-module, the electronic coding element engages completely in the front connector. If you remove the front connector from the F-module, the memory with the PROFIsafe address of the fail-safe module remains in the front connector.
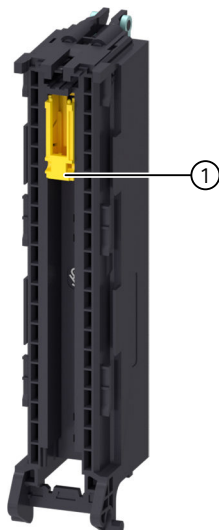
①   Electronic coding element

Figure 15-6   Front connector with electronic coding element

15.3.2   Replacing an I/O module

Introduction

- When the front connector is first inserted into the I/O module, a part of the coding element clips onto the front connector.

- In the case of fail-safe modules, the electronic coding element with the PROFIsafe address of the F-module also engages completely in the front connector.

When you replace an I/O module with the same type of module, the correct coding element or coding elements in the case of F-modules are already present in the front connector.

Result: Before inserting the previous front connector, you must remove the coding element or coding elements from the new I/O module.

Procedure

To replace the I/O module, follow these steps:

The I/O module to be replaced is uninstalled.
You can find information on removing the I/O module in section Installing I/O modules (Page 196).

1. For a new I/O module, use a screwdriver to break out the half of the mechanical coding element that is designated for the front connector.

NOTE

The arrangement of the mechanical coding element depends on the module type: First, check the position of the coding element on the front connector before you break out the matching half from the I/O module.

For a new fail-safe module you must also remove the electronic coding element from the F-module.
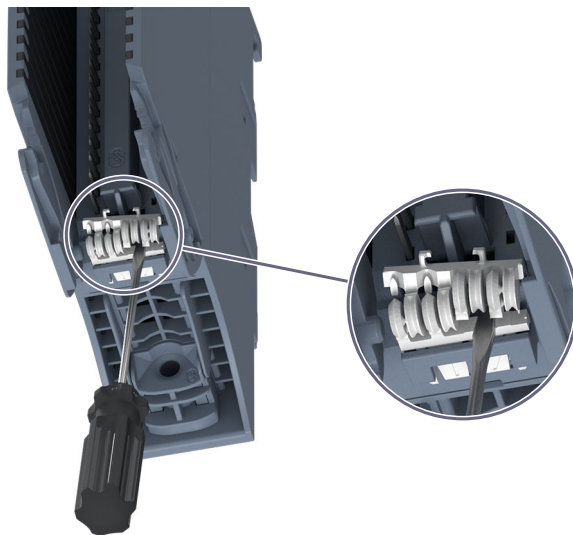
Figure 15-7 Breaking the coding element out of the I/O module

2. Insert the existing front connector into the new I/O module (same module type) until your hear it click into place.

15.3.3 Replacing a front connector

Introduction

- When the front connector is first inserted into the I/O module, a part of the mechanical coding element engages on the front connector.

- In the case of fail-safe modules, the electronic coding element with the PROFIsafe address of the F-module also engages completely in the front connector.

When you replace a defective front connector with a new front connector, you must transfer the coding element(s) to the new front connector.

Procedure

You have already removed the front connector from the module and loosened the wiring. If you are using the front connector for an analog module, you also need to remove the power supply element and shield element. Proceed as follows to replace the front connector:

1. Carefully remove the mechanical coding element from the front connector. Take care not to damage the coding element.
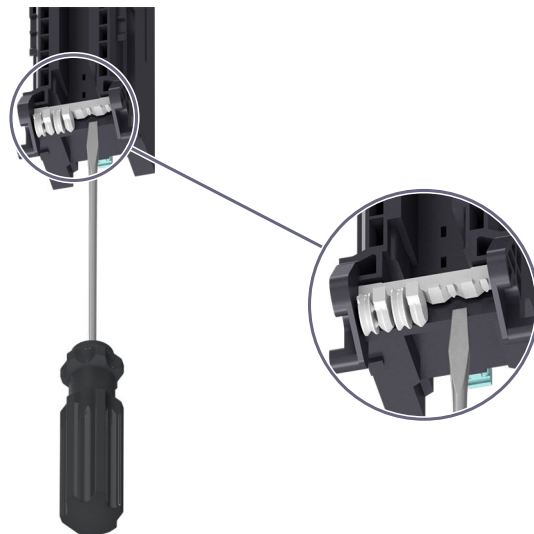
Figure 15-8 Removing the mechanical coding element from the front connector

---

NOTE

The coding elements are dependent on the module type.

---

2. Insert the removed mechanical coding element into the new front connector.
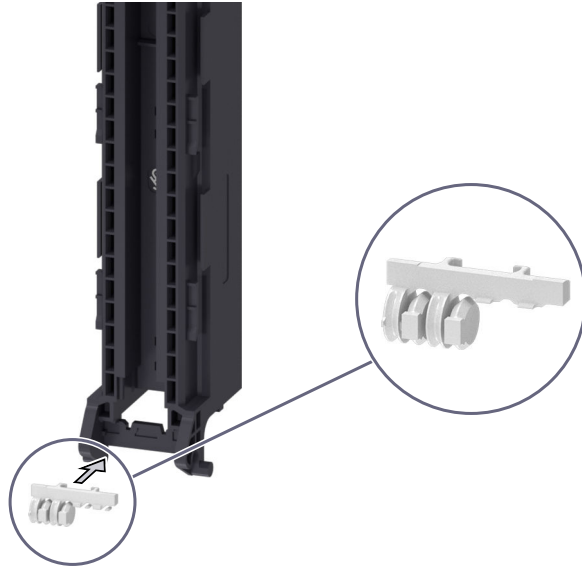

Figure 15-9   Inserting the mechanical coding element into a new front connector

3. Additionally for F-modules:

– Carefully remove the electronic coding element from the front connector. Take care not to damage the coding element.

– Insert the removed electronic coding element into the new front connector.

Figure 15-10   Removing the electronic coding element from the front connector and inserting it into a new front connector

4. Insert the new front connector into the existing I/O module, until your hear it click into place.

5. Wire the new front connector.

15.4 Replacing the coding element at the power connector of the system power supply and load current supply

Introduction

The coding consists of a 2-part coding element.

Ex factory a part of the coding element is inserted into the back side of the power connector. The other part is firmly inserted in the system power supply or load power supply.

This prevents the insertion of a power connector of a system power supply or load power supply into a module of a different type.

⚠ **DANGER**

Do not manipulate the coding element, or leave it off

- Changing or replacing the coding element can result in dangerous system states.
- To avoid damage, do not change or replace the coding element.
- You must not remove the coding element.

Replacement parts scenario

Insertion of the coding element into a new power connector in the case of a replacement part.

⚠ **DANGER**

Dangerous voltage

When installing the coding element, you must take into account the supply voltage of the system power supply and load power supply: 24 V DC, 24/48/60 V DC or 120/230 V AC/DC

Only install the coding element with switched-off voltage.

You must insert the coding element in such a way that the power connector matches the power supply module in terms of voltage.

Procedure

To replace the coding element on the power connector of the system power supply and load current supply, follow these steps:

1. Orient yourself using the labeling on the power cable connection.
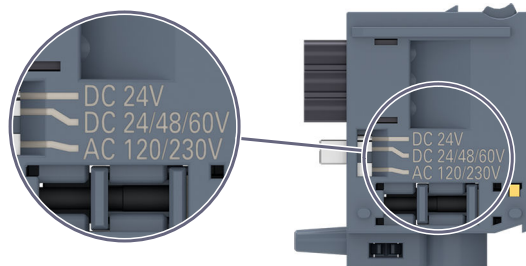

Figure 15-11 Labeling on the power connector

2. Orient yourself using the red marking on the coding element.

3. The coding element has 3 red markings. Turn the coding element in such a way that one of the 3 red markings corresponds to the voltage indicated on the connector.

4. Insert the coding element into the back side of the power cable connector, until you hear it click into place. The figure below shows you how to insert a coding element into a power cable connector for 24 V DC.
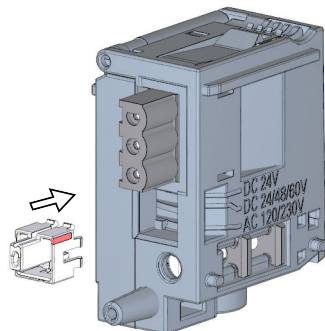
Figure 15-12 Inserting a coding element into a power connector

15.5   Firmware update

Introduction

Update the firmware of the CPU/interface module, display and the I/O modules using firmware files. The retentive data is retained after the execution of the firmware update.

We recommend that you always update to the latest firmware version available for the respective article number. The previous versions of the firmware are only intended as a backup to enable you to downgrade to the original version.

A firmware update has no effects on the user program of the CPU on which the update was performed. However, a downgrade can have effects on the user program if you use new functions in the user program which were not yet supported by the firmware of the CPU.

NOTE

Possible older firmware versions for CPU with firmware version as of V3.0

You can load a CPU with firmware version as of V3.0 with a STEP 7 project based on an earlier firmware version:

- For CPUs with article numbers 6ES751x-xxx03-0AB0: Firmware versions V2.9 to V1.8
- For CPUs with article number 6ES751x-xRx03-0AB0: Firmware versions V2.9 to V2.6
- For all other article numbers of the CPUs (firmware version lower than 4.0): Firmware versions V2.9 to V1.5

The CPU with firmware version as of V3.0 then responds like the CPU with the previous firmware version and supports only the functionality of this earlier version. This also applies to the configuration limits.

The following entry (https://support.industry.siemens.com/cs/de/en/view/109478459) lists all firmware versions for the S7-1500 CPUs including displays. You will also find a description of the new functions of the respective firmware versions.

Requirement

- You have downloaded the data/files for the firmware update from Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps).

  On this web site, select:

  – For the S7-1500 automation system: Automation Technology > Automation Systems > Industrial Automation Systems SIMATIC > Controllers > SIMATIC S7 Advanced Controller > SIMATIC S7-1500.

  – For the ET 200MP distributed I/O system: Automation Technology > Automation Systems > Industrial Automation Systems SIMATIC > SIMATIC ET 200 I/O systems > ET 200 systems for the cabinet > ET 200MP.
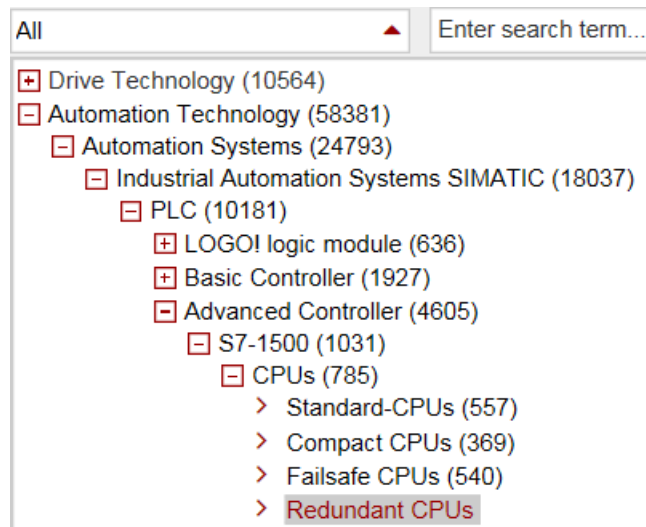
Figure 15-13 Product tree using the S7-1500 as an example:

From this position, navigate to the specific type of module that you want to update. To continue, click on the "Software downloads" link under "Support". Save the desired firmware update files.

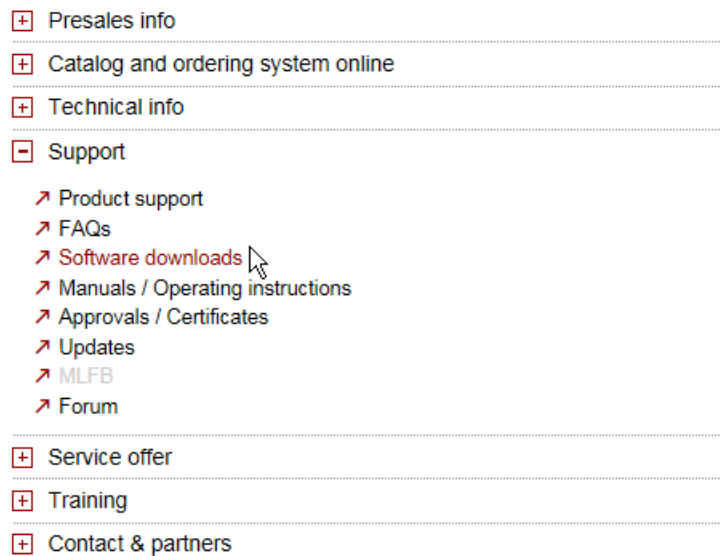Before installing the firmware update, make sure that the modules are not being used.

Figure 15-14 Selecting the software downloads

Additional requirement for fail-safe modules

⚠ WARNING
Check the firmware version for F-approval
When using a new firmware version, always check that the version is approved for use in the respective module.
The attachments of the certificate (https://support.automation.siemens.com/WW/view/en/49368678/134200) for SIMATIC Safety specify which firmware version is approved.

Special feature when updating the firmware of CPUs with Linux-based operating system

For the 1518(F)-4 PN/DP MFP CPUs, also observe the procedure for firmware updates from the CPU 1518-4 PN/DP MFP (https://support.industry.siemens.com/cs/ww/en/view/109749061) manual.

Options for the firmware update

The firmware update has to be carried out manually. There are the following options for performing a firmware update:

- Online in STEP 7 via Online & Diagnostics
- Online in STEP 7 via accessible devices (PROFINET)
- Via SIMATIC memory card: for CPU, display, and all centrally inserted modules
- Via the integrated Web server
- Online via the SIMATIC Automation Tool

The table below gives an overview of the various options for a firmware update.

Table 15-1 Overview of firmware update options

Firmware update	CPU	Central I/O module	Interface module	Distributed I/O module
STEP 7 (V12 or higher)	✔	✔	✔	✔
Accessible devices	✔	✔	✔	✔
SIMATIC memory card	✔	✔	--	--
Web server of the CPU	✔	✔	✔	✔
SIMATIC Automation Tool	✔	✔	✔	✔

Downtime during the firmware update

When you start a firmware update, for example online in STEP 7 via "Online & Diagnostics", the CPU goes into STOP mode and executes the firmware update. The time from start of the firmware update until RUN of the CPU with the new firmware takes a few minutes (typically < 3 minutes).

Installation of the firmware update

⚠ WARNING
Impermissible plant states possible
Installation of the firmware update causes the CPU to carry out a restart and go into STOP mode. The interface module changes into the station failure state. STOP or station failure can have an adverse effect on the operation of an online process or a machine.
Unexpected operation of a process or a machine can lead to fatal or severe injuries and/or to material damages.
Ensure before installing the firmware update that the CPU is not controlling any active process.

Procedure: online in STEP 7 via Online & diagnostics

Requirement: There is an online connection between the CPU/module and PG/PC.

Proceed as follows to perform an online firmware update via STEP 7:

1. Select the module in the device view.

2. Select the "Online & diagnostics" menu command from the shortcut menu.

3. In the "Functions" folder, select the "Firmware update" group.
   For a CPU, you can select whether you want to update the CPU or the CPU's display.

4. Click the "Browse" button to select the firmware update files in the "Firmware update" area.

5. Select the matching firmware file. The table in the firmware update area lists all modules for which an update is possible with the selected firmware file.

6. Click the "Run update" button. If the module can interpret the selected file, the file is downloaded to the module. If you must change the CPU mode, STEP 7 prompts you to do so with dialogs.

Updating the firmware

The "Run firmware after update" check box is always selected.

After a successful loading process the CPU includes imports the firmware and subsequently operates with the new firmware.

NOTE

If a firmware update is interrupted, you need to remove and insert the module before starting the firmware update again.

Procedure: online in STEP 7 via accessible devices

To perform a firmware update online via accessible devices, follow these steps:

1. From the "Online" menu, select the "Accessible devices" menu item.

2. In the Accessible devices dialog, search for the accessible devices for the selected PROFINET interface.

3. To go to a device in the project tree, select the desired device from the list of accessible devices and click the "Show" button.

4. In the project tree, select the "Online & diagnostics" option of the relevant device and perform the firmware update under the category Functions/Firmware Update (CPU, Display, Local modules).

You can find information on how to perform a firmware update when your project has no connection to a CPU in the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109779881).

Procedure via the SIMATIC memory card

Proceed as follows perform a firmware update via the SIMATIC memory card:

1. Insert a SIMATIC memory card into the SD card reader of your PG/PC.

2. To store the update file on the SIMATIC Memory Card, select the SIMATIC Memory Card in the "Card Reader/USB memory" folder in the project tree.

3. Select the "Card Reader/USB memory > Create firmware update memory card" command in the "Project" menu.

4. Use a file selection dialog to navigate to the firmware update file. In a further step you can decide whether you are deleting the content of the SIMATIC memory card or adding the firmware update files to the SIMATIC memory card.

5. Insert the SIMATIC memory card with the firmware update files into the CPU.

   The firmware update begins shortly after the SIMATIC memory card has been plugged.

   The display indicates that the CPU is in STOP mode, and that a firmware update is being executed: "STOP - FW UPDATE". The display shows the progress of the firmware update. The CPU shows any errors that occur during the firmware update on the display.

   The display shows a results screen after the completion of the firmware update.

6. Remove the SIMATIC Memory Card after the firmware update is complete.
   The RUN LED on the CPU lights up in yellow and the MAINT LED flashes yellow.
   If you subsequently wish to use the SIMATIC Memory Card as a program card, leave the SIMATIC Memory Card in the CPU. To do so, after completion of the firmware update, select the "Convert memory card" menu item on the display.

   Alternatively, you can convert the SIMATIC memory card to a program card via STEP 7.

NOTE

If your hardware configuration contains several modules, the CPU updates all affected module in the slot sequence, i.e. in ascending order of the module position in the STEP 7. device configuration.

NOTE

Memory size of the SIMATIC memory card

If you perform a firmware update via the SIMATIC memory card, you must use a large enough card based on the CPU used and the associated I/O modules.

Check the specified file sizes of the update files when downloading them from Siemens Industry Online Support. The file size information is especially important when you perform the firmware update not only for the CPU but also, e.g., for the associated I/O modules, communication modules. The total size of the update files must not exceed the available memory size of your SIMATIC memory card.

You can find more information on the capacity of SIMATIC Memory Cards in the section Accessories/spare parts (Page 425) and in the function manual Structure and use of the CPU memory (https://support.industry.siemens.com/cs/de/en/view/59193101).

Procedure: via the integrated Web server

The procedure is described in the Web server (https://support.automation.siemens.com/WW/view/en/59193560) Function Manual.

Procedure: online via the SIMATIC Automation Tool

The procedure is described in the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300) manual (included in the SIMATIC Automation Tool).

Special feature at a firmware update of analog modules

When you carry out a firmware update for analog modules, you have to supply 24 V DC load supply to the module through the infeed element.

Behavior after the firmware update

After the firmware update, check the firmware version of the updated module.

Possibilities for verifying the firmware update:

- Online via STEP 7 (e.g. Signature), SIMATIC Automation Tool or web server
- Offline via LED display, I&M0 data or display (if existing)

Reference

For more information on the topic of firmware update, refer to the STEP 7 online help and the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/89257657).

15.6 Reset to factory settings

15.6.1 Resetting the CPU to factory settings

Introduction

"Reset to factory settings" restores the CPU to its delivery state. The function deletes all information that was stored internally on the CPU.

Recommendation:

Switch the CPU to its as-delivered condition if:

- You remove a CPU and use it elsewhere with a different program.

- You store the CPU.

NOTE

Standard and F-CPUs with article number 6ES751x-xxx02-0AB0, compact CPUs with article number 6ES751x-xxx01-0AB0, technology, TF-CPUs with article number 6ES751x-xxx03-0AB0

"Reset to factory settings" restores the status of the operating mode button to the factory setting, i.e. the CPU remains in STOP mode. To set the CPU to RUN mode, local operation via the RUN button is required.

It does not matter here whether you perform the "Reset to factory settings" via the operating mode button, the display or STEP 7.

Options for resetting a CPU to factory settings

To reset the CPU to its delivery state, follow these steps:

- Via the operating mode keys/mode switches

- Using the display

- Using STEP 7

- Using the SIMATIC Automation Tool

Procedure via the mode selector keys (standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0)

Make sure that the CPU is in STOP mode (the CPU display shows STOP mode or RUN/STOP LED lights up yellow).

NOTE

Reset to factory settings ↔ Memory reset

The procedure described below also corresponds to the procedure for a memory reset:

- Key operation with inserted SIMATIC memory card: CPU executes a memory reset
- Key operation without inserted SIMATIC memory card: CPU executes reset to factory settings

---

Perform a reset to factory settings as follows:

1. Press the STOP mode selector key.

   Result: The STOP-ACTIVE and RUN/STOP LED light up yellow.

2. Remove the SIMATIC Memory Card from the CPU. Wait until the RUN/STOP LED stops flashing.

3. Press the STOP operating mode button until the RUN/STOP LED lights up for the 2nd time and remains continuously lit (after 3 seconds). After this, release the button.

4. Press the STOP mode selector key again within the next three seconds.

Result: The CPU executes a "Reset to factory settings", during which time the RUN/STOP LED flashes yellow. When the STOP-ACTIVE and RUN/STOP LED light up yellow, then the CPU has been reset to factory settings, and is in STOP mode. The "Reset to factory settings" event is entered into the diagnostics buffer.

NOTE

The IP address of the CPU is also deleted when the CPU is reset to the factory settings using the mode selector keys.

Procedure using the mode selector

Make sure that the CPU is in STOP operating state: The CPU display indicates the STOP operating mode. The RUN/STOP LED lights up yellow.

NOTE

Reset to factory settings ↔ Memory reset

The procedure described below corresponds to the procedure for a memory reset:

- Selector operation with inserted SIMATIC memory card: CPU executes a memory reset
- Selector operation without inserted SIMATIC memory card: CPU executes reset to factory settings

---

Restore the factory settings of the CPU as follows:

1. Set the mode selector to the STOP position.

   Result: The RUN/STOP LED lights up yellow.

2. Remove the SIMATIC Memory Card from the CPU. Wait until the RUN/STOP LED stops flashing.

3. Set the mode selector to the MRES position. Hold the mode selector in this position until the RUN/STOP LED lights up for the second time and remains lit (this takes three seconds). After this, release the selector.

4. Within the next three seconds, switch the mode selector back to the MRES position, and then back to STOP again.

Result: The CPU executes a "Reset to factory settings", during which time the RUN/STOP LED flashes yellow. When the RUN/STOP LED lights up yellow, then the CPU has been reset to factory settings, and is in the STOP mode. The "Reset to factory settings" event is entered into the diagnostics buffer.

NOTE

The IP address of the CPU is also deleted when the CPU is reset to the factory settings through the mode selector.

Procedure using the display

Make sure that the CPU is in STOP operating state: The CPU indicates STOP mode. The RUN/STOP LED lights up yellow.

To reach the desired menu command, "Factory setting", select the following sequence of menu commands. Confirm with "OK" after each selection.

- Settings → Reset → Factory settings

Result: The CPU executes a "Reset to factory settings", during which time the RUN/STOP LED flashes yellow. When the RUN/STOP LED lights up yellow, then the CPU has been reset to factory settings, and is in STOP mode. The "Reset to factory settings" event is entered into the diagnostics buffer.

NOTE

Resetting the CPU to factory settings via the display also deletes the IP-address of the CPU and the password for protecting confidential PLC configuration data.

Procedure using STEP 7

To reset a CPU to factory settings via STEP 7, follow these steps:

Make sure that there is an online connection to the CPU.

1. Open the Online and Diagnostics view of the CPU.

2. In the "Functions" folder, select the "Reset to factory settings" group.

3. If you want to keep the IP address, select the "Keep IP address" option button. If you want to delete the IP address, select the "Delete IP address" option button.

NOTE

"Delete IP address" deletes all IP addresses, regardless of how you established the online connection.

If a SIMATIC Memory Card is inserted, selecting the "Delete IP address" option has the following effect:

– The IP addresses are deleted and the CPU is reset to factory settings.

– The existing configuration (including IP address) on the SIMATIC Memory Card is then loaded into the CPU. If no configuration is stored (e.g. after the SIMATIC Memory Card has been erased or formatted), no new IP address is assigned.

---

4. Click the "Reset" button.

5. Click "OK" in response to the confirmation prompts.

Result: The CPU executes a "Reset to factory settings", during which time the RUN/STOP LED flashes yellow. When the RUN/STOP LED lights up in yellow, the CPU has been reset to factory settings and is in STOP mode. The "Reset to factory settings" event is entered into the diagnostics buffer.

Procedure using the SIMATIC Automation Tool

The procedure is described in the SIMATIC Automation Tool (https://support.industry.siemens.com/cs/ww/en/view/98161300) manual (included in the SIMATIC Automation Tool).

Result after resetting to factory settings

The following table provides an overview of the contents of the memory objects after the reset to factory settings.

Table 15-2 Result after resetting to factory settings

Memory object	Contents
Actual values of the data blocks, instance data blocks	Initialized
Bit memories, timers and counters	Initialized
Retentive tags of technology objects (e.g. adjustment values of absolute encoders)	Initialized

[1] Only for standard, F-CPUs with article number 6ES751x-xxx02-0AB0, compact CPUs with article number 6ES751x-xxx01-0AB0

Memory object	Contents
Entries in the diagnostics buffer	Are initialized, including a startup entry, that informs about the resetting to factory settings.
Entries in the syslog storage	Now only contains a startup entry that informs about the reset to factory settings.
IP address	Depends on the procedure: • Using mode switch: is deleted • Using display: is deleted • Using STEP 7: Depends on the setting of the "Retain IP-address"/"Delete IP-address" option button.
Device name	Set to "CPU"
Counter readings of the runtime meters	Initialized
Time of day	Is set to "00:00:00, 01.01.2012"
CPU operating mode	The CPU is set to STOP.
Operating mode of the CPU	"STOP Active" is activated [1]
Deleting passwords for protecting confidential PLC configuration data	Depends on the procedure: • Using the mode selector / mode selector keys: Retained • Using the display: is deleted • Using STEP 7: Depends on the setting of the "Delete password for the protection of confidential PLC configuration data" option button

[1] Only for standard, F-CPUs with article number 6ES751x-xxx02-0AB0, compact CPUs with article number 6ES751x-xxx01-0AB0

If there was a SIMATIC Memory Card inserted in the CPU prior to the reset to factory settings, the CPU loads the configuration contained on the SIMATIC Memory Card (hardware and software):

• A configured IP address is then valid again.

• If you have backed up adjustment values of absolute encoders on the SIMATIC Memory Card with the "MC_SaveAbsoluteEncoderData" instruction, these become valid after the reset to factory settings with SIMATIC Memory Card inserted in the CPU.

NOTE

Password for protecting confidential configuration data after resetting the CPU to factory settings

• **Via the mode switch / mode selector keys (SIMATIC Memory Card is not inserted):** The password for protection of confidential configuration data is retained.

• **Using the display:** The password for protection of confidential configuration data is deleted.

• **Using STEP 7:** The password for protection of confidential configuration data is retained. The password is only deleted when the "Delete password for protection of confidential PLC configuration data" option is set.

You can find more information on the password for protection of confidential configuration data in the Communication (https://support.industry.siemens.com/cs/ww/de/view/59192925/en) Function Manual.

Reference

More information on "Reset to factory settings" can be found in the Function Manual Structure and use of the CPU memory (https://support.automation.siemens.com/WW/view/en/59193101) in the section on memory areas and retentivity, and in the online help for STEP 7. For information on the memory reset of the CPU, refer to the section CPU memory reset .

15.6.2 Resetting interface module (PROFINET IO) to factory settings

Introduction

The interface module can be reset to its factory state using "Reset to factory settings".

Method of resetting an interface module to factory settings

- Via STEP 7 (online via PROFINET IO)

Procedure using STEP 7

To reset an interface module to factory settings via STEP 7, follow these steps:

Make sure that an online connection to the interface module exists.

1. Open the online and diagnostics view of the interface module.

2. In the "Functions" folder, select the "Reset to factory settings" group.

3. Click the "Reset" button.

4. Click "OK" in response to the confirmation prompts.

Result: The interface module then performs a "Reset to factory settings".

Result after resetting to factory settings

Table 15-3 Properties of the interface module when shipped

Properties	Value
Parameter	Default setting
IP address	Not present
Device name	Not present
MAC address	Present
I&M data	Identification data (I&M0) present Maintenance data (I&M1, 2, 3) reset
Firmware version	Present

NOTE

Failure of downstream stations is possible

Stations downstream from the interface module can fail when the factory settings are restored on an interface module.

NOTE

Substitute value behavior of the installed I/O modules during reset to factory settings

The I/O modules in the station do not have the configured status after a "reset to factory settings". The interface module does not acquire any input data and does not output any output data.

Reference

You will find more information on the procedure in the STEP 7 online help.

15.7 Fault reactions with fail-safe modules

Safe state (safety concept)

The basic principle behind the safety concept is the existence of a safe state for all process variables.

NOTE

For fail-safe input and output modules, this safe state is the value "0".

Fault reactions and startup of the F-system

The safety function requires that substitute values (safe state) be output instead of process values for a fail-safe module (**passivation of the fail-safe module**) in the following cases:

- When the F-system is started up

- If errors are detected during safety-related communication between the F-CPU and the F-module via the PROFIsafe safety protocol (communication error)

- If fail-safe I/O faults or channel faults are detected (e.g., wire break, discrepancy error)

Detected faults are written to the diagnostic buffer of the F-CPU and communicated to the safety program in the F-CPU.

F-modules cannot save errors as retentive data. When the system is powered down and then restarted, any faults still existing are detected again during startup. However, you have the option of saving faults in your safety program.

⚠ **WARNING**

Channel faults do not trigger any diagnostic reactions or error handling for channels that have been set to "deactivated" in STEP 7, even if this channel is affected indirectly by a channel group fault (channel parameter "activated/deactivated").

Remedying faults in the F-system

To remedy faults in your F-system, follow the procedure described in IEC 61508-1:2010 section 7.15.2.4 and IEC 61508-2:2010 section 7.6.2.1 e.

The following steps must be performed:

1. Diagnostic and repair of the fault

2. Revalidation of the safety function

3. Recording in the service report

Fail-safe value output for F-modules

In the case of F-modules with inputs, if there is passivation, the F-system provides substitute values (0) for the safety program instead of the process data pending at the fail-safe inputs.

In the case of F-modules with outputs, if there is passivation, the F-system transfers substitute values (0) to the fail-safe outputs instead of the output values provided by the safety program. The output channels are de-energized. This also applies when the F-CPU goes into STOP mode. The parameter assignment of fail-safe values is not possible.

Substitute values are used either for the relevant channel only or for all channels of the relevant fail-safe module, depending on:

- The F-system used
- The type of fault that occurred (fail-safe I/O fault, channel fault or communication error)
- The parameter assignment of the F-module

Reintegration of a fail-safe module

The system changes from fail-safe to process values (reintegration of an F-module) either automatically or only after user acknowledgment in the safety program. If channel faults occur, it may be necessary to remove and reinsert the F-module. A detailed listing of faults requiring removal and insertion of the F-module can be found in the section Diagnostic messages of the respective F-module.

After reintegration, the following occurs:

- In the case of an F-module with inputs, the process data pending at the fail-safe inputs is made available to the safety program again
- In the case of an F-module with outputs, the output values provided in the safety program are transferred to the fail-safe outputs again

Additional information on passivation and reintegration

For additional information on passivation and reintegration of F-I/O, refer to the SIMATIC Safety, Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126) manual.

Reaction of the F-module with inputs to communication errors

F-modules with inputs respond differently to communication errors compared to other errors.

If a communication error is detected, the current process values remain set at the inputs of the F-module. There is no passivation of the channels. The current process values are passivated in the F-CPU.

15.8 Maintenance and repair

The components of the S7-1500 automation system/ET 200MP distributed I/O system are maintenance-free.

NOTE

Repairs to the components of the S7-1500 automation system/ET 200MP distributed I/O system may only be carried out by the manufacturer.

Test and service functions

<div style="text-align: right; font-size: 3em;">**16**</div>

16.1 Test functions

Introduction

You can test the operation of your user program on the CPU. You monitor signal states and values of tags, and preassign tags with values so that you can simulate specific situations for program execution.

NOTE

Using test functions

Using test functions affects the program execution time and thus the cycle and response times of the controller to a slight extent (a few milliseconds).

Requirements

- There is an online connection to the relevant CPU.
- An executable user program is available in the CPU.

Test options

- Testing with program status
- Testing with breakpoints
- Testing with a watch table
- Testing with a force table
- Testing with a PLC tag table
- Testing with a data block editor
- Testing with the LED flash test
- Testing with a trace function

Testing with program status

The program status allows you to monitor the execution of the program. You can hereby display the values of operands and the results of logic operations (RLO). This allows you to detect and fix logical errors in your program.

NOTE

Restrictions with the "Program status" function

Monitoring loops can significantly increase the cycle time. The increase in cycle time depends on the following factors:

- The number of tags to be monitored
- The actual numbers of loops run through

⚠ **WARNING**

Testing with program status

A test with the "Program status" function can cause serious damage to property or injury to persons if there are functional disturbances or program errors.

Make sure that you take appropriate measures to exclude the risk of hazardous conditions occurring before running a test with the "Program status" function!

Testing with breakpoints

With this test option, you set breakpoints in your program, establish an online connection, and enable the breakpoints on the CPU. You then execute a program from one breakpoint to another.

Requirements:

- Setting breakpoints is possible in the programming language SCL or STL.
- You can only set breakpoints in the startup OB (OB 100) when the CPU is in STOP mode.

Testing with breakpoints provides you with the following advantages:

- Localization of logic errors step by step
- Simple and quick analysis of complex programs prior to actual commissioning
- Recording of current values within individual executed loops
- Use of breakpoints for program validation also possible in SCL/STL networks within LAD/FBD blocks

---

NOTE

Restriction during testing with breakpoints

- When you test with breakpoints, there is a risk of overwriting the cycle time of the CPU.
- If you are using technology objects and test them with breakpoints, the CPU switches to STOP mode.

NOTE

F-System SIMATIC Safety

Setting breakpoints in the standard user program results in errors in the safety program:

- Sequence of F cycle time monitoring
- Error in communication with the F-I/O
- Error during safety-oriented CPU-CPU communication
- Internal CPU error

If you nevertheless want to use breakpoints for testing, you must disable safety mode. This will result in the following errors:

- Error in communication with the F-I/O
- Error during safety-oriented CPU-CPU communication

Testing with watch tables

The following functions are available in the watch table:

- Monitoring of tags

  You can use the watch tables to monitor the current values of the individual tags of a user program or a CPU on the programming device/PC, on the display of the CPU, and on the web server. A symbolic name for the tags must be specified in the "Name" column of the watch table to allow the display of the CPU and the web server to show the value of the tags.

  You monitor the following operand areas:

  – Inputs and outputs (process image) and bit memory

  – Contents of data blocks

  – Peripheral inputs and peripheral outputs

  – Timers and counters

- Modifying tags

  Use this function to assign fixed values to the individual tags of a user program or CPU on the PG/PC. Modifying is also possible with Test with program status.

  The following operand areas are modifiable:

  – Inputs and outputs (process image) and bit memory

  – Contents of data blocks

  – Peripheral inputs and peripheral outputs (for example, %I0.0:P, %Q0.0:P)

  – Timers and counters

- "Enable peripheral outputs" and "Modify now"

  These two functions enable you to assign fixed values to individual peripheral outputs of a CPU in the STOP mode. You can also use them to check your wiring.

Testing with a force table

The following functions are available in the force table:

- Monitoring of tags

  Force tables are used to monitor the actual values of the individual tags of a CPU user program or a CPU

  - On the PG/PC
  - On the display of the CPU
  - On the web server

  You monitor the table with or without a trigger condition.

  A symbolic name for the tags must be specified in the "Name" column of the force table in order that the display of the CPU and the web server can display the value of the tags.

  You monitor the following tags:

  - Bit memory
  - Contents of data blocks
  - Peripheral inputs

- Modifying tags

  You use this function to assign fixed values to individual tags of a user program or a CPU on the programming device/PC or on the display of the CPU. Modifying is also possible with Test with program status.

  The following tags are modifiable:

  - Bit memory
  - Contents of data blocks
  - Peripheral inputs (e.g. %I0.0:P)

- Forcing of peripheral inputs and peripheral outputs

  You can force individual peripheral inputs or peripheral outputs.

  - Peripheral inputs: Forcing of peripheral inputs (for example %I0.0:P) is a "bypassing" of sensors / inputs by the specification of fixed values to the program. The program receives the force value instead of the actual input value (via process image or via direct access).
  - Peripheral outputs: Forcing of peripheral outputs (for example %Q0.0:P) is a "bypassing" of the complete program by the specification of fixed values to the actuators.

With the force table you can simulate different test environments and also overwrite tags in the CPU with a fixed value. This enables you to intervene in the running process in a regulating way.

Difference between modifying and forcing

The fundamental difference between the modifying and forcing functions consists in the storage behavior:

- Modifying: Modifying of tags is an online function and is not stored in the CPU. You can end modifying of tags in the watch table or force table or by terminating the online connection.

- Forcing: A force job is written to the SIMATIC memory card and is retained after a POWER OFF. The S7-1500 CPU displays an active force job with a corresponding symbol. You can only end the forcing of peripheral inputs and peripheral outputs in the force table.

Testing with a PLC tag table

You can monitor the current data values of tags in the CPU directly in the PLC tag table. To do so, open the PLC tag table and start the monitoring.

You also have the option of copying PLC tags to a watch table or force table so that you can monitor, control or force them in the table.

Testing with a data block editor

The data block editor offers different options for monitoring and modifying tags. These functions directly access the actual values of the tags in the online program. Actual values are the current values of tags in the CPU work memory at any moment during program execution. The following functions for monitoring and modifying are available in the database editor.

- Monitor tags online

- Modify individual actual values

- Create a snapshot of the actual values

- Overwrite actual values with a snapshot

NOTE

Setting data values during commissioning

During plant commissioning, you often need to adjust data values to adapt the program to local conditions.

To this end, the declaration table offers a few functions for data blocks.

Testing with the LED flash test

In many online dialogs, you can perform an LED flash test. This feature is useful if you are not sure which device in the hardware configuration corresponds to the device currently selected in the software.

If you click on the "Flash LED" button in STEP 7 under Online & diagnostics (online access), an LED flashes on the device currently selected. The RUN/STOP, ERROR, and MAINT LEDs flash on the CPU. The LEDs flash until you cancel the flash test.

Testing with a trace function

> The trace function is used to record the CPU tags, depending on the settable trigger conditions. Tags are, for example, drive parameters or system and user tags of a CPU. The CPU saves the recordings. If necessary, you can display the recordings with STEP 7 and evaluate them.

> Procedure: The trace function can be called from the CPU's folder in the project tree, under the name "Traces".

> In connection with trace functions, please also note the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/102781176).

Simulation

> With STEP 7 you can run and test the hardware and software of the project in a simulated environment. Start the simulation using the menu command "Online" > "Simulation" > "Start".

Reference

> More information on the test functions can be found in the STEP 7 online help.

> More information about testing with trace functions is available in the Function Manual Using the trace and logic analyzer function (https://support.automation.siemens.com/WW/view/en/64897128).

16.2 Reading out/saving service data

Service data

> In addition to the contents of the diagnostics buffer, the service data contains a great deal more information about the internal status of the CPU. If a problem occurs with the CPU that you cannot resolve with other methods, send the service data via a Service Request to the Industry Online Support. More information on creating a Support Request is available in the following entry on the Internet (https://support.industry.siemens.com/cs/ww/en/view/18194667). The service data allows Industry Online Support to quickly analyze problems that have occurred.

NOTE

While reading out the service data of the CPU, you cannot simultaneously execute a download to the device.

Methods of reading service data

You can read service data with:

- the web server

- STEP 7

- the SIMATIC memory card

Procedure using the Web server

To read service data using the Web server, follow these steps:

1. Open a web browser that is suitable for communication with the CPU.

2. Enter the following address in the address bar of the web browser:
   https://<CPU IP address>/save_service_data, e.g. https://172.23.15.3/save_service_data

3. The service data page will appear on your screen, with a button for saving the service data.
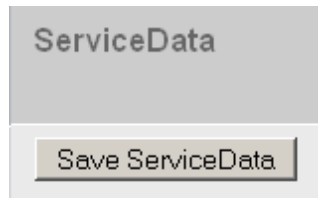
Figure 16-1 Saving service data via the Web server

4. Save the service data locally on your PC/programming device, by clicking "Save ServiceData".

Result: The data is saved in a .dmp file with the following naming convention: "<Article number> <Serial number> <Time stamp>.dmp". You can change the file name.

NOTE

If you have defined your user page as the home page of the Web server, direct access to the service data by inputting the IP address of the CPU is not possible. For more information on reading out service data via a user-defined page, refer to the Web server (https://support.automation.siemens.com/WW/view/en/59193560) function manual.

Procedure using STEP 7

You can find more information on saving service data of the CPU (and interface module) with the keyword "Saving service data" in the STEP 7 online help.

Procedure via the SIMATIC memory card

If no communication with the CPU is possible via Ethernet, use the SIMATIC memory card to read out the service data. In all other cases, read and back up the service data via the web server or STEP 7.

The procedure via the SIMATIC memory card is more complex than the other options. You must also ensure before backing up that there is sufficient memory space on the SIMATIC memory card.

To back up service data using the SIMATIC memory card, follow these steps:

1. Insert the SIMATIC memory card into the card reader of your PC / programming device.

2. Open the job file S7_JOB.S7S in an editor.

3. Overwrite the entry PROGRAM with the string DUMP in the editor.
   To ensure that the file size is exactly 4 bytes, do not use any spaces/line breaks/quotation marks.

4. Save the file under the existing file name.

5. Ensure that the SIMATIC Memory Card is not write-protected and insert the SIMATIC Memory Card in the card slot of the CPU. Up to CPU 1516 you need a card ≥ 32 MB and from CPU 1517 a card ≥ 2 GB.

Result: The CPU writes the service data file DUMP.S7S to the SIMATIC memory card and remains in STOP mode.

Service data transfer is complete when the STOP LED stops flashing and is lit continuously. If service data transfer has been successful, only the STOP LED lights up.

In the event of errors in transfer, the STOP LED is lit continuously and the ERROR LED flashes. In addition, the CPU creates a text file containing information about the error in the DUMP.S7S folder.

Technical specifications $\mathbf{17}$

Introduction

This chapter lists the technical specifications of the system:

- The standards and test values which the modules of the S7-1500 automation system/ET 200MP distributed I/O system comply with and fulfill.

- The test criteria according to which the S7-1500 automation system/ET 200MP distributed I/O system was tested.

Technical specifications for the modules

The technical specifications of the individual modules can be found in the manuals of the modules themselves. In the event of deviations between the statements in this document and the manuals, the statements in the manuals take priority.

17.1 Standards, approvals and safety instructions

Currently valid markings and approvals

NOTE

Details on the components of the S7-1500 automation system/ET 200MP distributed I/O system

The currently valid markings and approvals are printed on the components of the S7-1500 automation system/ET 200MP distributed I/O system.

Safety information

⚠️ **WARNING**

Personal injury and damage to property may occur

In hazardous areas, injury to persons and material damage may occur if you disconnect plug-in connections during operation of an S7-1500 automation system/ET 200MP distributed I/O system.

Always switch off the power to the S7-1500 automation system/ET 200MP distributed I/O system when disconnecting plug-in connections in hazardous atmospheres.

> ⚠️ **WARNING**
>
> **Explosion hazard**
>
> If you replace components, compliance with Class I, DIV 2 may become invalid.

> ⚠️ **WARNING**
>
> **Deployment requirements**
>
> This device is only suitable for use in Class I, Div. 2, Group A, B, C, D, or in non-hazardous areas.

Safety of the plant or the system

> **NOTICE**
>
> **Safety is the responsibility of the assembler**
>
> The safety of any plant or system incorporating the equipment is the responsibility of the assembler of the plant or system.

CE marking

The S7-1500 automation system/ET 200MP distributed I/O system complies with the harmonized European standards (EN) for programmable logic controllers published in the official journals of the European Union. The S7-1500 automation system/ET 200MP distributed I/O system meets the requirements and protection targets of the following directives:

- 2014/35/EU "Electrical equipment designed for use within certain voltage limits" (Low-Voltage Directive)

- 2014/30/EU "Electromagnetic Compatibility" (EMC Directive)

- 2014/34/EU "Equipment and protective systems intended for use in potentially explosive atmospheres" (Explosion Protection Directive)

- 2011/65/EU "Restriction of the use of certain hazardous substances in electrical and electronic equipment" (RoHS Directive)

- 2006/42/EC "Machinery Directive" for S7-1500/ET 200MP F-modules

EU declarations of conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg

The EU declarations of conformity are also available for download from the Siemens Industry Online Support website, under the keyword "Declaration of Conformity".

UKCA marking

The S7-1500 automation system / ET 200MP distributed I/O system complies with the designated British standards (BS) for programmable logic controllers published in the official consolidated list of the British Government. The S7-1500 automation system / ET 200MP distributed I/O system meets the requirements and protection targets of the following regulations and related amendments:

- Electrical Equipment (Safety) Regulations 2016 (Low Voltage)

- Electromagnetic Compatibility Regulations 2016 (EMC)

- Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 2016 (Explosion Protection)

- Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012 (RoHS)

- Supply of Machinery (Safety) Regulations 2008 for S7-1500/ET 200MP safety components (fail-safe modules)

UK Declarations of Conformity for the respective authorities are available from:

Siemens AG
Digital Industries
Factory Automation
DI FA TI COS TT
P.O. Box 1963
D-92209 Amberg

The UK Declaration of Conformity is also available for download from the Siemens Industry Online Support website under the keyword "Declaration of Conformity".

cULus approval

Underwriters Laboratories Inc. in accordance with

- UL 508 (Industrial Control Equipment) **OR** UL 61010-1 and UL 61010-2-201

- CAN/C22.2 No. 142 (Process Control Equipment) **OR** CAN/CSA. C22.2 No. 61010-1 and CAN/CSA C22.2 No. 61010-2 201

OR

cULus HAZ. LOC. approval

Underwriters Laboratories Inc. in accordance with

- UL 508 (Industrial Control Equipment) **OR** UL 61010-1 and UL 61010-2-201

- CANCSA C22.2 No. 142 (Process Control Equipment) **OR** CAN/CSA. C22.2 No. 61010-1 and CAN/CSA C22.2 No. 61010-2 201

- ANSI/ISA 12.12.01

- CAN/CSA C22.2 No. 213 (Hazardous Location)

APPROVED for use in
Class I, Division 2, Group A, B, C, D T4;
Class I, Zone 2, Group IIC T4

Installation Instructions for cULus haz.loc.

- WARNING - Explosion Hazard - Do not disconnect while circuit is live unless area is known to be non-hazardous.

- WARNING - Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2 or Zone 2.

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

- These products need to be connected by means of the front connector Cat. No. 6ES7592...

WARNING: EXPOSURE TO SOME CHEMICALS MAY DEGRADE THE SEALING PROPERTIES OF MATERIALS USED IN THE RELAYS.

FM approval

Factory Mutual Research (FM) according to

- Approval Standard Class Number 3611, 3600, 3810

- ANSI/UL 121201

- ANSI/UL 61010-1

- CAN/CSA C22.2 No. 213

- CAN/CSA C22.2 No. 61010-1

- CAN/CSA C22.2 No. 0-10

APPROVED for use in Class I, Division 2, Group A, B, C, D T4;
Class I, Zone 2, Group IIC T4

Installation Instructions for FM

- WARNING - Explosion Hazard - Do not disconnect while circuit is live unless area is known to be non-hazardous.

- WARNING - Explosion Hazard - Substitution of components may impair suitability for Class I, Division 2 or Zone 2.

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

- These products need to be connected by means of the front connector Cat. No. 6ES7592-1AM00-0XB0

WARNING: EXPOSURE TO SOME CHEMICALS MAY DEGRADE THE SEALING PROPERTIES OF MATERIALS USED IN THE RELAYS.

ATEX approval

According to EN 60079-15 (Electrical apparatus for potentially explosive atmospheres - Part 15: Type of protection "n") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex nA IIC T4 Gc

DEKRA 12ATEX0004 X

OR

According to EN IEC 60079-7 (Electrical apparatus for potentially explosive atmospheres - Part 7: Increased safety "e") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex ec IIC T4 Gc

DEKRA 20ATEX0003 X

T-CPUs:

According to EN 60079-15 (Electrical apparatus for potentially explosive atmospheres - Part 15: Type of protection "n") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex nA IIC T4 Gc

DEKRA 16ATEX0092 X

OR

According to EN IEC 60079-7 (Electrical apparatus for potentially explosive atmospheres - Part 7: Increased safety "e") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex ec IIC T4 Gc

DEKRA 21ATEX0046 X

Special conditions in hazardous areas:

- The equipment shall only be used in an area of not more than degree of pollution 2, as defined in EN 60664-1.

- The equipment shall be installed in a suitable enclosure providing a degree of protection not less than IP54 in accordance with EN IEC 60079-0. The ambient conditions must be taken into consideration for use.

- Provisions shall be made to prevent the nominal voltage from being exceeded by transient disturbances of more than 119 V.

System power supplies (PS)

According to EN IEC 60079-7 (Electrical apparatus for potentially explosive atmospheres - Part 7: Increased safety "e") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex ec IIC T4 Gc

DEKRA 23ATEX0077 X

UKEX approval

According to EN IEC 60079-7 (Explosive atmospheres – Part 7: Equipment protection by increased safety "e") and EN IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex ec IIC T4 Gc

DEKRA 21UKEX0008 X

T-CPUs:

According to EN IEC 60079-7 (Explosive atmospheres - Part 7: Equipment protection by increased safety "e") and EN IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex ecnA IIC T4 Gc

DEKRA 21UKEX0007 X

Special conditions in explosive atmospheres:

- The equipment shall only be used in an area of not more than degree of pollution 2, as defined in EN 60664-1.

- The equipment shall be installed in a suitable enclosure providing a degree of protection not less than IP54 in accordance with EN IEC 60079-0. The ambient conditions must be taken into consideration for use.

- Provisions shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 119 V.

System power supplies (PS)

According to EN IEC 60079-7 (Electrical apparatus for potentially explosive atmospheres - Part 7: Increased safety "e") and EN IEC 60079-0 (Electrical apparatus for potentially explosive gas atmospheres - Part 0: General requirements).

II 3 G Ex ecnA IIC T4 Gc

DEKRA 23UKEX6012 X

IECEx approval

According to IEC 60079-15 (Explosive atmospheres - Part 15: Equipment protection by type of protection "n") and IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex nA IIC T4 Gc

IECEx DEK 13.0010 X

OR

According to IEC 60079-7 (Explosive atmospheres - Part 7: Equipment protection by increased safety "e") and IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex ec IIC T4 Gc

IECEx DEK 19.0087 X

T-CPUs:

According to IEC 60079-15 (Explosive atmospheres - Part 15: Equipment protection by type of protection "n") and IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex nA IIC T4 Gc

IECEx DEK 16.0045 X

OR

According to IEC 60079-7 (Explosive atmospheres - Part 7: Equipment protection by increased safety "e") and IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex ec IIC T4 Gc

IECEx DEK 21.0028 X

Special conditions in hazardous areas:

*   The equipment shall only be used in an area of not more than pollution degree 2, as defined in IEC 60664-1.

*   The device must be installed in a suitable housing that ensures at least IP54 degree of protection according to IEC 60079-0. The ambient conditions must be taken into consideration for use.

*   Provisions shall be made to prevent the nominal voltage from being exceeded by transient disturbances of more than 119 V.

System power supplies (PS)

According to IEC 60079-7 (Explosive atmospheres - Part 7: Equipment protection by increased safety "e") and IEC 60079-0 (Explosive atmospheres - Part 0: Equipment - General requirements).

II 3 G Ex ec IIC T4 Gc

IECEx DEK 23.0057 X

CCCEx approval

In accordance with GB/T 3836.3 (Explosive atmospheres - Part 3: Equipment protection by type of protection "e"), GB/T 3836.1 (Explosive atmospheres - Part 1: Equipment - General requirements).

Ex ec IIC T4 Gc

Special conditions in hazardous areas:

*   The equipment shall only be used in an area of not more than degree of pollution 2, as defined in GB/T 16935.1.

*   The equipment shall be installed in a suitable enclosure providing a degree of protection not less than IP54 in accordance with GB/T 3836.1. The ambient conditions must be taken into consideration for use.

*   Provisions shall be made to prevent the nominal voltage from being exceeded by transient disturbances of more than 119 V.

RCM Declaration of conformity for Australia/New Zealand

The S7-1500 automation system/ET 200MP distributed I/O system fulfills the requirements of the standard IEC 61000-6-4.

Korea Certification

Please note that this device corresponds to limit value class A in terms of the emission of radio frequency interference. This device can be used in all areas, except residential areas.

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

Marking for the Eurasian Customs Union

EAC (Eurasian Conformity)

Customs Union of Russia, Belarus and Kazakhstan

Declaration of conformity with the technical requirements of the Customs Union (TR CU).

EN 61131-2

The S7-1500 automation system/ET 200MP distributed I/O system meets the requirements and criteria of EN 61131-2

(Programmable logic controllers, Part 2: Equipment requirements and tests) and the EMC requirements for use in Zone B.

IEC 61010-2-201

The S7-1500 automation system/ET 200MP distributed I/O system meets the requirements and criteria of the standard IEC 61010-2-201

(Safety regulations for electrical equipment for measurement, control, and laboratory use Part 2-201: Particular requirements for control equipment).

PROFINET standard

The PROFINET interfaces of the S7-1500 automation system/ET 200MP distributed I/O system are based on the standard IEC 61158 Type 10.

PROFIBUS standard

The PROFIBUS interfaces of the S7-1500 automation system/ET 200MP distributed I/O system are based on the standard IEC 61158 Type 3.

Marine approval

Classification societies:

- ABS (American Bureau of Shipping)

- BV (Bureau Veritas)

- DNV (Det Norske Veritas)

- LRS (Lloyds Register of Shipping)

- Class NK (Nippon Kaiji Kyokai)

- KR (Korean Register of Shipping)

- CCS (China Classification Society)

- RINA (Registro Italiano Navale)

At ambient temperatures above 60 °C, the following CPUs may experience a reduction in performance:

Article number	Short designation
6ES7516-3xP10-0AB0	CPU 1516T(F)-3 PN
6ES7517-3xQ10-0AB0	CPU 1517(F)-3 PN
	CPU 1517T(F)-3 PN
6ES7518-3xT10-0AB0	CPU 1518(F)-3 PN
	CPU 1518T(F)-3 PN

Information on how a CPU changes back into normal operation is available in the section "Configurable ambient conditions" in the Function Manual Cycle and response times (https://support.industry.siemens.com/cs/us/en/view/59193558).

Industrial use

The S7-1500 automation system ET 200MP / distributed I/O system is designed for the industrial field. It meets the following standards for this type of use:

- Requirements on interference emission EN 61000-6-4: 2019

- Requirements on immunity EN 61000-6-2: 2019

Use in mixed areas

Under certain conditions you can use the S7-1500 automation system ET 200MP / distributed I/O system in a mixed area. A mixed area is used for residential purposes and for commercial operations that do not significantly impact the residential purpose.

If you use the S7-1500 automation system / ET 200MP distributed I/O system in a mixed area, you must comply with the radio frequency interference limits of the generic standard EN 61000-6-3. Suitable measures for observing these limits for use in a mixed area are, for example:

- Installation of the S7-1500 automation system / ET 200MP I/O system in grounded control cabinets

- Use of noise filters in the supply lines

An additional individual acceptance test is also required.

Use in residential areas

NOTE

S7-1500 automation system / ET 200MP I/O system not intended for use in residential areas

The S7-1500 automation system ET 200MP / distributed I/O system is not intended for use in residential areas. If you use the S7-1500 automation system / ET 200MP distributed I/O system in residential areas, this may have an impact on radio/TV reception.

Environmental Product Declaration (EPD)

Siemens is committed to the development and production of environmentally compatible and sustainably produced equipment.

With the help of an Environmental Product Declaration (EPD), you can obtain information on the "ecological footprint" of your Siemens product.

The EPD is based on the ISO 14021 "Environmental labels and declarations – Self declared environmental claims – Type II" international standard.

EPDs are based on independently verified data from life cycle assessments, life cycle inventory analyses, or information modules which comply with the ISO 14040 series of standards. The EPD contains comprehensive data relating to ingredients and substances (REACH, RoHS), fire load, energy consumption, packaging, and disposal information for your Siemens product.

Reference

At Siemens Industry Online Support in Internet (https://www.siemens.com/automation/service&support) you will find:

- The current Environmental Product Declarations (EPDs) for Siemens products, with a search using the keyword "Environmental Product Declaration"

- Certificates for markings and approvals

17.2 Electromagnetic compatibility

Definition

Electromagnetic compatibility (EMC) is the ability of an electrical installation to function satisfactorily in its electromagnetic environment without interfering with that environment.

The S7-1500 automation system/ET 200MP distributed I/O system also meets the requirements of the EMC legislation for the European single market. The prerequisite for this is that the S7-1500/ET 200MP system complies with the requirements and guidelines relating to electrical equipment.

EMC in accordance with NE21

The S7-1500 automation system/ET 200MP distributed I/O system meets the EMC specifications of the NAMUR guideline NE21.

Pulse-shaped disturbances

The following table shows the electromagnetic compatibility of the S7-1500 automation system/ET 200MP distributed I/O system with regard to pulse-shaped disturbances.

Table 17-1 Pulse-shaped disturbances

Pulse-shaped disturbance	Tested with	Corresponds to degree of severity
Electrostatic discharge in accordance with IEC 61000-4-2 *)	Air discharge: ±8 kV Contact discharge: ±6 kV	3 3
Burst pulses (fast transient interference) in accordance with IEC 61000-4-4 *)	±2 kV (power supply cable) ±2 kV (signal cable >30 m) ±1 kV (signal cable <30 m)	3 4 3
High-energy single pulse (surge) in accordance with IEC 61000-4-5 **)		
• Asymmetric coupling (phase-ground) ***)	±1 kV (24 V DC supply cable)	2
	±1 kV (24 V DC signal/data line only > 30 m)	2
	2 kV (230 V AC supply cable)	3
• Symmetric coupling (phase-phase) ***)	±0.5 kV (24 V DC supply cable)	2
	±1 kV (230 V AC supply cable)	3
*) The maximum brief influence of analog modules during the duration of the EMC tests can be ±10% of the full-scale value. **) Analog value deviation beyond the limits of the nominal range and diagnostics possible. ***) If higher phase-ground or phase-phase values are required, you will need an additional external protective circuit (see Designing interference-free controllers (https://support.automation.siemens.com/WW/view/en/59193566) Function Manual).		

Sinusoidal disturbances

The following table shows the electromagnetic compatibility of the S7-1500 automation system/ET 200MP distributed I/O system with regard to sinusoidal disturbances (RF radiation).

Table 17-2 Sinusoidal disturbances with RF radiation

RF radiation in accordance with IEC 61000-4-3/NAMUR 21 Electromagnetic RF field, amplitude-modulated		Corresponds to degree of severity
80 MHz to 2.7 GHz	10 V/m	3
2.7 GHz to 6 GHz	3 V/m	2
80 % AM (1 kHz)		

The maximum short-term influence on analog modules during the duration of the EMC tests can be ±1% of the full-scale value.

The following table shows the electromagnetic compatibility of the S7-1500 automation system/ET 200MP distributed I/O system with regard to sinusoidal disturbances (RF coupling).

Table 17-3 Sinusoidal disturbances with RF coupling

RF coupling in accordance with IEC 61000-4-6	Corresponds to degree of severity
from 10 kHz	3
10 V_{rms}	
80 % AM (1 kHz)	
150 Ω source impedance	

The maximum short-term influence on analog modules during the duration of the EMC tests can be ±1% of the full-scale value.

Emission of radio interference

Interference emission of electromagnetic fields in accordance with EN 55016.

Table 17-4 Interference emission of electromagnetic fields

Frequency	Interference emission	Measuring distance
30 MHz to 230 MHz	< 40 dB (µV/m) QP	10 m
230 MHz to 1000 MHz	< 47 dB (µV/m) QP	10 m
from 1 to 3 GHz	< 76 dB (µV/m) P	3 m
from 3 to 6 GHz	< 80 dB (µV/m) P	3 m

Interference emission via the AC power supply according to EN 55016.

Table 17-5 Interference emission via the AC power supply

Frequency	Interference emission
from 0.15 to 0.5 MHz	< 89 dB (µV) Q < 76 dB (µV) M
from 0.5 to 30 MHz	< 83 dB (µV) Q < 70 dB (µV) M

17.3 Electromagnetic compatibility of fail-safe modules

Pulse-shaped interference

The fail-safe I/O modules S7-1500/ET 200MP **without** external protective circuit meet the severity level 2 for the high-energy individual pulse (surge) according to IEC 61000-4-5:2014.

Protecting S7-1500/ET 200MP against overvoltages with fail-safe modules

If your equipment requires protection from overvoltage, we recommend that you use an external protective circuit (surge filter) between the load voltage power supply and the load voltage input of the fail-safe modules to ensure surge immunity for the S7-1500 automation system/ET 200MP distributed I/O system with fail-safe modules.

NOTE

Lightning protection measures always require a case-by-case examination of the entire system. An almost complete protection from overvoltages, however, can only be achieved if the entire building surroundings have been designed for overvoltage protection. In particular, this involves structural measures in the building design phase.

If you want detailed information regarding overvoltage protection, we recommend that you contact your Siemens representative or a company specializing in lightning protection.

You can find more information on protection from overvoltage in the Designing interference-free controllers (https://support.automation.siemens.com/WW/view/en/59193566) function manual.

17.4   Shipping and storage conditions

Introduction

The S7-1500 automation system / ET 200MP I/O system meet the specifications regarding transport and storage conditions pursuant to IEC 61131-2. The following information applies to modules that are shipped and/or stored in their original packaging.

Shipping and storage conditions for modules

Table 17-6 Shipping and storage conditions

Type of condition	Permissible range
Free fall (in shipping package)	≤ 1 m
Temperature	from -40 °C to +70 °C
Barometric pressure	From 1140 to 540 hPa (corresponds to an altitude of -1000 to 5000 m)
Relative humidity	5% to 95%, without condensation
Sinusoidal vibrations in accordance with IEC 60068-2-6	5 - 9 Hz: 3.5 mm 9 - 500 Hz: 9.8 m/s^2
Shock in accordance with IEC 60068-2-27	250 m/s^2, 6 ms, 1000 shocks

17.5   Mechanical and climatic ambient conditions

Operating conditions

The S7-1500 automation system/ET 200MP distributed I/O system is suitable for use in weather-proof, fixed locations. The operating conditions are based on the requirements of IEC 61131-2:2017.

- OTH4 (S7-1500 CPUs: For the minimum ambient temperature, see the Climatic ambient temperatures table)

- STH4 (S7-1500 CPUs: Minimum ambient temperature -40 °C, minimum relative humidity 5%)

- TTH4 (S7-1500 CPUs: Minimum relative humidity 5%)

Test of mechanical ambient conditions

The table below provides important information with respect to the type and scope of the test of ambient mechanical conditions.

Table 17-7 Test of mechanical ambient conditions

Condition tested	Test Standard	Comment
Vibration	Vibration test according to IEC 60068-2-6 (Sinus)	Type of oscillation: Frequency sweeps with a rate of change of 1 octave/minute. 5 Hz ≤ f ≤ 8.4 Hz, constant amplitude 7 mm 8.4 Hz ≤ f ≤ 150 Hz, constant acceleration 2 g Duration of vibration: 10 frequency sweeps per axis, along each of the 3 mutually perpendicular axes
Shock	Shock, tested according to IEC 60068-2-27	Type of shock: Half-sine Shock intensity: 15 g max., duration 11 ms Direction of shock: 3 shocks each in (+/-) direction, along each of the 3 mutually perpendicular axes
Continuous shock	Shock, tested according to IEC 60068-2-27	Type of shock: Half-sine Shock intensity: 250 m/s^2 peak value, 6 ms duration Direction of shock: 1 000 shocks each in +/- direction, along each of the 3 mutually perpendicular axes

Reduction of vibrations

If your S7-1500 automation system/ET 200MP distributed I/O system is exposed to severe shock or vibration, take appropriate measures to reduce the acceleration or the amplitude.

We recommend installing the S7-1500 automation system/ET 200MP distributed I/O system on damping materials (for example, rubber-bonded metal mounting).

Climatic ambient conditions

The following table shows the permissible climatic ambient conditions for the S7-1500 automation system/ET 200MP distributed I/O system during operation.

Table 17-8 Climatic ambient conditions

Ambient conditions	Permissible range	Comments
Temperature: Horizontal and vertical mounting	See product data sheets for the respective module on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/td)	The lower permissible ambient temperature was extended for the S7-1500 automation system/ET 200MP distributed I/O system to -30 °C. Differences may exist for specific modules and depending on the mounting position and, if applicable, load. You must check the lower permissible ambient temperature for each module in the product data sheets. The product data sheets with daily updated technical specifications can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/td) at Industry Online Support. Enter the article number or the short description of the desired module on the website.

Ambient conditions	Permissible range	Comments
Temperature: Horizontal and vertical mounting	See product data sheets for the respective module on the Internet (https://support.industry.siemens.com/cs/ww/en/ps/td)	To increase the service life of the display, the display switches off when the permitted operating temperature is exceeded. At certain temperatures, the display switches off an on again. You can find more information in the technical specifications in the CPU manuals.
Temperature variation	10 K/h	-
Relative humidity	from 10 % to 95 %	Without condensation
Barometric pressure	from 1140 to 795 hPa	Corresponds to an altitude of -1 000 m to 2 000 m. See below under "Using the S7-1500 automation system/ET 200MP distributed I/O system over 2 000 m above sea level".
Pollutant concentration	ANSI/ISA-71.04 severity level G1; G2; G3	-

Using the S7-1500 automation system/ET 200MP distributed I/O system over 2 000 m above sea level

This information is available in the Use above 2 000 m above sea level and extended temperature range section.

17.6 Information on insulation tests, protection class, degree of protection and rated voltage

Insulation

The insulation is designed in accordance with the requirements of EN 61010-2-201.

NOTE

In the case of modules with 24 V DC (SELV/PELV) supply voltage, galvanic isolations are tested with 707 V DC (type test).

Pollution degree/overvoltage category in accordance with EN 61131-2: 2007 and IEC 61010-2-201

- Pollution degree 2
- Overvoltage category: II

Protection class according to IEC 61131-2: 2007 and IEC 61010-2-201

The S7-1500 automation system/ET 200MP distributed I/O system meets protection class I and contains parts of protection classes II and III.

Degree of protection IP20

Degree of protection IP20 in accordance with IEC 60529 for all modules of the S7-1500 automation system/ET 200MP distributed I/O system:

- Protection against contact with standard test fingers
- Protection against foreign objects with diameters in excess of 12.5 mm
- No protection against water

Rated voltage for operation

The S7-1500 automation system/ET 200MP distributed I/O system works with the rated voltages and corresponding tolerances listed in the following table.

Note the supply voltage of each module when selecting the rated voltage.

Table 17-9 Rated voltage of all modules of the S7-1500 automation system/ET 200MP distributed I/O system for operation

rated voltage	Tolerance range
24 V DC	19.2 V DC to 28.8 V DC [1]
48 V DC	40.8 to 57.6 V DC
60 V DC	51.0 to 72.0 V DC
120 V AC	93 V AC to 132 V AC
230 V AC	187 V AC to 264 V AC

[1]   Static value: Generation as protective extra-low voltage with safe electrical isolation in accordance with IEC 61131-2 or IEC 61010-2-201.

17.7   Use of the S7-1500/ET 200MP in zone 2 hazardous areas

Reference

You can find more information in the product information Use of modules in a Zone 2 Hazardous Area (https://support.automation.siemens.com/WW/view/en/19692172).

Dimension drawings

<div style="text-align: right; font-size: 2em;">A</div>

A.1 Dimension drawings of the mounting rails

Mounting rail 160 mm
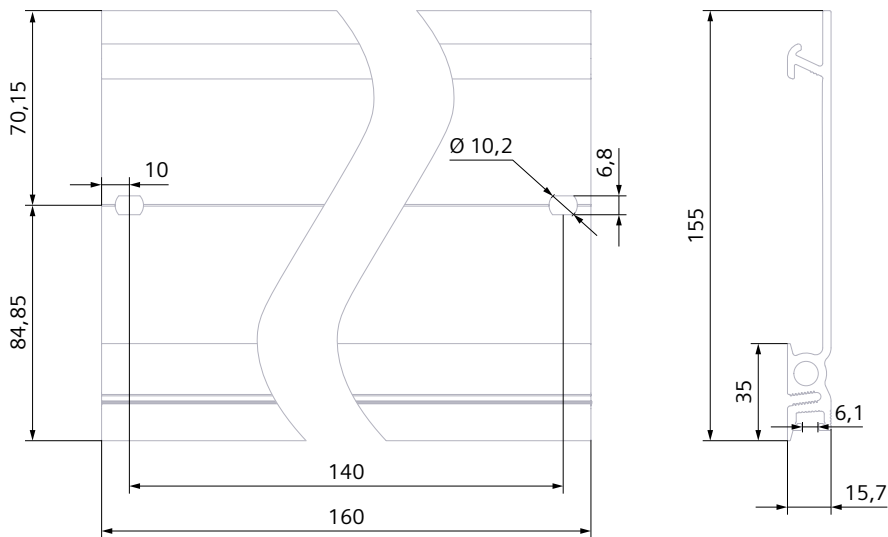
Figure A-1 Mounting rail 160 mm

Mounting rail 245 mm
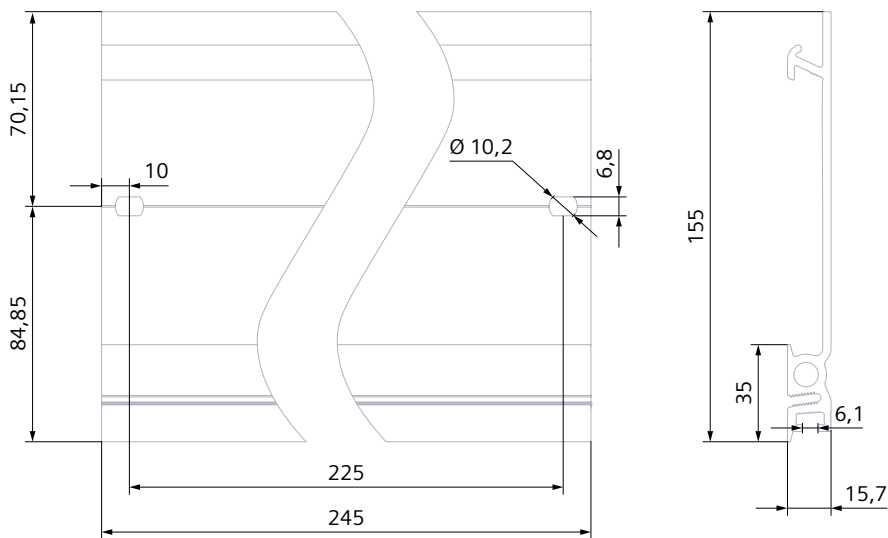
Figure A-2 Mounting rail 245 mm

Mounting rail 482.6 mm
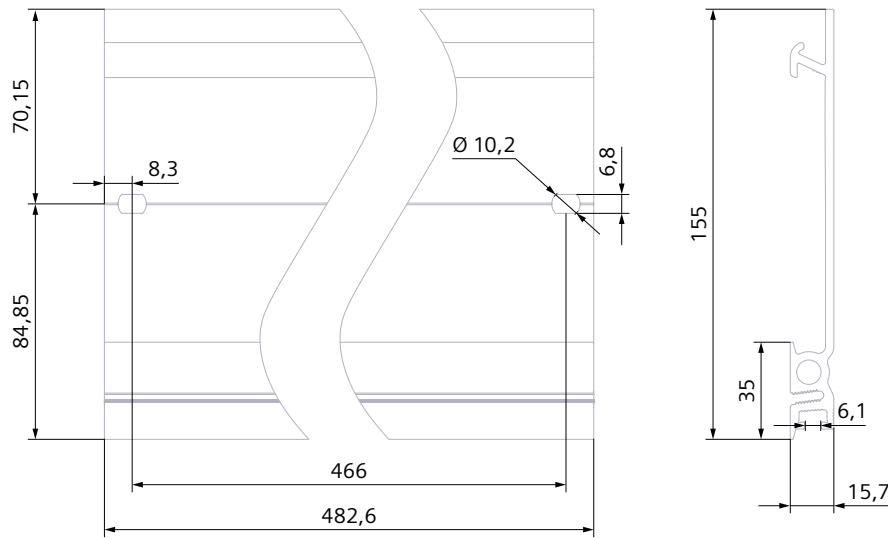
Figure A-3 Mounting rail 482.6 mm

Mounting rail 530 mm
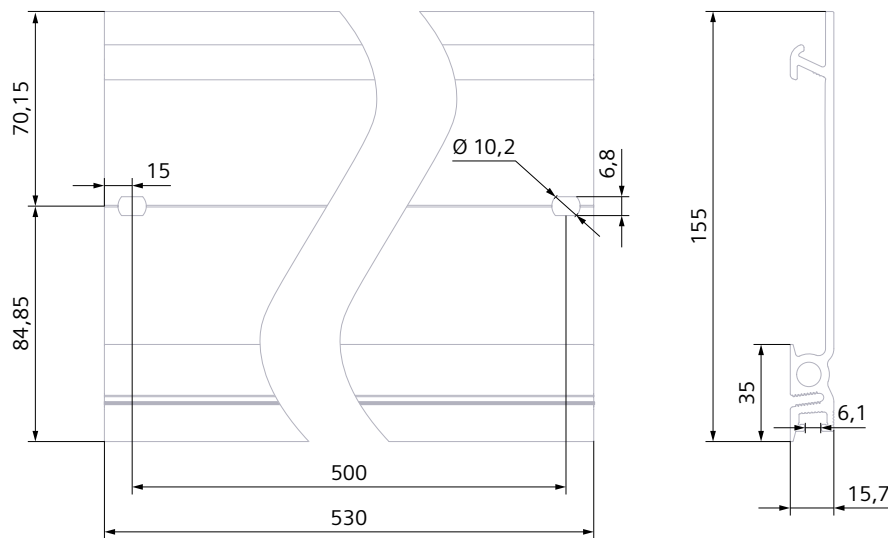
Figure A-4 Mounting rail 530 mm

Mounting rail 830 mm
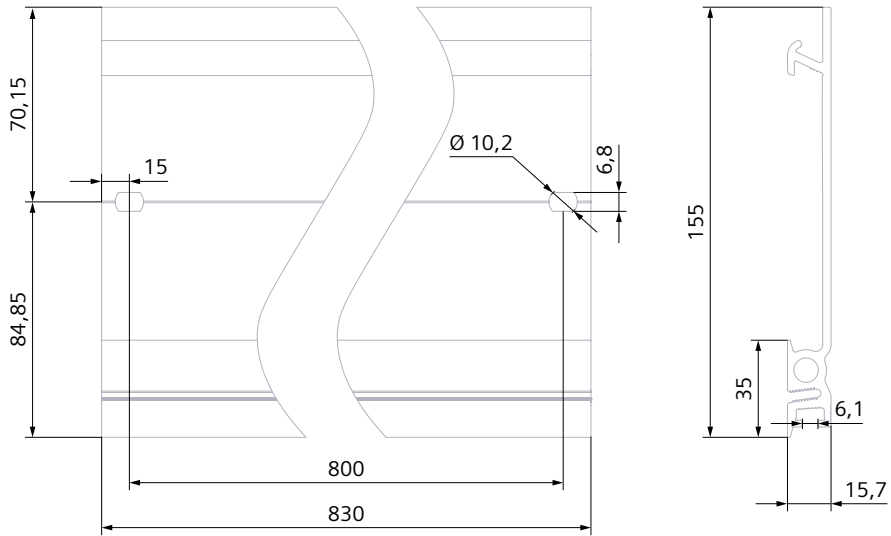
Figure A-5 Mounting rail 830 mm

Mounting rail 2 000 mm
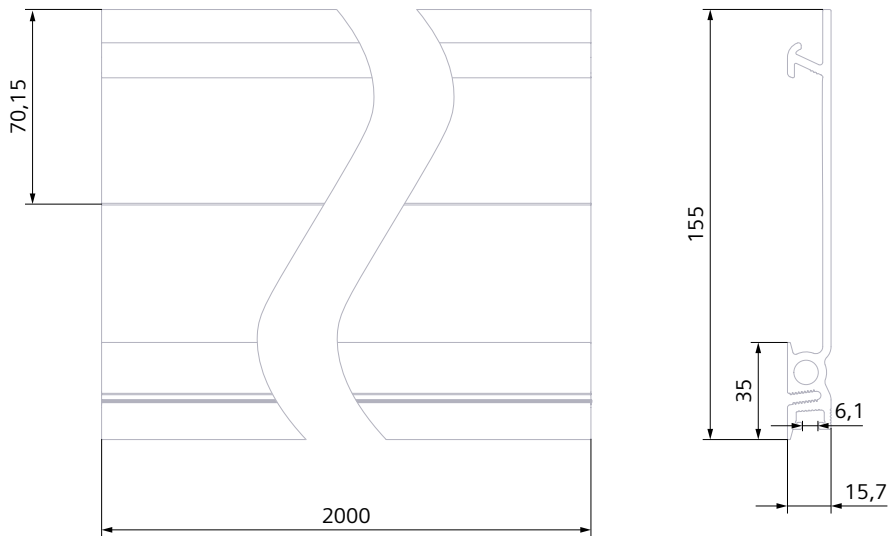
Figure A-6 Mounting rail 2 000 mm

A.2 Dimension drawing of shielding bracket for 35 mm modules
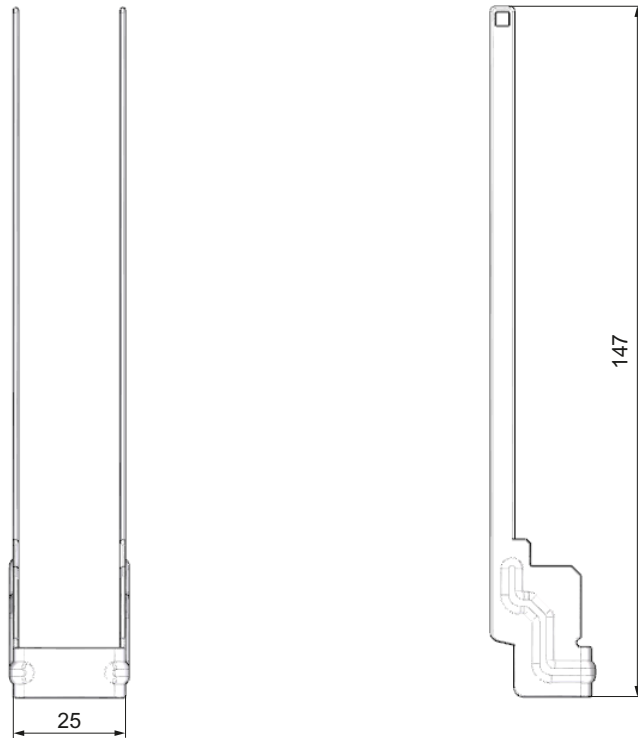
Figure A-7 Dimension drawing of shielding bracket for 35 mm modules

A.3 Dimension drawing of shielding bracket for 25 mm modules
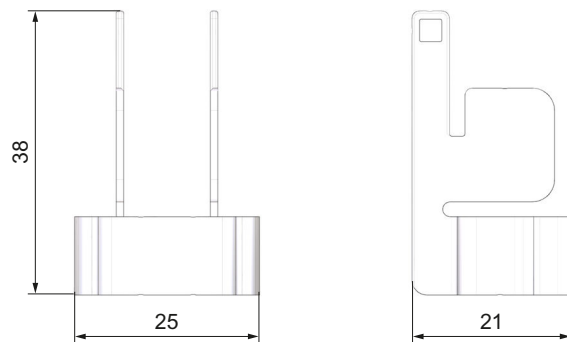
Figure A-8 Dimension drawing of shielding bracket for 25 mm modules

A.4 Dimension drawing of shielding bracket for 35 mm modules
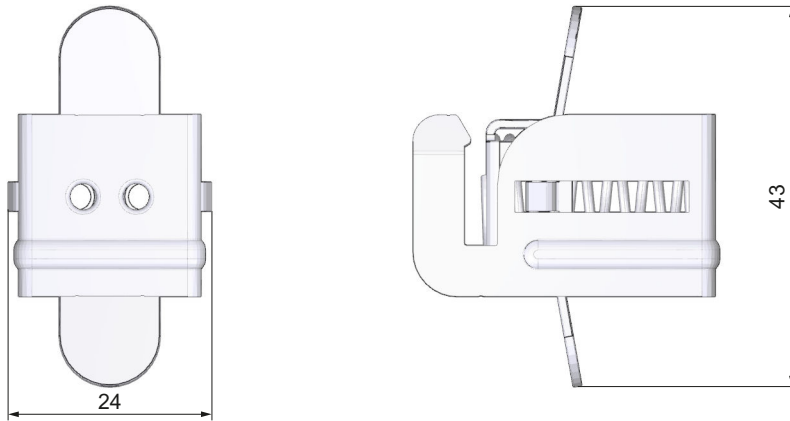
Figure A-9   Dimension drawing of shielding bracket for 35 mm modules

A.5 Dimension drawing of shielding bracket for 25 mm modules
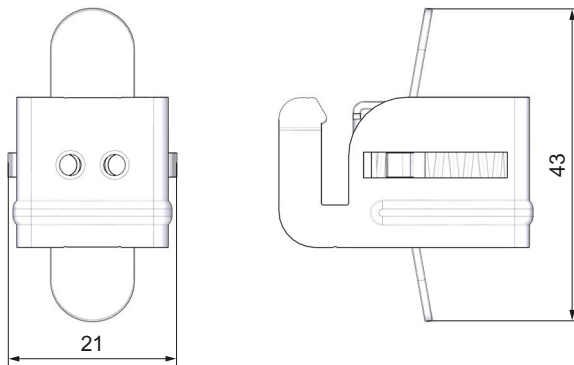
Figure A-10   Dimension drawing of shielding bracket for 25 mm modules

A.6 Dimension drawing of infeed element for 35 mm modules
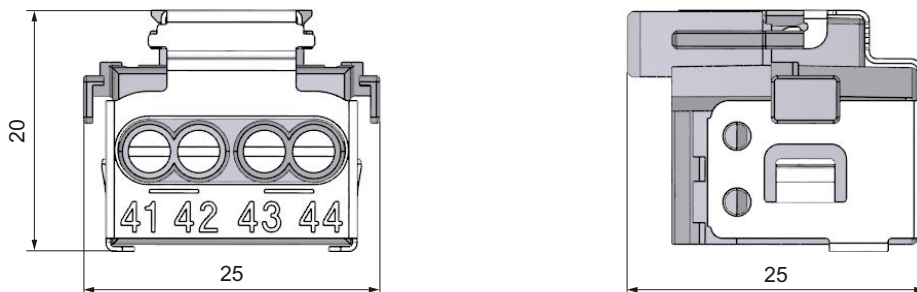
Figure A-11   Dimension drawing of infeed element for 35 mm modules

A.7   Dimension drawing of infeed element for 25 mm modules
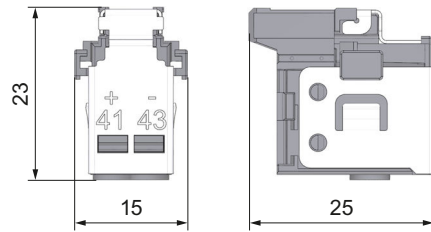
Figure A-12   Dimension drawing of infeed element for 25 mm modules

A.8   Dimension drawings of the labeling strips
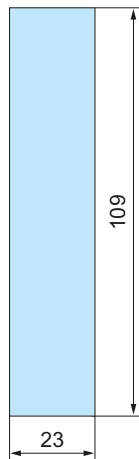
Figure A-13   Dimension drawing of labeling strips for 35 mm modules
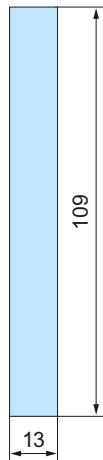
Figure A-14   Dimension drawing of labeling strips for 25 mm modules

A.9 Dimension drawing of test probe for measurement tap

To perform measurements on the front connector of the S7-1500/ET 200MP automation system, you need a test probe with the following properties:

- Maximum diameter at measuring tip: 1 mm

- Length of measuring tip: ≥ 10 mm
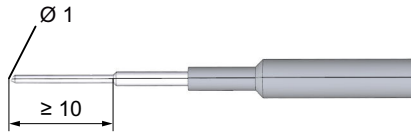
Figure A-15 Dimension drawing of test probe for measurement tap

Corresponding test probes are available from electrical retailers.

Accessories/spare parts

<div style="text-align: right">**B**</div>

Accessories for the S7-1500 automation system/ET 200MP distributed I/O system

Table B-1 General accessories

Designation	Article number
Mounting rail	
• Mounting rail, 160 mm (with drill holes)	6ES7590-1AB60-0AA0
• Mounting rail, 245 mm (with drill holes)	6ES7590-1AC40-0AA0
• Mounting rail, 482 mm (with drill holes)	6ES7590-1AE80-0AA0
• Mounting rail, 530 mm (with drill holes)	6ES7590-1AF30-0AA0
• Mounting rail, 830 mm (with drill holes)	6ES7590-1AJ30-0AA0
• Mounting rail, 2 000 mm (without drill holes) for cutting to length	6ES7590-1BC00-0AA0
DIN-rail adapter, 10 adapters, 10 hexagon socket screws and 10 washers	6ES7590-6AA00-0AA0
Active backplane bus	
• For one interface module and 12 I/O modules (ST 1+12)	6ES7590--0BL00-0AA0
• For one interface module and 8 I/O modules (ST 1+8)	6ES7590-0BH00-0AA0
• For one interface module and 4 I/O modules (ST 1+4)	6ES7590-0BD00-0AA0
PE connection element for mounting rail, 2 000 mm (spare part), 20 units	6ES7590-5AA00-0AA0
Front connector (incl. four potential bridges, cable tie, and individual labeling strip) for 35 mm modules	
• Screw-type terminals, 40-pin	6ES7592-1AM00-0XB0
Front connector (incl. four potential bridges, cable tie, and individual labeling strip) for 35 mm modules	
• Push-in terminal (40-pin)	6ES7592-1BM00-0XB0
Front connector (incl. cable tie and individual labeling strip) for 25 mm modules	
• Push-in terminal (40-pin)	6ES7592-1BM00-0XA0
4-pole connection plug for supply voltage (spare part), 10 units	6ES7193-4JB00-0AA0
DIN A4 labeling sheet (10 x for labeling the 35 mm I/O modules)	
• Pre-perforated, AI gray	6ES7592-2AX00-0AA0
DIN A4 labeling sheet (10 x for labeling the 25 mm I/O modules)	
• Pre-perforated, AI gray	6ES7592-1AX00-0AA0
U connector (spare part), 5 units	6ES7590-0AA00-0AA0
I/O shielding set for 35 mm modules (consists of: Power supply element, shielding bracket, and shield connection clamp), (spare part), 5 units	6ES7590-5CA00-0AA0

'* The PROFIBUS FastConnect bus connector 0BB70 is supplied with the IM 155-5 DP ST interface module and can also be ordered as a spare part.

Designation	Article number
I/O shielding set for 25 mm modules (consists of: Power supply element, shielding bracket, and shield connection clamp), (spare part), 4 units	6ES7590-5CA10-0XA0
Shield clamp (spare part), 10 units	6ES7590-5BA00-0AA0
Display 35 mm (spare part) for standard and F technology, TF-CPUs up to article number 6ES751x-xxx01-0AB0, compact CPUs with article number 6ES751x-xxx00-0AB0	6ES7591-1AA01-0AA0
Display module 35 mm (spare part) for standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0	6ES7591-1AB00-0AA0
Display module 35 mm (spare part) for standard and F-CPUs, technology, TF-CPUs, compact CPUs as of article number 6ES751x-xxx03-0AB0	6ES7591-1AB10-0AA0
Protective cover 35 mm (spare part) with cutout for display and display keys for standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, compact CPUs as of article number 6ES751x-xxx01-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0, 5 units	6ES7591-4AB00-0AA0
Display 70 mm (spare part) for standard and F-technology, TF-CPUs up to article number 6ES751x-xxx01-0AB0	6ES7591-1BA02-0AA0
Display module 70 mm (spare part) for standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0	6ES7591-1BB00-0AA0
Protective cover 70 mm (spare part) with cutout for display and display keys for standard, F-CPUs as of article number 6ES751x-xxx02-0AB0, technology, TF-CPUs as of article number 6ES751x-xxx03-0AB0, 5 units	6ES7591-4BB00-0AA0
Power cable connector with coding element for power supplies (spare part), 10 units	6ES7590-8AA00-0AA0
Potential bridges for front connector (spare part), 20 units	6ES7592-3AA00-0AA0
Universal front cover for 35 mm I/O modules (spare part), 5 units	6ES7528-0AA00-7AA0 Consists of: • 5 x front cover • 5 x front labeling strip (per module - article number) • 5 x wiring diagram (per module article number)
Universal front cover for 25 mm I/O modules (spare part), 5 units	6ES7528-0AA00-0AA0 Consists of: • 5 x front cover • 5 x front labeling strip (per module - article number) • 5 x wiring diagram (per module article number)
Universal front cover for interface module (spare part), 5 units	6ES7528-0AA70-7AA0 Consists of: • 5 x front cover
Industrial Ethernet FastConnect RJ45 plug 180 degrees, 1 unit	6GK1901-1BB10-2AA0
Industrial Ethernet FastConnect RJ45 plug 180 degrees, 10 units	6GK1901-1BB10-2AB0

'* The PROFIBUS FastConnect bus connector 0BB70 is supplied with the IM 155-5 DP ST interface module and can also be ordered as a spare part.

Designation	Article number
Industrial Ethernet FastConnect RJ45 plug 90 degrees, 1 unit	6GK1901-1BB20-2AA0
Industrial Ethernet FastConnect RJ45 plug 90 degrees, 10 units	6GK1901-1BB20-2AB0
PROFIBUS-FastConnect bus connector without programming device socket, up to 12 MBaud, 1 unit	6ES7972-0BA70-0XA0
PROFIBUS FastConnect bus connector with programming device socket, up to 12 MBaud, 1 unit *	6ES7972-0BB70-0XA0
PROFIBUS-FastConnect bus connector without programming device socket, up to 12 MBaud, 1 unit	6ES7972-0BA52-0XA0
PROFIBUS FastConnect bus connector with programming device socket, up to 12 MBaud, 1 unit	6ES7972-0BB52-0XA0

'* The PROFIBUS FastConnect bus connector 0BB70 is supplied with the IM 155-5 DP ST interface module and can also be ordered as a spare part.

SIMATIC Memory Cards

Article number	Capacity
6ES7954-8LC0x-0AA0	4 MB
6ES7954-8LE0x-0AA0	12 MB
6ES7954-8LF0x-0AA0	24 MB
6ES7954-8LL0x-0AA0	256 MB
6ES7954-8LP0x-0AA0	2 GB
6ES7954-8LT0x-0AA0	32 GB

SIMATIC Memory Cards for S7-1500 Motion Control KinPlus

Article number	Capacity
6ES7954-8LP80-0AA0	2 GB
6ES7954-8LT80-0AA0	32 GB

Online catalog

Additional article numbers for the S7-1500 automation system/ET 200MP distributed I/O system can be found on the Internet (https://mall.industry.siemens.com) in the online catalog and online ordering system.

Accessories for S7 1500/ET 200MP fail-safe modules

Table B-2 Accessories for fail-safe modules

Designation	Article number
Electronic coding element with rewritable memory for fail-safe modules (spare part), 5 units	6ES7592-6EF00-1AA0
Front cover for 35 mm F-I/O modules (spare part), 5 units	6ES7528-0AA10-7AA0 Consists of: • 5 x front cover • 5 x front labeling strip (per module - article number) • 5 x wiring diagram (per module article number)
DIN A4 labeling sheet (10 x for labeling the fail-safe I/O modules), pre-perforated, yellow	6ES7592-2CX00-0AA0

Use over 2000 m above sea level and extended temperature range

C

C.1 Ambient temperature and installation altitude

Extension of the temperature range and the installation altitude

The previously permissible range of ambient temperatures of **0 °C** to 60 °C for the horizontal mounting position has been extended for a large number of modules to a range of ambient temperatures of **-30 °C** to 60 °C or **-25 °C** to 60 °C (in each case without condensation or icing). In addition, depending on the module, the permitted installation altitudes has been extended to installation height of up to 5,000 meters.

The accessory components offered for S7-1500/ET 200MP (labeling strips, shield terminals, mounting rails, front connectors, etc.) can also be used down to -30 °C and for altitudes up to 5 000 m.

The following tables show an overview of the current climatic ambient conditions for ambient temperature and installation altitude of modules of the S7-1500, ET 200MP product families.

Reference

The current status of the respective modules can be found in the online published technical specifications.

In general, the module-dependent extended climatic operating conditions are described in the "Technical specifications" section of the respective modules in the equipment manuals.

C.2 CPUs

Standard CPUs

CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CPU 1511-1 PN	6ES7511-1AK01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1511-1 PN	6ES7511-1AK02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1511-1 PN	6ES7511-1AL03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1513-1 PN	6ES7513-1AL01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1513-1 PN	6ES7513-1AL02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1513-1 PN	6ES7513-1AM03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1515-2 PN	6ES7515-2AM01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1515-2 PN	6ES7515-2AM02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1515-2 PN	6ES7515-2AN03-0AB0	-30 to +60	FS 01	5,000	FS 01

CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CPU 1516-3 PN/DP	6ES7516-3AN01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1516-3 PN/DP	6ES7516-3AN02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1516-3 PN/DP	6ES7516-3AP03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1517-3 PN	6ES7517-3AQ10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1517-3 PN/DP	6ES7517-3AP00-0AB0	0 to +60	FS 01	5,000	FS 05
CPU 1518-3 PN	6ES7518-3AT10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1518-4 PN/DP	6ES7518-4AP00-0AB0	0 to +60	FS 01	5,000	FS 05
CPU 1518-4 PN/DP O-DK	6ES7518-4AP00-3AB0	0 to +60	FS 01	5,000	FS 08
CPU 1518-4 PN/DP MFP	6ES7518-4AX00-1AB0	0 to +60	FS 01	5,000	FS 08

Compact CPUs

CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CPU 1511C-1 PN	6ES7511-1CK00-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1511C-1 PN	6ES7511-1CK01-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1511C-1 PN	6ES7511-1CL03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1512C-1 PN	6ES7512-1CK00-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1512C-1 PN	6ES7512-1CK01-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1512C-1 PN	6ES7512-1CM03-0AB0	-30 to +60	FS 01	5,000	FS 01

Fail-safe CPUs

CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CPU 1511F-1 PN	6ES7511-1FK01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1511F-1 PN	6ES7511-1FK02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1511F-1 PN	6ES7511-1FL03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1511TF-1 PN	6ES7511-1UK01-0AB0	0 to +60	FS 03	5,000	FS 03
CPU 1511TF-1 PN	6ES7511-1UL03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1513F-1 PN	6ES7513-1FL01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1513F-1 PN	6ES7513-1FL02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1513F-1 PN	6ES7513-1FM03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1515F-2 PN	6ES7515-2FM01-0AB0	0 to +60	FS 01	5,000	FS 03

CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [℃]	As of version	Max. altitude [m]	As of version
CPU 1515F-2 PN	6ES7515-2FM02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1515F-2 PN	6ES7515-2FN03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1515TF-2 PN	6ES7515-2UM01-0AB0	0 to +60	FS 03	5,000	FS 03
CPU 1515TF-2 PN	6ES7515-2UN03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1516F-3 PN/DP	6ES7516-3FN01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1516F-3 PN/DP	6ES7516-3FN02-0AB0	-25 to +60	FS 01	5,000	FS 01
CPU 1516F-3 PN/DP	6ES7516-3FP03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1516TF-3 PN	6ES7516-3UP10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1516TF-3 PN/DP	6ES7516-3UN00-0AB0	0 to +60	FS 05	5,000	FS 05
CPU 1517F-3 PN	6ES7517-3FQ10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1517F-3 PN/DP	6ES7517-3FP00-0AB0	0 to +60	FS 01	5,000	FS 05
CPU 1517F-3 PN/DP	6ES7517-3FP01-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1517TF-3 PN	6ES7517-3UQ10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1517TF-3 PN/DP	6ES7517-3UP00-0AB0	0 to +60	FS 04	5,000	FS 05
CPU 1518F-3 PN	6ES7518-3FT10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1518F-4 PN/DP	6ES7518-4FP00-0AB0	0 to +60	FS 01	5,000	FS 05
CPU 1518F-4 PN/DP ODK	6ES7518-4FP00-3AB0	0 to +60	FS 04	5,000	FS 05
CPU 1518F-4 PN/DP MFP	6ES7518-4FX00-1AB0	0 to +60	FS 01	5,000	FS 01
CPU 1518TF-3 PN	6ES7518-3UT10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1518TF-4 PN/DP	6ES7518-4UP00-0AB0	0 to +60	FS 10	5,000	FS 10

PFDavg and PFH values for F-CPUs for operating altitudes up to 3,000 m or 5,000 m.

Below you will find the probability of failure values (PFDavg and PFH values) for the fail-safe CPUs mentioned in the table with a service life of 20 years and with a repair time of 100 hours:

Operation in low demand mode in accordance with IEC 61508:2010: PFDavg = Average probability of a dangerous failure on demand	Operation in high demand or continuous mode in accordance with IEC 61508:2010: PFH = Average frequency of a dangerous failure [h-1]
< 2E-05	< 1E-09 at an installation altitude ≤ 3 000 m < 2E-09 at an installation altitude > 3 000 m to 5 000 m

Technology CPUs

CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CPU 1511T-1 PN	6ES7511-1TK01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1511T-1 PN	6ES7511-1TL03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1515T-2 PN	6ES7515-2TM01-0AB0	0 to +60	FS 01	5,000	FS 03
CPU 1515T-2 PN	6ES7515-2TN03-0AB0	-30 to +60	FS 01	5,000	FS 01
CPU 1516T-3 PN	6ES7516-3TP10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1516T-3 PN/DP	6ES7516-3TN00-0AB0	0 to +60	FS 01	5,000	FS 05
CPU 1517T-3 PN	6ES7517-3TQ10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1517T-3 PN/DP	6ES7517-3TP00-0AB0	0 to +60	FS 01	5,000	FS 05
CPU 1518T-3 PN	6ES7518-3TT10-0AB0	0 to +60	FS 01	5,000	FS 01
CPU 1518T-4 PN/DP	6ES7518-4TP00-0AB0	0 to +60	FS 01	5,000	FS 08

Replacement part displays

Replacement part displays for CPU	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CPU 1511-1 PN	6ES7591-1AA01-0AA0	0 to +60	FS 01	5,000	FS 01
CPU 1511F-1 PN					
CPU 1511C-1 PN					
CPU 1511T-1 PN					
CPU 1511TF-1 PN					
CPU 1512C-1 PN					
CPU 1513-1 PN					
CPU 1513F-1 PN					
CPU 1515-2 PN	6ES7591-1BA02-0AA0	0 to +60	FS 01	5,000	FS 01
CPU 1515F-2 PN					
CPU 1515T-2 PN					
CPU 1515TF-2 PN					
CPU 1516-3 PN/DP					
CPU 1516F-3 PN/DP					
CPU 1517-3 PN/DP					
CPU 1517F-3 PN/DP					
CPU 1518-4 PN/DP					
CPU 1518F-4 PN/DP					

Replacement part display modules

Replacement part display modules for S7-CPUs	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
35 mm	6ES7591-1AB00-0AA0	-25 to +60	FS 01	5,000	FS 01
70 mm	6ES7591-1BB00-0AA0				

C.3   S7-1500 I/O modules

Digital input modules

Digital input module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
DI 16x24VDC HF	6ES7521-1BH00-0AB0	-30 to +60	FS 05	5,000	FS 03
DI 16x24VDC HS	6ES7521-7BH00-0AB0	-30 to +60	FS 01	5,000	FS 01
DI 32x24VDC HF	6ES7521-1BL00-0AB0	-30 to +60	FS 05	5,000	FS 03
DI 64x24VDC SNK/SRC BA	6ES7521-1BP00-0AA0	-30 to +60	FS 01	5,000	FS 01
DI 16x24VDC SRC BA	6ES7521-1BH50-0AA0	0 to +60	FS 01	5,000	FS 01
DI 16x24VDC SRC BA	6ES7521-1BH50-0AA0	-25 to +60	FS 03	5,000	FS 05
DI 16x230VAC BA	6ES7521-1FH00-0AA0	0 to +60	FS 01	2,000	FS 01
DI 16x230VAC BA	6ES7521-1FH00-0AA0	-30 to +60	FS 03	2 000	FS 05
DI 16 x 24...125V UC HF	6ES7521-7EH00-0AB0	0 to +60	FS 01	2,000	FS 01
DI 16 x 24...125V UC HF	6ES7521-7EH00-0AB0	-30 to +60	FS 02	2 000	FS 01
DI 16x24VDC BA (25 mm)	6ES7521-1BH10-0AA0	0 to +60	FS 01	5,000	FS 01
DI 16x24VDC BA (25 mm)	6ES7521-1BH10-0AA0	-30 to +60	FS 03	5,000	FS 04
DI 32x24VDC BA (25 mm)	6ES7521-1BL10-0AA0	0 to +60	FS 01	5,000	FS 01
DI 32x24VDC BA (25 mm)	6ES7521-1BL10-0AA0	-30 to +60	FS 03	5,000	FS 04
DI 16xNamur HF	6ES7521-7TH00-0AB0	-30 to +60	FS 01	5,000	FS 01

Fail-safe digital input modules

Fail-safe digital input module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
F-DI 16X24VDC	6ES7526-1BH00-0AB0	0 to +60	FS 01	5,000	FS 01

Digital output modules

Digital output module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
DQ 16x24VDC/0.5A ST	6ES7522-1BH01-0AB0	-30 to +60	FS 03	5,000	FS 01
DQ 32x24VDC/0.5A ST	6ES7522-1BL01-0AB0	-30 to +60	FS 03	5,000	FS 01
DQ 64x24VDC/0.3A BA	6ES7522-1BP00-0AA0	-30 to +60	FS 01	5,000	FS 01
DQ 64x24VDC/0.3A SNK BA	6ES7522-1BP50-0AA0	-30 to +60	FS 01	5,000	FS 01
DQ 8x24VDC/2A HF	6ES7522-1BF00-0AB0	-30 to +60	FS 04	5,000	FS 06
DQ 8x230VAC/2A ST (Triac)	6ES7522-5FF00-0AB0	0 to +60	FS 01	2,000	FS 01
DQ 8x230VAC/2A ST (Triac)	6ES7522-5FF00-0AB0	-25 to +60	FS 03	2 000	FS 01
DQ 16x230VAC/1A ST (Triac)	6ES7522-5FH00-0AB0	0 to +60	FS 01	2,000	FS 01
DQ 16x230VAC/1A ST (Triac)	6ES7522-5FH00-0AB0	-25 to +60	FS 02	2 000	FS 01
DQ 8x230VAC/5A ST (Relay)	6ES7522-5HF00-0AB0	-30 to +60	FS 03	2,000	FS 01
DQ 16x230VAC/2A ST (Relay)	6ES7522-5HH00-0AB0	-25 to +60	FS 02	2,000	FS 01
DQ 16x24...48VUC/125V-DC/0.5A ST	6ES7522-5EH00-0AB0	0 to +60	FS 01	2,000	FS 01
DQ 16x24...48VUC/125V-DC/0.5A ST	6ES7522-5EH00-0AB0	-25 to +60	FS 03	2 000	FS 01
DQ 16x24VDC/0.5A BA (25 mm)	6ES7522-1BH10-0AA0	0 to +60	FS 01	5,000	FS 01
DQ 16x24VDC/0.5A BA (25 mm)	6ES7522-1BH10-0AA0	-30 to +60	FS 03	5,000	FS 01
DQ 32x24VDC/0.5A BA (25 mm)	6ES7522-1BL10-0AA0	0 to +60	FS 01	5,000	FS 01
DQ 32x24VDC/0.5A BA (25 mm)	6ES7522-1BL10-0AA0	-30 to +60	FS 03	5,000	FS 01

Fail-safe digital output modules

Fail-safe digital output module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
F-DQ 8x24VDC/2A PPM	6ES7526-2BF00-0AB0	0 to +60	FS 01	5,000	FS 01

Digital input/output modules

Digital input/ output module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
DI 16x24VDC / DQ 16x24VDC/0.5A BA	6ES7523-1BL00-0AA0	0 to +60	FS 01	5,000	FS 01
DI 16x24VDC / DQ 16x24VDC/0.5A BA	6ES7523-1BL00-0AA0	-30 to +60	FS 03	5,000	FS 01
DI 32x24VDC / DQ 32x24VDC/0.3A SNK BA	6ES7523-1BP50-0AA0	-30 to +60	FS 01	5,000	FS 01

Analog input modules

Analog input module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
AI 8xU/I/RTD/TC ST	6ES7531-7KF00-0AB0	-25 to +60	FS 06	5,000	FS 08
AI 8xU/I/RTD BA	6ES7531-7QF00-0AB0	-30 to +60	FS 03	5,000	FS 05
AI 16xI BA	6ES7531-7MH00-0AB0	-30 to +60	FS 01	5,000	FS 01
AI 16xU BA	6ES7531-7LH00-0AB0	-30 to +60	FS 01	5,000	FS 01
AI 8xU/I HS	6ES7531-7NF10-0AB0	-25 to +60	FS 02	5,000	FS 01
AI 8xU/I HF	6ES7531-7NF00-0AB0	-30 to +60	FS 02	2,000	FS 01
AI 8xU/R/RTD/TC HF	6ES7531-7PF00-0AB0	-30 to +60	FS 02	2,000	FS 01
AI 4xU/I/RTD/TC ST	6ES7531-7QD00-0AB0	0 to +60	FS 01	5,000	FS 01
AI 4xU/I/RTD/TC ST	6ES7531-7QD00-0AB0	-25 to +60	FS 02	5,000	FS 01
AI 8xHART HF	6ES7531-7TF00-0AB0	-30 to +60	FS 01	5,000	FS 01
AI 24xCVM HF	6ES7531-7LK00-0AB0	-30 to +60	FS 01	4 000	FS 01

Fail-safe analog input modules

Fail-safe analog input module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
F-AI 8XI	6ES7536-1MF00-0AB0	0 to +60	FS 01	5,000	FS 01

Analog output modules

Analog output module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
AQ 4xU/I ST	6ES7532-5HD00-0AB0	-30 to +60	FS 06	5,000	FS 03
AQ 4xU/I HF	6ES7532-5ND00-0AB0	-25 to +60	FS 02	2,000	FS 01
AQ 8xU/I HS	6ES7532-5HF00-0AB0	-30 to +60	FS 03	5,000	FS 02
AQ 2xU/I ST	6ES7532-5NB00-0AB0	0 to +60	FS 01	5,000	FS 01
AQ 2xU/I ST	6ES7532-5NB00-0AB0	-30 to +60	FS 02	5,000	FS 01
AQ 8xHART HF	6ES7532-8TF00-0AB0	-30 to +60	FS 01	5,000	FS 01

Analog input/output modules

Analog input/ output module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
AI 4x U/I/RTD/TC/AQ 2x U/I ST	6ES7534-7QE00-0AB0	-25 to +60	FS 04	5,000	FS 04

Communication modules

Communication module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
CM 8xIO-Link	6ES7547-1JF00-0AB0	0 to +60	FS 01	5,000	FS 01
CM 8xIO-Link	6ES 7547-1JF00-0AB0	-30 to +60	FS 02		
CM PtP RS422/485 BA	6ES7540-1AB00-0AA0	0 to +60	FS 01		
CM PtP RS232 BA	6ES7540-1AD00-0AA0				
CM PtP RS422/485 HF	6ES7541-1AB00-0AB0				
CM PtP RS232 HF	6ES7541-1AD00-0AB0				

Technology modules

Technology module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
TM Count 2x24V	6ES7550-1AA00-0AB0	0 to +60	FS 01	5,000	FS 01
TM PosInput 2	6ES7551-1AB00-0AB0				
TM Timer DIDQ 16x2-4V	6ES7552-1AA00-0AB0				
TM PTO 4	6ES7553-1AA00-0AB0				
TM MFP	6ES7558-1AA00-0AB0				
TM NPU	6ES7556-1AA00-0AB0	-25 to +60	FS 01	2,000	FS 01

Power supply modules

Power supply module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
PS 25W 24VDC	6ES7505-0KA00-0AB0	-25 to +60	FS 03	5,000	FS 01
PS 60W 24/48/60VDC	6ES7505-0RA00-0AB0	-25 to +60	FS 04	2,000	FS 01
PS 60W 24/48/60VDC HF	6ES7505-0RB00-0AB0	-25 to +60	FS 02	2,000	FS 01
PS 60 W 120/230V AC/DC	6ES7507-0RA00-0AB0	-25 to +60	FS 04	2,000	FS 01

Information on PFDavg, PFH values for fail-safe S7-1500 I/O modules

PFDavg and PFH values for fail-safe S7-1500 I/O modules for operating altitudes up to 5 000 m.

The safety parameters (PFDavg, PFH values) specified in the Equipment Manual for the fail-safe S7-1500 I/O modules already reflect the influence of higher cosmic radiation (soft error rate) for operation up to 5 000 m above sea level.

C.4　　ET 200MP

Interface modules

Interface module	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
IM 155-5 DP ST	6ES7155-5BA00-0AB0	-25 to +60	FS 04	5,000	FS 01
IM 155-5 PN BA	6ES7155-5AA00-0AA0	-30 to +60	FS 03	5,000	FS 01
IM 155-5 PN ST	6ES7155-5AA01-0AB0	-25 to +60	FS 03	5,000	FS 01
IM 155-5 PN HF	6ES7155-5AA00-0AC0	-25 to +60	FS 04	5,000	FS 01
IM 155-5 MF HF	6ES7155-5MU00-0CN0	-30 to +60	FS 01	5,000	FS 01

Active backplane buses

Active backplane bus	Article number	Ambient temperature		Installation altitude	
		Temperature range [°C]	As of version	Max. altitude [m]	As of version
Active backplane bus 4 slots	6ES7590-0BD00-0AA0	-30 to +60	FS 01	5,000	FS 01
Active backplane bus 8 slots	6ES7590-0BH00-0AA0				
Active backplane bus 12 slots	6ES7590-0BL00-0AA0				

C.5 Restrictions

Restrictions of the max. ambient temperature specified with regard to the installation altitude

Installation altitude	Derating factor for ambient temperature [1]
-1,000 to 2,000 m	1.0
2,000 to 3,000 m	0.9
3,000 to 4,000 m	0.8
4,000 to 5,000 meters	0.7

[1] Base value for the application of the derating factor is the maximum permissible ambient temperature in °C for 2,000 m

NOTE

- Linear interpolation between altitudes is permissible.
- The derating factors compensate for the decreasing cooling effect of air in higher altitudes due to lower density.
- Note the mounting position of the respective module in the technical specifications. The basis is the standard IEC 61131-2.
- Make sure that the power supplies you use are also rated for altitudes > 2 000 m.
- The displays of the S7-1500 CPUs are designed for an altitude of ≤ 3,000 m. When operating the device at altitudes > 3,000 m, you might experience problems with the CPU display in rare cases; however, these do not affect the mode of operation of the CPU.
- The function "Fail-safe shutdown of standard modules", as described in the Internet (https://support.industry.siemens.com/cs/us/en/view/39198632), is only released up to a maximum of 2,000 m.

Effects on availability

The higher cosmic radiation present during operation at altitudes above 2,000 m will also start to have an effect on the failure rate of electronic components (the so-called soft error rate). In rare cases this can result in a transition of the module into the safe state, especially for safety modules. However, the functional safety of the module is fully retained.

NOTE

Information on the components of the S7-1500 automation system

The markings and approvals printed on the components of the S7-1500 automation system are currently based on operation at an altitude of up to 2 000 m. The fail-safe components are certified for operation in safety mode up to the specified maximum altitudes (according to "Z10 067803 0020" certificate (https://support.industry.siemens.com/cs/ww/de/view/57141281/en)).

Reference

You can find more information in the Mechanical and climatic ambient conditions (Page 414) section.

Glossary

Automation system

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

Baud rate

Data transmission rate indicates the number of bits transmitted per second (baud rate = bit rate).

Bit memory

Bit memory is a component of the system memory of the CPU for saving intermediate results. It can be accessed in bit, byte, word or double word mode.

Bus

Joint transmission path to which all nodes of a fieldbus system are connected; has two defined ends.

Bus cable connector

Physical connection between the bus node and the bus cable.

Bus, self-assembling

The modules are lined up on the mounting rail, and are mechanically and electrically connected to each other with a U connector as they are swiveled into position. In this way the bus is extended with each module.

Code block

In SIMATIC S7, a code block is a block that contains a section of the STEP 7 user program. (in contrast to a data block, which contains only data)

Configuration

Systematic arrangement of the individual modules (configuration).

Connection plug

The connection plug provides the physical connection between devices and the cable, for example.

Consistent data

Data whose content belongs together and must not be separated is known as consistent data.

Counter

Counters are components of the system memory of the CPU. You can modify the content of the "counter cells" using STEP 7 instructions (e.g. count up/down).

CPU

The CPU uses the integrated system power supply to supply the electronics of the modules via the backplane bus. The CPU contains the operating system and executes the user program. The user program is located on the SIMATIC Memory Card and is processed in the work memory of the CPU. The PROFINET interfaces on the CPU allow simultaneous communication with PROFINET devices, PROFINET controllers, HMI devices, programming devices, other controllers and other systems. The S7-1500 CPUs support operation as an IO controller and I-device. Similarly to the PROFINET interface, the PROFIBUS interface available on some of the S7-1500 CPUs allows communication with other devices. When the interface is used as PROFIBUS DP interface, the CPU on the PROFIBUS DP also assumes the role of a DP master.

Crimping

Procedure whereby two components joined together, e.g. wire end sleeve and cable, are connected with one another through plastic strain.

Cycle control point

The cycle control point marks the end of a cycle and the start of the next cycle. The cycle time statistics and monitoring of the configured maximum cycle time start at the cycle control point.

Once the cycle control point has been reached, the CPU writes the process image output to the output modules, reads the state of the inputs to the input modules and then executes the first cyclic OB.

Cycle time

The cycle time represents the time a CPU requires to execute the user program once.

Cyclic interrupt

You can find relevant information under the entry "Interrupt, Cyclic "

Data block

Data blocks (DBs) are data areas in the user program that contain user data. There are global data blocks, which can be accessed from all code blocks, and instance data blocks, which are assigned to a specific FB call.

Device

A device can send, receive or amplify data via the bus, e.g. IO device via PROFINET IO.

Device names

Before an IO device can be addressed by an IO controller, it must have a device name. This approach was chosen for PROFINET because names are easier to administer than complex IP addresses.

In its delivery state, an IO device has no device name. An IO device be addressed by an IO controller only after a device name has been assigned using the PG/PC, e.g. for the transmission of configuring data (including the IP address) during start-up or for the exchange of useful data in cyclic mode.

Device station

A device may only exchange data with a master after being requested to do so by the master.

Diagnostic buffer

The diagnostic buffer is a battery-backed memory area in the CPU where diagnostic events are stored in their order of occurrence.

Diagnostic interrupt

You can find relevant information under the entry "Interrupt, Diagnostics"

Diagnostics

Monitoring functions for the detection, localization, classification, display, and further evaluation of errors, faults, and alarms. They run automatically while the system is in operation. This increases the availability of systems by reducing commissioning times and downtimes.

Distributed I/O system

System with I/O modules that are configured on a distributed basis, at a large distance from the CPU controlling them.

DP

Distributed I/O

Equipotential bonding

Electrical connection (potential equalization conductor) that brings the bodies of electrical equipment and other conductive bodies to the same or almost the same potential, in order to prevent disruptive or dangerous voltages between these bodies.

Firmware of the CPU

In SIMATIC, a distinction is made between the firmware of the CPU and user programs.

The firmware is a software embedded in electronic devices. The firmware is permanently connected to the hardware in functional terms. It is usually saved in a flash memory, such as EPROM, EEPROM or ROM, and cannot be replaced by the user or only with special tools or functions.

User program: You will find more information in the glossary entry "User program"

Firmware update

Upgrade of firmware for CPU and the modules (interface modules, I/O modules etc.), e.g. after function extensions, to the most recent firmware version (update).

Function

A function (FC) is a code block with no static data. A function allows you to pass parameters in the user program. Functions are thus suited for programming frequently recurring complex functions, such as calculations.

Function block

A function block (FB) is a code block with static data. An FB allows you to pass parameters in the user program. Function blocks are thus suited for programming frequently recurring complex functions, such as closed-loop controls or operating mode selection.

Functional ground

The functional ground is a low-impedance current path between electric circuits and ground. It is not intended as a protective measure but rather, for example, for improvement of interference immunity.

Ground

Conductive ground whose electrical potential can be set equal to zero at any point.

All interconnected, inactive parts of a piece of equipment that cannot accept any dangerous contact voltage, even in the event of a fault.

Ground

Conductive ground whose electrical potential can be set equal to zero at any point.

All interconnected, inactive parts of a piece of equipment that cannot accept any dangerous contact voltage, even in the event of a fault.

Grounding

Grounding means connecting an electrically conductive part to a grounding electrode by means of a grounding system.

GSD file

The Generic Station Description file contains all properties of a PROFINET or PROFIBUS device that are necessary for its configuration.

Hardware interrupt

You can find relevant information under the entry "Interrupt, Hardware "

I/O modules

All modules that can be operated with a CPU or an interface module.

Identification data

Information that is saved in modules, and that supports the user in reviewing the system configuration and locating hardware changes.

Instance data block

Each call of a function block in the STEP 7 user program is assigned a data block, which is automatically generated. Values of the input, output and in/out parameters, as well as local block data, are stored in the instance data block.

Interface module

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

Interrupt

The operating system of the CPU distinguishes between various priority classes that control the execution of the user program. These priority class processes include, for example, hardware interrupts. When an interrupt occurs, the operating system automatically calls an assigned organization block. The user can program the desired reaction in the organization block, e.g. in a FB.

Interrupt, cyclic

The CPU generates a cyclic interrupt periodically within a parameterizable time grid and then processes the corresponding organization block.

Interrupt, hardware

A hardware interrupt is triggered by interrupt-triggering modules due to a certain event in the process. The hardware interrupt is signaled to the CPU. The CPU then processes the assigned organization block according to the priority of this interrupt.

Interrupt, time-delay

The time-delay interrupt is one of the program execution priority classes of SIMATIC S7. The time-delay interrupt is generated upon expiration of a timer started in the user program. The CPU then processes the corresponding organization block.

Interrupt, time-of-day

The time-of-day interrupt is one of the program execution priority classes of SIMATIC S7.. The time-of-day interrupt is generated based on a defined date (or daily) and time (e.g. 9:50 or every hour, every minute). The CPU then processes the corresponding organization block.

Interrupt, update

When it receives an update interrupt, the operating system calls the update interrupt OB. This may happen if you changed a parameter on a slot of a device.

IP address

The IP address is made up of four decimal numbers with a range of values from 0 through 255. The decimal numbers are separated by a dot (for example 192.162.0.0).

The IP address consists of the following:

- Address of the network
- Address of the device (PROFINET interface of the IO controller/IO device)

Isolated modules

In the case of isolated input/output modules, the reference potentials of the control and load circuits are galvanically isolated, e.g. by means of optical isolators, relays or transformers. Input/output circuits can be connected to common potential.

Load current supply

Supply of the module's input and output electric circuits.

MAC address

Every PROFINET device is assigned a worldwide unique device identification before it leaves the factory. This 6-byte long device identification is the MAC address.

The MAC address is divided into:

- 3-byte manufacturer identification
- 3-byte device identification (consecutive number)

The MAC address is generally shown on the front of the device.
Example: 08-00-06-6B-80-C0

Non-isolated modules

In the case of non-isolated input and output modules, the reference potentials of the control and load circuits are electrically connected.

NTP

The Network Time Protocol (NTP) is a standard for synchronizing clocks in automation systems via Industrial Ethernet. NTP uses the UDP connectionless network protocol.

Operating modes

Operating states describe the behavior of a single CPU at a specific time.

Organization block

Organization blocks (OBs) form the interface between the operating system of the CPU and the user program. The organization blocks determine the order in which the user program is executed.

OT

OT (Operational Technology): The use of hardware and software to monitor and control industrial plants.

Parameter

- Tag of a STEP 7 code block:

- Tag for setting the behavior of a module (one or more per module). In as-delivered state, every module has an appropriate basic setting, which you can change by configuring in STEP 7. There are static and dynamic parameters

Parameters, dynamic

In contrast to static parameters, you can change dynamic parameters of modules during operation by calling an SFC in the user program, e.g. limit values of an analog input module.

Parameters, static

In contrast to dynamic parameters, you cannot change static parameters of modules with the user program but only by configuring in STEP 7, e.g. input delay of a digital input module.

PELV

Protective **E**xtra **L**ow **V**oltage = safety extra low voltage connected to protective earth

Pre-wiring

Wiring of the electrical system on the front connector before the front connector is used on the I/O module.

Process image (I/O)

The CPU transfers the values from the input and output modules to this memory area. At the start of the cyclic program the signal states of the input modules are transmitted to the process image of the inputs. At the end of the cyclic program the process image of the outputs is transmitted as signal state to the output modules.

Product version (PV) = Function version (FV)

The product version or function version provides information on the hardware version of the module.

PROFIBUS

PROcess FIeld BUS, process and fieldbus standard that is specified in IEC 61158 Type 3. It specifies functional, electrical and mechanical characteristics for a bit-serial field bus system.

PROFIBUS supports the protocols DP (= Distributed I/O), FMS (= Fieldbus Message Specification), PA (= Process Automation), or TF (= Technological Functions).

PROFINET

PROcess FIeld NETwork, open Industrial Ethernet standard which further develops PROFIBUS and Industrial Ethernet. A cross-manufacturer communication, automation, and engineering model defined by PROFIBUS International e.V. as an automation standard.

PROFINET IO

Communication concept for the realization of modular, distributed applications within the scope of PROFINET.

PROFINET IO controller

Device used to address connected I/O devices (e.g. distributed I/O systems). This means that: The IO controller exchanges input and output signals with assigned IO devices. Often, the IO controller is the CPU on which the automation program runs.

PROFINET IO device

Distributed field device that can be assigned to one or more IO controllers (e.g. distributed I/O system, valve terminals, frequency converters, switches).

Push-in terminal

Terminal for the tool-free connection of wires.

Reference potential

Potential from which the voltages of the circuits involved are observed and/or measured.

Restart

During a warm restart, all non-retentive bit memory is deleted and non-retentive DB contents are reset to the initial values from load memory. Retentive bit memory and retentive DB contents are retained. Program execution begins at the call of the first startup OB.

Retentivity

A memory area whose content is retained after power failure and after a STOP to RUN transition is retentive. The non-retentive area bit memory area, timers and counters are reset after a power failure and after a STOP to RUN transition. The non-retentive content of data blocks is reset to the initial values.

Row

> All the modules attached to a mounting rail.

Runtime error

> Error that occurs during execution of the user program in the automation system (thus not in the process).

SELV

> **S**afety **E**xtra **L**ow **V**oltage = Safety extra-low voltage

SNMP

> SNMP (Simple Network Management Protocol) is the standardized protocol for performing diagnostics on and assigning parameters to the Ethernet network infrastructure.
>
> In the office setting and in automation engineering, devices from a wide range of vendors on the Ethernet support SNMP.
>
> SNMP-based applications can be operated on the same network in parallel to applications with PROFINET.
>
> The scope of supported functions varies depending on the device type. For example a switch has more functions than a CP 1616.

Switch

> PROFIBUS is a linear network. The communication nodes are linked by means of a passive cable - the bus.
>
> By contrast, Industrial Ethernet consists of point-to-point connections: Each communication node is directly connected to exactly one communication node.
>
> If a communication node is linked to several communication nodes, this communication node is connected to the port of an active network component - the switch. Additional communication nodes (including switches) can now be connected to the other ports of the switch. The connection between a communication node and the switch remains a point-to-point connection.
>
> A switch thus has the task of regenerating and distributing received signals. The switch "learns" the Ethernet address(es) of a connected PROFINET device or additional switches and only forwards those signals that are intended for the connected PROFINET device or switch.
>
> A switch has a specific number of connections (ports). You connect at most one PROFINET device or additional switch to each port.

System power supply

> Consists of the integrated system power supply of the CPU/interface module and additional power supplies (PS), if necessary. The system power supply serves exclusively to supply the I/O modules via the backplane bus.

Technology object

A technology object supports you in the configuration and commissioning of a technological function.

The properties of real objects are represented by technology objects in the controller. Real objects can be, for example, controlled systems or drives.

The technology object contains all data of the real object required for its open-loop or closed-loop control, and it signals back status information.

TIA Portal

Totally Integrated Automation Portal

The TIA Portal is the key to the full performance capability of Totally Integrated Automation. The software optimizes operating, machine and process sequences.

Time-delay interrupt

You can find relevant information under the entry "Interrupt, time-delay"

Time-of-day interrupt

You can find relevant information under the entry "Interrupt, Time-of-day"

Timer

Timers are components of the system memory of the CPU. The operating system automatically updates the content of the "timer cells" asynchronously to the user program. STEP 7 instructions define the precise function of the timer cell (for example on-delay) and trigger its execution.

Update interrupt

You can find relevant information under the entry "Interrupt, Update "

User program

SIMATIC differentiates between the operating system of the CPU and user programs. The user program contains all the instructions, declarations and data for signal processing that control a plant or process. The user program is assigned to a programmable module, a CPU, for example. Structuring into smaller unit is supported.

Value status

The value status is additional binary information of a digital input or output signal. The value status is entered simultaneously with the process signal in the process image input and provides information about the validity of the signal.

Warm restart

You can find relevant information under the entry "Restart"

Index