SIEMENS

SIMATIC

S7-1500 Software Controller CPU 1505SP (F/T/TF), CPU 1507S (F), CPU 1508S (F/T/TF) V31.1

Operating Instructions

01/2025
A5E32565315-AS

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.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E32565315-AS
Ⓟ 01/2025 Subject to change

Copyright © Siemens 2014 - 2025.
All rights reserved

Table of contents

Documentation guide

1

1.1 S7-1500/ET 200MP documentation guide

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/ww/en/view/86140384)

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).

1.1.1 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/ww/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/cs/ww/en/)

     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/cs/ww/en/my)

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://sieportal.siemens.com/su/bjAFw)

1.1.2 Tool support

The tools described below support you in all steps: from planning, over commissioning, all the way to analysis of your system.

TIA Selection Tool

The TIA Selection Tool tool supports you in the selection, configuration, and ordering of devices for Totally Integrated Automation (TIA).

As successor of the SIMATIC Selection Tools , the TIA Selection Tool assembles the already known configurators for automation technology into a single 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://support.industry.siemens.com/cs/ww/en/view/109767888)

SINETPLAN

SINETPLAN, 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. This helps to 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 importing and simulation of existing STEP 7 projects
- Efficiency through securing existing investments in the long term and the optimal use of resources

You can find SINETPLAN on the Internet (https://new.siemens.com/global/en/products/automation/industrial-communication/profinet/sinetplan.html).

Security information 2

2.1 Security settings for IPCs

Recommended security settings for IPCs

Under the following link (https://support.industry.siemens.com/cs/ww/en/view/109475014) you will find the recommended security settings for IPCs to meet the highest security and reliability requirements in industrial environments.

For individual settings depending on your type of IPC, see chapter Reference information for use with SIMATIC IPC (Page 235).

2.2 Notes on data protection

Siemens observes the principles of data protection, in particular the principle of data minimization (privacy by design).

For this Software Controller, this means that the product stores/processes no personal data, only technical functional data (for example, a timestamp). If a user links this data with other data (for example, a shift schedule) or stores personal data on the same storage medium (for example, a hard disk) and thus establishes a connection to an identifiable person, the user must ensure compliance with the relevant data protection regulations.

2.3 Change of the operating mode with critical actions

Switch the CPU to "STOP" mode before actions that result in very high utilization of the hardware ("critical actions").

2.4 Information about third-party software updates

This product contains third-party software. Siemens accepts liability with respect to updates/patches for the third-party software only when these are distributed by Siemens in the context of a Software Update Service contract or officially approved by Siemens. Otherwise, updates/patches are installed at the user's own risk. You can find more information in our Software Update Service (https://www.siemens.com/sus).

2.5 Notes on protecting administrator accounts

A user with administrator rights has extensive access and manipulation possibilities.

Therefore, make sure that the administrator account is adequately protected to prevent unauthorized changes. Use secure passwords and use a standard user account for regular operation. Other measures, such as the use of security policies, should be applied as required.

2.6 Signatures and file integrity

Handling digital signatures and hashes

On the PC, the software for the Software Controller ("CPU.elf") is provided by the Windows operating system. Administrator rights can be used to modify the software or replace it with another software package. This is an intentional feature since the Windows operating system is an open platform. The open platform enables customers to tailor their individual operational, connectivity and security requirements. It is recommended to lock out administrative accounts and operate the Software Controller using low-privileged accounts, such as the default operator account.

On Windows, a mechanism is available to check the digital signatures of binary files that are signed with the Windows Authenticode Signature Format. The signature of CPU.elf is checked the Windows power shell command "Test-FileCatalog -Detailed -CatalogFilePath C:\Boot\Siemens\CPU.cat -Path C:\Boot\Siemens".

Industrial cybersecurity 3

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.

3.1 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 comprehensive, 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 more information on protective industrial cybersecurity measures that may be implemented, visit (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

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 customers' exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under (https://www.siemens.com/global/en/products/services/cert.html).

3.2 Security update notification

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 "Knowledge base" tab.
4. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".
5. Use the filter methods to search and select the document from which you want to create notifications.
6. Select "Add to mySupport favorites" using the 3 dots on the right.
7. In the following dialog, select the name, the storage location and the "Enable notification" option for the favorite. Then click on the "OK" 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.

3.3 Basic information on industrial cybersecurity

3.3.1 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))

3.3.2 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.

3.4 Comprehensive security concept and security strategies

3.4.1 Comprehensive "Defense in Depth" security concept

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 Web page (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html).

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.

3.4.2 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
- Using 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/global/en/products/services/cert.html) 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 Security update notification (Page 17). 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, for example:

- 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 gaps
- 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)

3.5 Operational application environment and security assumptions

3.5.1 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.

3.5.2 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/global/en/products/automation/topic-areas/industrial-cybersecurity.html) Web page.

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 devices (such as USB flash drives) and IT devices (such as laptops) classified as unsafe on systems.

3.6 Security properties of the devices

The security properties and settings of the individual devices are listed in this manual.

3.7 Secure operation of the system

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

3.7.1 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.

3.7.2 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).

3.7.3 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 207) and in the STEP 7 online help (TIA Portal).

3.7.4 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 32).

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.

Storage of security-relevant data

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

Also see the section Sensitive data (Page 30).

3.7.5 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 of I/O modules (Page 185)
- The section Security update notification (Page 17)

3.7.6 Notifications about security gaps (Siemens Security Advisories)

A vulnerability is a security gap 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

When Siemens identifies and resolves security gaps (vulnerabilities) in their products, this is published in Security Advisories.

You can find the documents for SIMATIC on the following Siemens Web page: Siemens ProductCERT and Siemens CERT (https://www.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 necessary 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 the Common Vulnerability Scoring System (CVSS)
  - Measures
  - Availability
  - Etc.

Set up Security Feeds (https://www.siemens.com/global/en/products/services/cert.html) 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/global/en/products/services/cert.html) and follow the instructions.

3.7.7 Data backup

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

3.7.8 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: Website Industrial Security) (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security.html)

3.7.9 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.

3.7.9.1 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

To delete all data from the data memories of the CPU, format and reset the CPU to factory settings.

For information on how to format the CPU volume, refer to the section Formatting the CPU volume (Page 191).

For information on how to reset the CPU to factory settings, refer to section Resetting the CPU (Page 187).

3.7.9.2 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.

3.8 Secure operation of the engineering software

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

3.9 Secure operation of CPUs

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

3.9.1 Secure configuration

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

3.9.2 User management and access control

3.9.2.1 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 section Local user management (Page 209) and in the STEP 7 online help (TIA Portal).

3.9.2.2 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 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 do not 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.

Components and functions with password protection

Components and functions with password protection	Comment
Web server	see Webserver function manual (https://support.industry.siemens.com/cs/ww/en/view/59193560)
CPU	see Communication function manual (https://support.industry.siemens.com/cs/ww/en/view/59192925)
OPC UA	
SNMP Community-String (similar to a password)	
Secure communication (with certificate protection)	

3.9.2.3 Password management

- You can find comprehensive recommendations for creating secure passwords in the Industrial security configuration manual (https://support.industry.siemens.com/cs/ww/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, see Communication function manual (https://support.industry.siemens.com/cs/ww/de/view/59192925).
- Change and reset of the password for confidential configuration data. The Communication function manual (https://support.industry.siemens.com/cs/ww/de/view/59192925) provides information on the following topics:
  - Changing passwords
  - Resetting or deleting passwords
- Access to a password-protected CPU can be configured in STEP 7, see section Using the display to change the protection level for display access (Page 214).
- For user management and access control, use the Local user management (Page 209).

- Using a password provider: In STEP 7, you can set up a password provider.
- 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.

3.9.2.4 Setting protection levels

For detailed information about setting up protection levels for the CPU and assigning user authorizations, refer to the section Protection (Page 207) and the STEP 7 online help (TIA Portal).

3.9.2.5 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 the relevant information about "Certificate management" in the Communication function manual (https://support.industry.siemens.com/cs/ww/en/view/59192925).

3.9.3 Protection functions

Integrated protection functions of the CPU protect against unauthorized access.

A description of the protection functions and their activation can be found in section Protection (Page 207).

3.9.4 Web server

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

The Web server 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 function manual (https://support.industry.siemens.com/cs/ww/en/view/59193560).

3.9.5 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).

3.9.6 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	You can find more information in
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	-	STEP 7 online help
Configuration of CPUs	Protection through PROFINET Security Class 1	PROFINET with STEP 7 function manual (https://support.industry.siemens.com/cs/ww/en/view/49948856)
Blocks (data blocks, logic blocks)	Know-how protection, copy protection, write protection	Section Protection (Page 207)
Data deemed sensitive by the operator	Backups, other configuration data, analysis data	Section Opening existing PC system configuration files (Page 127)

3.9.7 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 a STEP 7 project:

- Project backup via online backup, see article Online backup (https://support.industry.siemens.com/cs/ww/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/ww/en/view/92561565)

3.9.8 Additional measures for network security

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

- Different measures increase protection against unauthorized access to CPU functions and data from outside and via the network. For more information, refer to section Overview of the protective functions of the CPU (Page 207).
- For information on network security and network components for protection against unauthorized access, refer to the PROFINET function manual (https://support.industry.siemens.com/cs/ww/en/view/49948856) in chapter "Network security".

3.9.9 Remote access to CPU

3.9.9.1 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).

3.9.10 Recording security events

SysLog storage

Syslog stands for "System Logging Protocol," a standard for storing, transmitting, and collecting 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, 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-mentioned security events are also stored as syslog messages in the local cache of a CPU with a firmware version ≥V30.1. For an overview of all SysLog messages, refer to the following Entry (https://support.industry.siemens.com/cs/ww/en/view/109823696).

The content of a syslog message is based on the IEC 62443-3-3.

You can find more information in the section Syslog messages (Page 32).

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.

3.9.11 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 state

The collecting of security-relevant events cannot be deactivated. Each CPU as of FW version V30.1 saves syslog messages in a local cache. By querying this cache, you can view the syslog messages and identify potential security risks.

The local cache of a CPU is organized as a ring buffer. When the memory limit of the cache is reached and further security events occur, the oldest messages in the cache are overwritten.

If you want to access the local cache with the syslog messages, use the Web API of the web server (API method Syslog.Browse). You can find information on the procedure in the Web server (https://support.industry.siemens.com/cs/ww/en/view/59193560) function manual.

In addition, you can transfer the security events recorded by the CPU to a syslog server in the network.

Forwarding to a syslog server

As of STEP 7 V19 and a CPU as of FW version V30.1, it is possible to transfer syslog messages to a server, for example 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 by default via port 514 (UDP) or port 6514 (TLS over TCP).

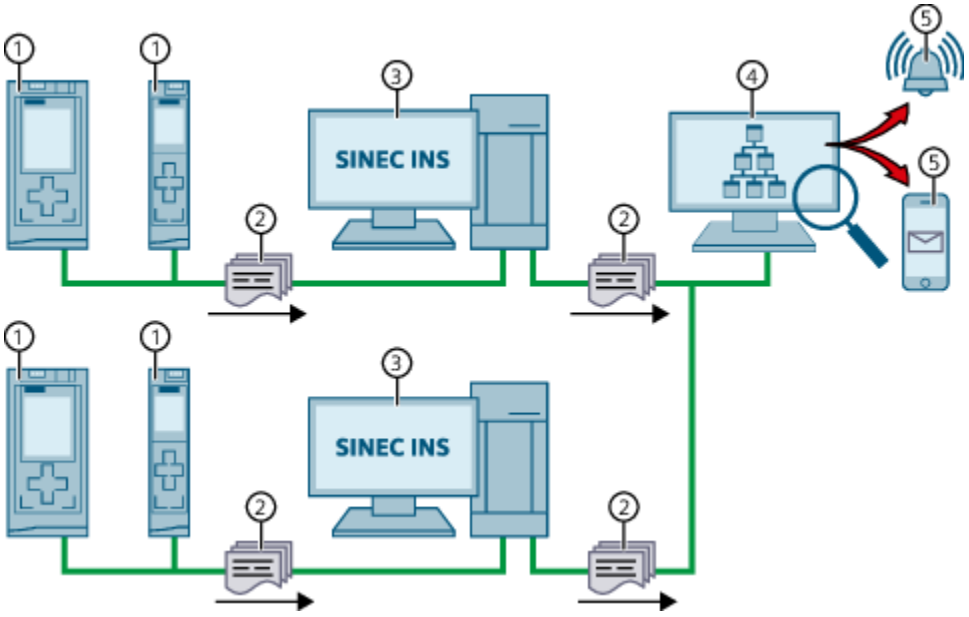
NOTE

If you use UDP as the transport protocol, the data is transferred unencrypted. In addition, authentication is not required 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 3-1 Forwarding and processing of syslog messages

More information

For information on network management using SINEC INS, refer to the following entry (https://support.industry.siemens.com/cs/ww/en/view/109781023).

For information on the structure of syslog messages, refer to section Structure of the Syslog messages (Page 38).

3.9.11.1 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 V30.1
- 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, 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 > Syslog Server".
3. In the "Connection to syslog server" area, activate the option "Enable transfer of syslog messages to a syslog server". 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.

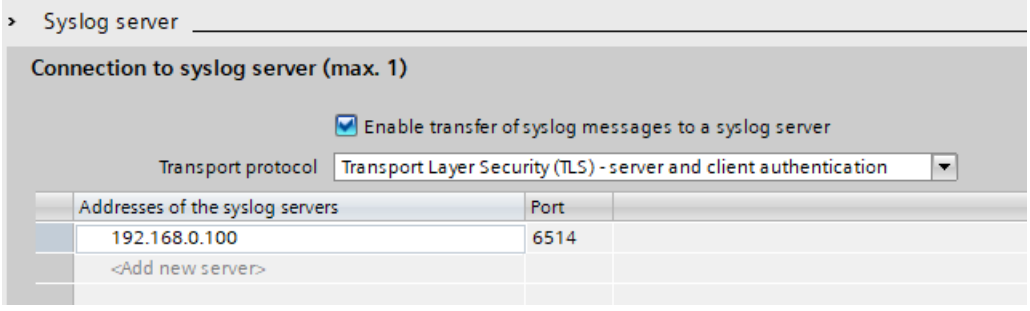
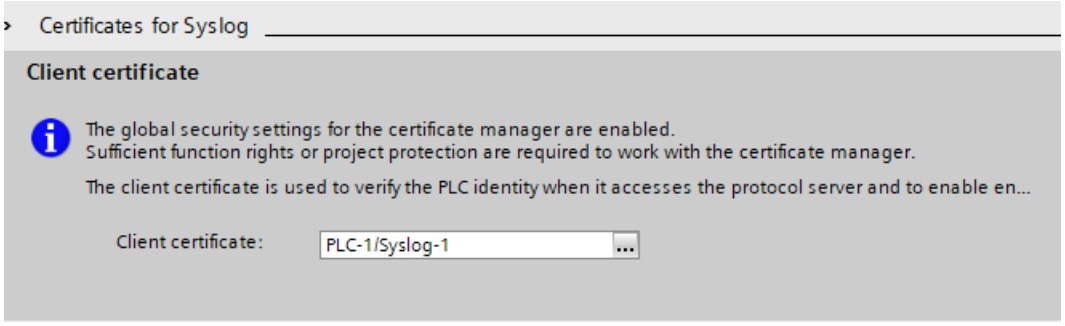


Figure 3-2 Transfer of syslog messages to a syslog server configured

Selecting the client certificate

STEP 7 provides the required client certificate for a CPU for the TLS transport protocol. If you manage the certificate 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 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.

3.9.11.2 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:

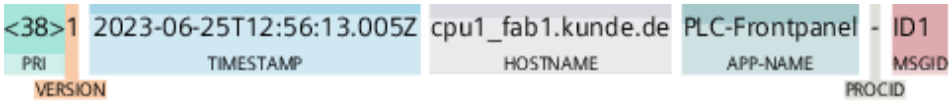


Figure 3-3 Example: HEADER of the syslog message of a CPU

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 A CPU does not use all of the listed severity/facility values.
VERSION	Version number of the syslog specification.

Parameter	Description
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 IP address 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 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:

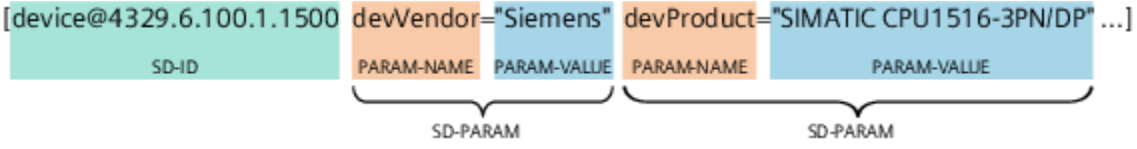


Figure 3-4 Example: SD ELEMENT of the syslog message of a CPU

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.

Parameter	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 transfer of the 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://datatracker.ietf.org/doc/html/rfc5425)
- Transferring syslog messages via UDP (RFC 5426) (https://datatracker.ietf.org/doc/html/rfc5426)

Product overview

4

4.1 Introduction to PC-based control

Overview

The SIMATIC S7-1500 Software Controller is a PC-based controller. The PC-based controller offers the same functionality as all CPUs of the SIMATIC S7-1500 automation system in a PC-based real-time environment.

As part of the SIMATIC series of products, the Software Controller can communicate with STEP 7 and other SIMATIC products, such as WinCC Unified, via Industrial Ethernet networks. Communication with the distributed I/O takes place in the same way as with PROFINET. The Software Controller uses distributed I/O to control the automation process. To network the Software Controller with the distributed I/O, you use the interfaces of your PC. In addition, the CPU 1505SP can use the centralized I/O of the ET 200SP Open Controller.

The Software Controller uses communication via programming devices and operator panels (Industrial Ethernet) for connection with STEP 7 or other programming packages on a different PC.

The following figure shows a product overview when using a Windows PC.

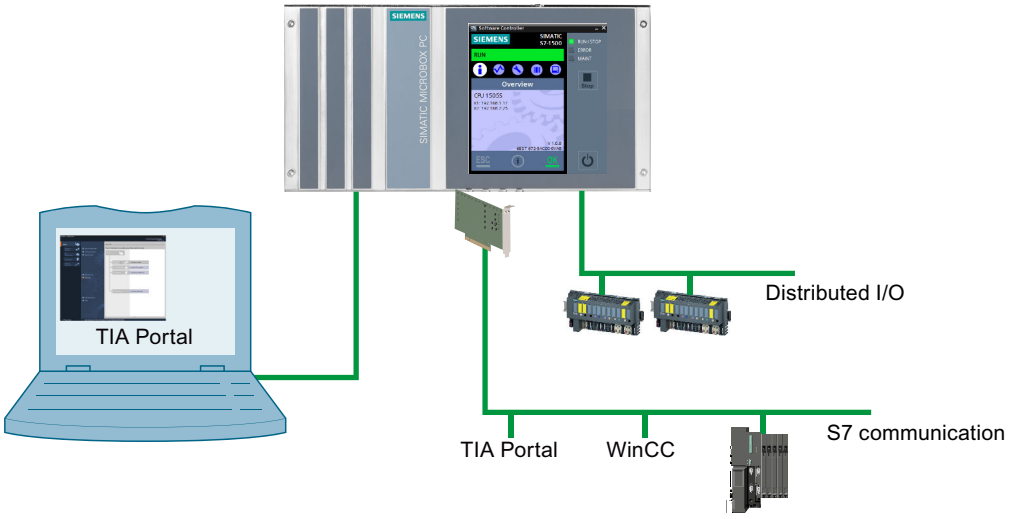


Figure 4-1 Product overview (Windows)

You use the same programming languages, program structure, and programming interface (STEP 7) to develop your user programs with the PC-based controller as for hardware controllers. For the SIMATIC S7-1500 Software Controller, you can use the same user program as for a hardware controller.

On Windows PCs, the Software Controller also offers a display application that is executed under Windows on the same PC. The display application displays the Software Controller's operating mode. Similarly to a hardware CPU's display, you can use the display application to execute diagnostic and commissioning tasks.

NOTE

Available operating systems

The present manual describes Software Controllers using the Windows operating system. The latest manual for Software Controllers using Linux (Industrial OS) is available on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109808199).

4.2 Overview of functions

The S7-1500 Software Controller performs the function of an S7-1500 hardware controller as a software package on a PC.

The Software Controller has the following technical properties:

Configuration and programming with STEP 7 in the TIA Portal

All programming languages defined in IEC 61131-3 are supported.

Innovative real-time system based on virtualization technology

The real-time system of the S7-1500 Software Controller enables you to operate the Software Controller in parallel with, but independent of, Windows.

- Real-time and deterministic behavior
- Fast power-up at Power On of the PC

Fast program execution with multiple priority-controlled execution levels

- Cyclically, time-controlled, isochronously with PROFINET
- Event-driven via hardware and diagnostic interrupts

Storing of retentive data

The Software Controller ensures protection of system data even after a power failure:

- Storing of retentive data on the hard drive of the PC (UPS required)
- Backup of retentive data on the NVRAM (on SIMATIC IPCs with this option) possible in case of a power failure

Communication

The S7-1500 Software Controller uses interfaces of the PC for PROFINET.

- Windows-independent use of PC interfaces for PROFINET for operating distributed I/O. Depending on the interface hardware used, the following functions are possible:
  - PROFINET IO RT
  - PROFINET IO IRT
  - PROFIenergy
  - Media redundancy
  - I-Device
  - Isochronous mode
  - MRP/MRPD
- Communication (SIMATIC Communication, Open User Communication, OPC UA) with Windows applications or external devices

Integrated Web server

All CPUs of the SIMATIC S7-1500 automation system support querying of the CPU via the Web server. The Web server provides the following diagnostics possibilities:

- CPU mapping with LEDs and current operating mode
- Reading out entries from the diagnostics buffer
- Querying module states
- Querying current alarms
- Information on communication
- Information on the status of the topology/PROFINET devices
- Firmware updates
- Transferring user data to the load memory of the CPU and managing this data
- User-programmable web pages for support of service- and commissioning-specific machine functions
- API (Application Programming Interface) as an interface for
  - Writing CPU data
  - Executing functions (for example, changing the operating state)

Trace functionality

All CPUs of the SIMATIC S7-1500 automation system support the trace functionality. The trace functionality supports the recording of analog and digital tags for each cycle and their representation as a trend with STEP 7. This is particularly useful for motion control and closed-loop control applications.

Integrated technology

- S7-1500 Motion Control
  - PLC Open blocks for programming motion functionality by means of PROFINET IO and PROFIdrive interface.
  - The functionality supports speed-controlled axes, positioning axes, synchronous axes, external encoders, output cam, cam track and measuring inputs.
- Integrated closed-loop control functionality: The CPU has three PID controllers with integrated optimization for a wide range of closed-loop control tasks:
  - PID_Compact for universal closed-loop control tasks
  - PID_3Step for valves
  - PID_Temp for closed-loop temperature control tasks

Motion control functions of the technology CPUs

Supported technology objects:

- Speed-controlled axes
- Positioning axes
- Synchronous axes
- External encoders
- Output cams
- Cam track
- Measuring inputs
- Cams
- Cams 10k
- Kinematics
- Leading Axis Proxy
- Interpreter
- Interpreter Mapping
- Interpreter Program

Advanced synchronization functions:

- Synchronizing with or without specification of synchronous position
- Setpoint value or actual value coupling
- Shift of master value on the following axis
- Camming

Other functions:

- A maximum of 4 encoders or measuring systems as actual position for position control
- Cyclic specification of motion vector from the application (MotionIn interface)

- Technology object for control of kinematics with up to 6 interpolating axes, for example, Cartesian portal, delta picker, roll picker, articulated arm, cylindrical robot, tripod, SCARA
- Support of user-defined kinematics
- Trace functions for all CPU tags, both for diagnostics in real-time as well as for sporadic error detection, can also be called via the Web server of the CPU
- Extensive closed-loop control functionalities, for example, easy-to-configure blocks for automatic optimization of the controller parameters for optimized control quality

Integrated system diagnostics

System diagnostics are generated automatically and displayed by:

- Programming device
- PC
- HMI
- Web server
- Display application

System diagnostics are also available when the CPU is in STOP mode.

Integrated security

- Protection of confidential configuration data

  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.
- Know-how protection

  Algorithms can be securely protected against unauthorized access and modification.
- Copy protection

  Copy protection links user blocks with the serial number of one or more SIMATIC memory cards, or the serial number of one or more CPUs. User programs cannot run without the corresponding SIMATIC memory card or CPU.
- Access protection

  Extended access protection provides comprehensive protection against unauthorized configuration changes. Authorization levels can be used to assign separate rights to different user groups.
- Integrity protection

  The system protects the data transferred to the CPU from unauthorized manipulation. Altered or external transmission of engineering data is reliably detected by the CPU.

- Password provider

  As an alternative to manual password input, you can connect a password provider to STEP 7. A password provider offers the following advantages:

  – Convenient handling of passwords. STEP 7 reads in the password automatically for the blocks.

  – Optimum block protection because the users themselves do not know the password.

Local user management

As of TIA Portal V19 and FW version V30.1, the S7-1500 Software Controllers, along with the S7-1500 hardware CPUs, the management of users, roles, and CPU function rights (User Management & Access Control, UMAC) has been improved. As of V19, you manage all project users and their individual rights (e.g. access rights) for all CPUs within the project. User management is done in the editor for 'Users and roles' under 'Security settings' in the project tree in TIA Portal.

Reference

You can find additional information on integrated security, access protection and UMAC in the system manual S7-1500 Automation System (https://support.automation.siemens.com/WW/view/en/59191792).

4.3 Functions

4.3.1 Real-time concept of the CPU

Advantages of hypervisor technology

Due to its innovative real-time system based on hypervisor technology, the SIMATIC S7-1500 Software Controller offers the following advantages:

- Compatibility with S7-1500 hardware controllers
- Security and protection for controller applications

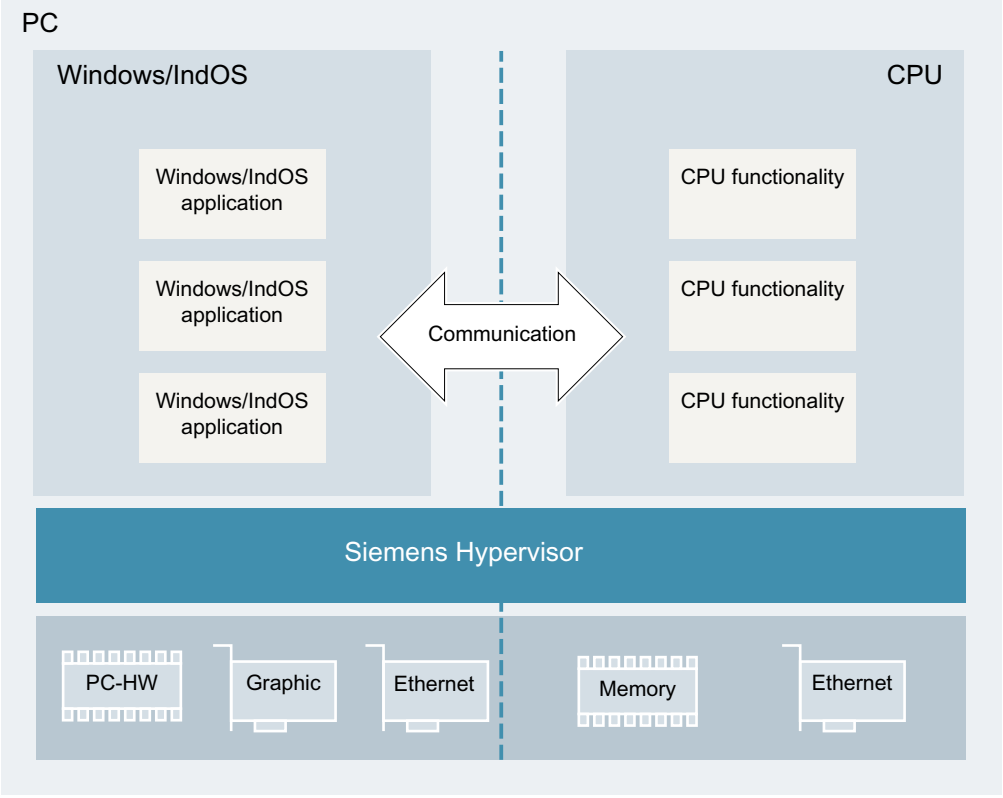


Figure 4-2 Real-time concept

Division of the PC resources

The hypervisor technology divides the PC and assigns all resources necessary for the control task exclusively to the SIMATIC S7-1500 Software Controller. Windows and Windows applications have no access to these resources.

The communication architecture allows secure and transparent communication between Windows applications and the CPU:

- Local communication with the HMI or other Windows applications
- Controlled access to PROFINET modules for STEP 7 or HMI
- Controlled communication with external devices via Windows interfaces

4.3.2 Memory concept of the CPU

4.3.2.1 CPU memory areas

Introduction

This section describes the structure of the memory of the CPU.

Memory areas

The CPU makes use of the mass storage of the PC on which it is installed. During the installation, a discrete CPU volume is created in the mass storage (Page 64), in which all CPU data is stored. The load and retentive memories are integrated into this CPU volume.

The following figure shows the memory division on the PC:

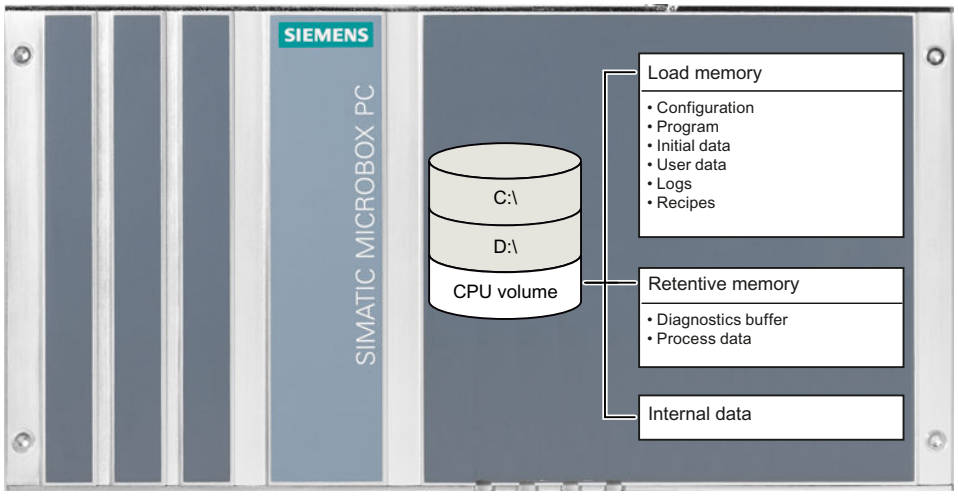


Figure 4-3 Memory division on the PC

Work memory

The RAM of the PC is used for the work memory. A portion of the RAM memory is allocated exclusively by the SIMATIC hypervisor when the CPU starts. As a result, this RAM memory is available exclusively to the CPU. The work memory is volatile memory that contains the code and data blocks. The work memory is permanently allocated to the CPU and cannot be extended.

Load memory

The load memory is located in the mass storage of the PC. The CPU volume contains not only the load memory, but also internal configuration data and even retentive data, depending on the configuration. The CPU volume is not assigned to Windows. This ensures operation of the CPU independent of the operating system.

NOTICE

Load memory capacity

Make sure that there is still enough free memory space available in the CPU's load memory. Insufficient load memory space may have the following consequences:

- A project cannot be downloaded to the CPU successfully
- A CPU does not change into RUN operating state after project download
- Retentive data might be lost

Retentive memory

Retentive memory is non-volatile memory for saving a limited quantity of data in the event of a power failure. Retentive data can be stored in two ways, depending on the resources of the PC:

- In the NVRAM of a PC (if the PC used has this option)
- On the CPU volume

The data defined as retentive is stored in retentive memory. This data is retained beyond a power-off or power failure.

If you are using PC mass storage, use a UPS (Page 183) to ensure a complete backup of the retentive data in case of a power failure.

NVRAM

When NVRAM is used (on SIMATIC IPCs with this option), it is also possible to store retentive data in the event of a power failure. The volume of data that can be stored retentively is limited and can depend upon the properties of the PC used.

NOTE

Note that NVRAM is necessary for using the fail-safe feature "Fast Compile & Fast Commissioning".

For more information on fail-safe feature "Fast Compile & Fast Commissioning", refer to the SIMATIC Safety - Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126) manual.

CPU memory area

The CPU volume is a partition on the mass storage of the PC used. The CPU volume is already created and has the following contents:

- Load memory
- Configuration data
- Retentive data

  Retentive data is saved to the mass storage of the PC if:

  – you select "PC mass storage" in the configuration of category "Retentive memory" in TIA Portal

  – you set "nvram_usage" to "false" in the Resource Configuration file

    For more information on the Resource Configuration file, refer to section Parameters (Page 93).

  If "PC mass storage" is selected, the complete data storage can be kept retentive. Use a UPS (Page 183) to ensure complete backup of the retentive data in case of a power failure.

NOTE

Universal write filter

The CPU volume cannot be protected by the universal write filter (UWF).

Reference

Additional information about the memory structure and the basic meaning of these memory areas can be found in the Structure and Use of the CPU Memory (https://support.automation.siemens.com/WW/view/en/59193101/0/en) function manual. This documentation also describes how you obtain information about the memory utilization using STEP 7.

4.3.2.2 Storage of retentive data

Introduction

When you stop the Software Controller or a power failure occurs, you can store data retentively:

- In the PC mass storage or
- In the NVRAM

  The NVRAM module is pluggable for IPC227G, IPC277G and IPCs BX-39A/PX-39A. For all other devices, the NVRAM module is onboard.

The following data is saved:

- The current data from data blocks, bit memory, timers, counters, and technology objects that is marked as retentive in the TIA Portal
- Contents of the diagnostics buffer
- Contents of the message buffer
- Current operating mode (RUN/STOP)

The retentive data is stored automatically in the following situations:

- Shutdown of the CPU via the display of the CPU or using command line commands
- Shutdown of the operating system (standard or triggered by a UPS signal)
- Power failure (by using a UPS or NVRAM)

NOTE

Options for storage of retentive data

For information on the memory type and memory size of your hardware platform, check your PC system's technical specifications.

Deleting the data

To delete the data, perform a "Memory reset". For detailed information on how to perform a "Memory Reset", refer to section Resetting the CPU (Page 187).

Saving in mass storage

The Software Controller has its own CPU volume in the mass storage of your PC. The storage operation is thus independent of the operating system status and universal write filter (UWF).

NOTE

Preservation of retentive data when saving in mass storage

To retain the retentive data of the original configuration, proceed as follows:

1. Copy the mass storage.
2. Start the CPU with the copied data.

When saving retentive data on the PC's mass storage, note that the quantity of retentive data to be saved on the mass storage differs from the quantity of memory in NVRAM.

NOTICE
Uninterruptible power supply (UPS) A power failure without shutting down the operating system can cause damage to the file structure of the operating system. Use a UPS (Page 183) to protect the file system. You also have the option of activating the enhanced write protection functionalities (UWF) and the usage of NVRAM.

Storage in NVRAM

Storing retentive data in NVRAM protects you from losing important program data after a power failure. The advantage of storing retentive data in NVRAM is that the storage process can take place even in the event of a sudden power failure. But the storage process with this method depends on the buffer capacity of the power supply of your PC. This reduces the amount of retentive data that can be saved compared to saving in the mass storage.

NOTE

Availability of NVRAM

For information which IPCs support NVRAM, refer to section Reference information for use with SIMATIC IPC (Page 235).

In TIA Portal, the memory location "PC mass storage" is set by default in the delivery state of the SIMATIC IPC. To utilize NVRAM, you must change the storage location.

Reference

Additional information on setting the type of storage can be found in section "Setting storage location for retentive data (Page 119)".

Additional information on setting the size of the diagnostic buffer and the retentive areas of bit memories, timers, and counters is available in the STEP 7 online help.

4.3.3 Interface types

The list below provides an overview of the interfaces used by your Windows PC:

- CPU 1505SP:
  - 1 PROFINET onboard interface of CPU 1515SP PC2.

    Isochronous data exchange via Isochronous Real Time (IRT) is possible.
  - 1 PROFIBUS interface, plug-in (optional)
- CPU 1507S:
  - 2 PROFINET interfaces, onboard or plug-in. One interface is IO-compatible.

    If the IPC used has a CP 1625 communications processor, isochronous data exchange over Isochronous Real Time (IRT) is possible.
- CPU 1508S:
  - 2 PROFINET interfaces, onboard or plug-in. Both interfaces are IO-compatible.

    If the IPC used has a CP 1625 communications processor, isochronous data exchange over Isochronous Real Time (IRT) is possible.

Additional information on the interfaces of the PC used is available in the technical specifications for your device.

4.3.4 PROFINET IO

Properties of PROFINET IO

PROFINET is a fieldbus standard of the PROFIBUS user organization that defines a cross-vendor communication and engineering model.

As part of PROFINET, PROFINET IO is a communication concept that is used to implement modular, distributed applications.

A PROFINET IO system consists of the following PROFINET devices:

- IO controller
  Device used to address the connected IO devices.
- IO device
  A distributed field device that is assigned to an IO controller.

The PROFINET IO controller operating mode enables direct access to IO devices via Industrial Ethernet.

The PROFINET IO device operating mode enables you to operate S7 stations as "intelligent" PROFINET IO devices on Industrial Ethernet.

For this purpose, the CPU uses PC interfaces that you must assign (Page 87) during configuration.

NOTE

Using the "Prioritized startup" functionality

If you want to use the "Prioritized startup" functionality in STEP 7 for the PROFINET interface of the CPU 1507S or CPU 1508S, separate the CPU and the device with the help of a PROFINET switch.

Reference

You can find additional information on the "PROFINET IO" topic in the STEP 7 online help and in the PROFINET (https://support.industry.siemens.com/cs/ww/en/view/49948856) function manual.

4.3.5 PROFIenergy

PROFIenergy

PROFIenergy (for PROFINET) reduces energy consumption by using PROFIenergy commands during production-free time.

Additional information

- Function manual: PROFINET (https://support.industry.siemens.com/cs/ww/en/view/49948856)
- Additional information on PROFIenergy is available on the Internet (https://www.profibus.com) under Common Application Profile PROFIenergy; Technical Specification for PROFINET; Version 1.0; January 2010; Order no: 3.802.

4.3.6 PROFIBUS DP

The PROFIBUS DP interface is used to connect distributed I/O (via CPU 1515SP PC2 and CM DP or IE/PB Link). PROFIBUS DP allows you to create extensive subnets, for example.

NOTE
Support of PROFIBUS DP
Note that PROFIBUS DP is only supported for legacy applications with CPU 1515SP PC2. For IPCs, you can use IE/PB Link to integrate legacy devices into your solution.

Properties of the PROFIBUS DP interface

The PROFIBUS DP interface provides the following properties and functions:

- PROFIBUS DP master and device
- S7 services

NOTE
Time-of-day synchronization
Note that the function Time-of-day synchronization is not supported.

NOTE
HART modules with PROFIBUS
The Software Controller does not support HART modules for the PROFIBUS interface.

NOTE
Configuring PROFIBUS DP interface
When configuring the address of the Software Controller PROFIBUS DP interface in TIA Portal, use one of the addresses offered in the drop-down list (Addresses 1 to 126), rather than Address 0.

4.3.7 Centralized I/O

Centralized I/O are available when you use CPU 1505SP on CPU 1515SP PC2. You can use any commonly used ET 200SP input and output modules with the CPU.

4.3.8 Web server of the CPU

The CPU has an integrated Web server that enables, among other things, the display of system diagnostics information via PROFINET.

You use an Internet browser on any web client, such as a PC, multi panel, or smartphone, to access:

- Module data
- User program data
- Diagnostics data of the CPU

This means access to the CPU is possible without STEP 7 installed. The Web server can only be configured using STEP 7.

The following options are available for accessing the Web server of the CPU:

- Web browser on the same PC
- Web browser on an external device using (virtual) Ethernet interfaces
- Web browser on an external device using the assigned PROFINET interfaces

Benefits of the Web server

The Web server enables monitoring and administering of the CPU by authorized users over a network. This enables long-distance evaluations and diagnostics. Monitoring and evaluation is possible without STEP 7. All you need is a web browser.

NOTE

Protection of the CPU

Make sure that you protect the CPU from being compromised, for example, by restricting network access using firewalls (Page 219).

Web browser

To access the HTML pages of the CPU, you need a web browser. The following web browsers have been tested for communication with the CPU:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Opera
- Mobile Safari and Chrome for iOS
- Android Browser
- Chrome for Android

Specific websites for the Software Controller

The functionalities of the Web server apply to all CPUs of the S7-1500 automation system. The Software Controller has the following special features:

- "Start page" web page

  The start page before the login provides general information about the CPU.

  The "Start page" web page also reflects the position of the mode selector. When the Software Controller is on a hardware platform that does not have a physical mode selector, the switch position of the mode selector always shows RUN mode in the Web server. When the Software Controller is working on a hardware platform that has a physical mode switch, the position of the mode switch always shows the current operating state of the hardware platform in the Web server.

- "Identification" web page

  The "Identification" web page gives you an overview of important specifications of the CPU.

- "View of Things" web page

  The "View of Things" web page allows you to operate objects that you have created in WinCC.

Reference

You can find additional information about the Web server in the Web Server (https://support.industry.siemens.com/cs/ww/en/view/109977246) function manual.

4.3.9 Fail-safe

Areas of application

The F-CPU is mainly designed for personal and machine protection and burner controls. In addition to the safety program, you can also program standard applications.

You can operate the F-CPU in safety mode or in standard mode.

Information on using the F-CPU in safety mode is available in the manual SIMATIC Safety - Configuring and Programming (https://support.automation.siemens.com/WW/view/en/54110126).

You can find additional information on the F-CPU in the Product Information for F-CPUs (https://support.industry.siemens.com/cs/document/109478599/simatic-s7-1200-s7-1500-f-cpus?dti=0&lc=en-WW).

When you load a project with fail-safe functionality to the CPU, it is shown on the display.

NOTE

DiagBase for F-CPUs on IPCs

If you are using a fail-safe Software Controller on IPCs, DiagBase must be uninstalled

Display

The status bar of the display shows the status of the safety mode.

Figure 4-4 Status bar

	Safety mode activated
	Safety mode deactivated

The display shows you the following in the "Overview" menu under "Fail-safe":

- Safety mode activated/deactivated
- Collective F-signature
- Last fail-safe change
- The version of *STEP 7 Safety* with which the safety program was compiled.

- Information on the F-runtime groups
  - Name of the F-runtime group
  - Remaining time for disabled safety mode
  - F-runtime group signature
  - Current cycle time
  - Maximum cycle time
  - Current runtime
  - Maximum runtime

The following is displayed for each F-I/O under "Fail-safe parameters":

- F-parameter signature (with address)
- Safety mode
- F-monitoring time
- F-source address
- F-destination address

The following additional menu command is displayed in the "Settings" menu under "Protection":

- Enable/disable F-password

Write access to F-blocks is not permitted.

NOTE

Controlling fail-safe inputs/outputs can result in an F-CPU STOP.

You can find detailed information on the individual display options, a training course and a simulation of the selectable menu commands in the SIMATIC S7-1500 Display Simulator (https://support.industry.siemens.com/cs/ww/en/view/109761758).

Web server

On the start page, the Web server displays the following under "General":

- The version of STEP 7 Safety with which the safety program was compiled.

On the start page, the Web server displays the following under "Fail-safe":

- Safety mode activated/deactivated
- Collective F-signature
- Last fail-safe change

On the "Module information" web page, the following is displayed under "Details" of the respective fail-safe I/O in the "Safety" tab:

- F-parameter signature (with address)
- Safety mode
- F-monitoring time
- F-source address
- F-destination address

Write access to F-blocks is not permitted.

NOTE

Controlling fail-safe inputs/outputs can result in an F-CPU STOP.

On the "Diagnostics" web page, the following is displayed under "Fail-safe":

- Name of the F-runtime groups
- Remaining time for disabled safety mode
- F-runtime groups signature
- Current cycle time
- Maximum cycle time
- Current runtime
- Maximum runtime

You can find additional information about the "Web server" topic in the Web Server (https://support.industry.siemens.com/cs/ww/en/view/109977246) function manual.

Installing

5

5.1 Delivery forms of the CPU

The CPU is delivered in different variants with different article numbers.

The CPU 1505SP is pre-installed on a CPU 1515SP PC2. The CPU 1505SP Software Controller cannot be ordered separately, but only in a bundle together with the hardware.

Install the CPU 1507S or CPU 1508S on a SIMATIC IPC which meets the system requirements.

The following table shows which CPUs can be installed on which IPCs:

	CPU 1507S	CPU 1507S F	CPU 1508S	CPU 1508S F	CPU 1508S T *	CPU 1508S TF *
IPC227G	✓	✓	--	--	--	--
IPC277G (PRO)	✓	✓	--	--	--	--
IPC427E	✓	✓	✓	✓	--	--
IPC477E (PRO)	✓	✓	✓	✓	--	--
BX-39A	✓	✓	✓	✓	--	--
PX-39A (PRO)	✓	✓	✓	✓	--	--
IPC627E	✓	✓	✓	✓	✓	✓
IPC677E	✓	✓	✓	✓	✓	✓
IPC647E	✓	✓	✓	✓	--	--
IPC847E	✓	✓	✓	✓	--	--

✓ installation is possible

-- installation is not supported

* 1508S T/TF only support a subset of possible configurations

For reference information on the SIMATIC IPCs, see chapter Reference information for use with SIMATIC IPC (Page 235).

5.2 System requirements

To use the Software Controller, your system must meet the following minimum requirements. For additional requirements that depend on the type of IPC used, refer to section Reference information for use with SIMATIC IPC (Page 235).

Category	Requirement
Operating system	• Windows 10 Enterprise LTSC 2019 • Windows 10 Enterprise LTSC 2021
	Note: Operation was only tested with the official operating system images provided by the SIMATIC IPCs. **Note:** Windows error handling features like recovery options, advanced startup settings, chkdsk, memory diagnostics, antivirus offline scan or similar may only be used after the PC has been restarted in "Windows-only" mode. For more information on how to start the system in "Windows-only" mode, see section Restarting Windows (Page 203).
Processor and memory	PC system: • Systems with dual core processor, at a minimum • 1.2 GHz or higher • RAM memory: – For CPUs 1507 and 1508, at least 8 GB **Note:** Hyperthreading systems are supported, however, enabling hyperthreading might decrease the speed of code execution and the Software Controller performance. When using Level 4 "plc_priority", you must deactivate hyperthreading.
Mass storage	• 1.6 GB free storage space on mass storage for full installation including: – Automation License Manager – SIMATIC device drivers – .net Runtime • 500 MB of temporary hard disk memory • CPU 1507S: 561 MB of unpartitioned storage space for the CPU volume, or 610 MB of free storage space on the unencrypted hard disk D • CPU 1508S: 1661 MB of unpartitioned storage space for the CPU volume, or 2760 MB of free storage space on the unencrypted hard disk D **Note:** The CPU cannot be installed on a mass storage with activated RAID technology. The setup program needs at least 430 MB of free memory on drive C: (the setup files are deleted again after installation is complete).
Disk controllers	For proper execution of the Software Controller, the use of Microsoft standard disk controllers is required. For this reason, the Software Controller installer will change disk controller drivers from 3rd party (Intel) drivers to Microsoft standard drivers for both AHCI and NVMe controllers in cases where a 3rd party driver is in use. Upon uninstallation of the Software Controller, the disk drivers wil not be changed back to their previous state.
Operator interface	Color monitor, keyboard and mouse or other pointing device (optional) that are supported by Windows

Category	Requirement
Communication interface	One or more communication interfaces for communication with STEP 7 or other S7 applications, or for communication with distributed I/O
Supported platforms	CPU 1515SP PC2 or SIMATIC IPC; see section Delivery forms of the CPU (Page 61) and section Reference information for use with SIMATIC IPC (Page 235).
BIOS settings	**Disabling memory test in the BIOS** PCs provide the option of a memory test. Some hardware tests, such as the memory test, are disabled by default in the BIOS setup program and are skipped during startup of the PC. This speeds up the boot process. If you are using the CPU on a SIMATIC IPC, the BIOS memory test should not be enabled. **Disabling booting from external media** The Hypervisor does not automatically prevent booting from external media. For reliable, defined real-time operation, the BIOS settings of the IPC platforms used must be managed. For additional BIOS settings required for the individual IPCs, see section Reference information for use with SIMATIC IPC (Page 235).

NOTE

PC systems with GPT and MBR partitioning

Except for the CPU 1515SP PC2, the Software Controller ≥ V30.0 does not support PC systems with MBR partitioning. If you used IPCs together with the Software Controller V21.9 before, reinstall the IPC using UEFI and update the operating system.

For the CPU 1515SP PC2 with MBR partitioning, note that MBR only allows a maximum number of 4 primary partitions. To extend the number of partitions, you must configure an extended partition.

NOTE

NTFS compression

If you use the Software Controller, NTFS compression must not be enabled for the following folders:

- C:\Boot\Grub2 with all included files
- C:\Boot\Siemens

Recommended splitters for CPU 1505SP (F)

The following display and HDMI splitters are recommended for the CPU 1505SP (F):

- Display splitter: Multi Stream Transport (MST) Hub DisplayPort™ 1.2 Quad Monitor CSV-5400
- HDMI splitter: Delock Display Port 1.2 Splitter 87720

NOTE

IWLAN/PB-Link

The Software Controller does not support the "IWLAN/PB-Link" functionality.

5.3 Creation of the CPU volume

Introduction

The CPU uses the mass storage of the PC on which it is installed. During the installation, a discrete CPU volume in which all CPU data is stored is created in the mass storage. The load and retentive memories are integrated into this CPU volume.

NOTE

Size of the CPU volume

To ensure reliable operation of the CPU, the CPU volume must not be reduced during operation. If you reduce the assigned mass storage area, this can lead to data loss or even a CPU crash.

Requirement for creation of a CPU volume

The CPU volume is allocated and formatted automatically during the installation process. The following requirements must be met:

- Except for the CPU 1515SP PC2, the partition style must be a "GUID Partition Table (GPT)".

  You can find the partition style in the "Volumes" tab under "Computer Management > Data storage medium management > Properties of the data storage medium".
- For CPU 1507S, one of the following requirements must be met:
  - At least 561 MB of unpartitioned memory on the hard drive, or
  - At least 610 MB available memory on the unencrypted D: drive
- For CPU 1508S, one of the following requirements must be met:
  - At least 1661 MB of unpartitioned memory on the hard drive, or
  - At least 2760 MB available memory on the unencrypted D: drive

Result

The CPU volume is created automatically as part of the installation process.

Manual creation of the CPU volume

If the CPU volume cannot be created automatically, you have the following options available:

- The installation process outputs a message that provides you the opportunity to manually adapt the partition structure of the mass storage device. Alternatively, you can cancel the installation process at any time.
- You must remove files from partition D: to create enough free space for the CPU volume by shrinking the size of partition D:.
- You must manually decrypt partition D:.

5.4 Overview of the installation tasks

You need administrator rights on your PC to install the CPU software.

NOTE

Installation with multiple hard disks

Install the CPU software on the same hard disk on which the operating system is installed.

Systems where more than one operating system is installed to the same or to different mass storage devices are not supported.

Requirement

Observe the following requirements for the installation:

- Your PC must meet the system requirements (Page 62).
- You must have Windows administrator (ADMIN) rights.
- The CPU cannot be installed on encrypted drives.

NOTE

Parallel use of virtual machine and installed Software Controller

Note that it is not possible to install/activate a virtual machine on the IPC while a Software Controller is already installed. The "Hyper-V" Windows feature is grayed out as soon as there is a Software Controller installed on the IPC.

NOTE

Set the Windows time to the current time.

NOTE

MAC addresses of interfaces

After installing the Software Controller, the X2 interface of the IPC will be assigned automatically to the Software Controller. Thus, it does not appear under Windows. If you use multiple devices in your network, before installation, take note of the MAC addresses of the interfaces to be able to select the correct interface during TIA Portal download.

NOTE

Recommended power plan

To guarantee the real-time behavior of your CPU, make sure that you are using one of the following power plans set by default on your PC:

- CPU 1505SP: "SIMATIC S7" power plan
- CPU 1507S/1508S: "SIMATIC IPC" power plan

Do not select the "Balanced" setting recommended by Windows.

Effect of the installation on the power saving settings of the PC

The CPU does not allow the use of "Hibernate" or "Standby" of the operating system.

Even if your PC supports these power saving settings, they will be disabled by default after installation of the Software Controller.

Procedure

To perform the installation properly, follow these steps:

1. Deactivate the universal write filter (UWF).
2. If a virus scanner is installed, disable it for the installation.
3. Ensure that no other version of the CPU or SIMATIC NET software is installed at the time of installation. If a version of the above-mentioned software is already installed, uninstall that version first.
4. Configure your PC according to the Reference information for use with SIMATIC IPC (Page 235) section and check if all conditions prior to installation are met.
5. Install the CPU software on the same mass storage device on which the operating system is installed.
6. License the installation (Page 84) with the Automation License Manager.

NOTE

Data loss

An uninstallation or repair of the CPU deletes the STEP 7 user program on the controller, the configurations and retentive data, and all settings changed by you from the display of the CPU.

NOTE

Effect of the installation on existing ODK directories

The default value that describes the file path is:

%ProgramData%\Siemens\Automation\ODK1500S\

The SIMATIC S7-1500 Software Controller setup checks whether the file path already exists and the necessary administrator rights are stored.

If this is not the case, the directory is renamed to "ODK1500S_OLD1" or "ODK1500S_OLD2", and a new directory with the correct access rights is created.

Automatic configuration of BIOS settings

During installation, the mandatory and recommended BIOS settings can be set automatically. If you choose automatic BIOS configuration, you do not need to select the correct settings prior to installing the Software Controller.

Mandatory parameters are parameters that are critical or strongly recommended to be set to the correct value. Failure to meet the required value may lead to improper installation of the Software Controller or cause significant performance issues. Recommended parameters are parameters that enable the Software Controller to work more efficiently, even if they do not have a direct effect on its installation.

The automatic selection of the correct BIOS settings is supported by the following IPCs:

- IPC BX39A
- IPC PX39A
- IPC 627E
- IPC 677E
- IPC 647E
- IPC 847E

NOTE

Note that the automatic configuration of BIOS settings only works for clean installations where the default BIOS settings have not been changed yet.

If you have already changed the BIOS settings before, change the BIOS settings to the correct values manually. You can find the correct BIOS settings in section Reference information for use with SIMATIC IPC (Page 235).

Customer certificate and key files

A certificate and key are required to configure BIOS settings automatically. For security reasons, we recommend that you use your own certificate and key files. For creating your own certificate and key file, use an appropriate tool such as OpenSSL.

Example of an OpenSSL command:

```
openssl req -x509 -nodes -days 3650 -newkey rsa:2048 -keyout
tmpkey.pem -outform DER -out tmpcert.crt -sha256
```

Place these two files into a directory. The certificate file must be named **tmpcert.crt** and the key file **tmpkey.pem**.

Afterwards, create an environment variable named `SWCPU_USER_CERT`, which has a value of the path for the certificate folder.

Provide your own certificate and key file to be used to configure the BIOS settings. If you do not provide your own certificate and key, the installer will display a warning message and ask for confirmation to continue with the default certificate and key. If you do not provide your own certificate and key and also do not approve the use of the default certificate and key, the installation process will terminate due to security reasons.

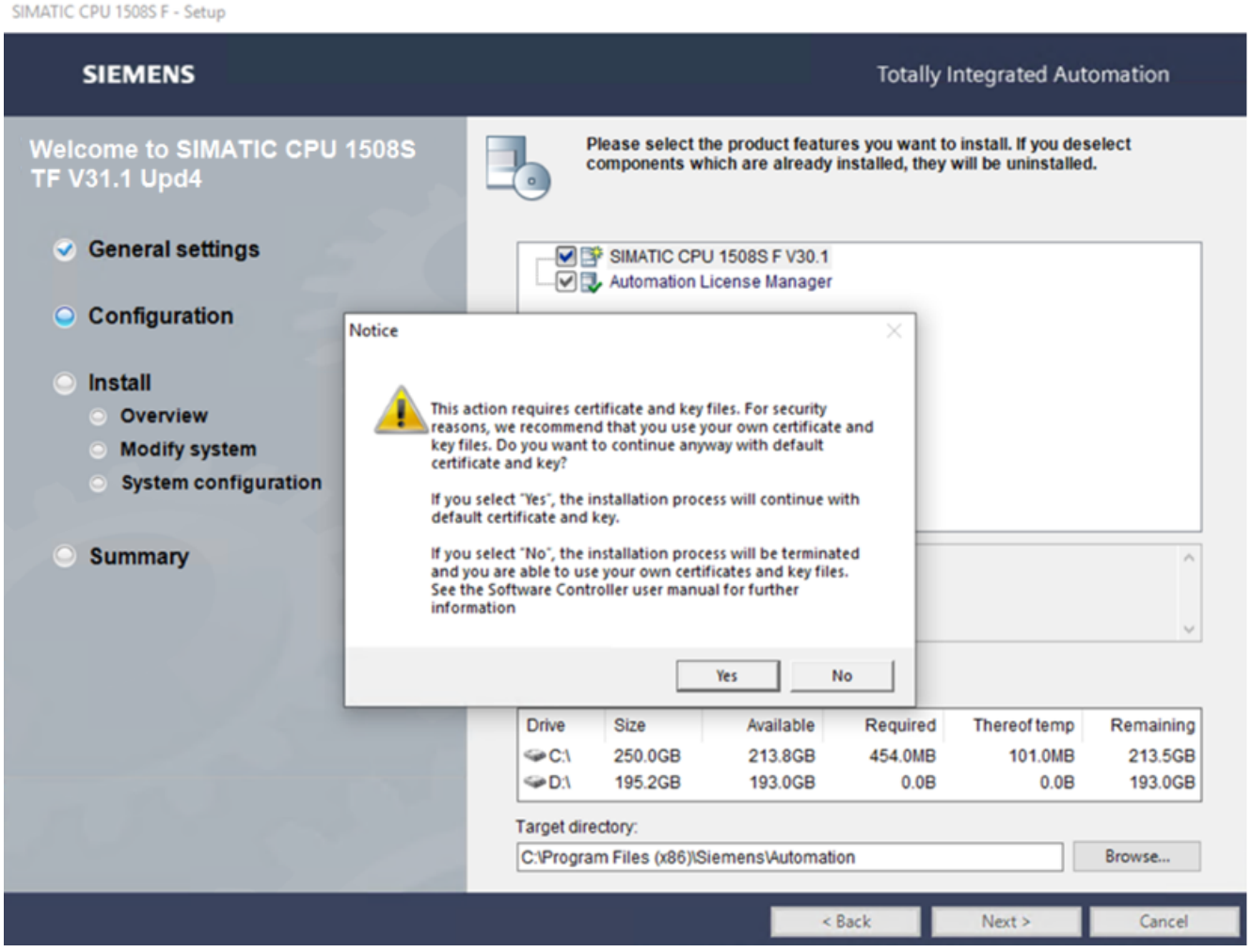


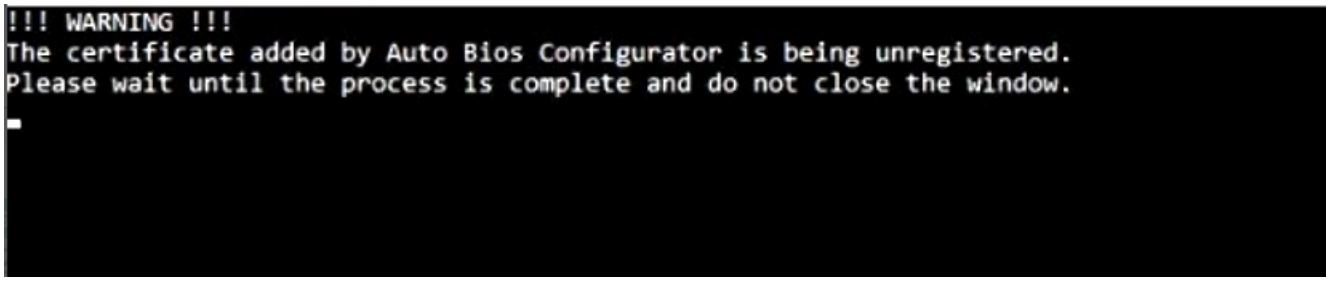
Figure 5-1 Automatic selection of BIOS settings

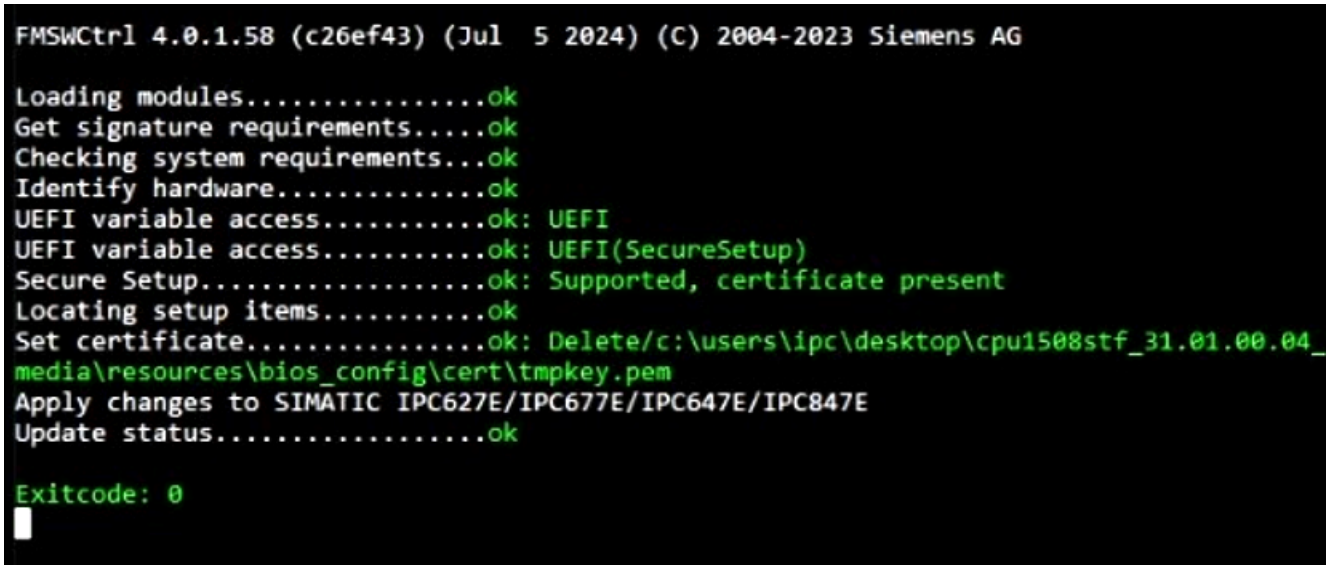
NOTE

After the BIOS settings are configured and the process is completed, the certificate and key will be unregistered from BIOS and deleted from the related partition.

A script will then run after the initial reboot to remove the certificate, which is essential for security and must not be disabled.

The following images show the the removal of the certificate by the script.





Prerequisites before starting the installation

Before starting the installation, make sure that the "Setup Management interface" option is enabled in the BIOS. If this feature is not enabled, the automatic BIOS configuration tool will not function.

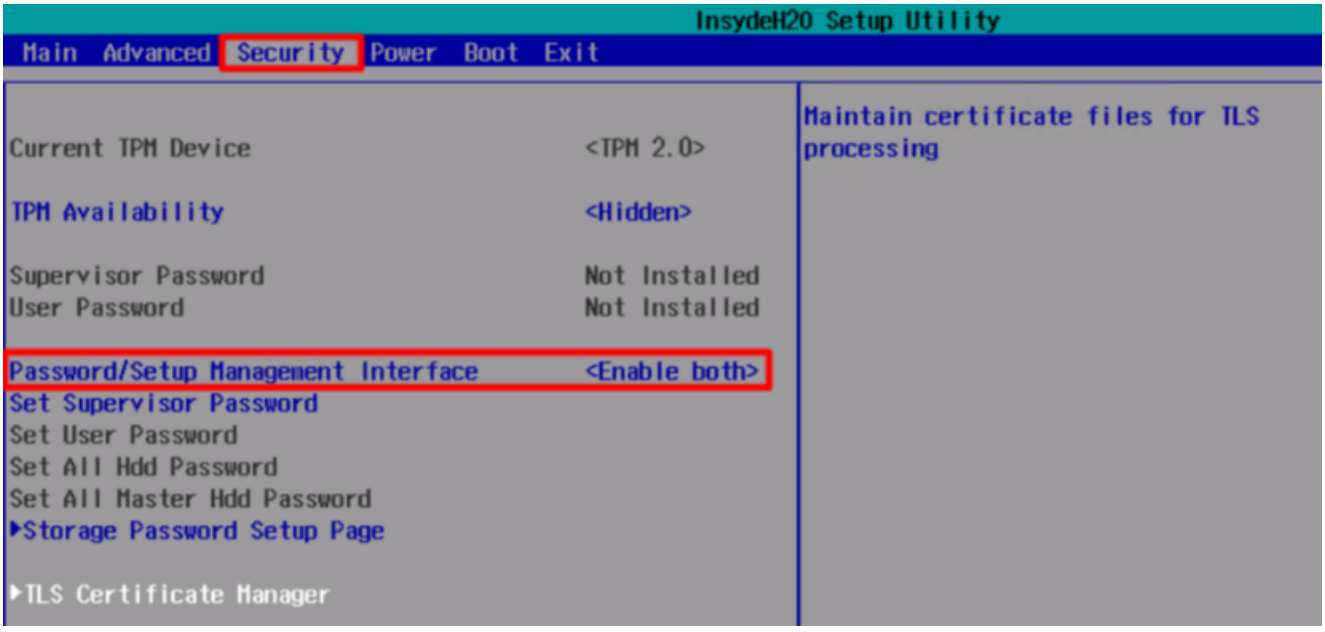


Figure 5-2 BIOS Security options

Setting the "Supervisor Password" and "User Password" is optional. These choices will not affect the new BIOS functionality.

Procedure

The following outlines the steps required to activate the automatic BIOS configuration:

1. Start the installation of the Software Controller V31.1 setup.
2. Choose the installation language and click "Next" to continue.

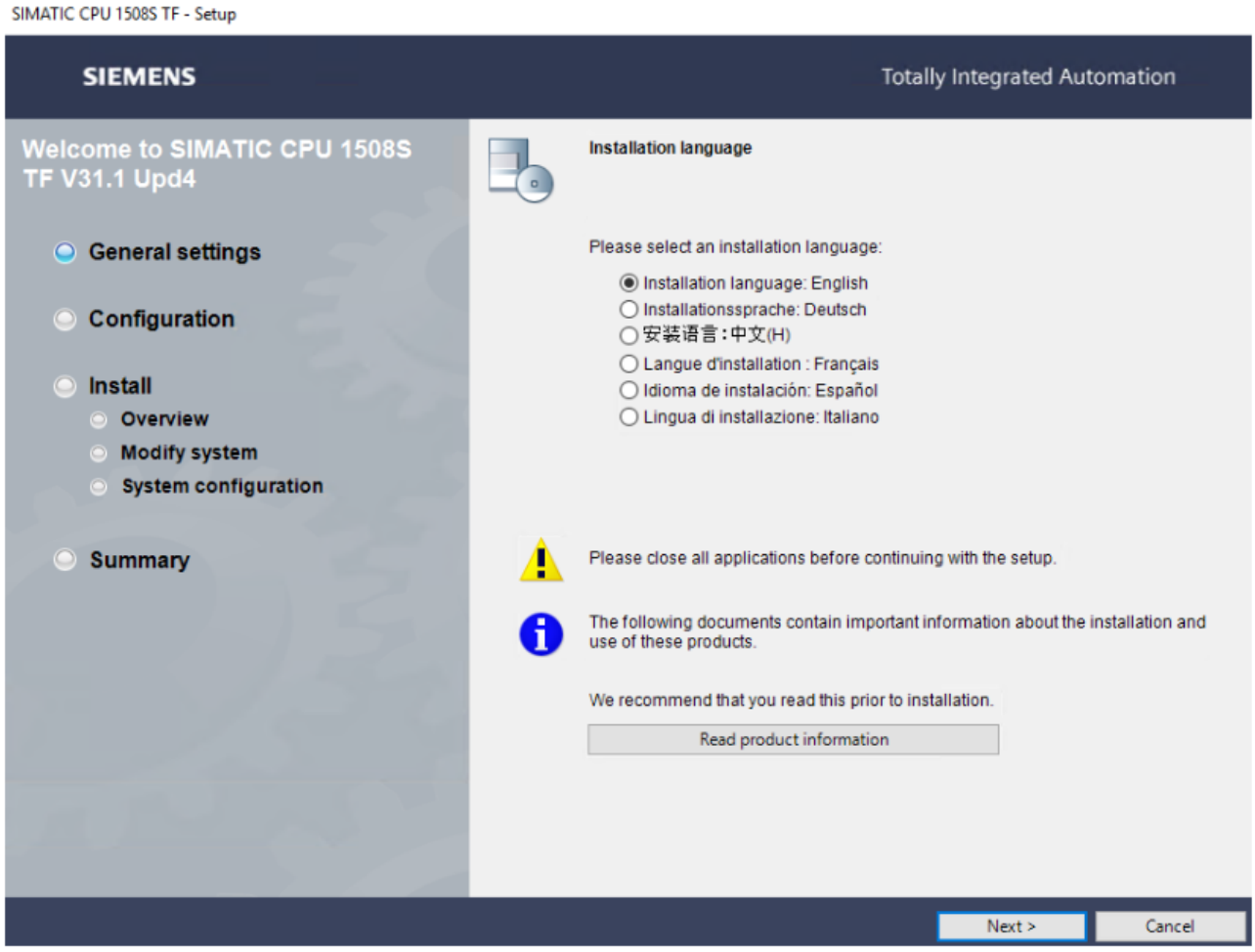


Figure 5-3 Installation language

3. Select the components to be installed and the target directory.

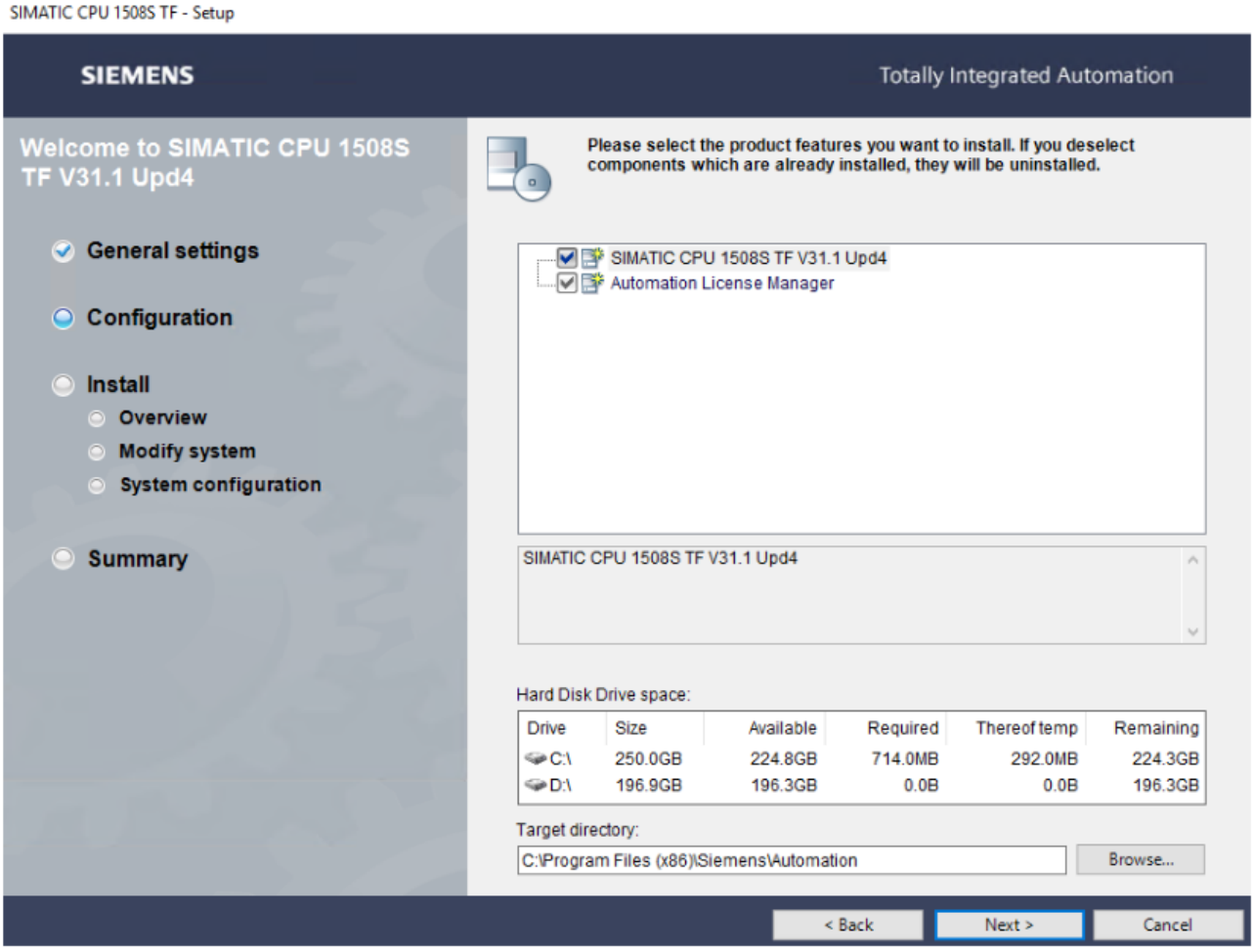


Figure 5-4 Components and directory

NOTE

Verification of BIOS version used

For BX39A and PX39A devices, the BIOS version must be 29.01.07 or later. If the BIOS version is earlier than 29.01.07, the installation process will be halted and will not proceed.

4. Confirm the use of the tool for automatically setting the correct BIOS settings.

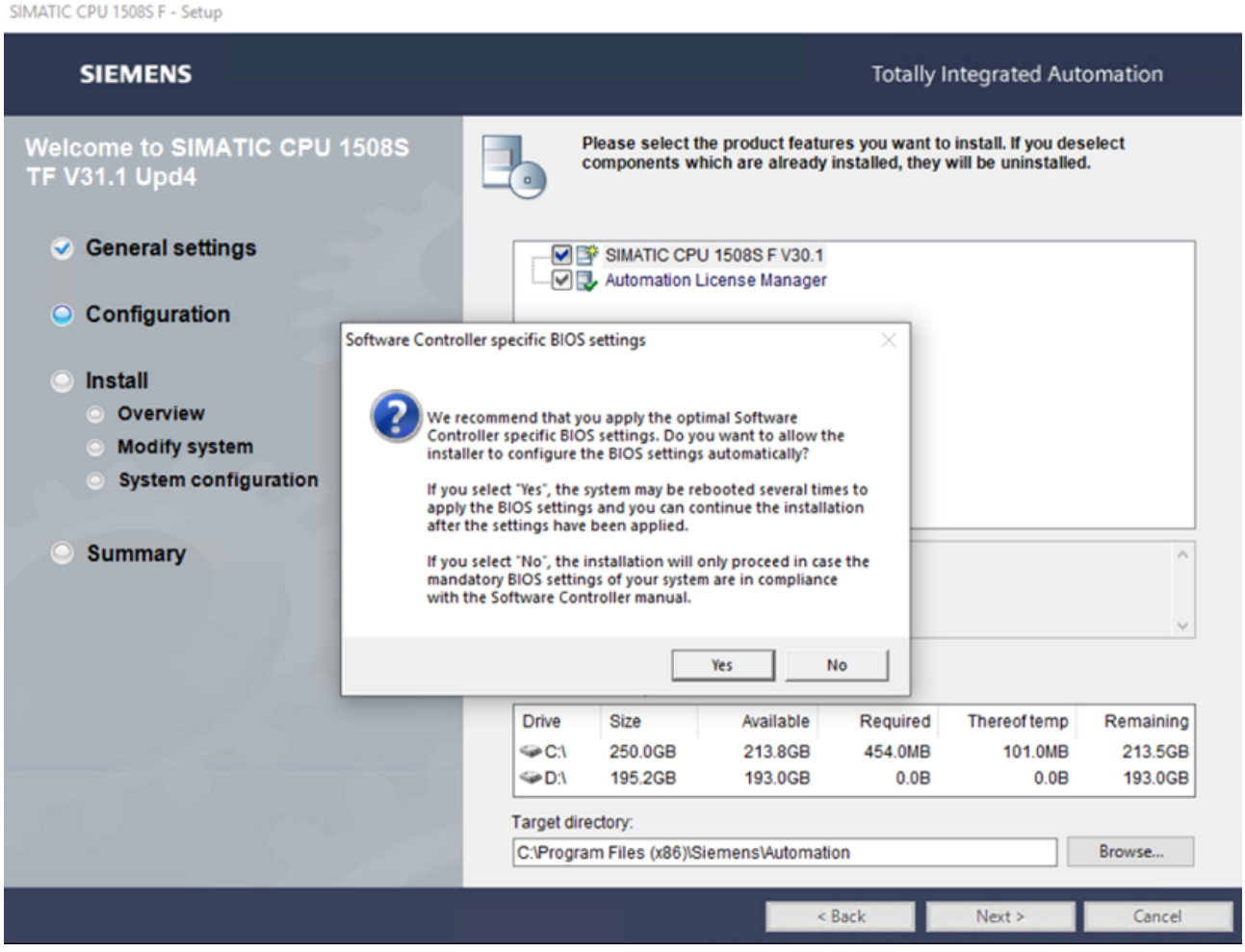


Figure 5-5 Configuration of BIOS settings

If you select "Yes", the system may be rebooted several times to apply the BIOS settings. You can continue the installation after the BIOS settings have been applied. Once the BIOS settings are correct, they will be logged in the system and the dialog does not appear any more.

If you select "No" and the mandatory settings are not correct, the installation will not proceed. If the mandatory settings are correct, the setup will continue without changing any BIOS settings.

NOTE

If the mandatory and recommended BIOS settings already have their correct value, the pop-up window shown above will not appear.

5. Click "Yes" to confirm the use of the standard certificate or click "No" to add your own certificate information and restart the setup.

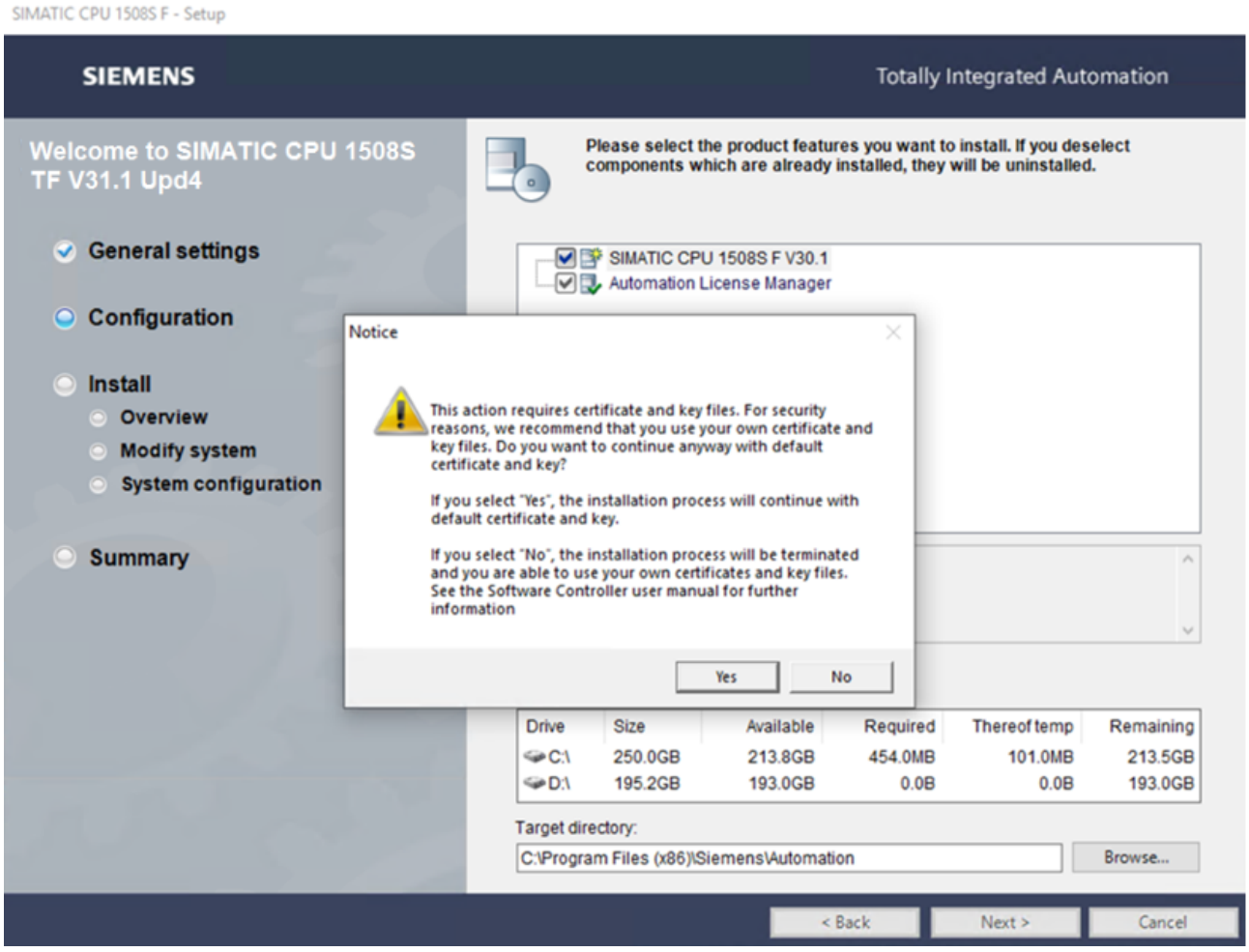


Figure 5-6 Standard certificate

NOTE

Automatic configuration of BIOS settings

Note that the automatic configuration of the BIOS settings during the Software Controller installation may take several minutes. Do not cancel or close the installation process.

After successful installation, the CPU will be in STOP mode.

Verification of BIOS settings

You can verify the result of the automatic BIOS configuration by comparing the settings with the values mentioned in section Reference information for use with SIMATIC IPC (Page 235) of your IPC used.

NOTE

Automatic configuration of BIOS settings in upgrade scenarios

During an upgrade, the BIOS settings are not automatically configured for IPC 627E, IPC 677E, IPC 647E, and IPC 847E. For these IPCs, you need to configure the mandatory and recommended BIOS settings manually.

For BX39A and PX39A IPCs, the automatic configuration of BIOS settings is supported only if the upgrade is started in "Windows-only" mode. Otherwise, the following note appears:

"The installation can not continue. Please restart the system in Windows-only mode and start the installation again."

For more information on upgrades and updates, refer to section Upgrades and updates (Page 80).

Users of the external NVIDIA graphics card

To prevent the NVIDIA graphics card from influencing the real-time behavior of the CPU, we recommend that you use the power management mode "Prefer consistent performance":

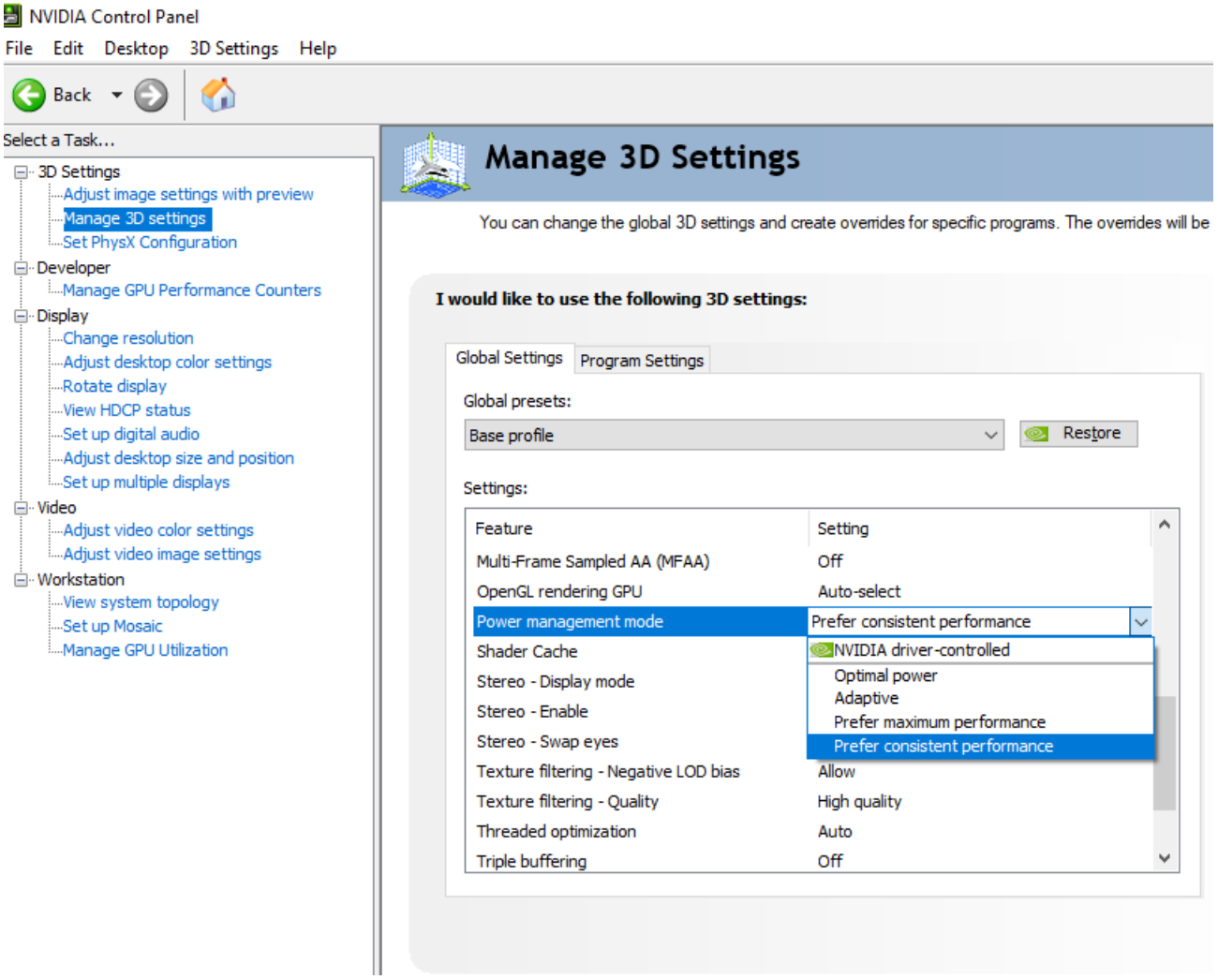


Figure 5-7 NVIDIA power management

NOTE

Using NVIDIA AI cards

Note that the following NVIDIA AI card is not supported:

AI Unit NVIDIA A2

NOTE

External graphics cards for 1508S T/TF are not supported

Due to possible impacts on stable real-time behavior, external graphics cards are not supported for the CPU 1508S T/TF.

5.5 Installing the Software Controller via Online Software Delivery

Requirements

To download the software as a data packet from the Online Software Delivery (OSD) platform, enter the e-mail address to which the download link is to be sent when you place the order. You will then receive a download notification e-mail. The e-mail contains a link to the Online Software Delivery (OSD) platform.

Procedure

1. Log in to Online Software Delivery using your login name and personal password. You will find your access data in the download notification email.
2. Follow the download and license procedure.

   For detailed information on the Online Software Delivery (OSD) and download procedure, visit Online Software Delivery (OSD) (https://support.industry.siemens.com/cs/ww/en/view/109759444).

Result

Depending on your purchase, the following installation files are available:

CPU	Article number	File
1507S	6ES7672-7AC02-0YG0	SIMATIC_CPU_1507S_V31.1.exe
1507S F	6ES7672-7FC02-0YG0	SIMATIC_CPU_1507SF_V31.1.exe
1508S	6ES7672-8AC02-0YG0	SIMATIC_CPU_1508S_V31.1.exe
1508S F	6ES7672-8FC02-0YG0	SIMATIC_CPU_1508SF_V31.1.exe
1508S T	6ES7672-8TC02-0YG0	SIMATIC_CPU_1508ST_V31.1.exe
1508S TF	6ES7672-8UC02-0YG0	SIMATIC_CPU_1508STF_V31.1.exe

Transfer these files to your target system, for example, with a USB device, and execute the files to install the CPU.

For the installation, follow the installation procedure as described in Installing the Software Controller via DVD (Page 78).

5.6 Installing the Software Controller via DVD

To install the Software Controller, copy the installation files from the DVD to a USB flash drive. Follow the instructions of the setup program.

If the setup program does not start automatically, manually start the "Start.exe" file by double-clicking it.

If you are logged in with an account that does not have administrator rights, run the "Start.exe" file using the "Run as administrator" shortcut menu command.

Procedure

To install the Software Controller, follow these steps:

1. If a Software Controller <V30.0 is already installed, uninstall it first. Also delete the RAW CPU volume partition after uninstallation.
2. Execute the installation of the Software Controller.
3. Select the language for performing the installation.

   NOTE
   Chinese as installation language
   To display Chinese correctly as an installation language, install the Chinese font first.

4. Read the product information.
5. Confirm with "Next".

   The installation continues.
6. Select the components to be installed from the list.

   Select an installation path.
7. Continue to follow the instructions, which will guide you through the installation.
8. Choose whether you want to carry out the licensing (Page 84) during the installation or at a later time.
9. Confirm the installation dialog with the "Install" button.
10. Restart the PC after successful completion of the installation.

NOTE
Installed files
We recommend that you do not change the access rights to the installed files.

Result

The installation is complete. During the installation process, all product languages were installed by default. The installation creates an entry in the Windows Start menu.

You can choose between the following options, which will appear in the boot menu when the PC is restarted:

- **Windows**

  All hardware resources are assigned to Windows. The hypervisor and the Software Controller are not started.

- **Windows and S7-1500 Software Controller**

  Windows starts normally and you can open the display in "Power on" mode. Switch on the Software Controller using the "Power" button. The Software Controller starts in "STOP" mode.

NOTE

If you do not select one of the two options within five seconds, the PC starts with the option "Windows and S7-1500 Software Controller" by default.

5.7 Scripted installation without user interaction

You can use a script to carry out a silent installation that does not require any user interaction.

NOTE

To carry out a silent installation, the correct BIOS settings must be configured before starting the silent installation script.

To install the Software Controller without user interaction, proceed as follows:

1. Download the software as a data packet from the Online Software Delivery (OSD) platform or use the installation DVD.
2. Execute the downloaded executables and enable the option "Extract the setup files without being installed".

   The setup objects are extracted to a local temporary folder where a silent installation script is also available.

3. Run the "SilentInstall_CPU150xS.bat" file as an administrator.

   When the script runs, the Software Controller installation screen is shown without any selectable option. The script starts the installation directly. The pop-up windows that might appear during silent installation are in German. After the installation finishes, the installation window closes automatically. A shortcut to the Software Controller is created on the desktop.

   NOTE

   Messages during silent installation

   During silent installation, BIOS-related pop-ups appear. If you want to prevent these pop-ups from appearing, set the correct BIOS settings manually before installation. You find all mandatory and recommended BIOS settings in section Reference information for use with SIMATIC IPC (Page 235).

4. Reboot the system manually.

5.8 Upgrades and updates

Definition of upgrade and update

For the Software Controller and Open Controller, we distinguish between upgrades and updates.

Upgrades include new features and functionality, for example, when upgrading from V21.8 to V21.9.

Updates include minor changes such as bug fixes and performance improvements, for example, when updating from V21.9 to V21.9.4.

This chapter describes the rules, behavior and known issues when updating/upgrading between different versions.

NOTE

Updating Windows operating system

Apart from keeping the Software Controller up to date, also remember to regularly update Windows in a secure environment.

Upgrading from a version < V30.0 to V31.1

It is not possible to upgrade from a Software Controller version < V30.0 to V31.1. To install the Software Controller V31.1 to a system where a version < V30.0 is installed, proceed as follows:

NOTE

Note that the following description does not apply to the CPU 1505SP on CPU 1515SP PC2. For the CPU 1505SP on CPU 1515SP PC2, a completely new bundle image is necessary.

Also take note of the information in section "Open Controller CPU 1515SP PC2 + HMI bundle" at the end of this section.

1. Uninstall any older version of the Software Controller first.
2. After uninstalling the older version, run the Software Controller V31.1 setup from scratch.

   IPCs 6x7/8x7E: Manually delete the RAW Partition used as CPU volume after uninstallation.

   IPCs 4x7E: Reinstall the Windows operating system using UEFI boot. Note: Move the license key from the device before reinstalling the device. This way, you can use an upgrade license for V31.1.

   For converting the old license key to a V31.1 license key, refer to chapter Licensing the Software Controller (Page 84).
3. Open an existing TIA Portal project containing an older version of the Software Controller in TIA Portal V20.
4. Exchange existing Software Controllers (< V31.1) in the project to V31.1 by their new MLFBs.

   Result: The user program and interface assignments to the Software Controller will be kept after the exchange but the assignments to “Simatic PC Station” will be removed.
5. For the Software Controller V31.1 you need to make the resource configuration consistent with the TIA Portal hardware configuration. For the resource configuration, use Resource Configurator. Resource Configurator is part of the installer setup and is installed automatically on the target device. For more information on Resource Configurator, go to section Resource Configurator (Page 91).

PC Station

When you add a Software Controller ≥ V30.0, the hardware configuration properties of the PC Station are removed and the checkbox is disabled.

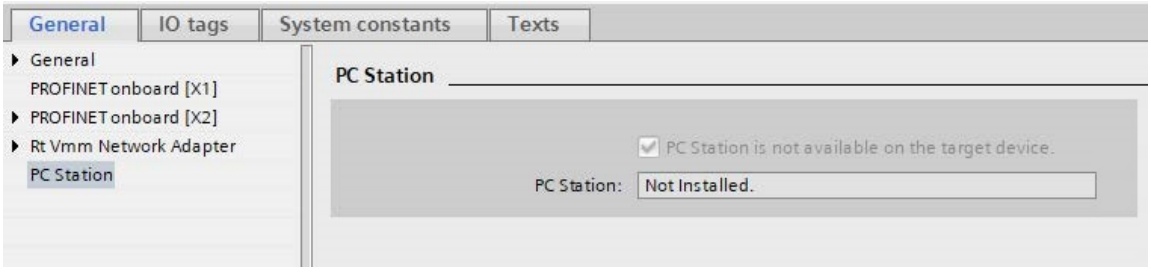


Figure 5-8 Grayed out PC Station checkbox

The "W1" Runtime communication interface is available as an option on the "Extended download to device" and "Extended go online" dialogs.

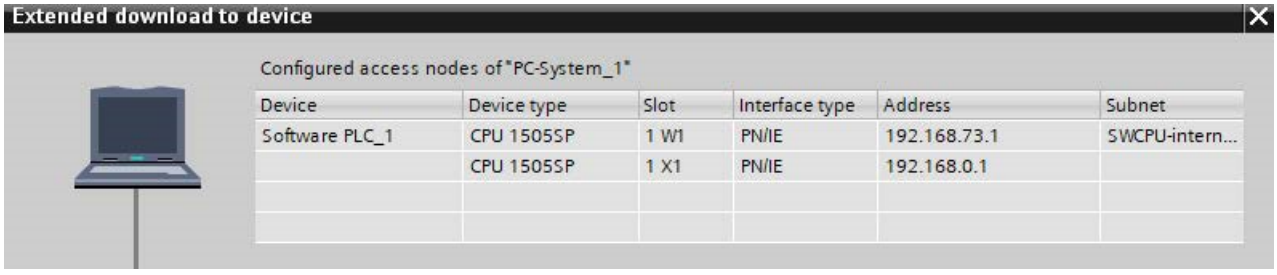


Figure 5-9 W1 interface

Open Controller CPU 1515SP PC2 + HMI bundle

For version V31.1, there is no Open Controller CPU 1515SP PC2 + HMI bundle available in TIA Portal V20. However, you can plug WinCC Unified RT to version V31.1 of Open Controller CPU 1515SP PC2.

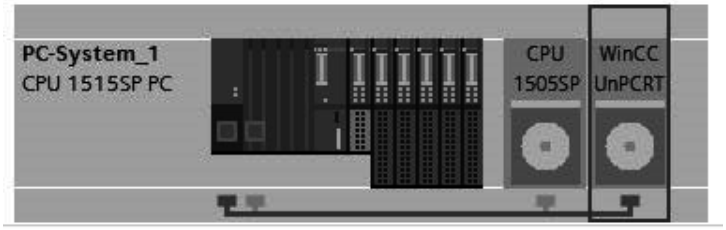


Figure 5-10 Open Controller and WinCC Unified RT

If you have WinCC RT Advanced plugged into your project, WinCC RT Advanced will be removed when you change the Open Controller bundle from a version ≤ V21.9 to V31.1.

Version scenarios

- When you change from a version ≤ V21.9 of Open Controller CPU 1515SP PC2 + HMI bundle to a version ≥ V31.1, WinCC RT Advanced for Open Controller CPU 1515SP PC2 will be removed.
- When you change from version ≥ V30.0 Open Controller CPU 1515SP PC2 with HMI to a version ≤ V21.9 of Open Controller CPU 1515SP PC2 + HMI bundle, WinCC RT Unified will be kept on the device.

Upgrading from V30.x to V31.1

It is possible to upgrade the Software Controller from V30.x to V31.1. For the upgrade, proceed as follows:

1. Open an existing TIA Portal project containing an older version of the Software Controller in TIA Portal V20.

   NOTE

   Version compatibility

   You can download a V30.x TIA Portal project to a V31.1 Software Controller.

   It is also possible to download a V31.1 TIA Portal project to a V30.1 Software Controller installation. However, if you load a V31.1 TIA Portal project to a V30.1 Software Controller installation, the new V31.1 functions, such as higher Motion Control resources, will not be accessible and usable. There is a risk of such projects affecting the system negatively.

   It is possible to exchange older versions of Software Controllers (< V30.0) to V31.1 with new MLFBs.

   The Software Controller V31.1 targets are only available in TIA Portal V20. However, it is possible to go online and obtain diagnostic information with older TIA Portal versions (V19, V18).

2. Exchange existing Software Controllers (< V31.1) in the project to V31.1 by their new MLFBs.
3. For the Software Controller V31.1 you need to make the resource configuration consistent with the TIA Portal hardware configuration. For the resource configuration, use Resource Configurator. Resource Configurator is part of the installer setup and is installed automatically on the target device. For more information on Resource Configurator, go to section Resource Configurator (Page 91).

NOTE

IP address of SIMATIC RT-VMM Network Adapter

After completing the upgrade to V31.1, the IP address of the SIMATIC RT-VMM Network Adapter will be lost. After the upgrade, set the SIMATIC RT-VMM Network Adapter again.

TIA Portal Openness

Unlike older versions of the Software Controller, this version does not support PC Station download via the TIA Portal Openness API. You can only perform a configuration download to the Software Controller over the physical interface assigned to the Software Controller or via the Runtime communication interface (W1).

5.9 Licensing the Software Controller

The software requires a product-specific license key that you install with the Automation License Manager. Each SIMATIC software product for automation (for example, STEP 7) has its own license key. You must install the license key for each product.

You do not require a license key for CPU 1505SP and CPU 1505SP F.

Working with the Automation License Manager

The Automation License Manager is a product of Siemens and is used for managing license keys. The Automation License Manager is supplied on the installation data medium of the Software Controller by default and is transferred automatically during the installation process.

Software products that require license keys for operation automatically notify the Automation License Manager that license keys are needed. If the Automation License Manager finds a valid license key for this software, then the software can be used according to the conditions of use associated with this license key.

Certificate of License

A Certificate of License is included in the scope of delivery. The Certificate of License contains your unique license number that matches the license number of the license key. The license certificate serves as proof that you have a valid license key. Keep this certificate in a safe place that is easily accessible from the platform on which the Software Controller is running.

NOTE

Resellers

Note that resellers must deliver the Certificate of License together with the purchased solution or machine.

NOTE

Obtaining a replacement license key

You must have a valid Certificate of License to get a replacement license key.

The Certificate of License of, for example, Version 3.0 also allows the operation of a CPU Version 20.8, 21.8 or 21.9.

License key

The license key for the CPU is located on a USB device that is included in the scope of delivery. If you obtain the software via download, the license key is provided using the download link.

The license key of Version 3.0 is valid for Version V31.1.

If the USB device with the license key is lost or damaged, contact Siemens Support (https://support.industry.siemens.com/cs/ww/en/). You need the Certificate of License to receive a replacement license key from Siemens.

Transferring the license key

The license key can be transferred during the installation or afterwards.

NOTE

The license key must be installed on a file system of type NTFS.

If the USB device with the relevant license key is inserted in the USB port of the PC at the start of installation, the license key will be transferred automatically during the installation. If necessary, the following options are available for installing the license key subsequently:

- To transfer the license key **manually** from a network computer or other storage medium, select the "Manual license transfer" button.
- Insert the USB device with license key and select the "Retry license transfer" button. The Automation License Manager opens to transfer the license key.

If you do not want to install a license key for the time being, select the "Skip license transfer" button.

NOTE

Working with the CPU without a license key

For legal reasons, a valid license key is required for this product.

If no license key is present on your PC, the CPU will continue running. However, a message will inform you at regular intervals that a valid license key has not been found.

Manually transferring the license key subsequently

When you start the CPU without a transferred license key, a message is displayed on the screen. Ensure that the Automation License Manager is installed on your computer.

To **manually** transfer the license key for the CPU subsequently, use one of the following two possibilities:

1. Transfer the license locally via the Automation License Manager from a USB device.
2. Transfer the license remotely via the Automation License Manager over the network.

For a detailed description on how to transfer licenses, refer to the Automation License Manager (https://support.industry.siemens.com/cs/ww/en/view/102770153).

Recovering the license key in case of defective mass storage

If an error has occurred on the mass storage or USB flash drive containing your license key file, contact Siemens Support (https://support.industry.siemens.com/cs/ww/en/). Make sure you have your Certificate of License available when you contact the hotline.

5.10 Uninstalling the Software Controller

Procedure

To uninstall the Software Controller on your PC, follow these steps:

1. In the "Control Panel > Programs > Uninstall program" menu, select the entry "SIMATIC CPU 1505SP", "SIMATIC CPU 1507S" or "SIMATIC CPU 1508S".

   A dialog for the uninstallation opens.
2. Select the CPU.
3. Follow the rest of the steps for the uninstallation.
4. Restart the PC system.

NOTE
Uninstallation when the CPU display is open
When you uninstall the CPU, the CPU display is closed automatically if it was still open.

Result

The software for the CPU and the CPU display are uninstalled. The CPU volume is formatted, and CPU-specific data and links are deleted.

The CPU volume is formatted but is retained. In case of a new installation, the CPU volume is reused.

The Automation License Manager is not uninstalled automatically with the uninstallation of the software for the CPU. If necessary, uninstall the Automation License Manager separately.

NOTE
BIOS settings
Note that the BIOS settings will not automatically revert to their original state during Software Controller uninstallation.

Commissioning

6

6.1 Assigning interfaces for communication

Interfaces can be used by the Software Controller. Only these exclusively assigned interfaces enable connection of distributed I/O. In addition, communication is also possible.

Communication between devices

The basis of all types of communication is always a previously configured network. In order to configure a network for the CPU, you must assign the interfaces for communication to the CPU or PC system beforehand. An interface is:

- A communications processor such as Intel Springville i210/CP 1625 for PROFINET
- An onboard PROFINET interface on a Siemens Box, Rack, or Panel PC, or on CPU 1515SP PC2

NOTE

Use of two PROFINET interfaces

With the CPU 1507S, you can use two PROFINET interfaces in your configuration. In this case, one of the PROFINET interfaces acts as a PN IO controller for the PROFINET IO communication concept and other communication services. You use the second PROFINET interface for the available communication services.

With the CPU 1508S, both interfaces are IO-compatible.

A detailed list of the supported interfaces and on-board interfaces of the IPC is available in the Product Information.

Requirement

- STEP 7 is open.
- The project view is open.
- The device view is open.

Procedure

To assign the interfaces for the communication with the CPU, follow these steps:

1. Select the onboard interface in the device view.

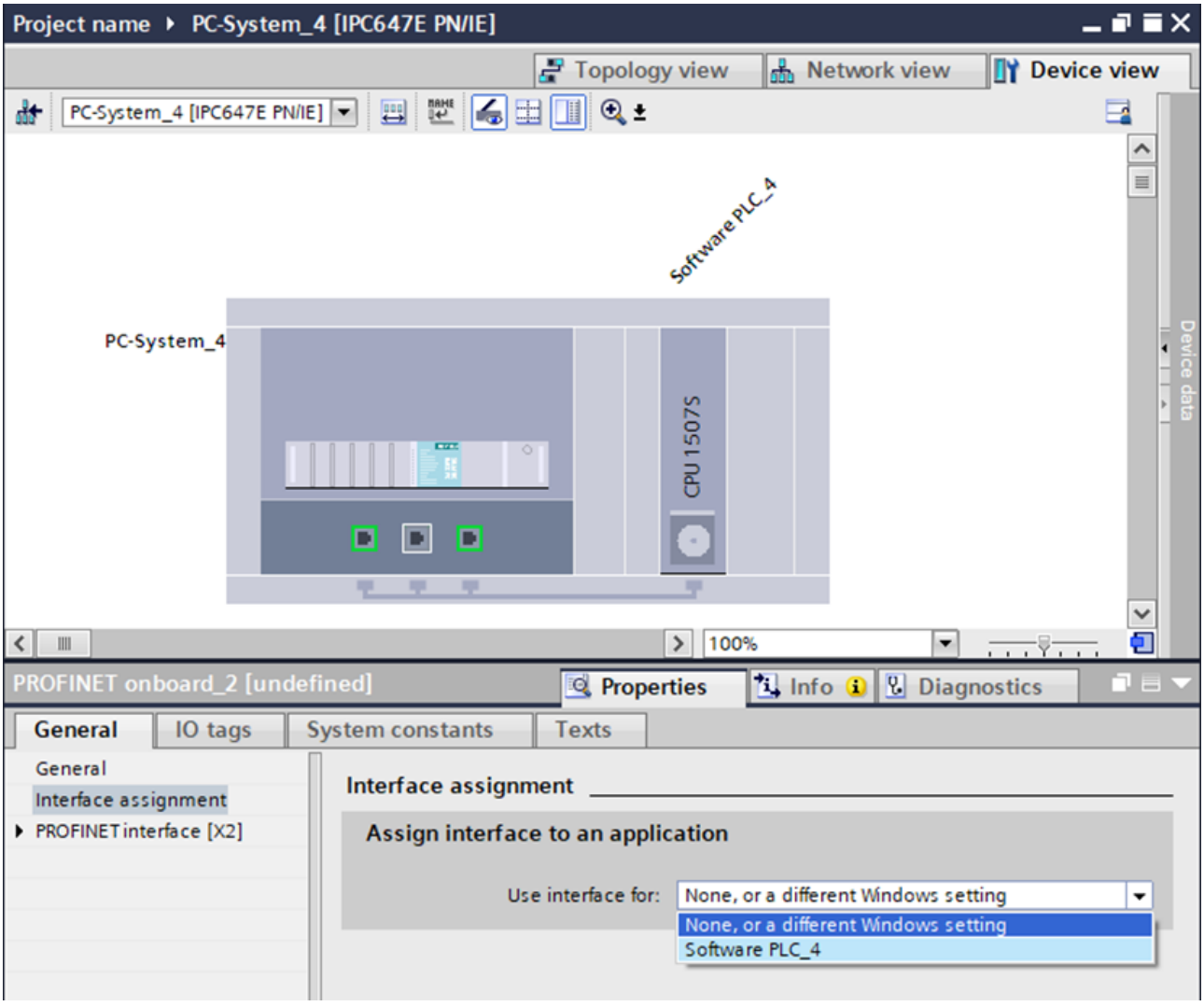


Figure 6-1 Assign interface to the CPU

2. Assign the interface in the properties of the CPU.

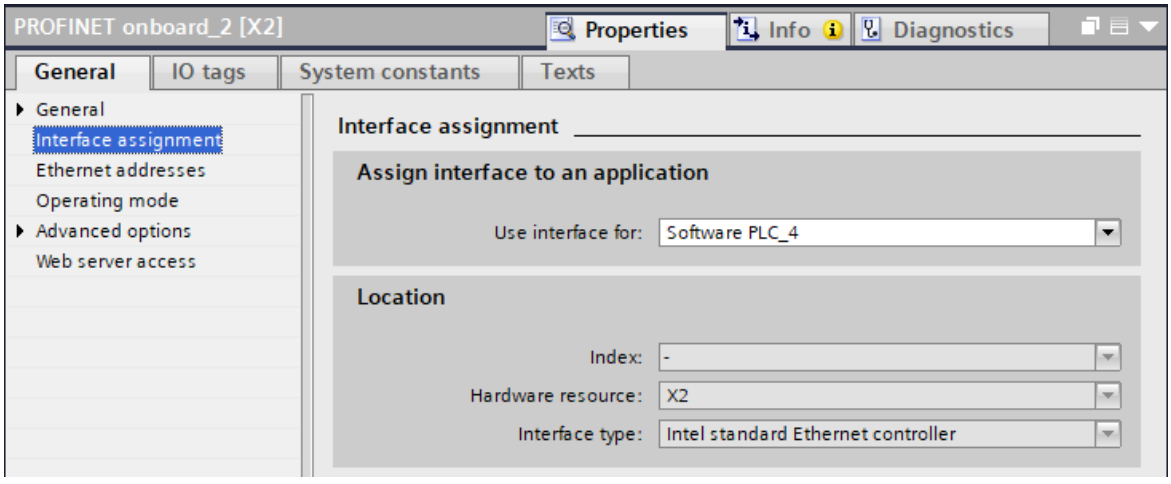


Figure 6-2 Select the interface

Depending on the interface and PC type, the following properties are available:

- Index: fixed
- Selected IPC extension (HW): PCI/PCIe slot configuration
- Hardware resource: Slot on PC

  Assign the X2 interface to the Software Controller (or X1 for Open Controller CPU 1515SP PC2). The interface is associated with HW_ID 64.
- Interface type: Interface type for standard Ethernet interfaces, fixed

3. Add the desired PN/IE communication processor from the catalog.

NOTE

You can only assign a CP 1625 to the CPU 1507S and the CPU 1508S.

4. Assign the communication processor in the CPU properties.
5. Compile the project with "Edit > Compile".
6. For downloading the project into the Software Controller, select the Software Controller by clicking on it. Do not click on the entire PC system the Software Controller is part of but only on the Software Controller.

Reference

You can find more information on the topic "Assigning interfaces" in the STEP 7 online help.

Ethernet addresses

Among other options, this section offers the possibility of setting and obtaining the IP address.

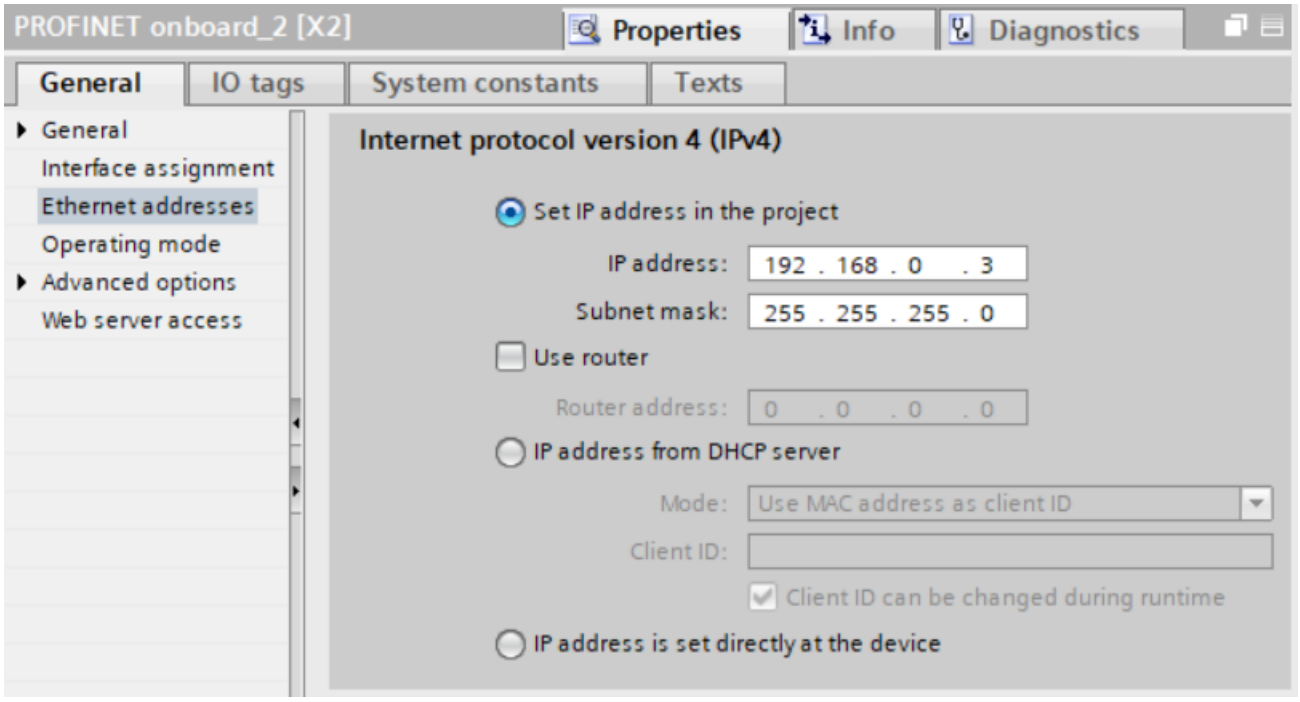


Figure 6-3 Ethernet addresses

NOTE

Runtime communication interface

If you want to use the option "IP address from DHCP server", the DHCP server must be installed on the Windows side of the device (IPC or CPU1515SP PC2) used.

If the DHCP server is installed outside of the device, the IP address cannot be set.

Reference

You can find information on all the other options of the category "Ethernet addresses" in the STEP 7 online help.

6.2 Resource Configurator

6.2.1 Example of a Resource Configuration file

Resource Configurator configures all IPC system resources which are necessary for operating the Software Controller. Resource Configurator is part of the installer setup of the Software Controller. The tool is automatically installed on the target device. Resource Configurator does not have a graphical user interface but is a command line tool that you execute by using the Windows command prompt.

The Resource Configuration file consists of Software Controller parameters which are also available in TIA Portal. Use this file to modify these parameters so that they match the actual values of your TIA Portal project. Then apply these values to the CPU runtime via the command line of Resource Configurator.

NOTE

Avoid parameter mismatches

Note that a mismatch between the parameters in TIA Portal and in the Resource Configuration file (such as inconsistent hardware identifiers or interfaces) result in errors during CPU download.

Make sure that the parameters in the Resource Configuration file correspond to the actual values of your TIA Portal project.

If the download fails due to an inconsistent project, use the following command to delete the project from the Software Controller:

`"CPU_ResourceConfigurator --set-initial"`

Afterwards, reconfigure your project with the matching parameters and download again.

Example Resource Configuration file

The following figure shows a Resource Configuration file with an example resource configuration. Use this file to change the values to your desired parameters.

```
{
"content_id": "resource_assignment",
"article_number": "auto",
"led_usage": true,
"nvram_usage": false,
"start_cpu_on_pc_boot": true,
"interfaces": [
{
"name": "X2",
"hw_identifier": 64,
"type": "Intel Standard Ethernet Controller"
},
{
"name": "X101",
"hw_identifier": 72,
```

```
"type": "Intel i210 or Compatible"
}
]
}
```

NOTE

Structure of a Resource Configuration file

Resource Configurator configures the target device according to the information provided in the Resource Configuration file. Resource Configurator does not check whether the Resource Configuration file content and the configuration in TIA Portal match. It is the responsibility of the user to make sure that the Resource Configuration file content matches the project configuration in TIA Portal.

Apart from changing the parameters to your actual values, do not change the file structure by removing/deleting or adding properties that do not actually exist in your project.

6.2.2 Example of a Resource Configuration file for Safety Processing Unit

The Safety Processing Unit is a special card to monitor safe movements of kinematics in the Cartesian Space for protection of the operating personal. The Safety Processing Unit consists of an optional library that provides separate fail-safe function blocks for each available kinematics. It is configured in the interfaces (Page 93) area of the Resource Configuration file. Unlike the CP 1625 and IE General cards, this card does not have a hardware identifier and cannot be configured in TIA Portal. The card is commonly used with a CP 1625.

NOTE

The Safety Processing Unit can only be used with CPU 1508S F/TF.

Example Resource Configuration file

The following figure shows a Resource Configuration file with an example resource configuration for the Safety Processing Unit. Use this file to change the values to your desired parameters.

```
{
"content_id": "resource_assignment",
"article_number": "auto",
"led_usage": true,
"nvram_usage": false,
"start_cpu_on_pc_boot": true,
"interfaces": [
{
"name": "X2",
"hw_identifier": 64,
"type": "Intel Standard Ethernet Controller"
```

```
},
{
"name": "X101",
"hw_identifier": 72,
"type": "CP 1625"
},
{
"name": "X102",
"type": "Safety Processing Unit"
}
]
}
```

6.2.3 Parameters

Below you will find the parameters that can be configured in Resource Configurator.

"content_id"

The parameter "content_id" is an internal key to distinguish between individual files. Do not modify this key or its corresponding value.

"article_number"

The parameter "article_number" determines the IPC that is being used.

Change "article_number" to the article number of your IPC that is being used. The article number must match the article number of the IPC selected in TIA Portal.

For standard IPCs, always use the "auto" value. If "auto" is set, Resource Configurator automatically retrieves the correct article number from the BIOS Desktop Management Interface (DMI).

Defining the article number is only necessary for customized IPCs.

NOTE

Customized IPCs

If you are using a customized article number, an automated setting of article numbers is not possible.

In case of doubt, ask Customer Support for the correct article number to be entered.

"led_usage"

The parameter "led_usage" determines whether the status of the CPU will be displayed via the user LEDs of the IPC being used.

If you want to use the hardware LEDs, set "led_usage" to "true". If you want to keep the hardware LEDs deactivated, set "led_usage" to "false".

NOTE

Note that in the basic configuration of the file, "true" is the default value.

If the selected IPC does not support LEDs, this parameter is ignored.

"nvram_usage"

The parameter "nvram_usage" determines whether the IPC's NVRAM will be used to store retentive data.

If you want to use PC mass storage for retentive data, set "nvram_usage" to "false". For using the NVRAM as storage for retentive data, set "nvram_usage" to "true".

For using the "Fast Compile & Fast Commissioning" function, you do not need to set the "nvram_usage" flag to true. If NVRAM is available on the device, then this feature will be active automatically, independent of the "nvram_usage" setting in Resource Configurator.

NOTE

For the following devices, the usage of NVRAM is only supported if the IPC was ordered with NVRAM from the factory:

IPC427E, IPC477E, IPC627E, IPC677E

For the following devices, the use of NVRAM is supported if the IPC was ordered with NVRAM from the factory or the NVRAM module was ordered separately and installed in the device by the user:

BX-39A, PX-39A, 227G, 277G

NVRAM limits the amount of retentive data but supports the memory even in case of a hard, unexpected power-off.

The parameter "nvram_usage" corresponds to the "Retentive memory" category in TIA Portal:

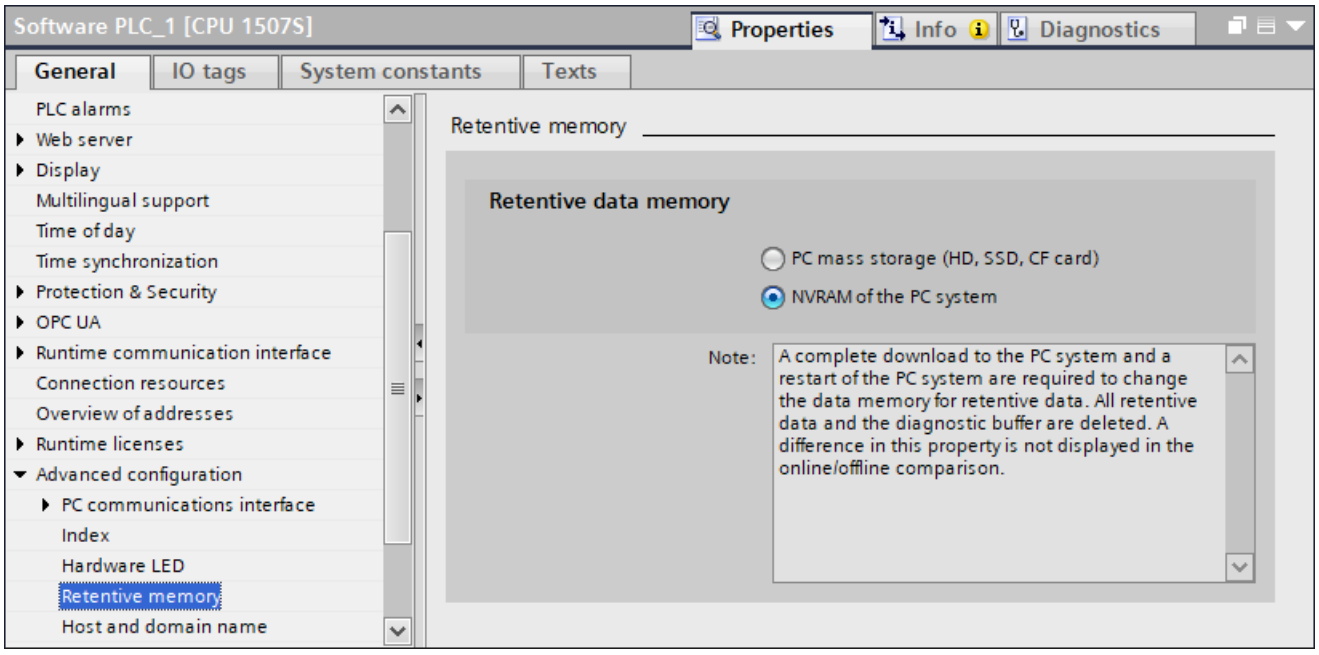


Figure 6-4 Retentive memory

"start_cpu_on_pc_boot"

The parameter "start_cpu_on_pc_boot" triggers an automatic start of the CPU when the IPC is powered on.

If you want to start the Software Controller automatically after booting the IPC, set "start_cpu_on_pc_boot" to "true".

NOTE

If you set "start_cpu_on_pc_boot" to "false", power on the CPU manually via the CPU Control Tool or the CPU display. Otherwise, the CPU download fails.

NOTE

Also note that changing this parameter will not delete the current project in the CPU.

"plc_priority"

As PLC priority levels, levels 1 and 4 are accepted by Resource Configurator . The impact of these two levels is as follows:

- Level 1 (default level)

  Windows and the CPU have the same priority on the system. This level reflects the behavior of the Software Controller from previous releases.

- Level 4 (maximum level)

  In this level, Windows slows down considerably in critical scenarios. As result, the Windows UI does not always respond immediately, but it does allow the best real-time behavior of the Software Controller.

  – Use of SFC97 Mode = 4 and Mode = 5 is not supported

  – When PLC priority level 4 is used, you should configure Windows to remain in blue screen in case of a crash to prevent the loss of retentive data.

The PLC priority parameter is optional and is not present in the Resource Configuration files delivered with the product. If you want to use this functionality, add this parameter manually to the Resource Configuration file. After adding the parameter to the Resource Configuration file, execute Resource Configurator and restart the complete system to apply the new configuration to the system.

If you do not specify the PLC priority parameter in the file, the Hypervisor will apply Level 1 to the system

NOTE

Limits of the Level 4 "plc_priority" parameter

Level 4 does not have the expected effect if SMIs (System Management Interrupts) are being executed on the system. The "Windows-only" reboot functionality is therefore disabled in level 4. If you initiate a Windows reboot with Level 4 activated, the entire system will be restarted, including the Software Controller.

DiagBase also triggers SMIs during system reboot. For this reason, we strongly recommend that you uninstall DiagBase on systems where the "plc_priority" parameter is set to Level 4.

You should also deactivate "Hyperthreading" in the BIOS.

NOTE

Changing PLC priority levels

Changing the PLC priority level does not delete the current project in the CPU.

Optimizing real-time behavior

For all CPU 1508 based Software Controllers installed to 627E/677E devices with an Intel i7-8700 processor, you can configure the hypervisor to lower the impact of Window's activities on the Software Controller's real-time behavior.

For the Software Controllers listed below, you can configure the hypervisor to lower the impact of Windows' activities on the Software Controller's real-time behavior:

- CPU 1508 based Software Controllers installed to 627E/677E devices with an Intel i7-8700 processor
- CPU 1507/CPU 1508 based Software Controllers installed to BX39A/PX39A/PX39A Pro devices with the following processor types:
  - Intel Xeon 11155
  - Intel Xeon 11555
  - Intel Xeon 11865

Examples of Windows activities impacting the real-time behavior are:

- User logins/logouts
- Establishing remote desktop connections
- Establishing TeamViewer connections
- Moving an Explorer window on the desktop
- Processes which are accessing memory (impact rises with number of times memory is accessed)

To configure the system for optimum real-time behavior, use the Resource Configurator tool. In Resource Configurator add the parameter "plc_priority" with value 4 to the Resource Configuration file used on the system to assign the PC resources to the Software Controller.

NOTE

Real-time capability during Windows boot phase

To ensure real-time capability during the Windows boot phase and to prevent SMIs (System Management Interrupts) on Windows start/restart, DiagBase must be uninstalled. After uninstalling DiagBase, the download preview will report that a configured component is not installed.

As an alternative to uninstalling DiagBase, you can start the Software Controller manually after booting/rebooting Windows by disabling the option "Automatic start after booting the PC" in Resource Configurator.

The following image shows an example of a file with "plc_priority" parameter added to it.

NOTE

Motion Control use cases

For Motion Control use cases with CPU 1508S T/TF, always use plc_priority: 4 to ensure optimum real-time behavior.

Also note that plugging additional PCI/PCIe devices available for Windows is not supported.

```
{
"content_id": "resource_assignment",
"article_number": "auto",
"led_usage": true,
"nvram_usage": false,
```

```
"start_cpu_on_pc_boot": true,
"plc_priority": 4,
"interfaces": [
{
"name": "X2",
"hw_identifier": 64,
"type": "Intel Standard Ethernet Controller"
}
]
}
```

NOTE

Additional BIOS setting for the highest real-time requirement

With "plc_priority" value 4, the following BIOS setting is additionally recommended for reaching optimum real-time behavior:

- Power and Performance→GT - Power Management Control→Maximum GT Frequency = 100MHz

  Note that Maximum GT Frequency is only available from BIOS version V25.02.14 onwards. For this reason, make sure that your BIOS is up to date.

"interfaces"

In the "interfaces" section, you assign which interface or other IPC hardware is to be used by the Software Controller.

Before executing Resource Configurator, take note of the MAC address of the interface(s) assigned to the Software Controller in your TIA Portal project. The MAC address must be noted because the interface is no longer visible in Windows tools after it has been assigned. TIA Portal shows the MAC address in the Software Controller download dialog. Alternatively, you can also write down the MAC address that is printed on the type label of the device.

"name" and "type"

Set "name" to the name of the interface assigned to the Software Controller. Valid values are "X1", "X2", "X3", "X4", "X100" to "X111".

NOTE

Note that not all interfaces are valid for all IPCs. The valid values depend on the individual IPC. For information on which interfaces can be used for which IPC, refer to section Reference information for use with SIMATIC IPC (Page 235).

The parameter "type" informs the Software Controller about the interface technology and driver that the Software Controller must use internally. Allowed values are:

- "Intel Standard Ethernet Controller" for Intel i210 based (or compatible) interfaces
- "Intel Advanced Ethernet Controller" for Intel i216 based interfaces (for example, 2x7G IPCs)
- "CP 1625"
- "Safety Processing Unit"

Set "type" to the interface type assigned to the Software Controller (for example, "Intel Standard Ethernet Controller" or "Intel Advanced Ethernet Controller").

The parameter "type" is optional for onboard interfaces but is necessary for external cards (e.g. CP 1625 and Safety Processing Unit).

NOTE

Project download to different IPCs

If the hardware configuration is same, you can download projects flexibly (e.g. download an IPC427E TIA Portal project to a BX-39A).

The parameters "name" and "type" correspond to the "Interface assignment" section of TIA Portal:

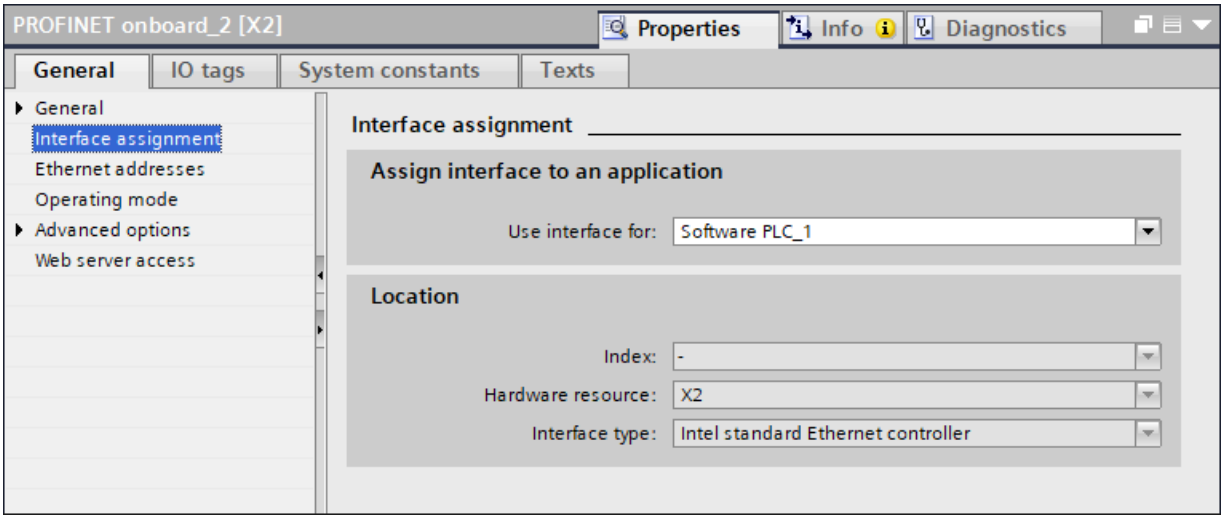


Figure 6-5 Interface assignment

NOTE

Also note that changing this parameter will delete the current project in the CPU.

"hw_identifier"

The parameter "hw_identifier" identifies the function of the interface within the CPU. This parameter must match the interface of the hardware configuration that is to be used over the IPC interface. Valid values are 64 and 72.

Set "hw_identifier" to the hardware ID of the interface assigned to the Software Controller (for example, "64").

The parameter "hw_identifier" corresponds to the "System constants" section of TIA Portal:

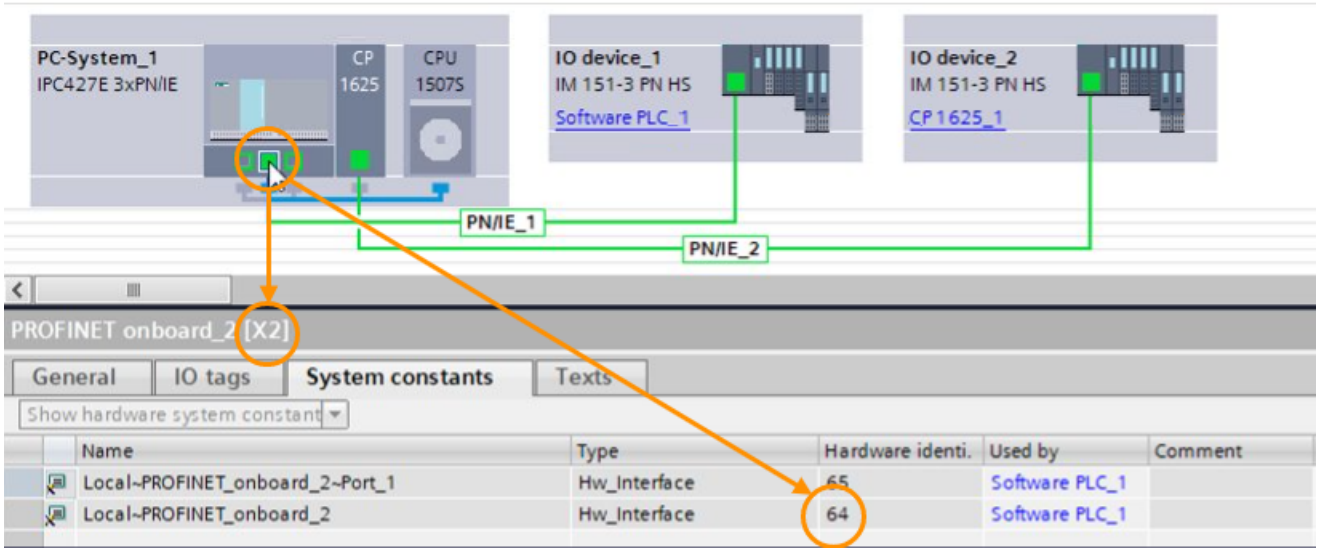


Figure 6-6 Hardware Identifier

If there is more than one interface configured in TIA Portal, define additional interfaces in the Resource Configuration file. For the definition of additional interfaces, the following applies:

- The interfaces defined in the Resource Configuration file and in TIA Portal must be identical.
- The number of interfaces must not exceed the maximum number of interfaces that can be assigned to the Software Controller.

NOTE

PROFINET IO configuration on BX-39A and PX-39A (PRO)

Note that on the BX-39A / PX-39A (PRO) devices, configuring PROFINET IO is supported in the following combinations:

- X2 + X3
- X2 + X4
- X2 + CP 1625 or IE General
- X3 + CP 1625 or IE General
- X4 + CP 1625 or IE General

Basic configuration of IPCs

The following basic configuration file (IPC_basic_configuration.json) is included in the setup and stored in the following default path:

C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator

```
{
     "content_id": "resource_assignment",
     "article_number": "auto",
     "led_usage": true,
     "nvram_usage": false,
     "start_cpu_on_pc_boot": true,
     "interfaces": [
         {
             "name": "X2",
             "hw_identifier": 64
         }
     ]
}
```

You can apply this configuration to your device or use this file as a reference for creating your specific configuration.

Basic configuration of the Open Controller

The CPU 1505SP is already preconfigured with factory settings on the Open Controller (CPU 1515SP PC2):

- The interfaces have already been completely assigned.
- The NVRAM has already been activated as the storage location for retentive data.
- The CPU 1505SP is configured for automatic start when the PC boots up.
- The LEDs are activated.

The following basic configuration file (OC_basic_configuration.json) is included in the setup and stored in the following default path:

C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator

```
{
     "content_id": "resource_assignment",
     "article_number": "auto",
     "led_usage": true,
     "nvram_usage": true,
     "start_cpu_on_pc_boot": true,
     "interfaces": [
         {
             "name": "X1",
```

```
                "hw_identifier": 64
            }
        ]
    }
```

Configuration update

If you apply the same configuration more than once, the following message appears:

"Hardware configuration is up to date. No changes will be applied!"

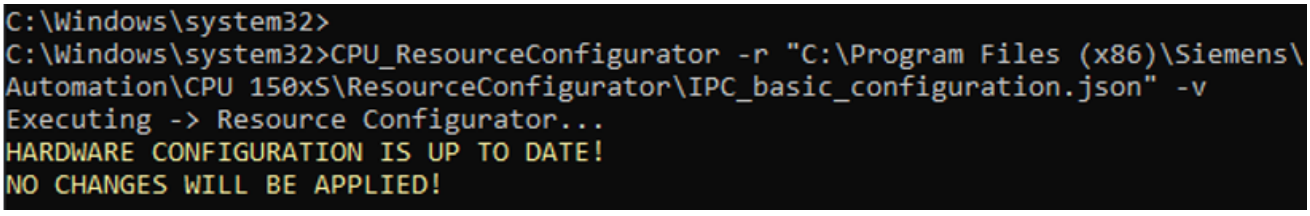


Figure 6-7 Configuration update

NOTE

Automated commissioning through scripting

If you have automated the commissioning phase through scripting, we recommend that you use integer return values of the tool instead of strings for correct representation of the operation result.

Configuration

Resource Configurator allows you to configure the following system resources:

- Assign/remove Software Controller interfaces, for example, external network interface cards (Intel i210 or CP 1625)
- Configure NVRAM or Mass Storage as the storage medium for storing retentive data
- Activate/deactivate LED usage
- Enable/disable automatic start of the Software Controller during startup of PC

Storage location

You will find Resource Configurator and its dependent files under the following storage locations:

- If you have installed the Software Controller to the default path (C:\Program Files (x86)\Siemens\Automation), the Resource Configuration files are located under:

  C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator

  If you have installed the Software Controller to a different location, the location of the Resource Configuration files changes accordingly.
- If it becomes necessary during hardware configuration to undo the previous configurations, the last successfully applied resource configuration file is used. This file is located under:

  C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator\successful_-config

  If you have installed the Software Controller in a different location, the location of the successful_config folder changes accordingly.

NOTE

This file is generated automatically. Do not modify its content. However, you can copy this file for debugging or analysis purposes.

The following image shows the files under C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator:

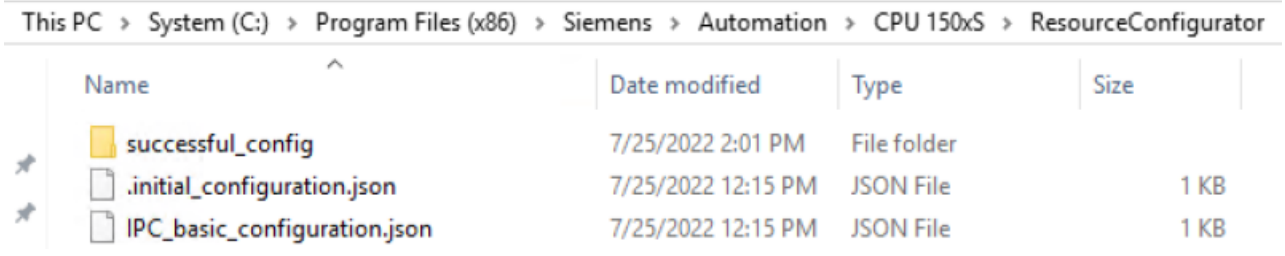


Figure 6-8 Resource Configuration files

NOTE

Secure storage location

If your created resource configuration file is different from the predefined file, store this file securely or delete it after you have finished the resource configuration and loaded your project.

Only users with administrator rights are allowed to modify predefined resource configuration files.

Executing Resource Configurator

Execute Resource Configurator manually via command line to apply your configuration changes as desired. The following figure shows the help screen which can be executed via the "--help" command.

```
C:\Windows\system32>CPU_ResourceConfigurator /help
Copyright © Siemens AG, 2023
Command Line Configuration utility of S7-1500 Software Controller

Usage:
   CPU_ResourceConfigurator --resource-config <json-file> [--force-reboot] [--verbose]
   CPU_ResourceConfigurator --set-initial [--force-reboot] [--verbose]

Parameters:
  -r, --resource-config=FILE      resource assignment JSON file
  -s, --set-initial               remove hardware assignment and program of SWCPU
  -f, --force-reboot              force to reboot after a successful operation with root privilege
  -h, --help                      display help menu and exit
  -v, --verbose                   set verbose logging
  -V, --Version                   display version info and exit

Examples:
  CPU_ResourceConfigurator -r /<path>/Resource_Assignment.json
  CPU_ResourceConfigurator --resource-config /<path>/Resource_Assignment.json --force-reboot --verbose
  CPU_ResourceConfigurator -s -f -v
```

Figure 6-9 Help screen

Parameters:

- "-r, --resource-config=FILE >" (mandatory)
- "-s, --set-initial"

  This parameter resets the device configuration to a state where there is no interface assigned to CPU (initial state).

- "-f, --force-reboot"

  This parameter forces Windows to reboot automatically after successful execution of Resource Configurator to make the changes effective. Alternatively, you can manually reboot the system later.

- "-h, --help"

  The command displays the help screen

- "-v, --verbose"

  When the status is "Failure", you can use the --verbose parameter (-v) to collect detailed information about the error reason. For more information about possible errors, see chapter Error handling (Page 106).

- "-V, --Version"

  The command displays the product version number

The following image shows the result after successful execution of Resource Configurator on an IPC.

```
C:\Windows\system32>CPU_ResourceConfigurator -r "C:\Program Files (x86)\Siemens\Automation\
CPU 150xS\ResourceConfigurator\IPC_basic_configuration.json" -v
Executing -> Resource Configurator...
Article number from JSON  : AUTO
Article number from SMBIOS: 6ES7647-8CE22-2BA1
Corresponding PCI_MAP file: PCI_MAP_6ES7647-8CXXX-XXXX.json
NVRAM Available : YES
NVRAM PCI path (hardcoded): PCIROOT(0)#PCI(1C05)#PCI(0000)
Executing -> Update VMM configuration...
Executing -> Update config area...
Executing -> Save Successful Configuration...
SUCCESSFUL!
Executing -> Preparing System for Complete Reboot...
REBOOT THE SYSTEM FOR CHANGES TO BE APPLIED!
```

Figure 6-10 Successful execution of Resource Configurator on IPC

Resource Configurator shows the corresponding information message and informs the user to reboot the system. A reboot enables configuration changes to become effective on the device.

NOTE

Load memory

The Software Controller's load memory is deleted when a new configuration is applied.

6.2.4 Error handling

Configuration errors

If a configuration error occurs, Resource Configurator sets the target to the last successfully applied configuration file stored in the system.

If a configuration error occurs during the last successfully applied configuration, Resource Configurator sets the target to its initial configuration.

NOTE

If you execute Resource Configurator in "Windows-only" mode, the following message might appear: "Failed to load Hypercall dll!"

This is expected behavior and does not have a negative effect on the functionality of the Software Controller.

Error messages

Resource Configurator displays status messages about the operation results. Possible results are "Success" or "Failure". When the status is "Failure", you can use the --verbose parameter (-v) to collect detailed information about the cause of the error. A return value of "0" means that no error occurred and the operation was successful.

The following list gives you an overview of possible error causes:

Error message	Meaning
HWCONFIG_SAME_AS_BEFORE	Hardware configuration is up to date
ERR_NO_PARALLEL_EXEC	Parallel execution is not supported
ERR_NO_FILE	No such JSON file can be found
ERR_NOT_JSON	Given file(s) extension is not a JSON type
ERR_LOAD_CFG_FILE_FAILED	Resource Configuration file could not be read properly
ERR_RM_PCI_DEVICE_FAILED	Removing PCI device from VMM configuration failed
ERR_ADD_PCI_FAILED	Adding PCI device to VMM configuration failed
ERR_WRITE_CFG_FILE_FAILED	VMM configuration file could not be written properly
ERR_RES_CFG_PARSE_FAILED	Parsing Resource Configuration file failed
ERR_RES_CFG_DUPLICATE_VALUES	Check for duplicate values in Resource Configuration file
ERR_RES_CFG_FILE_NAME_EMPTY	Resource Configuration file name is empty
ERR_PCI_PARSE_FAILED	Parsing PCI map file failed
ERR_WRITE_CONFIG_AREA_FAILED	Writing attributes to config area failed
ERR_PREPARE_CONFIG_AREA_FAILED	Preparing config area failed
ERR_CREATE_CPU_PARTITIONS_FAILED	Creating CPU partition failed
ERR_CPU_PARTITIONS_ALREADY_EXIST	CPU partitions already exist
ERR_FETCH_SWCPU_DISK_NUMBER_FAILED	Fetching Software Controller disk number failed
ERR_DECODE_PCI_PATH_FAILED	Decoding PCI path location failed
ERR_SET_ADN_BOOT_DELAY_FAILED	Setting Adonis boot delay failed

Error message	Meaning
ERR_SET_GPOS_BOOT_DELAY_FAILED	Setting GPOS boot delay failed
ERR_NO_PCI_MAP_FILE_FOUND	No suitable PCI_MAP.json file found in directory
ERR_SET_RT_TUNING_FAILED	Handing over PLC priority to hypervisor failed
ERR_INVALID_CONTENT	Invalid content in Resource Configuration file
ERR_INVALID_MLFB	Article number is invalid
ERR_SMBIOS_MLFB_EMPTY	Article number could not be retrieved from SMBIOS
ERR_SAVE_SUCCESS_FILE_FAILED	Saving resource assignment file failed
ERR_WRONG_ATTRIBUTE	Wrong attribute in Resource Configuration file
ERR_ADD_AHCI_FAILED	Adding an AHCI to VMM configuration failed
ERR_RM_FLAG_FAILED	Removing MSI_MSIX flag failed
ERR_UNSUPPORTED_PLC_PRIORITY	Device does not support PLC priority setting
ERR_UNSUPPORTED_SPU_CONFIG	Device does not support Safety Processing Unit
ERR_RM_ALL_AHCI_FAILED	Removing AHCI from VMM configuration failed
ERR_ADD_VIRT_NVME_FAILED	Adding virtual NVME device failed
ERR_ADD_SET_ACPI_VIRT_FAILED	Setting ACPI virtualization failed
ERR_ADD_MEM_REG_FAILED	Adding memory region failed
ERR_ADD_VM_MEM_FAILED	Adding VM memory failed
ERR_ADD_REBOOT_VIRT_FAILED	Adding Reboot Virtualization flag failed
ERR_REMOVE_REBOOT_VIRT_FAILED	Removing Reboot Virtualization flag failed
ERR_SET_VM_CORES_FAILED	Setting VM core count failed
ERR_UPDATE_VM_MEMORY_FAILED	Updating VMM memory configuration failed
ERR_UPGRADE_VMM_CONFIG_FAILED	Upgrading VMM configuration failed
ERR_GET_NVRAM_PCI_PATH_FAILED	Getting NVRAM PCI path failed

6.3 Configuration steps

Configuration steps

The steps below provide a summary of the configuration process and links to the sections where the steps are explained in detail.

1. Create a STEP 7 project (Page 108)
2. Prepare the target IPC with the installed Software Controller (Page 108)
3. Transfer the configuration to the target IPC (Page 109)
4. Configure the retentive data storage (Page 109)
5. Configure interfaces for PROFINET IO use (Page 110)
6. Configure the LED usage (Page 110)
7. Configure CPU start on PC boot (Page 110)
8. Transfer the configuration using file import/export (Page 111)

6.3.1 Creating a STEP 7 project

Procedure

To create the basic configuration, create a new project in STEP 7 and proceed as follows:

1. Add an IPC to your project.

   Make sure that the IPC matches the physical IPC that is being used.
2. Add a Software Controller from the Hardware Catalog to the IPC.
3. Assign the X2 interface of the IPC to the Software Controller (X1 interface for Open Controller).
4. For other hardware configuration settings and programming the Software Controller, refer to the STEP 7 online help.

NOTE

Special characters in the name of the CPU

Do not use slashes "/" and "\" in the name of the CPU.

NOTE

Special features with a CPU 1505SP

If you add a CPU 1515SP PC2 to the project, the settings described in section Necessary pre-configuration for CPU 1505SP (Page 144) are applied.

6.3.2 Preparing the target IPC with the installed Software Controller

Default configuration of IPC

The default configuration for the IPC after installation is as follows:

- Retentive data is recorded by default in the PC mass storage.
- The X2 interface is assigned to the CPU with PN RT.
- The use of LEDs is enabled.
- Simultaneous startup of the CPU on booting the PC is enabled.

Default configuration of Open Controller

The default configuration for the Open Controller CPU 1515SP PC2 after installation is as follows:

- Retentive data is recorded by default in the NVRAM.
- The X1 interface is assigned to the CPU with PN RT.
- The use of LEDs is enabled.
- Simultaneous startup of the CPU on booting the PC is enabled.

Changing default configuration

To change the default configuration according to your requirements, use Resource Configurator. For more information on Resource Configurator, refer to section Resource Configurator (Page 91).

6.3.3 Transferring the configuration to the target IPC

To transfer the configuration to the target IPC, proceed as follows. Note that the following procedure assumes that you have not changed the default settings.

- Use STEP 7 to connect the X2 interface of the target IPC (which by default is assigned to the CPU).
- Go online over this interface and download the project.

  The first project download must be executed using the MAC address of the assigned interface. For this reason, we recommend that you note down the MAC address of the interfaces to be assigned to the Software Controller before the assignment takes place for the first time (in case of the X2 interface on IPCs before starting the "Windows and Software Controller" boot option).
- After downloading the project, carry out the desired online functions.

For detailed information on how to download a project, refer to chapter Downloading project to target system (Page 121).

6.3.4 Configuring the retentive data storage

Since the capacity available for storing retentive data of the NVRAM and of the mass storage is different, the configuration of STEP 7 and the configuration on the target IPC must match.

NOTE

Note that changing the storage location of the retentive data will delete the current project.

To configure the retentive data memory, proceed as follows:

1. Select the desired storage location for retentive data (PC mass storage or NVRAM) in the properties for the storage of retentive data in STEP 7.
2. Also set this parameter accordingly in the Resource Configuration file.
3. Execute Resource Configurator with this Resource Configuration file.
4. Reboot the PC.
5. Download the changed configuration.

For more information on how to set the storage location in STEP 7, refer to section Setting storage location for retentive data (Page 119).

6.3.5 Configuring interfaces for PROFINET IO use

The configuration in STEP 7 and the configuration on the target IPC must match so that the correct interfaces are used for IO operation or communication.

NOTE

Note that changing the interface assignment will delete the current project.

For configuring the interfaces for PROFINET IO use, proceed as follows:

1. Change the interface assignment in STEP 7.
2. Change the interface assignment in the Resource Configuration file correspondingly.
3. Execute Resource Configurator with this Resource Configuration file.
4. Reboot the PC.
5. Download the changed configuration.

6.3.6 Configuring LED usage

For configuring the LED usage, the configuration in STEP 7 can be ignored. Changing the LED usage will not delete the current project.

For configuring the LED usage, proceed as follows:

1. Change the LED parameter in the Resource Configuration file.
2. Execute Resource Configurator with this Resource Configuration file.
3. The LED usage will take effect on the next complete IPC reboot (including Software Controller).

6.3.7 Configuring CPU start on PC boot

For configuring the CPU to start on PC boot, the configuration in STEP 7 can be ignored. Changing this parameter will not delete the current project.

For configuring the LED usage, proceed as follows:

1. Change the "start_cpu_on_pc_boot" parameter in the Resource Configuration file.
2. Execute Resource Configurator with this resource configuration file.
3. The "start_cpu_on_pc_boot" setting will take effect on the next complete IPC reboot (including Software Controller).

6.3.8 Transferring the configuration using file import/export

You can import the configuration for the CPU by using a PC system configuration file (*.psc) and the CPU Configuration Tool as an alternative to a download with STEP 7 (TIA Portal). The .psc file can be exported from STEP 7 or it can be exported from an already configured CPU for backing up the current configuration or copying it to a second installation. The configuration file does not contain the actual data (current data) in case of an export from a CPU.

NOTE

Exporting and importing .psc files across different operating systems

The CPU Configuration Tool only supports the export and import of .psc files for the same operating system. If you want to export and import .psc files between Windows and IndOS operating systems, use STEP 7 (TIA Portal) instead.

NOTE

Confidential configuration data

If you use a password for confidential configuration data, the password must be set with an online connection using STEP 7, or alternatively using the CPU Control Tool, before the configuration file can be imported.

NOTE

Resetting password for access protection for fail-safe CPUs

As of V30.0, there is no more PC Station available. Therefore, it is no longer possible to reset a password for access protection for fail-safe CPUs. However, an import of a .psc file that does not have an access level password will automatically remove an existing password.

For the export and import of the .psc file, proceed as follows:

1. Export the .psc file from STEP 7.
2. Import the .psc file to the CPU using the CPU Configuration Tool.
3. Export the .psc file from the CPU using the CPU Configuration Tool.

For detailed information on exporting and importing configuration files, refer to section Opening existing PC system configuration files (Page 127).

6.4 Creating Resource Configuration file corresponding to TIA Portal project

Resource Configuration file

The Resource Configuration file consists of Software Controller parameters which are also available in TIA Portal. Use this file to modify these parameters so that they match the actual values of your TIA Portal project. Then apply these values to your project via the command line of Resource Configurator.

The template files are located under:

C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator

The following example shows a Resource Configuration file with an example configuration that you need to change to your actual project settings.

```
{
     "content_id": "resource_assignment",
     "article_number": "auto",
     "led_usage": true,
     "nvram_usage": false,
     "start_cpu_on_pc_boot": true,
     "interfaces": [
         {
             "name": "X2",
             "hw_identifier": 64,
             "type": "Intel Standard Ethernet Controller"
         }
     ]
}
```

Generating Resource Configuration file in TIA Portal

To make sure that the Resource Configuration file is consistent with the hardware configuration of your TIA Portal project, you can export the Resource Configuration file directly from TIA Portal as of V20.0.

To access the export feature, select the Software Controller in the Device view. In the "General" tab, go to category "Advanced configuration > Export". In the "Export" category, select "Export to .json".

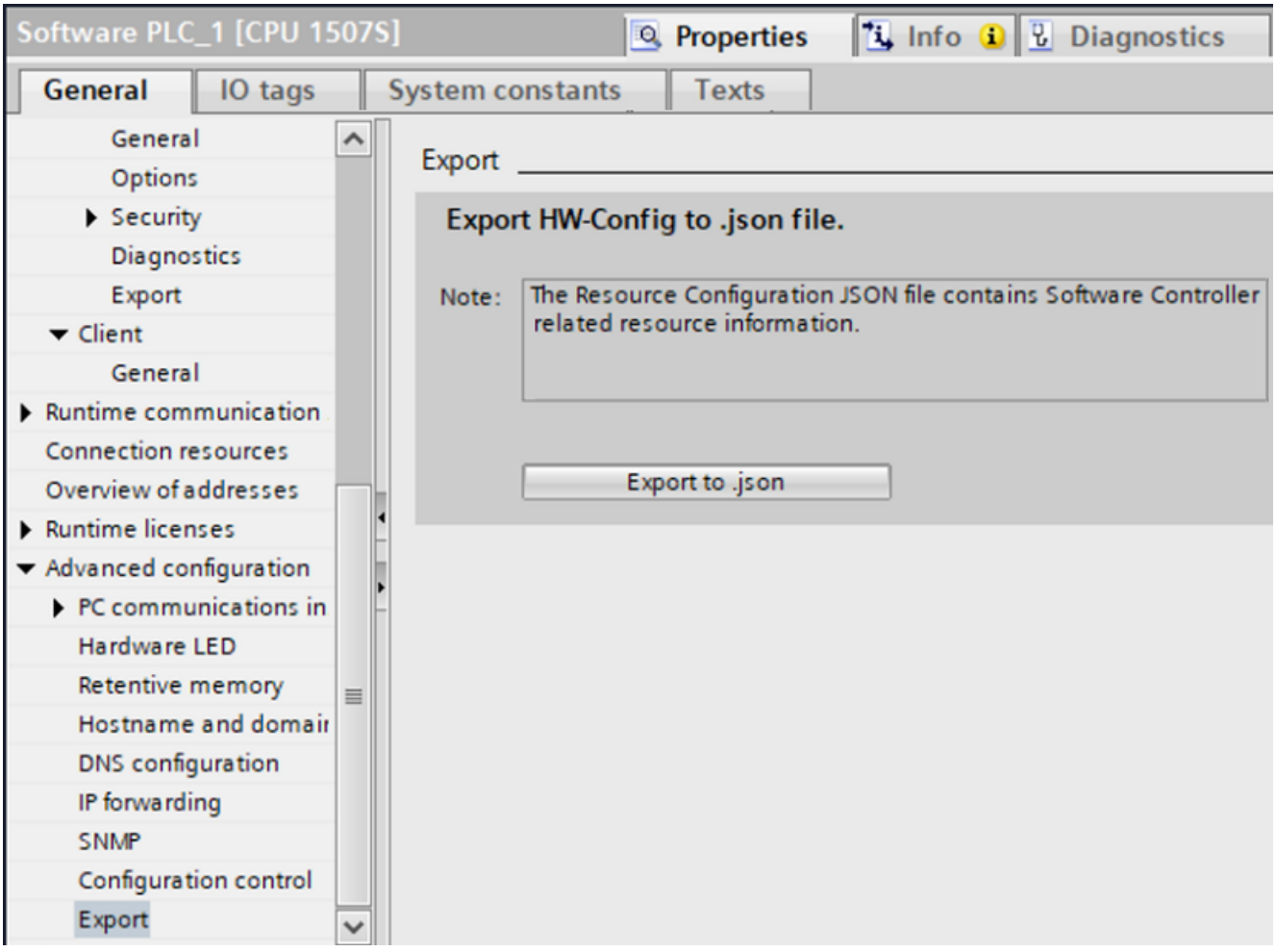


Figure 6-11 Export hardware configuration

In the file explorer, select the desired storage location of the .json file. As default path, the file explorer opens the path of the current project.

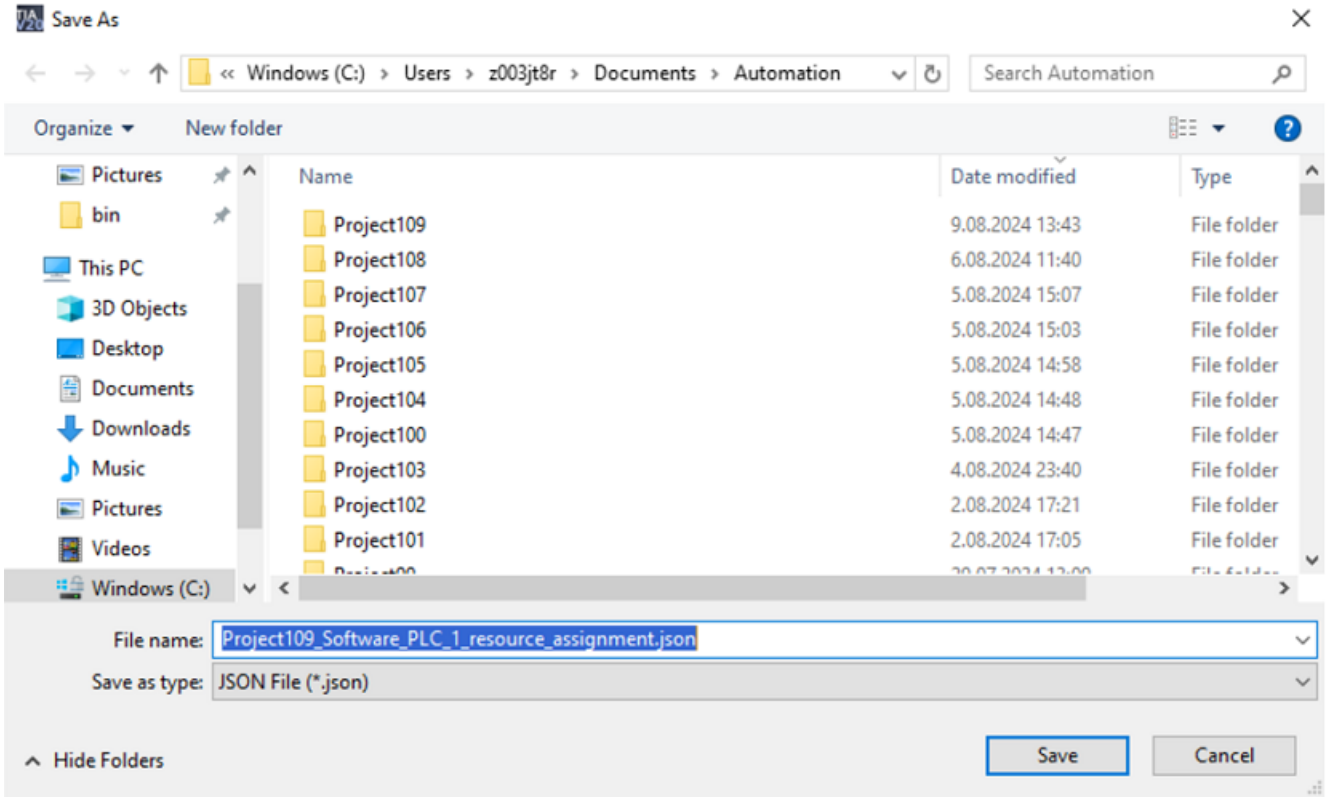


Figure 6-12 File explorer

Setting the PLC Priority

For optimizing real-time behavior, the CPU 1508 Software Controllers on IPCs 627E and 677E also allow you to enter the PLC Priority.

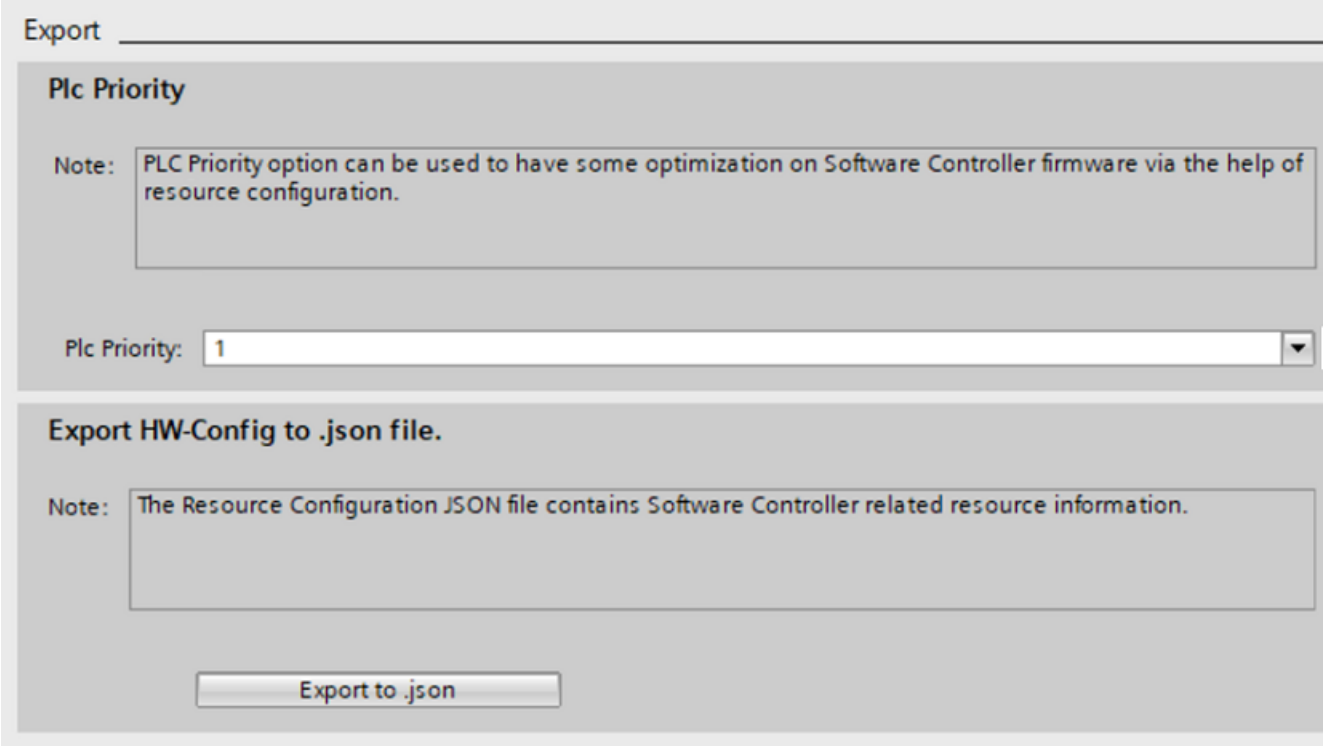


Figure 6-13 PLC Priority

For more information on PLC Priority and optimizing real-time behavior, refer to section Parameters (Page 93).

6.5 Executing Resource Configurator and system restart

Execution of Resource Configurator

1. Use the Command Prompt and run it as administrator.
2. Make sure the user is member of the "Software Controller Operators" or "Failsafe Operators" group as explained in section Windows User Management for CPU operations (Page 117).

```
C:\Program Files (x86)\Siemens\Automation\CPU 150xS\bin>CPU_ResourceConfigurator.exe -r
\Automation\CPU 150xS\ResourceConfigurator\IPC_basic_configuration.json" -v
Executing -> Resource Configurator...
Article number from JSON  : AUTO
Article number from SMBIOS: 6AG4131-3CC10-8AA1
Corresponding PCI_MAP file: PCI_MAP_6AG4131-XXXXX-XXX1.json
NVRAM Available : NO
Executing -> Update VMM configuration...
Executing -> Update config area...
Executing -> Save Successful Configuration...
SUCCESSFUL!
Executing -> Preparing System for Complete Reboot...
REBOOT THE SYSTEM FOR CHANGES TO BE APPLIED!
```

Figure 6-14 Execution of Resource Configurator

3. After executing Resource Configurator, perform a complete restart of the PC to apply the configuration changes.

NOTE

Rebooting the system

After executing Resource Configurator, remember to reboot the system. If you omit this step, it will not be possible to download the configuration from TIA Portal to the CPU since the configuration changes made by Resource Configurator have not been applied due to a missing reboot.

4. When the restart operation is completed, you can proceed with the creation and download of the TIA project.

6.6 Windows User Management for CPU operations

To be able to run Resource Configurator and the CPU Configuration Tool, add the user as a member of the "Software Controller Operators" group and also of the "Failsafe Operators group" for the fail-safe Software Controller.

User groups and CPU control rights

During installation, user groups are automatically created.

The following table shows you the available user groups and the groups' access authorizations for standard Software Controllers.

Table 6-1 Standard Software Controllers

User Group	CPU Control	Tools	
		Resource Configurator	CPU Configuration Tool
Administrator	yes*	yes	yes*
Software Controller Operators	yes	yes	yes
no administrator/no group membership	yes	no	no

*except for RUN, STOP operating mode changes

The following table shows you the available user groups and the groups' access authorizations for fail-safe Software Controllers.

Table 6-2 Fail-safe Software Controllers

User Group	CPU Control	Tools	
		Resource Configurator	CPU Configuration Tool
Administrator	yes[1]	no	no
Software Controller Operators	yes[2]	no	no
Failsafe Operators	yes[3]	yes	yes
no administrator/no group membership	yes[1]	no	no

[1] except for RUN, STOP operating mode changes and ConfirmCollectiveFSignature

[2] except for ConfirmCollectiveFSignature

[3] for ConfirmCollectiveFSignature, membership to both "Failsafe Operators" and "Software Controller Operators" group is required

Command for adding user to group

The administrator can add a user to the group with the following command:

```
net localgroup "Software Controller Operators" <Username> /add
```

The command prompt should look like the following:

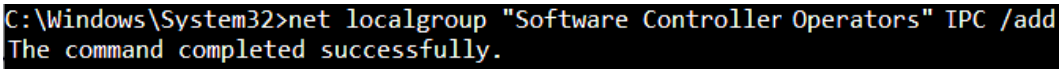


Figure 6-15 Command prompt: Add user

Command for creating user group in fail-safe systems

For fail-safe CPUs, the administrator creates the "Failsafe Operators" group with the following command:

```
net localgroup "Failsafe Operators" /add
```

The command prompt should look like the following:

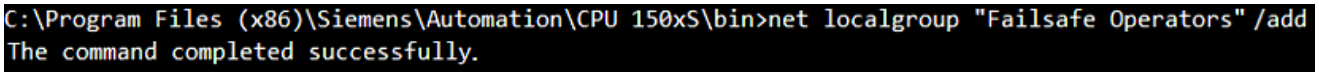


Figure 6-16 Command for creating Failsafe Operators group

6.7 Setting storage location for retentive data

The CPU provides the option of storing data retentively in the PC mass storage or in the onboard NVRAM when the CPU is stopped or a power failure occurs. You set the type of data storage in the CPU properties in STEP 7.

NOTE

Data loss when changing the storage type

The current retentive data and the contents of the diagnostic buffer are deleted when you change the storage type.

Procedure

To configure the type of storage, follow these steps:

1. Select the CPU.
2. Select the "Advanced configuration" area on the "Properties" tab of the Inspector window.
   - Select the "PC mass storage" option button to store the retentive data in the mass storage of your PC.
   - Select the "NVRAM of the PC system" option button to save the retentive data in the onboard NVRAM of your PC.

NOTE

SIMATIC IPC with NVRAM

"PC mass storage" is activated by default in a SIMATIC IPC. To select NVRAM as retentive memory, select the option button "NVRAM of the PC system".

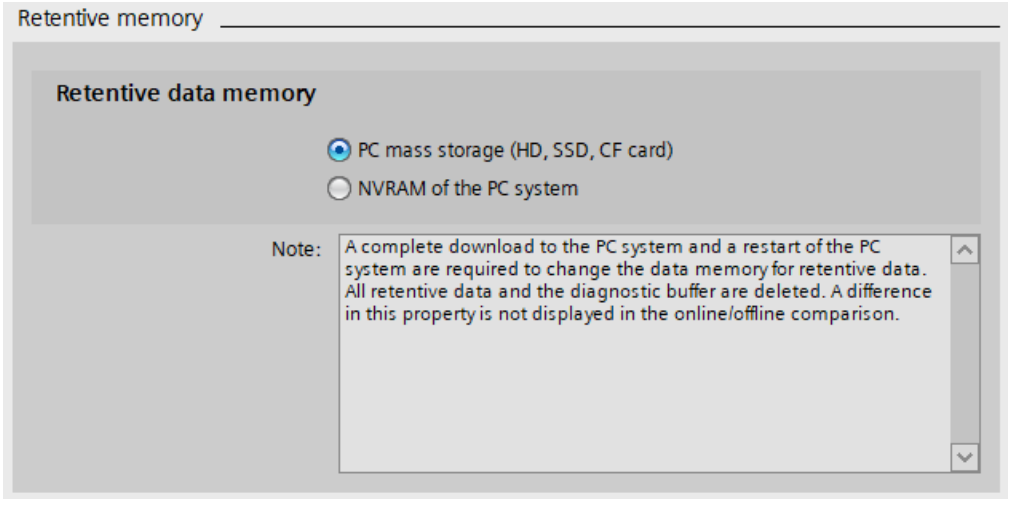


Figure 6-17 Properties for storage of retentive data in STEP 7

3. To complete a change in the type of data storage in STEP 7, download the project to the target device again.

Reference

Additional information on setting the size of the diagnostic buffer and the retentive areas of bit memories, timers, and counters is available in the STEP 7 online help.

6.8 Synchronizing time according to Windows clock

Introduction

The CPU supports various time sources, including the internal system clock and the Windows clock. This time information can be different, especially in the case of extended operating times. To prevent this, perform a time synchronization at regular intervals.

NOTE

Time synchronization based on Windows and NTP

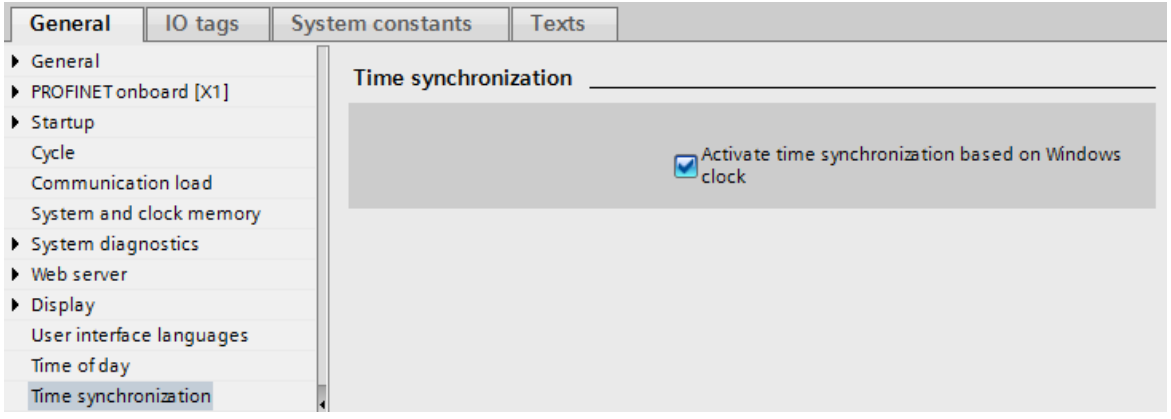
Time synchronization based on Windows and NTP cannot be configured at the same time.

With STEP 7, you have the option of configuring time synchronization based on Windows for your CPU.

Procedure

To configure time synchronization based on Windows, follow these steps:

1. Select the CPU.
2. On the "Properties" > "General" tab of the Inspector window, select the "Time synchronization" area.



3. Select the "Activate time synchronization based on Windows clock" check box.

   A period of 10 seconds is the default setting for the synchronization cycle.
4. Download the program to the CPU.

Result

As soon as the configuration of the time synchronization has been downloaded to the CPU, the internal system clock of the CPU is synchronized with the Windows clock every 10 seconds.

6.9 Loading the Software Controller

6.9.1 Downloading project to target system

Requirement

- The SIMATIC IPC hardware component is physically connected via Ethernet to the PC on which STEP 7 is installed.
- The interface settings and all parameters set during the resource configuration on the SIMATIC IPC and in STEP 7 match.

NOTE

Recommended interfaces

With a SIMATIC IPC, we recommend using interface "X2" (assigned by default). For a CPU 1515SP PC 2, use interface "X1".

This interface must be assigned to the Software Controller in the project.

NOTE

Interfaces for the Web server

The Web server is still accessible via the interface "X1". Note, however, that using the X1 interface for the Software Controller Web server is a legacy functionality. Since a PC Station is no longer available, do not use the following interfaces to access the Web server:

– X1 on SIMATIC IPCs
– X2 on CPU 1515SP PC2

Procedure

To download the STEP 7 project, follow these steps:

1. Search for the Software Controller.
2. Select the Software Controller in the device view.
3. Select the "Download to device" shortcut menu command.

   The "Extended download to device" dialog opens.
4. Configure the settings for the interface and start the device search for the Software Controller.

   TIA Portal shows the relevant device together with its MAC address.
5. Select this device to obtain its IP address.
6. Click the "Load" button to start the download.

Result

The project is downloaded. A dialog shows the download progress.

The CPU starts in STOP mode to ensure the continuation of the download.

STEP 7 establishes a connection to the CPU automatically. Click the "Load" button again to complete the download.

NOTE

Downloading a safety program to an S7-1500 F Software Controller

When downloading a safety program to an IPC without NVRAM, in very rare cases, the S7-1500 F Software Controller needs to be restarted. Repeat the download after restart for the download to be carried out successfully.

Also note that the feature "Fast Compile & Fast Commissioning" is supported on fail-safe IPCs using NVRAM.

In the execution of motion OBs, downloading a safety program to an IPC without NVRAM may lead to buffer overflows. To prevent this behavior, use devices with NVRAM.

NOTE

Downloading high amount of TO changes in RUN

For Software Controllers V31.1, we recognized a rare and sporadic misbehavior after carrying out multiple changes in technology objects (TOs) and downloading these changes to the Software Controller in RUN.

As a precaution, we recommend that you only download TO changes when the Software Controller is in STOP mode.

Download to target device does not work

For the download to target device to be successful, make sure that the device type is correct (CPU 1507S, CPU 1508SF, ...). If you use the wrong IPC, interface configuration or retentive data storage, the CPU may start, but in a faulty state. For the download to be successful, check the following:

- Does the article number in the Resource Configuration file fit to the target IPC (use "Auto" if a standard IPC)?
- Does the interface configuration match?

  For more information on assigning interfaces, refer to section Assigning interfaces for communication (Page 87).
- Does the retentive data storage location match?

  For more information on assigning interface, refer to section Storage of retentive data (Page 51).

6.9.2 Loading the Software Controller with file

The possibility to save and transport the system configuration of the Software Controller in a configuration file offers the following advantages:

- Update of large plants without the TIA Portal
- Simple provision of program and configuration updates
- Plant-level update no longer necessary
- No special software required

NOTE

Note that for successful application, both a PC System Configuration file (.psc file) and a matching Resource Configuration file (.json) are necessary.

6.9.2.1 Creating PC system configuration file

Creating configuration file

The Software Controller configuration is saved in a configuration file from the TIA Portal. The data may be re-used and distributed. The configuration file has the extension *.psc.

To create a configuration file, follow these steps:

1. In TIA Portal, select the "New > PC system configuration file (.psc)" command in the "Project > Memory Card-File" menu.
2. Enter the file name in the "Create memory card file" dialog that opens. To avoid error messages, make sure that the entries are correct:
   - Use a short and unique name.
   - Name may not contain more than 255 characters
   - Name may not contain spaces
   - Only use permitted characters; these are letters and digits, and the special characters '-' and '_'.
3. Select the desired directory in which you want to create the file. To avoid error messages, also make sure that the entries are correct, as in 2.
4. Confirm with "Create".

NOTICE
Protect data from access by third parties The customer is fully responsible for the secure transport of data.

NOTE

Characters for importing and exporting a PC system configuration file

Note that for the path and the name of the .psc file only ASCII characters are allowed for file import and export.

Result

The "Memory card file" folder is created in the project tree under "Card Reader/USB memory" with the following structure:

- PC system configuration file
  This file contains the Software Controller configuration file. The information indicates the file name and path information, for example, "Drive:\PC-SystemConfiguration01.psc"
  - Icon "PC-Systeminformation.psc"
    Double-clicking the icon displays all project-, device- and module-relevant information about the loaded configuration. If more data is loaded, you can use the "Update" button to display the latest metadata.
  - Folder with station name already assigned in the project navigation, for example, PC-System_1.
    This folder contains the configuration of the Software Controller.

NOTE

Storage of retentive data in PC system configuration files (.psc)

Note that retentive data and current process data of variables are not retained in .psc files. Current values are initialized to the start values after applying the .psc file.

However, in some scenarios retentive data can also be stored in the .psc file when using the CPU Configuration Tool with the /r or /retain command for exporting an already loaded Software Controller. For more information on the /retain command, refer to section Exporting and importing operations (Page 127).

6.9.2.2 Exporting Software Controller configuration into PC System configuration file from TIA Portal project

To load data into the configuration file, you have the following options:

- Load project data to a memory card using drag and drop or copy and paste.
- Write project data to a memory card.

Requirement

- A Software Controller is configured in the STEP 7 project.
- A .psc file is created and opened in the project tree.

NOTE

The Software Controller alone cannot be exported into the .psc file, export the complete PC system instead.

Loading project data to a memory card file

To load project data to a memory card file, follow these steps:

1. Drag the project data that you want to load from the project tree to the memory card.
   The project data will be compiled if necessary.
2. Then, the "Load preview" dialog opens. This dialog displays messages and recommends actions necessary for loading.
3. Check the messages and enable the actions in the "Action" column if necessary. As soon as loading is possible, the "Load" button is enabled.
4. Click the "Load" button.
   The loading is performed.

or:

1. Select the "PC system" folder in the project tree.
2. Right-click the selection and select the "Copy" command from the shortcut menu.
   Alternatively, you can also use the shortcut <Ctrl+C>.
3. Right-click the "*.psc" file level in the memory card file and select the "Paste" shortcut menu command. Alternatively, you can also use the shortcut <Ctrl+V>.
   All other levels are locked. The project data will be compiled if necessary.
4. Then, the "Load preview" dialog opens. This dialog displays messages and recommends actions necessary for loading.
5. Check the messages and enable the actions in the "Action" column if necessary. As soon as loading is possible, the "Load" button is enabled.
6. Click the "Load" button.
   The loading is performed.

or:

1. Select the "PC system" folder in the project tree.
2. In the "Project" menu, select the command "Card Reader / USB memory > Write to memory card".
   The "Select memory card" dialog opens.
3. Select a Memory Card.
   Click the "*.psc" box below the memory card to enable the button with the green check mark.
4. Click the button with the green check mark.
   The project data will be compiled if necessary.
5. Then, the "Load preview" dialog opens. This dialog displays messages and recommends actions necessary for loading.
6. Check the messages and enable the actions in the "Action" column if necessary. As soon as loading is possible, the "Load" button is enabled.
7. Click the "Load" button.
   The loading is performed.

Reference

For loading project data to a memory card file, also refer to the practical example in section Porting a configured Software Controller to another IPC (Page 137).

Result

The .psc file contains the configuration for all components in corresponding subfolders. The name of the subfolder is changed to the current Software Controller name.

NOTE

Check that file is complete

Check the .psc file in your TIA Portal to make sure it is complete because the file can only be edited in the TIA Portal.

6.9.2.3 Opening existing PC system configuration files

Opening configuration file

To view a configuration file in the project tree, follow these steps:

1. In the menu, select "Project > Memory Card-File > Open > PC system configuration file (.psc)".
2. Select the directory containing the .psc file.

The memory card file appears with the mentioned content under "Card Reader / USB memory" in the project tree.

You have the possibility of exporting configuration files from a source to a target system without having to use a connected TIA Portal. The file export function is useful in the following cases:

- Backup and restore

  You may make changes in the operation of your plant. For example, you may add new devices, update devices, replace existing ones or adapt the user program. If these changes result in undesirable behavior, you can fall back on the previously exported configuration file to restore the plant to its earlier state.

- Setting up serial machines

  You may have serial machines in operation at different locations. You want to store the project configuration at one particular plant and export the same configuration to other plants.

Exporting and importing files via the CPU Configuration Tool

In Software Controller versions < V30.0, import and export operations were carried out in the PC Station. As of V30.0 the tool for importing and exporting operations is the CPU Configuration Tool.

NOTE

For import operations, psc. files < V30.0 are not supported.

The CPU Configuration Tool and its dependent files are located in the following directory:

C:\Program Files (x86)\Siemens\Automation\CPU 150xS\bin

If you have installed the Software Controller to a different location, the location of the CPU Configuration Tool and its dependent files changes accordingly.

Access rights

The executable file "CPU_Configuration.exe" can be executed via command prompt by users who have the required rights. For more information refer to section Windows User Management for CPU operations (Page 117).

Command prompt

The following image shows the command prompt and the available commands.

```
C:\Windows\system32>CPU_Configuration /help
Copyright © Siemens AG, 2024
Command line tool for File Import/Export operations of S7 - 1500 Software Controller

Usage:
   CPU_Configuration [PARAMETERS]...

Parameters:
 /h,  /help                  Print Help
 /v,  /verbose               Set Verbose Logging
 /V,  /version               Print Version
 /p,  /print                 Print Configuration
 /e,  /export PSC_FILE_PATH  Name of the file to store exported data
 /i,  /import PSC_FILE_PATH  Name of the file to be imported
 /r,  /retain                Encrypted retentive data will be exported/imported by using password
 /clear                      Clear after an interrupted export
 /pwd                        Password for encryption
 /naj /noApplyJson          Do not apply json inside the .psc file

Example:
  CPU_Configuration /import <path>/ExportedFile.psc /verbose
  CPU_Configuration /import <path>/ExportedFile.psc /retain /verbose
  CPU_Configuration /import <path>/ExportedFile.psc /retain /pwd /verbose
  CPU_Configuration /import <path>/ExportedFile.psc /retain /pwd /noApplyJson /verbose
  CPU_Configuration /e <path>/ExportedFile.psc /v
  CPU_Configuration /e <path>/ExportedFile.psc /r /v
  CPU_Configuration /e <path>/ExportedFile.psc /r /pwd /v
  CPU_Configuration /print <path>/ExportedFile.psc
  CPU_Configuration /clear
```

Figure 6-18 Command prompt

The meaning of the commands is as follows:

- /help or /h

  The command displays a help screen.

- /verbose or /v

  This command can be combined with other commands to switch on verbose logging. This command is useful for error cases to print logs containing detailed error information.

- /version or /V

  The command shows the product version number.

- /print or /p <path>\filename.psc

  The command prints metadata information of the specified .psc file.
- /ramdisk
- /export or /e <path>\filename.psc

  The command exports the software configuration from the CPU to the specified .psc file.
- /import or /i <path>\filename.psc

  The command imports the configuration from the specified .psc file into the CPU.
- /r or /retain

  The command imports/exports retentive data.

  NOTE

  To make sure retentive data is imported correctly, carry out the import process as follows:

  1. Import the .psc file without the /r or /retain command.
  2. Import the .psc file with the /r or /retain command.

  The CPU must be powered on and powered off between the two import commands.

- /clear

  If an export together with a retain operation is stuck in the "Export" state, then, after aborting the process, use the "clear" command to make the system leave the export state (CPU_Configuration /clear).
- /pwd

  The command encrypts a .psc file with a user-defined password.
- /naj or /noApplyJson

  The command excludes the Resource Configuration JSON file from the .psc file. Without this command, the Resource Configuration JSON file is included in the .psc file by default.

6.9.2.4 Export operations

The following list gives you an overview of the steps necessary to carry out an export operation.

1. A Software Controller V30.0 or higher is installed via the setup installer.
2. You have created and applied a TIA Portal project to the CPU.
3. You have executed CPU_Configuration with the /export parameter via the command line.

Exporting CPU configuration

NOTE
Configuration export in STOP
Before carrying out a CPU configuration export to a .psc file, the Software Controller must be in STOP operating mode.

NOTE
Waiting time between export operations
To ensure that the current export operation completes correctly, wait about 10 seconds before you start the next export operation.

To carry out the CPU configuration export, proceed as follows:

1. Run the "CPU_Configuration /export <path>filename.psc" command in the command prompt.
2. Wait for execution.
3. After the confirmation that the operation was successful, the .psc file can be found at the given path.

```
C:\Windows\system32>CPU_Configuration /export C:\Users\IPC\Desktop\export_folder\my_project.psc /v
Executing -> File export...
Successfully exported C:\Users\IPC\Desktop\export_folder\my_project.psc.
Successfully exported.
Return code: 0x0.
```

Figure 6-19 Successful configuration export

Exporting CPU configuration including retentive data

To carry out the CPU configuration export including its retentive data, proceed as follows:

1. Run the command "CPU_Configuration /export <path>filename.psc /retain" or "CPU_Configuration /e <path>filename.psc /r".

   Provide an absolute path for the .psc file to be created. In this example it is “C:\Users\IPC\Desktop\export_folder\”. Absolute path cannot be an operating system specific folder like “C:\Windows\...”.

2. Wait for execution.
3. After the confirmation that the operation was successful, the .psc file including the retentive data can be found at the given path.

NOTE

Exporting CPU configuration on Open Controller devices

On Open Controller devices, the retain parameter is not supported when exporting the CPU configuration.

```
C:\Windows\system32>CPU_Configuration /export C:\Users\IPC\Desktop\export_folder\my_project_retain.psc /retain /v
Enter the password for retain, empty password is not acceptable
Password:
Executing -> File export...
Successfully exported C:\Users\IPC\Desktop\export_folder\my_project_retain.psc.
Successfully exported.
Return code: 0x0.

C:\Windows\system32>
```

Figure 6-20 Export including retentive data

Exporting CPU configuration with encryption

To export the CPU configuration to an encrypted .psc file, proceed as follows:

1. Run the command "CPU_Configuration.exe /export <path>filename.psc /pwd" or "CPU_Configuration /e <path>filename.psc /pwd".
2. Wait for execution.
3. After the confirmation that the operation was successful, the .psc file including the retentive data can be found at the given path.

```
Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>CPU_Configuration.exe /e "C:\Users\IPC\Desktop\out.psc" /pwd /v
Executing -> File export...
Enter the password for encrypting file, empty password is not acceptable
Password must contain at least 10 character and max 120 character.
Password must contain at least one numeric character.
Password:
Successfully exported C:\Users\IPC\Desktop\out.psc.
Successfully exported.
Return code: 0x0.
```

Figure 6-21 Encrypting .psc file

NOTE

Supported versions for exporting encrypted .psc files

Note that .psc files that are exported from a V30.1 Software Controller with encrypted retain data cannot be imported into V31.1.

Password for encryption

When choosing a suitable password, the following password policy applies:

- The password length must be between 10 and 120 characters.
- The password must contain at least one number.
- The password must contain at least one uppercase and one lowercase letter.
- The password must only contain ASCII characters.

To be able to view the content of the encrypted .psc file, compression tools, such as 7zip, prompt the user to enter the correct password.

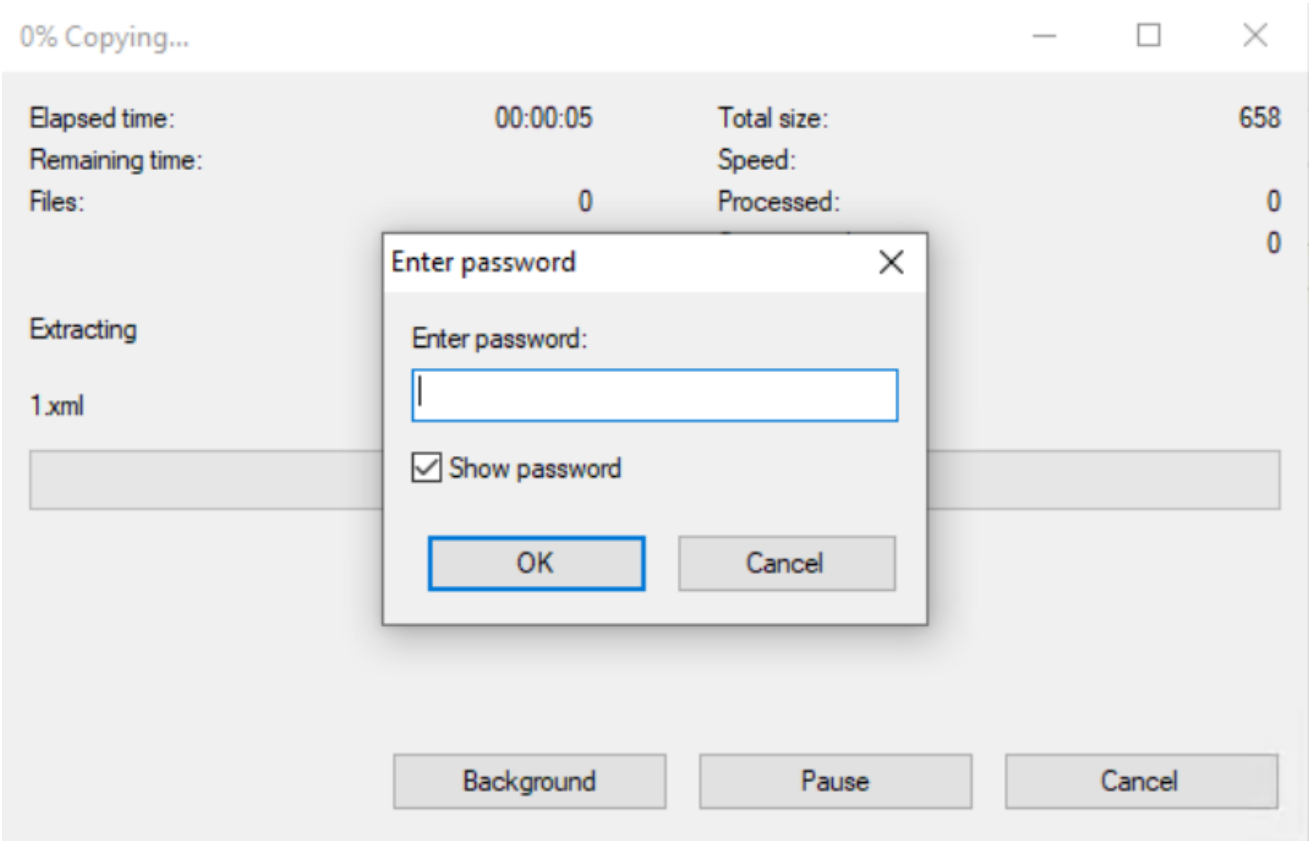


Figure 6-22 Password prompt

6.9.2.5 Import operations

The following list gives you an overview of the steps necessary to carry out an import operation.

1. A Software Controller V30.0 or higher is installed.
2. You have a .psc file, either created in TIA Portal or by CPU configuration export.
3. The Software Controller is in POWER OFF operating state.
4. You have executed CPU_Configuration with the /import parameter via the command line

Importing CPU configuration

Before carrying out a CPU configuration import, the Software Controller must be in POWER OFF operating state.

The user can use the graphical interface on the CPU panel or the CPU Control Tool to change the operating state to POWER OFF before executing the CPU Configuration Tool.

To carry out the CPU configuration import for a standard Software Controller, proceed as follows:

1. Power off the Software Controller.
2. Run the "CPU_Configuration /import <path>/filename.psc" command in the command prompt.
3. Wait for execution.
4. After the confirmation that the operation was successful, you can power on the Software Controller again.

To carry out the CPU configuration import for a fail-safe Software Controller, proceed as follows:

1. Power off the Software Controller.
2. Run the "CPU_Configuration /import <path>/filename.psc" command in the command prompt.
3. Wait for execution.
4. After the confirmation that the operation was successful, power on the Software Controller again.
5. For F-CPUs, confirm the collective fail-safe signature by using the CPU Control Tool and running the command "Cpu_Control.exe /ConfirmCollectiveFSignature -Signature 12345678" (example signature).

```
C:\Windows\system32>
C:\Windows\system32>CPU_Configuration /import C:\Users\IPC\Desktop\export_folder\my_project.psc /v
Executing -> Import Process...
Successfully imported.
Return code: 0x0.

C:\Windows\system32>
```

Figure 6-23 Successful configuration import

Importing CPU configuration including retentive data

To carry out the CPU configuration import from the exported configuration file including its retentive data, proceed as follows:

1. Power off the Software Controller.
2. Run the "CPU_Configuration /import <path>filename.psc" command without the /r or /retain command.
3. Wait for execution.
4. Power on the Software Controller.
5. Power off the Software Controller.
6. Run the "CPU_Configuration /import <path>filename.psc" this time with the /r or /retain command.
7. Wait for execution.
8. After the confirmation that the operation was successful, you can power on the Software Controller again.

```
C:\Windows\system32>
C:\Windows\system32>CPU_Configuration /import C:\Users\IPC\Desktop\export_folder\my_project_retain.psc /retain /v
Enter the password for retain, empty password is not acceptable
Password:
Executing -> Import Process...
Successfully imported.
Return code: 0x0.

C:\Windows\system32>
```

Figure 6-24 Retentive data import

NOTE

Behavior of diagnostics buffer when importing retentive data

If you export and then import a CPU configuration including retentive data from device A to device B, the diagnostics buffer of device B shows the diagnostics buffer entries of device A.

Importing CPU configuration with encryption

To import an encrypted .psc file, proceed as follows:

1. Power off the Software Controller.
2. Run the command "CPU_Configuration.exe /import <path>filename.psc /pwd" command or "CPU_Configuration.exe /i <path>filename.psc /pwd".
3. Enter the password.
4. Wait for execution.
5. After the confirmation that the operation was successful, you can power on the Software Controller again.

```
C:\Windows\system32>CPU_Configuration.exe /i "C:\Users\IPC\Desktop\out.psc" /pwd /v
Executing -> Import Process...
Enter the password for decrypting file, empty password is not acceptable
Password:
WARNING : PSC does not contain .json, please provide no apply option
Successfully imported.
Return code: 0x0.
```

Figure 6-25 Importing encrypted .psc file

6.9.2.6 Porting a configured Software Controller to another IPC

The following example shows how to port the hardware and software configuration from one IPC to another in TIA Portal.

1. In TIA Portal, go online with the source Software Controller by clicking the "Go online" button.

Figure 6-26 "Go online" button

2. Check that the parameters in the Resource Configuration file correspond to the actual values of your TIA Portal project.

   Check the matching status and make sure that the lights are green.

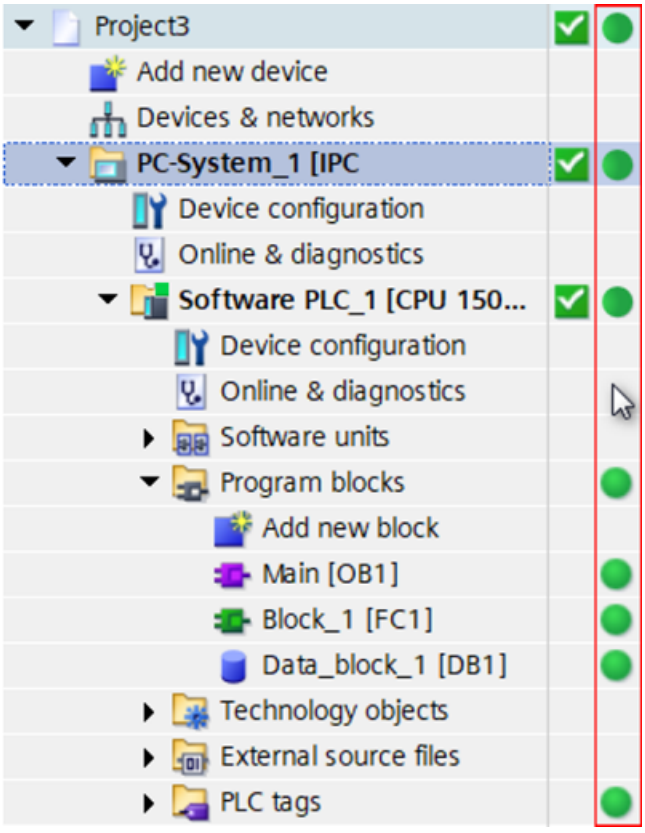


Figure 6-27 Matching status

3. Export the .psc file including the Resource Configuration JSON file.
   Select "Project > Memory card file > New > PC system configuration file (.psc)".

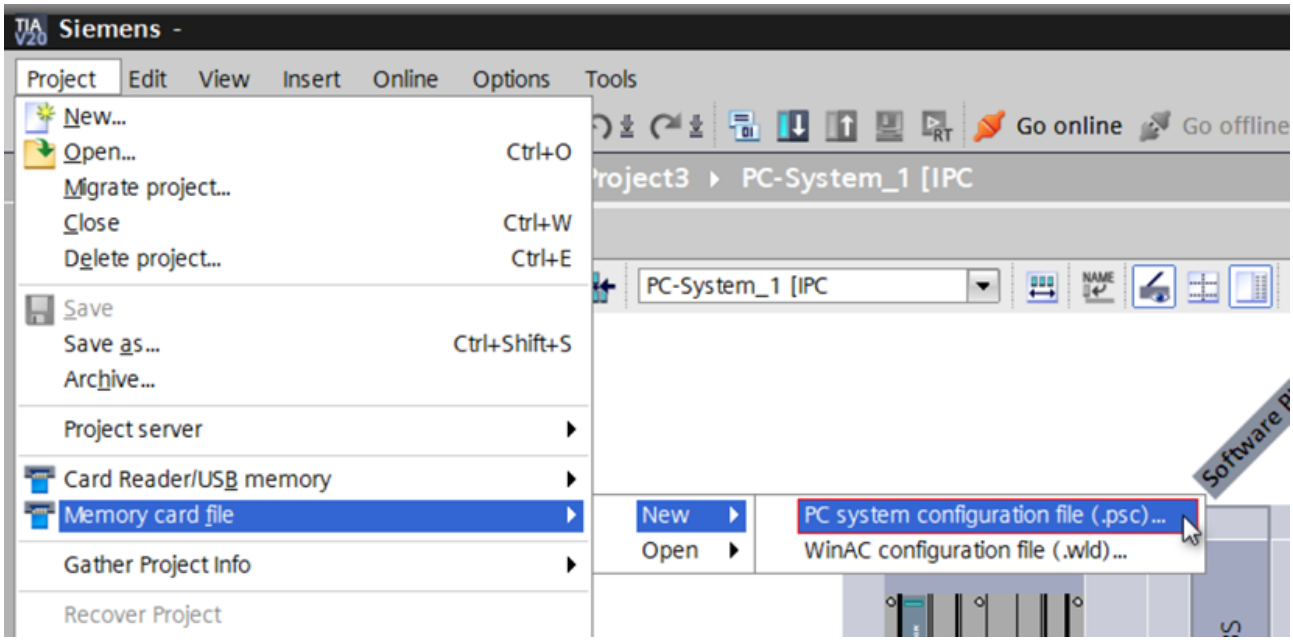


Figure 6-28 Selection of psc. file

4. Click "Create" and create the memory card file.

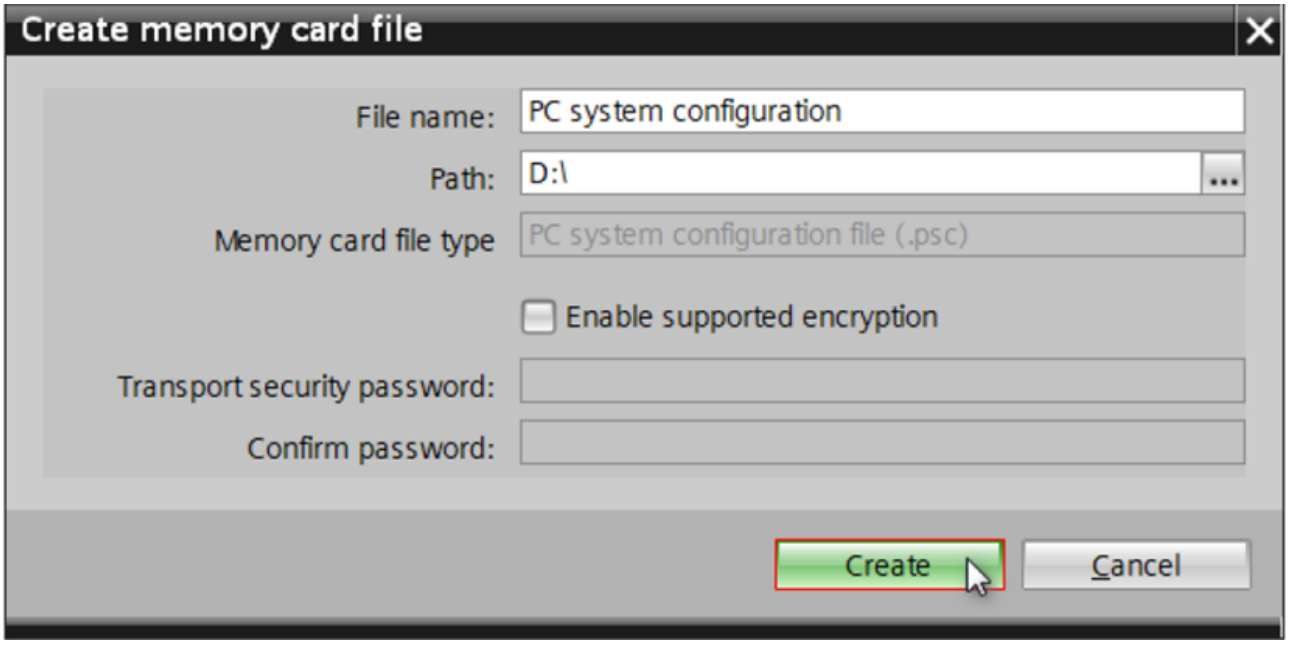


Figure 6-29 Creating .psc memory card file

5. To optionally encrypt the .psc file, enable the "Enable supported encryption" option and enter a valid password.

NOTE

Supported versions for exporting encrypted .psc files

Note that the encryption of .psc files is only supported on Software Controllers V31.1 and higher.

6. Compile the project and drag and drop the PC-System folder to the .psc memory card file.

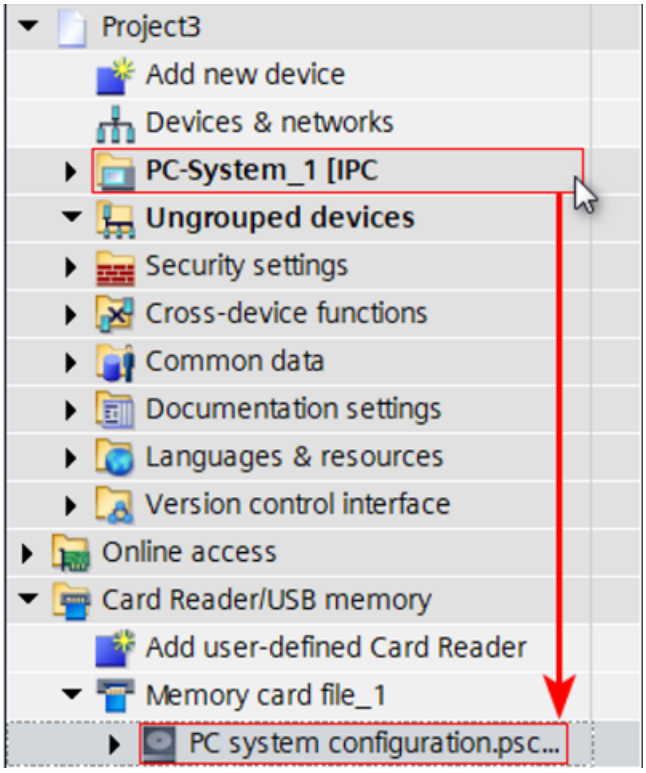


Figure 6-30 Transferring project data

7. In the "Load preview" window, click "Load" to start transferring the project data to the .psc file.

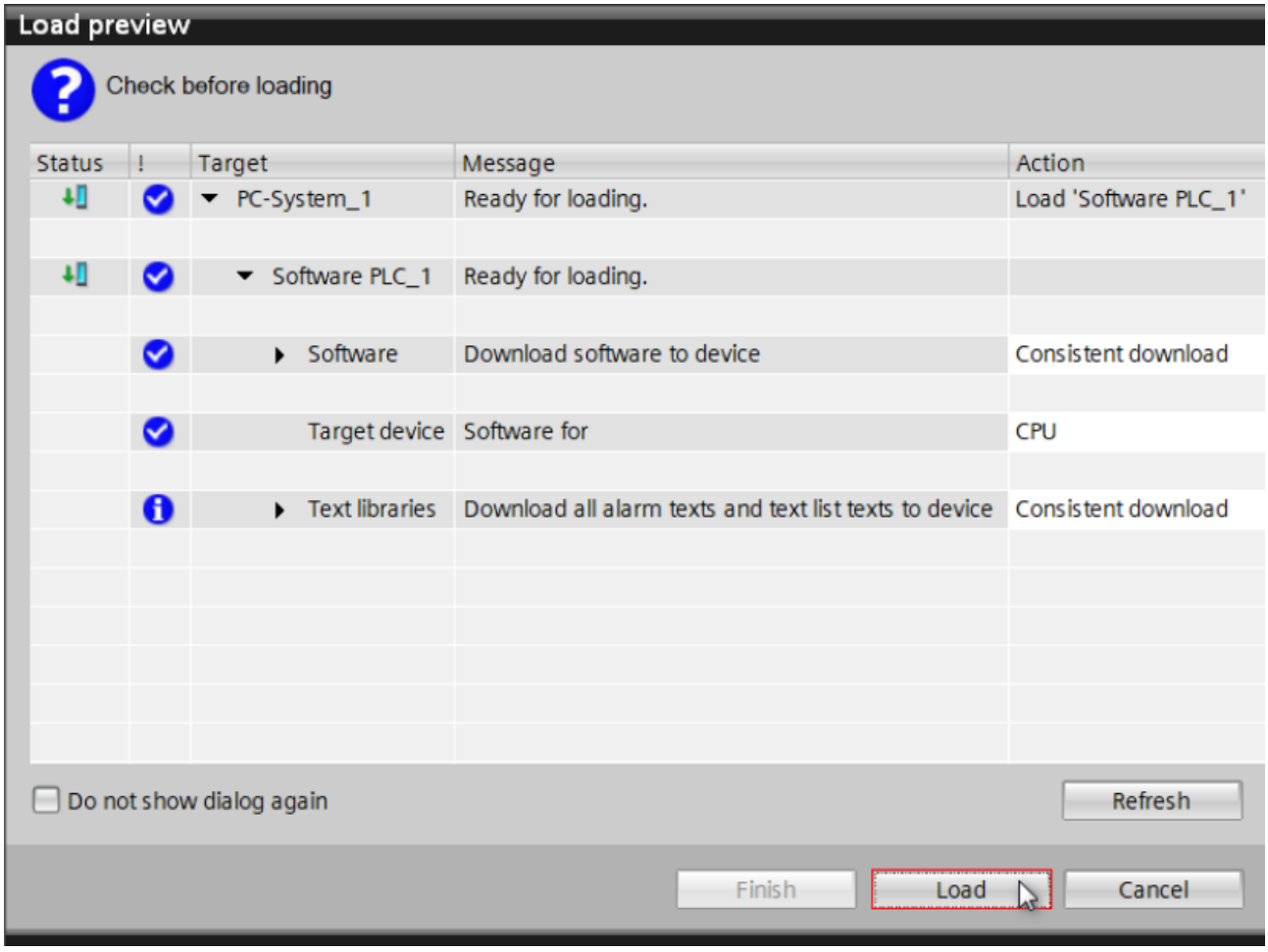


Figure 6-31 Load preview

8. Transfer the .psc file from the source IPC to the target IPC by using a USB removable storage or by connecting the target IPC via SSH.

   Use the command **CPU_Configuration.exe /import "C:\path\file.psc" /v** as shown in the following example:

```
C:\Windows\system32>CPU_Configuration.exe /import "C:\Users\IPC\Desktop\etrn_1507s.psc" /v
Executing -> Import Process...
Resource Configuration execution is starting
Path of Resource Configuration is found
Executing -> Resource Configurator...
NVRAM Available : YES
Article number from JSON  : AUTO
Article number from SMBIOS: 6AG4142-3FJ10-0BA0
Corresponding PCI_MAP file: PCI_MAP_6AG4142-YFXXX-XXXX.json
NVRAM PCI path (read from file): PCIROOT(0)#PCI(1C00)#PCI(0000)
Check NVRAM PCI path: PCIROOT(0)#PCI(1C00)#PCI(0000)
NVRAM PCI Path is valid!
Executing -> Update VMM configuration...
Executing -> Update config area...
Executing -> Save Successful Configuration...
SUCCESSFUL!
Executing -> Preparing System for Complete Reboot...
REBOOT THE SYSTEM FOR CHANGES TO BE APPLIED!
Resource Configuration execution finished successfully!
Resource Configuration is completed successfully!
Successfully imported.
Return code: 0x0.

C:\Windows\system32>CPU_Configuration.exe /import "C:\Users\IPC\Desktop\etrn_1507s.psc" /v
Executing -> Import Process...
Resource Configuration execution is starting
Path of Resource Configuration is found
Executing -> Resource Configurator...
NVRAM Available : YES
HARDWARE CONFIGURATION IS UP TO DATE!
NO CHANGES WILL BE APPLIED!
Resource Configuration execution finished successfully!
Resource Configuration is completed successfully!
Successfully imported.
Return code: 0x0.
```

Figure 6-32 Importing .psc file

9. Go online to the ported IPC using TIA Portal and compare the TIA project with the ported IPC.

   If all lights are green, the new IPC was ported successfully.

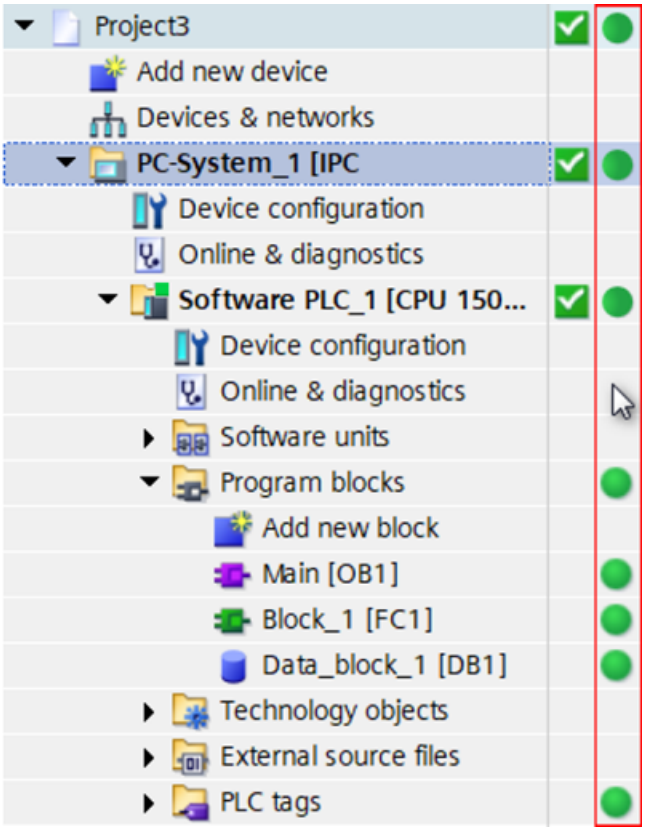


Figure 6-33 Matching status

6.9.2.7 Printing configuration information

You have the possibility to print the metadata information of a .psc file. The information comes from the "Metadata.xml" file.

To print file metadata, proceed as follows:

1. Run the "CPU_Configuration /print <path>/filename.psc" command in the command prompt.
2. Wait for execution.
3. After successful operation, you will find the metadata information printed on the command prompt.

```
C:\Windows\system32>CPU_Configuration /print C:\Users\IPC\Desktop\export_folder\my_project_retain.psc
Executing -> Print Process...
Metafile
  Component
    Index="1"
    Name="CPU 1507S"
    Id
    TypeId="975623"
    Author="ETRN_227G_2\IPC"
    Comment="Exported on Thu Nov 23 10:15:40 2023"
    TextList
    Software
    IuM
      Manufacturer="Siemens"
      OrderId="6ES7 672-7AC02-0YA0"
      SoftwareRevision="V 30.1.0"
      FunctionDesignation
      LocationDesignation
      InstallationDate="2023-11-22T07:09:00"
      AdditionalInfoText
Return code: 0x0.
```

Figure 6-34 Print metadata

6.9.2.8 Confidential configuration data

The .psc file does not include the password for confidential configuration data or any other security data.

Before you import configuration data exported from a password-protected CPU you need to set the same password for the CPU to which the data will be imported. You can set the new password by initially downloading the project to the CPU.

It is also possible for the Software Controller to download configurations having a password for confidential configuration data into a project with no password or with a different password. In such cases, TIA Portal displays the following error message in the "Load preview" window:

"The passwords for confidential PLC configuration data in the online PLC and in the project are not the same. Make sure that the passwords are identical either by changing the password in the online PLC (Online & Diagnostics > Functions > Define password to protect the PLC configuration data) or by changing the password in the project."

6.9.2.9 Special features for fail-safe configuration data

The export function also supports configurations from fail-safe CPUs. After exporting fail-safe configuration data, an internal checksum and the collective F signature is written into the metadata of the .psc file for identification of the safety program. Before importing the fail-safe configuration, you can display the F signature via the panel or query the F signature via a script.

You can also decide who is allowed to export fail-safe CPU configuration data. Exporting files is only possible for users who are members of the Windows user group "Failsafe Operators". If the current user is not a member of this group, the export command is rejected and an error message appears.

6.9.2.10 Error handling

The CPU Configuration Tool displays a status message about the result of its operation either as Success or Failure. In case of any failure during execution, you can use the --verbose parameter (-v) to collect detailed information about the error reason. Return Value “0” means that the operation was successful.

The following list gives an overview of possible error reasons:

Message	Code
SUCCESS	0x0
FAILSAFE_SUCCESS	0x51A3
ERR_NOT_IN_FAILSAFE_OPERATORS_GROUP	0x80040331
ERR_IMPORT_FAILED	0x80040332
ERR_EXPORT_FAILED	0x80040333
ERR_PRINT_FAILED	0x80040334
ERR_GET_ROOT_PATH_FAILED	0x80040335
ERR_LOAD_DLL_FAILED	0x80040336
ERR_UNLOAD_DLL_FAILED	0x80040337
ERR_CPU_TYPE_NOT_MATCH	0x80040338
ERR_RETAIN_ENCRYPTION_FAILED	0x80040339
ERR_RETAIN_DECRYPTION_FAILED	0x8004033A
ERR_GENERIC_FAIL	0x8004033F

6.10 Necessary pre-configuration for CPU 1505SP

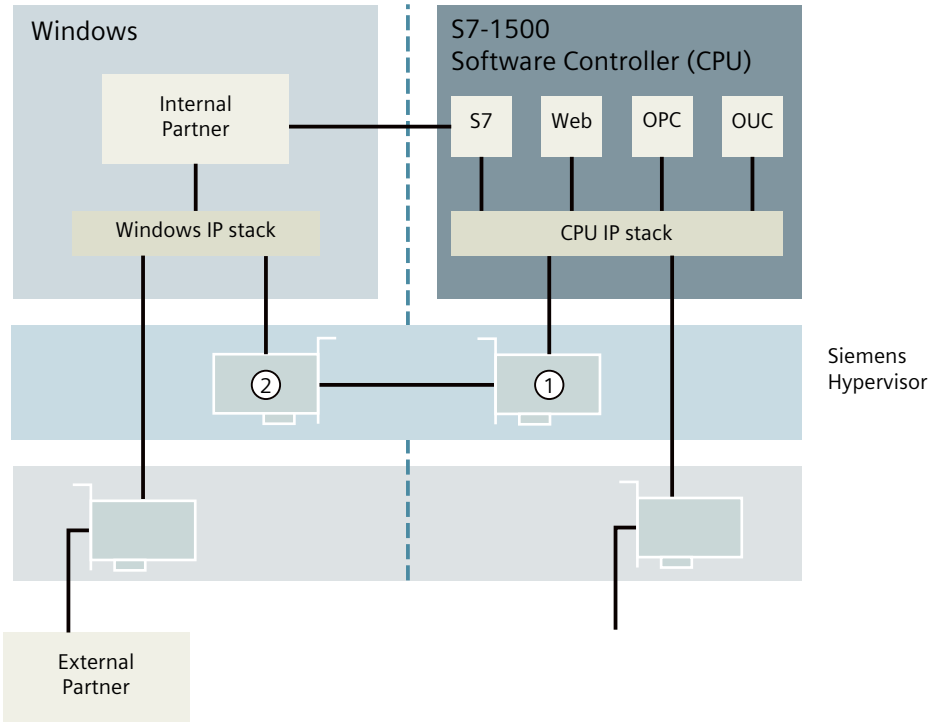
This section describes the differences between configuration of a STEP 7 project with a CPU 1505SP and configuration with a CPU 1507S/1508S.

- If you add the CPU 1515SP PC2 as a new device, the CPU 1505SP is already preconfigured.
- The interfaces have already been completely assigned.
- The NVRAM has already been activated as the storage location for retentive data.
- The CPU 1505SP is configured for automatic start during booting of the PC.
- The LEDs are activated.

6.11 Communication

The CPU has a virtual Ethernet network via which the CPU can communicate with Windows applications, and in particular with OPC UA. Two interfaces are available.

On the CPU, the Runtime communications interface is used as the interface for communication. The interface is displayed on Windows as "SIMATIC RT-VMM Network Adapter".



① Runtime communication interface
② SIMATIC RT-VMM Network Adapter

Figure 6-35 Overview of interfaces

The following options are available for using OPC UA:

- Using OPC UA locally on the same PC (Page 154)
- Using OPC UA remotely over Windows Ethernet interfaces
  - Establishing a connection with IP routing
  - Establishing a connection using port forwarding (Page 155)

NOTE

Output of the client IP address in the diagnostic buffer

The CPU cannot determine the IP address of the Windows interface. The client IP address output in the diagnostic buffer is only an internal address and can be ignored.

Timeout input in "Modbus_Client" program block has no effect

The timeout is approx. 38 seconds, regardless of the value entered under "Blocked_Proc_Timeout".

Certificate management via Global Discovery Server (GDS)

Via GDS push management functions you can:

- Update OPC UA certificates of an S7-1500 CPU
- Transfer updated certificates and lists in RUN operating state

The automation of certificate management eliminates any manual work required for reconfiguring the CPU, for example, after a certificate has expired, and a new download to the CPU.

For detailed information on this function, refer to the Communication (https://support.industry.siemens.com/cs/ww/en/view/59192925) function manual.

Deleting OPC UA certificates during TIA Portal download

In TIA Portal it is possible to delete OPC UA certificates with a consecutive download, as the following screenshot of the "Load preview" shows.

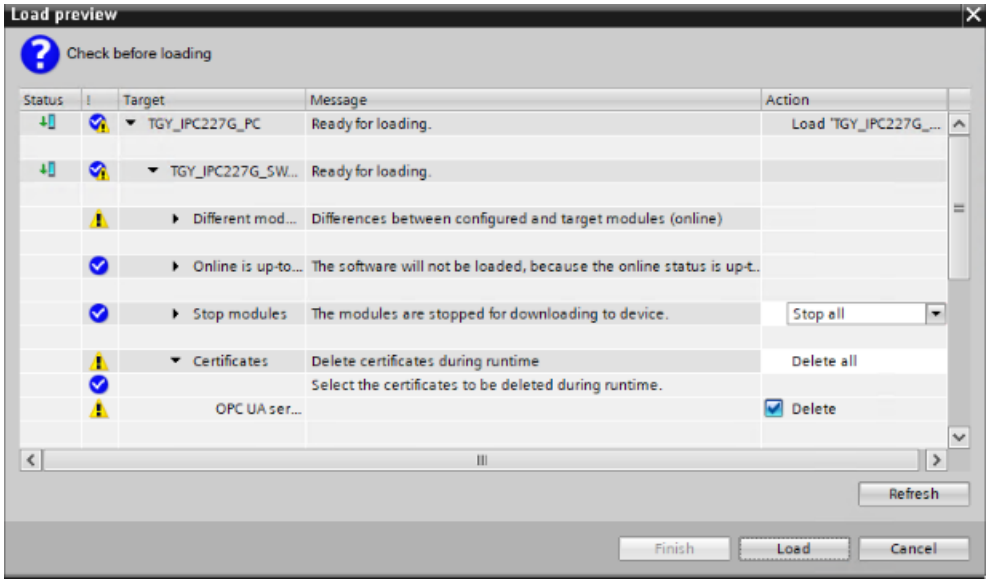


Figure 6-36 Deleting certificates

NOTE

Panel error message "Connection failed"

If during this process the panel error message "Connection failed" appears, a power cycle (Power Off/On) or a Software Controller restart via "CPU_ConfigTool /AllowReboot" is necessary.

6.11.1 PC-internal communication

The following image shows the PC-internal communication interfaces.

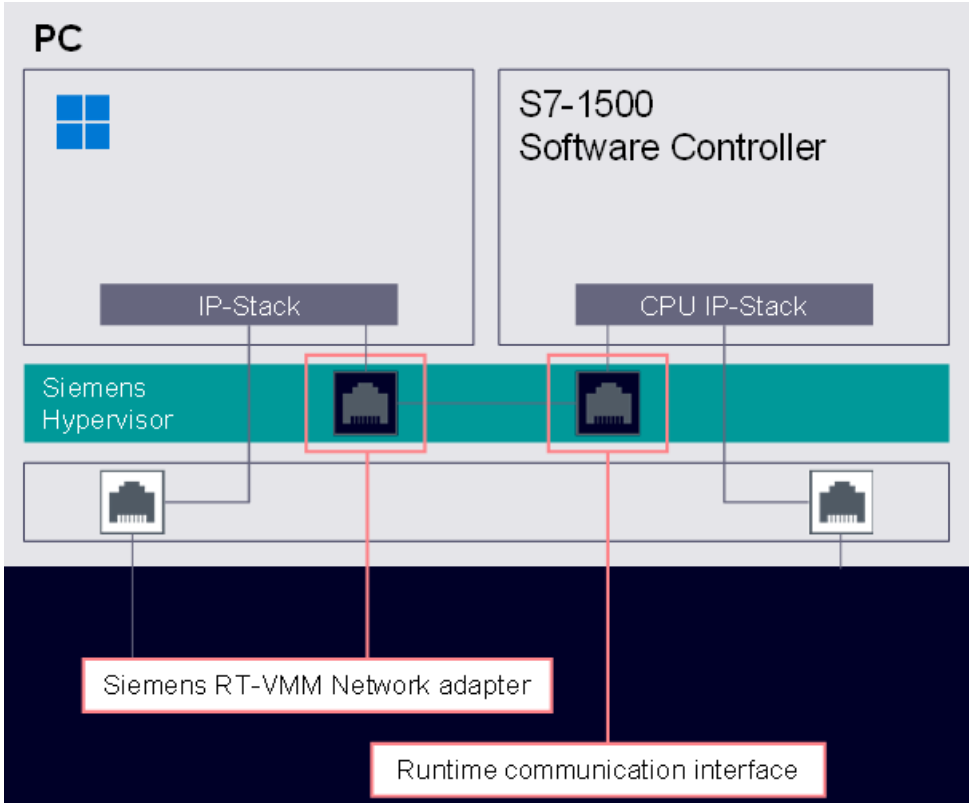


Figure 6-37 PC-internal communication

Inside the PC, the CPU uses a virtual Ethernet network. The CPU interface used for this network is the Runtime communication interface. The Windows interface for this network is called "SIMATIC RT-VMM Network Adapter".

The network can be used for:

- Configuration of the Software Controller with a locally installed TIA Portal
- Visualization with a locally installed HMI (for example, WinCC Unified)
- OPC UA communication with a locally installed OPC UA client or server
- Open User Communication with Windows
- S7 Communication with locally installed software

To configure PC-internal communication, proceed as follows:

1. Configure the SIMATIC RT-VMM Network Adapter using the Windows Control Panel.

   The IP address of the adapter must be in the same IP subnet as the planned IP address of the Runtime communication interface.
2. Assign an IP address to the Runtime communication interface for:
   - using STEP 7 online functions (when used on the same IPC)
   - downloading the configuration with a fixed IP address
3. Use a "Ping" to test the communication.

Command for setting IP address for SIMATIC RT-VMM Network Adapter

NOTE

IP address of SIMATIC RT-VMM Network Adapter after rebooting in "Windows-only" mode

If you reboot Windows in "Windows-only" mode, the assigned IP address of the SIMATIC RT-VMM Network Adapter will be lost. As a result, the IP configuration mode changes from manual to automatic. After rebooting in "Windows and Software Controller" mode, set the IP address for the SIMATIC RT-VMM Network Adapter again.

Detailed information on how to restore the IP configuration of the SIMATIC RT-VMM Network Adapter is available in the following FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109826746).

Reference

For HMI communication between the Software Controller and WinCC RT Advanced on the same device, also note the follow FAQ on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109814824).

6.11.2 Communication using the DCP Tool

DCP Tool stands for Discovery and Configuration Protocol Tool. You can use the DCP Tool to identify device information and configure device settings.

You will find the DCP Tool "DCPTool.exe" under the following path: C:\Program Files (x86)\Siemens\Automation\CPU 150xS\bin

Commands and parameters of the DCP Tool

The following image shows the help screen of the DCP Tool.

```
C:\Users\OC\Desktop>DCPTool.exe
Copyright Siemens AG, 2023

DCP Tool for Windows
Usage:
DCPTool.exe   nic <NIC>   mac <MAC>   setip <IP>   setmask <IP>   setgw <IP>

Parameters:
        -n, --nic=NIC                   Interface name of the Siemens RT-VMM Network Adapter
        -m, --mac=MAC                   MAC address of the Runtime Communication Interface
                                        (Address is seperated by ':'
        -s, --setip=IP                  Set IP address of the Runtime Communication Interface

Optionally, the setmask/setgw flag may be used for setting up for subnetmask or gateway.

        -t, --setmask           Set IP network mask for Runtime Communication Interface
        -g, --setgw             Set IP gateway for Runtime Communication Interface
        -h, --help               Display this help page and exit
        -v, --version            Display version of the tool and exit


Example:
DCPTool.exe --nic Ethernet_3 --mac 28:63:36:78:bc:bd --setip 192.168.1.1 --setmask 255.255.255.0
--setgw 0.0.0.0
DCPTool.exe --nic Ethernet_3 --mac 28:63:36:78:bc:bd --setip 192.168.1.1
```

Figure 6-38 DCP Tool

The following parameters are available.

Parameter	Explanation
Required parameters:	
-n, --nic	Interface name of the SIMATIC RT-VMM Network Adapter
-m, --mac	MAC address of the runtime communication interface
-s, --setip=IP	IP address of the runtime communication interface.
Optional parameters:	
-t, --setmask	Set IP network mask for runtime communication interface
-g, --setgw	Set IP gateway for runtime communication interface
-h, --help	Display this help page and exit
-v, --version	Display version of the tool and exit

The DCP Tool requires the adapter name of the SIMATIC RT-VMM Network Adapter and the MAC address.

To obtain the adapter name, use the `ipconfig /all` command. To obtain the MAC address, use the VMM_NICConfig tool (C:\Program Files (x86)\Siemens\Automation\CPU 150xS\bin).

The following image shows the successful sending of the adapter name (Ethernet_3), MAC address (28:63:36:78:b3:17) and the IP address (192.168.1.7).

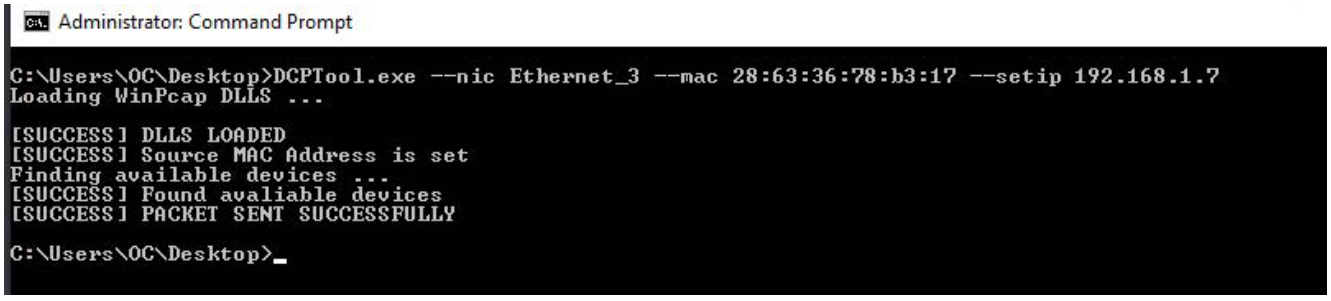


Figure 6-39 Successful Set IP operation

6.11.3 Communication with CPU using bridging

The following image shows the communication interface when bridging is used.

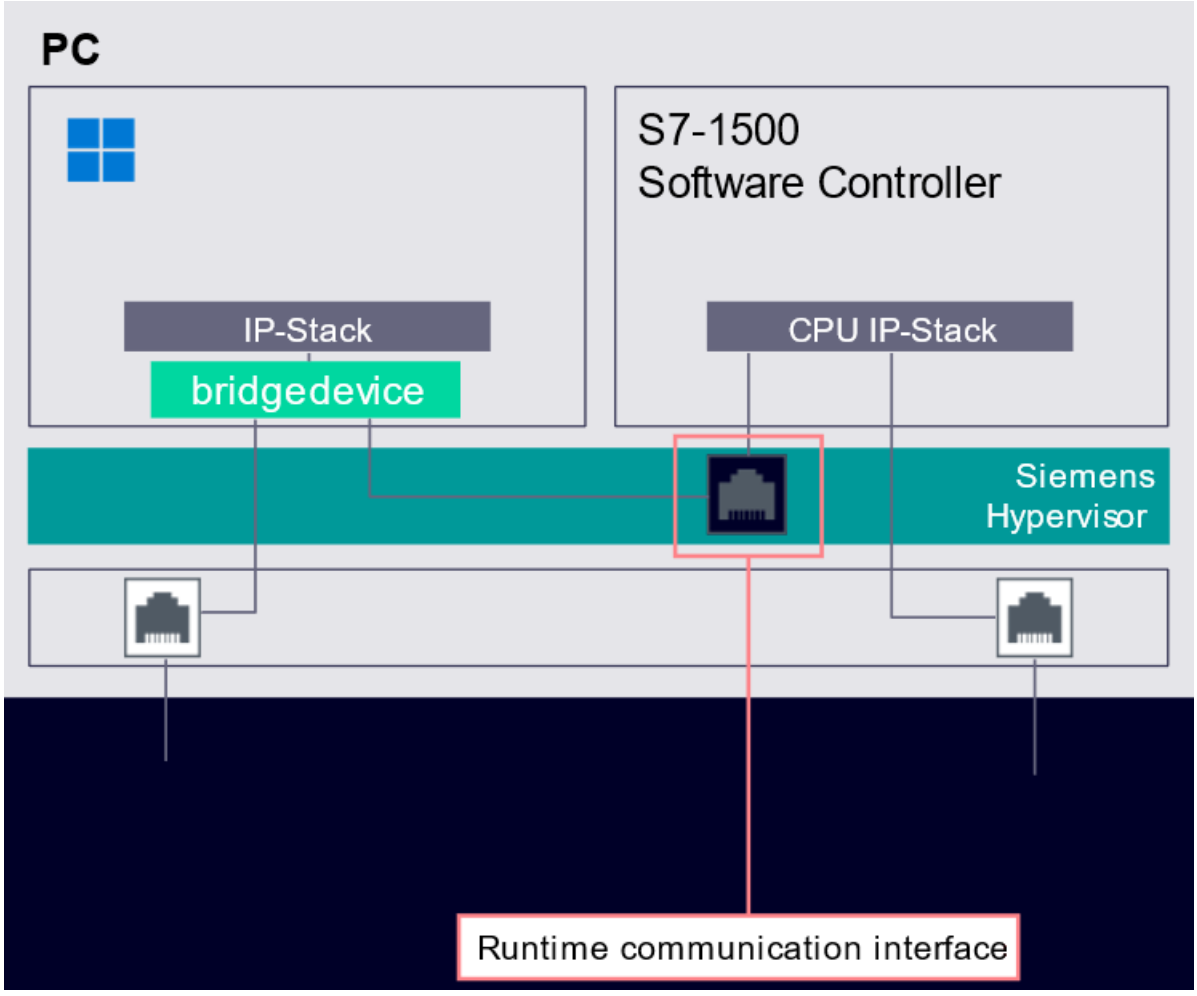


Figure 6-40 Communication with the CPU using bridging

The SIMATIC RT-VMM Network Adapter is bridged to one of the physical network interfaces with Windows.

The bridged interface can be used for:

- Configuration of the Software Controller with an external TIA Portal
- Visualization with an external HMI (for example, WinCC Unified)
- OPC UA communication with an external OPC UA client or server
- Open User Communication with external partners
- S7 communication with external partners

Communication with internal partners is possible if the new bridge interface of Windows and the Runtime communication interface are in the same IP subnet.

For bridging, proceed as follows:

1. Enable bridging for the physical network interface and the SIMATIC RT-VMM Network Adapter.

   NOTE

   When bridging is enabled, the existing IP configuration at both interfaces is lost.

2. Assign an IP address to the new Windows bridging interface.
3. Assign an IP address to the CPU Runtime communication interface in TIA Portal matching the subnet of the Windows bridging interface for:
   - using STEP 7 online functions (when used on the same IPC)
   - downloading the configuration with IP address set
4. Use a "Ping" to test the communication.

Status after bridging

The MAC address of the Runtime communication interface is visible to the outside.

Possible network problems

The following network problems might appear if multiple CPUs are used in the same network:

- The MAC address of the SIMATIC RT-VMM Network Adapter may be reused by Windows for the bridging interface. For this reason, it can happen that the MAC address of the bridging interface is not unique within the network.
- The Runtime communication interface and SIMATIC RT-VMM Network Adapter use random MAC addresses from a defined range to rule out potential conflicts.
- If the Runtime communication interface of more than one CPU within the same network are accidentally using the same MAC address, you must assign individual MAC addresses to each of the interfaces.

  NOTE

  Make sure that the Runtime communication interfaces of all CPUs in the network have a unique MAC address within the same network.

  If necessary, change the MAC addresses using the VMM_NICConfig tool under C:\Program Files (x86)\Siemens\Automation\CPU 150xS\bin.

To change the MAC address of the Runtime communication interface, use the VMM_NICConfig tool (C:\Program Files (x86)\Siemens\Automation\CPU 150xS\bin) and:

- Create a new random address.
- Assign a dedicated address (obtained from the relevant authority).

6.11.4 Communication with CPU using IP routing

The following image shows the communication interface when IP routing is used.

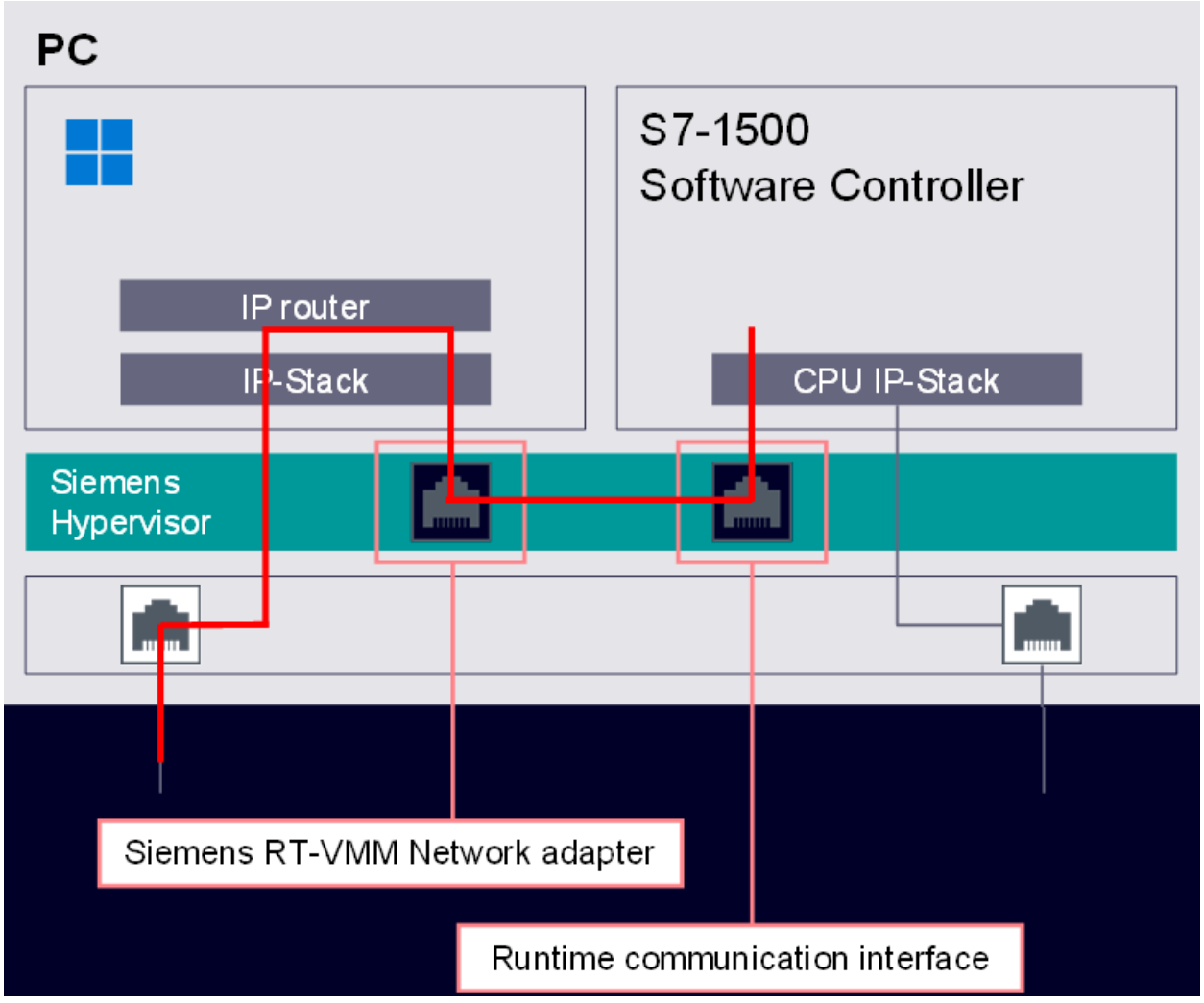


Figure 6-41 Communication using IP routing

IP Routing is used to make a connection to a physical network interface using Windows functionality. The IP-routed network can be used for:

- Configuration of the Software Controller with an external TIA Portal
- Visualization with an external HMI (for example, WinCC Unified)
- OPC UA communication with an external OPC UA client or server
- Open User Communication with external partners

NOTE

Each CPU within the same network must have an IP address with an individual IP subnet.

For IP routing, proceed as follows:

- Create proper IP settings in the CPU's configuration and download them to the CPU (for example, using X2 or file import).
- Set the IP address for the SIMATIC RT-VMM Network Adapter.
- Configure the Windows router.
- Use a "Ping" to test the connection.

NOTE

The IP address of the IPC configured in TIA Portal and the IP addresses of the interfaces assigned to the CPU must be in different IP subnets.

6.11.5 Using Open User Communication over Windows interfaces

Introduction

The S7-1500 Software Controller supports Open User Communication (OUC) via the assigned PROFINET interfaces.

In addition, the S7-1500 software controller supports Open User Communication with Windows applications, and with communications partners via Windows Ethernet interfaces with the following protocols:

- TCP

  With a passive TCP/IP connection, where you are only receiving and not sending data, you will not be informed about a loss of connection.
- UDP

The usual program blocks for Open User Communication can be used for this purpose:

- TSEND_C, TRECV_C
- TMAIL_C
- TCON/TSEND/TRCV/TUSEND/TURCV

NOTE

T_CONFIG instruction

Do not use an all-zero address for calls over NTP. Calls with all-zero addresses result in error "C080_D200".

Interface used

The CPU uses the "PC Communication Interface" (HW_ID 59) for configuration of OUC connections.

NOTE

Support of Hardware Identifier 59

Note that as of V30.0, the Software Controller and Open Controller no longer support HW-ID 59.

As an alternative, you can use HW-ID 140 (Runtime communication interface) with port forwarding or IP routing on the Windows side.

6.11.6 Using OPC UA with Windows applications

6.11.6.1 Using OPC UA locally on the same PC

Before you can use the virtual Ethernet network for OPC UA communication, the IP settings of the two virtual Ethernet interfaces must match. All virtual Ethernet interfaces must be located in the same IP subnet.

Use the following settings:

- Runtime communications interface:

  The address is set in the properties of the CPU in the hardware configuration in STEP 7.

- SIMATIC RT-VMM Network Adapter:

  You set the IP address and subnet mask under "Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings".

  Make the setting before commissioning; setting via STEP 7 is not possible.

6.11.6.2 Using OPC UA remotely over Windows Ethernet interfaces

Establishing a connection with IP routing

IP routing makes the runtime communications interface accessible through an external network. This allows an external OPC UA client to access the OPC UA server of the CPU or the client of the CPU to access an external server.

Procedure

Proceed as follows to implement external access to the OPC UA server over a routed TCP/IP connection:

1. In STEP 7, configure the Runtime communications interface of the CPU for routed IP connections.

   Enter the IP address of the SIMATIC RT-VMM Network Adapter as the default router address.

   You can find additional information in the STEP 7 online help.

2. Configure the Windows IP router and enter the IP route to the interface.

   For the Runtime communication interface and the SIMATIC RT-VMM Network Adapter, assign IP addresses that are located in the same IP subnet.

Establishing a connection using port forwarding

You can configure port forwarding using command line commands. An OPC UA request from an external OPC UA client is then forwarded straight to the OPC UA server of the CPU via the runtime communications interface.

NOTE

TIA Portal downloads via port forwarding are not supported

Note that while it is possible to establish an OPC UA connection via port forwarding, TIA Portal downloads are not possible via port forwarding.

Procedure

1. To open the command prompt, enter "cmd.exe" in the search field in the start menu, and then under the options for the app, click "Run as administrator".
2. Enter the following command with the corresponding port numbers and IP addresses:

   ```
   netsh interface portproxy add v4tov4 listenport=<Port number>
   connectaddress=<IP address> connectport=<Port number>
   listenaddress=<IP address> protocol=tcp
   ```

3. Confirm with the Enter key.

   The port under "listenport" is forwarded to the port under "connectport".

NOTE

- Port number 4840 is set by default.
- Enter the parameters "ServerEndPointUrl" and "ServerUri" manually in the configuration data block of the client interface.

Result

- The Runtime communications interface is not visible in the external network; the CPU can be accessed directly over the IP address of the Windows interface.
- Other OPC UA servers cannot be accessed on Windows.
- If you are using OPC UA Security, you will have to connect the certificates to the IP address or computer name in Windows.

6.11.7 Special features of communication interfaces

Internal partner

S7 Engineering (internal)	Special features
TIA Portal, STEP 7	Not supported

S7 HMI (internal)	Special features
WinCC V7.4 Service Packs (or higher)	See application example (https://support.industry.siemens.com/cs/ww/en/view/109750290)
WinCC flexible	Not supported

S7 SIMATIC NET OPC (internal)	Special features
	Local operation is not possible

S7 communication to SIMATIC controllers (internal)	Special features
	Not supported

S7 communication to third-party applications (internal)	Special features
Other libraries for various high-level languages (for example, LibNoDave)	• Supported communication methods – Data access to non-optimized data • Requirement – You have enabled "PUT/GET". – The index of the CPU is 1. • Addressing the CPU – Passive • Addressing the CPU via the internal partner – IP address: IP address of Runtime communication interface – Port number: 102 – Rack = 0, slot = set index = 1

Web browser (internal)	Special features
Any browser	Requirements • You have enabled the Web server. • You have enabled operation over the respective interface. Via PC communication interface • IP address: Local Host (127.0.0.1) • Port number: As configured in the display application (default: 81/343) Via Runtime communication interface • IP address: IP address of the Runtime communication interface • Port number: Default

OPC UA (internal)	Special features
OPC UA client application	• Supported communication methods – Data access to any (configured) data – Method call • Requirement – You have enabled OPC UA. • Addressing the CPU via internal OPC UA client application – IP address: IP address of the Runtime communication interface – IP port: Default
OPC UA server application	• Supported communication methods – Data access to any (configured) data – DataMethod Call • Requirement – You have enabled OPC UA. • Addressing internal server application via CPU – IP address: IP address of the SIMATIC RT-VMM Network Adapter – IP port: Default
OPC "classic" client (DA, DCOM-based)	Via OPC Wrapper applications under Windows (products from other manufacturers are available)

OUC (internal)	Special features
Any partner	Via Runtime communication interface • Supported communication methods – TCP programmed – UDP programmed – ISOonTCP programmed • Addressing the internal partner via the CPU – HW ID: 0 and 140 – IP address: SIMATIC RT-VMM Network Adapter – Port number: As defined • Addressing the CPU via the internal partner – IP address: Runtime communication interface – Port number: As defined

External partner

S7 Engineering (external)	Special features
TIA Portal, STEP 7	Can be configured over any Windows Ethernet interface

S7 HMI (external)	Special features
WinCC V7.4 Service Packs	see application example (https://support.industry.siemens.com/cs/ww/en/view/109750290)
WinCC flexible	Via unspecified connection • Requirement – You have enabled "PUT/GET". • Addressing – IP address: Windows interface in use – Rack = 0; slot = index

S7 SIMATIC NET OPC (external)	Special features
SIMATIC NET V14 and higher	Configuration in STEP 7 including connection configuration (S7 connection)

S7 communication to third-party applications (external)	Special features
Other libraries for various high-level languages (for example. LibNoDave)	• Supported communication methods – Data access to non-optimized data • Requirement – You have enabled "PUT/GET". – The index of the CPU is 1. • Addressing the external partner via the CPU – Not supported • Addressing the CPU via the external partner – IP address: IP address of one of the Windows Ethernet interfaces – Port number: 102 – Rack = 0, slot = set index = 1

Web browser (external)	Special features
Any browser	Requirements • You have enabled the Web server. • You have enabled operation over the respective interface. Via PC communication interface • IP address: As the connected Windows Ethernet interface • Port number: Configure as in the display application (default: 81/343) Via Runtime communication interface • With IP Routing or NAT Routing set up under Windows – IP address: IP address of the Runtime communication interface – Port number: Default • With port forwarding set up under Windows – IP address: IP address of the Windows Ethernet interface – Port number: Default

OPC UA (external)	Special features
Any OPC UA client device	Supported communication methods • Data access to any (configured) data • Method call Requirement • You have enabled OPC UA. Addressing the CPU via external client • With IP Routing or NAT Routing set up under Windows – IP address: IP address of the Runtime communication interface – IP port: Default • With port forwarding set up under Windows – IP address: IP address of the connected Ethernet interface – IP port: Default – **Note:** Some OPC UA clients do not support operation via port forwarding.
Any OPC UA server device	Addressing the external server via CPU client • With IP Routing or NAT Routing set up under Windows – IP address: IP address of the external client – IP port: Default • With port forwarding set up under Windows – IP address: IP address of the SIMATIC RT-VMM Network Adapter – IP port: Default

OUC (external)	Special features
Any partner	Via Runtime communication interface • Supported communication methods – TCP programmed – UDP programmed – ISOonTCP programmed • With IP Routing or NAT Routing set up under Windows – Addressing the external partner via the CPU HW ID: 0 and 140 IP address: IP address of the external partner Port number: As defined – Addressing the CPU via external partner IP address: Runtime communication interface Port number: As defined

OUC (external)	Special features
	• With port forwarding set up under Windows – Addressing the external partner via the CPU HW ID: 0 and 140 IP address: IP address of the SIMATIC RT-VMM Network Adapter Port number: As defined – Addressing the CPU via external partner IP address: IP address of the connected Windows Ethernet interface Port number: As defined

Operation 7

7.1 Operation using the display

7.1.1 Introduction to the CPU display

The CPU display is designed to resemble the removable display of a hardware controller. The CPU display is a Windows program on your PC, with which you can operate the CPU. 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/109977246).

Functions of the display

Starting or closing the display has no effect on the status of the CPU. The screen position of the display on your monitor is saved when the display is closed.

The display shows you various menu and submenu items.

Figure 7-1 CPU in RUN mode

With the display, the following functions and elements, among other things, are available to you for working with the CPU:

- Start or stop the CPU without shutting down the PC
- Change the operating mode of the CPU
- Status displays for the CPU
- Menus for operation of the CPU
- Display of diagnostic information
- Password assignment for operator input on the display via STEP 7

Advantages

The display offers the following advantages:

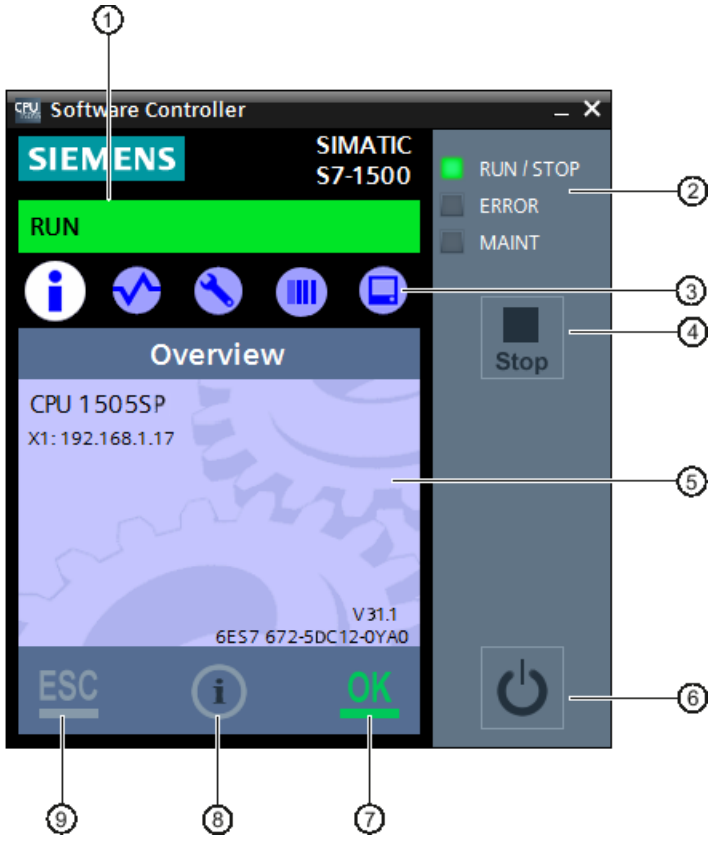
- Reduced downtimes through diagnostics alarms in plain text
- Changing of the interface settings on site without programming device

7.1.2 Operator controls and controller

Layout of the CPU display

The display offers a task-oriented view of the menus and the operating mode of the CPU. Here, you can quickly decide what you want to do and call up the tool for the task at hand.

The figure below shows an example view of the CPU display:



① CPU status information
② LED displays for the current operating mode and diagnostic status
③ Menu selection
④ "RUN/STOP" button (mode selector)
⑤ Information display field
⑥ "Power" button
⑦ "OK" (acknowledge) button
⑧ "Help" button
⑨ "ESC" (Cancel/Back) button

Figure 7-2 Layout of the user interface

NOTE

Example image

Note that the display image only serves as an example. The display differs depending on your used type of Software Controller.

NOTE

Operability with access protection

The selected access protection may limit the operability of the display and the display of menu items.

Observe the information on the Access protection (Page 210).

Menu overview

The table below shows the available submenus of the display:

Main menu items	Meaning	Description
	Overview	The "Overview" menu contains information about the properties of the CPU, such as the device name or software version.
	Diagnostics	The "Diagnostics" menu contains information about diagnostics alarms, the diagnostics description, and the display of alarms. There is also information about the network properties of each of the CPU interfaces.
	Settings	In the "Settings" menu, you assign IP addresses of the CPU; set the date, time of day, time zones, operating modes (RUN/STOP), and protection levels; perform a memory reset or a reset to factory settings of the CPU; and display the status of firmware updates.
	Module	The "Modules" menu contains information about the modules that are used in your configuration. The modules can be used as central modules and/or as distributed modules. Distributed modules are connected to the CPU via PROFIBUS or PROFINET. Here, you have the option of setting the IP addresses for a communication interface.
	Display	In the "Display" menu, you make all settings involving the CPU display, such as the language setting.

Control

Several options are available to control the display:

- Mouse
- Keyboard
- Touch screen (for SIMATIC IPC)

The following function keys and shortcut keys are available with the CPU display:

- **Arrow buttons**: For navigation in a menu
- **Enter**: Access to the menu command, confirmation of input, and exiting from edit mode

- **ESC**: Restoration of the original content, and navigation back to the previous menu command
- **F1**: Calls the online help
- **F2**: Puts an editable field into the processing status
- **F5**: Updates list entries that are not updated automatically
- **Ctrl + P**: Corresponds to the "Power on/off" button
- **Ctrl + M**: Changes the CPU operating mode to RUN or STOP

Functions of the "OK" and "ESC" buttons

- 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 (which means changes are not saved) and exit edit mode

    If changes are made to the settings "PROFINET device name" and "IP address", a note is displayed after the "ESC" button is pressed. Press the "ESC" button once again to discard the changes. Press the "OK" button to apply the changes.
- For menu commands in which no entry can be made:
  - OK → to next submenu item
  - ESC → back to previous menu item

Tool tips for support of usability

The CPU display provides tool tips for the most important buttons.

NOTE

What is a tool tip?

A tool tip is a small pop-up window in application programs or on web pages. It displays a description for an element of the graphical user interface. Tool tips either display the text that the element itself contains or contain supplementary information about the related element.

A tool tip appears only when the button is active.

The CPU display contains buttons that have different functionalities. These buttons have different tool tips depending on the functionality. These buttons include:

- "RUN/STOP" button (mode selector)
- "Power" button
- "OK" button
- "ESC" button

Starting help

You can open the online help for the CPU directly from the opened display in two ways:

- Click  . This button is always active in the CPU display. This button always opens the start page of the help.
- Press the "F1" key to open the help for a specific context. The help opens in a separate dialog. The start page of the help opens by default.

  Some menus and submenus in the CPU display are linked to a specific help topic. In this case, the "F1" key opens the relevant help.

NOTE

Language of the help

The help opens in the same language that you have selected for the CPU display.

Reference

You will find additional information on the topic of the "CPU's display" in the S7-1500 Automation System (https://support.automation.siemens.com/WW/view/en/59191792) system manual.

7.1.3 Manually starting and stopping the CPU via display

Starting via the CPU display

After the start of the CPU display, the CPU can have one of the following statuses:

- The CPU is not running and can be started manually.
- The CPU is already running and indicates the status "Connecting" while the connection is being established. Afterwards, the CPU starts automatically with the current operating mode.

The CPU display lets you manually start or stop the CPU without shutting down the PC. Starting or closing the display has no effect on the status of the CPU.

NOTE

Operating mode in the case of manual start via the display

If you start the CPU manually via the display, it is always in STOP mode.

Figure 7-3 Display of the CPU in "POWER OFF" state

Functionality in the "POWER OFF" state

When the CPU is in "POWER OFF" state, the following functionalities are active:

- LED displays indicate the "POWER OFF" state
- "Start CPU" button to start the CPU
- "Settings > Restore > Format volume" menu and "Settings > Web server" menu
- "Display" menu for changing the language of the display and the help
- "Show help" button to open the help

Starting the CPU

To start the CPU, follow these steps:

1. Open the CPU display.

   Only specific functionalities of the display are activated.

2. Click the "Start CPU" button .

   The status bar of the display initially shows the status "Connect". Once the start process has been successfully completed, the status bar shows the current operating mode of the CPU. The CPU is always in STOP mode when started manually as described.

Figure 7-4 CPU started

NOTE

Example image

Note that the display image only serves as an example. The display differs depending on your used type of Software Controller.

Procedure to power off

To power off the CPU, follow these steps:

1. Open the CPU display.
   All functionalities of the display are active.
2. Click .
   The display shows an acknowledgment query to power off the CPU.

Figure 7-5 Power off CPU

3. Confirm the prompt with "OK".

Result

The CPU is powered off. The display remains open. The status bar of the display shows the "POWER OFF" status.

NOTE

Using central backplane bus modules on a CPU 1515SP PC2

When central backplane bus modules are used on a CPU 1515SP PC2, the central output modules use default values or the preconfigured substitute values when the CPU is stopped.

NOTE

Retentive memory when powering off the CPU

When powering off the CPU while the retentive memory is filled to capacity (100MB), an error message appears prompting you to restart Windows.

Make sure that there is free retentive memory space available before powering off the CPU.

7.1.4 Setting language options in the display

The CPU display can be displayed in various user interface languages. The language is set directly in the corresponding menu on the display rather than in STEP 7. The language for alarms is also shown on the display. The two language settings are independent of one another. The language for alarms depends on your operating system's current setting.

NOTE

Language for the online help and the Web server

Changing the language setting for the display:

- **also** changes the language for the online help
- does **not** change the language for the Web server

Changing the display language

To change the language setting in the display, follow these steps:

1. Start the CPU.
2. Double-click the "Display" menu.

   The "Display" menu opens.

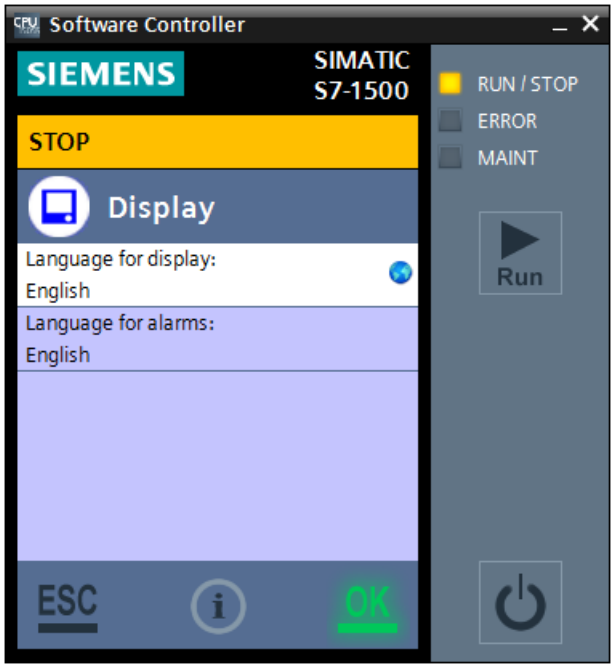


Figure 7-6 Language setting for display and alarms

3. To change the display language, double-click the "Language for display" entry.
   The language selection opens.

Figure 7-7 Language selection

4. Select the appropriate language.
5. Confirm your selection with "OK".

Result

The required language settings are applied.

The language settings are stored when the display is closed.

Explanation of the available languages

The display supports the following language settings:

Language	Meaning
Operating system	The display applies the language of your PC's operating system. If your operating system uses a language that the display does not support, the display automatically opens with the English user interface. If you change the language of your operating system, this will also affect the display language.
English	The display supports English (USA). This language setting is independent of your PC's operating system.
French	The display supports French (France). This language setting is independent of your PC's operating system.

Language	Meaning
German	The display supports German (Germany). This language setting is independent of your PC's operating system.
Italian	The display supports Italian (Italy). This language setting is independent of your PC's operating system.
Spanish	The display supports Spanish (Spain). This language setting is independent of your PC's operating system.
Chinese	The display supports Chinese (Simplified). This language setting is independent of your PC's operating system.

7.1.5 Setting the date and time

Introduction

The CPU display uses the date and time information of Windows by default. These settings can also be changed manually.

Changing the date and time in the CPU display

To change the date and time in the display, follow these steps:

1. Open the CPU display.
2. Select the "Settings > Date & Time > General" menu.
3. Change the desired settings.

   The date and time format depends on the language setting for the CPU display.

   You can only change the time zone if you have downloaded a project.

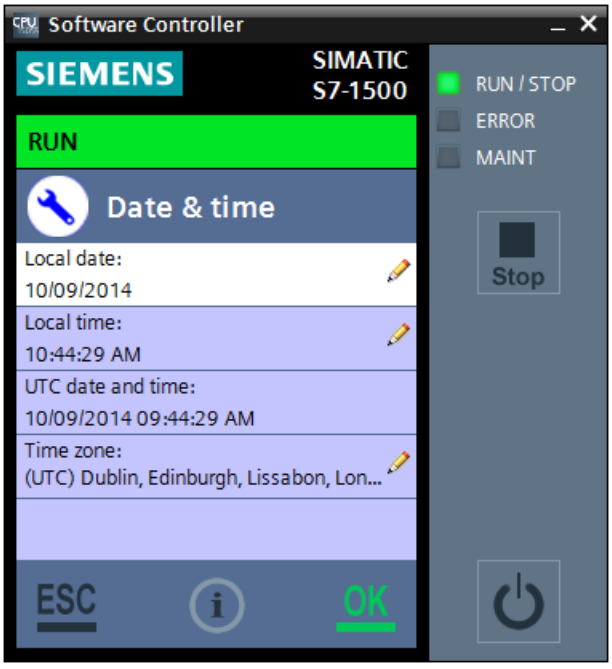


Figure 7-8 Settings for date and time

Result

The date and time settings applied.

Three other methods are available for changing the date and time:

- With the online and diagnostics function "Set time"
- In the CPU properties in STEP 7
- Using instructions in the user program

NOTE

Changing settings with time synchronization

When you use the time synchronization functionality, each change is overwritten via the CPU display during the next synchronization.

7.1.6 Changing the operating mode

General

The CPU display allows you to change the CPU operating mode from RUN to STOP, and vice versa, and to read the current operating mode using the "RUN/STOP" button. Start the CPU first.

The LED display indicates the current operating mode by changing color.

The "RUN" or "STOP" button always shows the operating mode that will be active after clicking the button.

NOTE

Setting of the mode selector of a CPU 1515SP PC2

The "RUN/STOP" button on the CPU display only controls the software.

If you are using the CPU in conjunction with a CPU 1515SP PC2, the position of the hardware mode selector takes priority. If the mode selector of CPU 1515SP PC2 is in STOP position, for example, the CPU cannot be put into RUN mode via the display.

The table below provides an overview of the available operating modes and their meaning:

Table 7-1 Display of the "RUN/STOP" button (mode selector)

Mode	Meaning	Explanation
RUN	RUN mode	The CPU is executing the user program.
STOP	STOP mode	The CPU is not executing the user program.

The status bar in the display shows the current operating mode. Different colors and texts are displayed for visualization. The status bar is visible in any menu view.

Figure 7-9 CPU status information shows RUN mode

NOTE

Example image

Note that the display image only serves as an example. The display differs depending on your used type of Software Controller.

Procedure

To change the operating mode, follow these steps:

1. Open the CPU display.
2. Start the CPU.

   The status bar and the LED display show the current operating mode (in this case STOP).
3. To set the CPU to RUN mode, click the button .

   The status bar changes to RUN mode.

   The button changes its display to "STOP".
4. To set the CPU to STOP mode again, click the button .

   The status bar changes back to STOP mode.

   The button changes its display to "RUN".

The different mode displays and mode symbols

The CPU status information can display the following statuses:

- CPU is in "RUN" mode.

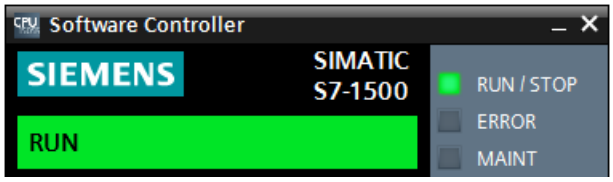


Figure 7-10 "RUN" mode

- CPU is in "STOP" mode.

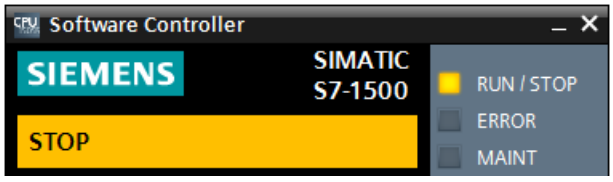


Figure 7-11 "STOP" mode

- CPU is in "FAULT" mode.

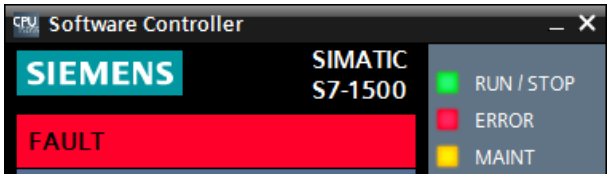


Figure 7-12 "Fault" mode

Various additional symbols can also be displayed in the CPU status information:

Additional symbol	Meaning
	Indicates whether a configured password has been entered or not (Page 214).
	Notifies you of an interrupt.
	Notifies you of the "Force Mode".

7.2 Operation using the command line commands

The CPU can be controlled in various ways. In addition to operation via the display application, it is also possible to control operation using command line commands. You can also automate the use of command line commands in batch files or scripts.

In the following situations, it may make sense to control the CPU with command line commands:

- You are using the CPU in the event of a power failure with a UPS (Page 183) and would like to safely stop the CPU.
- You are using functionalities of the CPU display as an HMI application, which occupies the screen.

In such cases, the command line is available to control the CPU with special commands. You can find additional information on using the command line in section Windows User Management for CPU operations (Page 117).

Commands for controlling the operating mode of the CPU

The following image shows the command line commands available in the CPU Control Tool.

```
C:\Windows\system32>CPU_Control /help
SIMATIC CPU_Control tool version V31.1.0.4
Copyright © Siemens AG, 2024

Command controlled management of S7-1500 Software Controller

Syntax: CPU_Control [/Command]

Commands:
  /PowerOffCPU [-Terminate]                          : Shutdown the CPU
  /PowerOnCPU  [-Auto]                               : Start the CPU
  /AllowReboot                                       : reboot the CPU on next Windows reboot as well
  /DisallowReboot                                    : do not reboot the CPU on next Windows reboot
  /DumpServiceData [-Path <path>]                    : Write Service Data to given directory path
  /GetStatus                                         : Get status of device
  /RUN                                               : Set CPU state into Run mode
  /STOP                                              : Set CPU state into Stop mode
  /GetCollectiveFSignature                           : Get actual Collective F-Signature
  /ConfirmCollectiveFSignature -Signature <signature>  : Confirm that given Collective F-Signature is correct
  /MemoryReset  [-Force]                             : Memory Reset
  /FactoryReset [-Force]                             : Factory Reset
  /GetSerialNumber                                   : Get serial number of CPU
  /SetPMSPassword -Password <password>               : Set PLC Master Secret password
  /DeletePMSPassword                                 : Delete PLC Master Secret password
  /? or /Help                                        : Help

NOTE:
 - Only one command is allowed at a time
 - /RUN and /STOP commands only work, if the Windows user account
   is member of the group  "Software Controller Operators"
 - /GetCollectiveFSignature and /ConfirmCollectiveFSignature commands only work, if the Windows user account
   is member of the both "Software Controller Operators" and "Failsafe Operators" groups
 - /SetPMSPassword command only works, if a PMS password is not already set

C:\Windows\system32>_
```

Figure 7-13 CPU Control Tool

The following table provides an overview of the command line commands and their purpose:

Command	Explanation
CPU_Control /PowerOnCPU	Starts the CPU in "STOP" mode.
CPU_Control /PowerOnCPU -Auto	Starts the CPU with the configured startup type.
Note: After executing a PowerOn command, you should wait at least 15 seconds before executing the next command. In scripts, for example, you can put sleep statements between the commands.	
CPU_Control /PowerOffCPU	Stops the CPU.
CPU_Control /PowerOffCPU -Terminate	Forces the CPU to stop in any situation. Retentive data cannot be stored with this operation.

Note:
After executing a PowerOff command, you should wait at least 9 seconds before executing the next command. In scripts, for example, you can put a sleep statement between the commands as the example below shows:
`CPU_Control /PowerOffCPU`
`sleep 9`
`CPU_Configuration /import project.psc`
`CPU_Control /PowerOnCPU`
`sleep 15`
`CPU_Control /RUN`	

CPU_Control /AllowReboot	Permits a complete restart of the PC. The CPU prevents the PC restart and by default only restarts the Windows operating system to continue monitoring the automation process. To prevent loss of retentive data, you must manually stop the CPU **beforehand**.
CPU_Control /DisallowReboot	Disables the CPU_Control /AllowReboot function if it was executed beforehand.
CPU_Control /Dumpservicedata -path <path>	Allows service data to be saved in a file after "FAULT" mode. Siemens can evaluate this file for diagnostic purposes if requested through Siemens Customer Support.
CPU_Control /GetStatus	Obtains the current status of the CPU
CPU_Control /RUN	Sets the CPU to "RUN".
CPU_Control /STOP	Sets the CPU to "STOP".
CPU_Control /MemoryReset	Resets the CPU memory. When the CPU is in "RUN", you are prompted for a confirmation before the control tool continues.
CPU_Control /FactoryReset	Resets the CPU to the factory setting. When the CPU is in "RUN", you are prompted for a confirmation before the control tool continues.
CPU_Control /GetSerialNumber	Displays the serial number of the CPU.
CPU_Control /SetPMSPassword	Sets a password for protecting confidential configuration data. This command allows you to import PMS-protected projects without a memory card or having online access from TIA and makes automation possible by scripting. Note that the command only works if a password has not already been set. For the password, the following policy applies: • The password length must be between 10 and 120 characters. • The password must contain at least one number. • The password must contain at least one uppercase and one lowercase letter. • The password must only contain ASCII characters.

Command	Explanation
	Note that for setting a password, the CPU must be in STOP mode.
CPU_Control /DeletePMSPassword	Deletes the password for protecting confidential configuration data Note that for deleting the password, the CPU must be in STOP mode.
CPU_Control /Help	Displays the help text in the command line editor.

The following table shows additionally command line commands that are available for F-CPUs:

Command	Explanation
CPU_Control /GetCollectiveFSignature	Outputs the collective F-signature.
CPU_Control /ConfirmCollectiveFSignature	Confirms the collective F signature after entry of the collective F-signature.

The following table provides an overview of the feedback messages based on the supported command line commands:

Feedback	Code	Explanation
CPU_Control tool operation result: SUCCESS	0	The command was executed successfully.
CPU_Control tool operation result: FAIL	1	An error occurred when executing the command.
Invalid parameters. See help for more information	64	The command parameters were invalid. The help opens automatically.
Too many parameters. See help for more information		

7.3 Operating modes

7.3.1 Basic principles of the operating modes

Introduction

Operating modes describe the states of the CPU. The following operating modes can be set via the CPU display:

- RUN
- STOP

The CPU can communicate in these operating modes, for example, via the PN/IE interface.

The status LEDs indicate the current operating mode.

Reference

You can find additional information in the STEP 7 online help.

7.3.2 Operating mode transitions

Operating modes and operating mode transitions

The following figure shows the operating modes and the operating mode transitions:

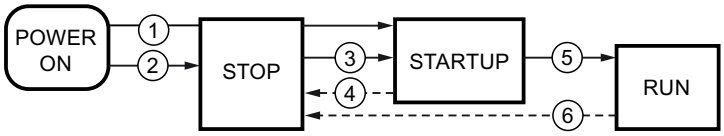


Figure 7-14 Operating modes and operating mode transitions

The following table shows the conditions under which the operating modes change:

Table 7-2 Operating mode conditions

No.	Operating mode transitions	Conditions
①	POWER ON → STOP → STARTUP	After switching on, the CPU goes to "STARTUP" mode if: • The hardware configuration and program blocks are consistent. • The startup type "Warm restart - RUN" is set or the startup type "Warm restart - mode before POWER OFF" is set and RUN mode was active before POWER OFF. Non-retentive memory is cleared, and the content of non-retentive DBs is reset to the start values of the load memory. Retentive memory and retentive DB contents are retained.
②	POWER ON → STOP	After switching on, the CPU goes to "STOP" mode if: • The hardware configuration and program blocks are not consistent or • the "No restart" startup type is set or • if the CPU is manually started from the display. Non-retentive memory is cleared, and the content of non-retentive DBs is reset to the start values of the load memory. Retentive memory and retentive DB contents are retained.
③	STOP → STARTUP	The CPU goes to "STARTUP" mode if: • The hardware configuration and program blocks are consistent. • The CPU is set to "RUN" by the programming device or via the display and the mode selector is in the RUN position or • the mode selector is switched from STOP to RUN. Non-retentive memory is cleared, and the content of non-retentive DBs is reset to the start values of the load memory. Retentive memory and retentive DB contents are retained.
④	STARTUP → STOP	The CPU returns from "STARTUP" mode to "STOP" mode in the following cases: • An error is detected during start-up. • The CPU is set to "STOP" from the programming device. • A STOP command is executed in the Startup OB.
⑤	STARTUP → RUN	The CPU goes to "RUN" mode in the following cases of "START-UP": • The CPU has initialized the PLC tags. • The CPU has executed the startup blocks successfully.
⑥	RUN → STOP	The CPU returns from "RUN" mode to "STOP" mode in the following cases: • An error is detected that prevents continued processing. • A STOP command is executed in the user program. • The CPU is set to "STOP" mode via the programming device, the display, or the mode selector.

Maintenance 8

8.1 Status display in the notification area

An icon is displayed in the notification area of the Windows taskbar during operation of the CPU. The icon indicates, among other things, the current operating mode of the CPU and special diagnostic information.

Double-click the icon in the notification area to open the display of the CPU.

Displaying the notification area icon permanently

Windows displays only certain icons in the notification area permanently by default. The CPU icon is displayed only when there is a change of operating mode and is then hidden again. You can enable permanent display of the CPU icon.

To enable permanent display of the CPU icon, follow these steps:

1. Select the "Change notification icons" shortcut menu command in the notification area.

   The Control Panel opens.
2. Select the CPU icon.
3. Change the behavior to "Show icon and notification".

Functionality of the notification area icon

The notification area icon provides the following functionalities and information:

- Double-clicking the icon in the notification area opens the display.
- Each operating mode of the CPU has a different display.
- A message window provides special information  , such as a missing license key.
- Tool tips identify the corresponding CPU instance.

States of the notification area icon

The status of the icon for the CPU in the notification area of the taskbar changes as soon as the CPU mode changes.

The notification area icon can display the following states:

RUN	STOP	Fault
		

NOTE

Created link

Only the symbols automatically created during setup show the correct operating modes. Any links you have created may not always show the current mode.

Displaying the notification area icon in the active area of notification area

The icon for the CPU in the notification area of the taskbar can automatically be moved to the inactive area of the Windows notification area after a period of time specified by the operating system. Change the visibility settings in the settings for the notification area of the taskbar.

8.2 Using an uninterruptible power supply (UPS)

A UPS system can help to ensure that the CPU shuts down correctly and saves the current state in case of a power failure. Siemens recommends the use of a UPS for operation with the Windows operating system.

Setting up the UPS for your PC

The CPU provides two options for using a UPS:

- Connect the UPS to the PC via USB. The UPS notifies Windows.

  The PC detects a power failure and sends a power failure signal to the CPU. The CPU can then trigger a quick shutdown and back up the retentive data, if such a configuration was made. Systems that use a CFast file system that is protected with the UWF are stable in the event of an unexpected power failure.

  Enter the command "CPU_Control /PowerOffCPU" in the shutdown script of the UPS.

- Connect the UPS to the CPU via a digital input. Windows can be shut down in the CPU's user program by means of the "SHUT_DOWN: Shutdown target system" instruction.

Consequences of a power loss without an operating system shutdown

A power failure without shutting down the Windows operating system with deactivated UWF can damage the file systems of the operating system. Use a UPS system to protect the file systems.

Reference

The following application example (https://support.industry.siemens.com/cs/ww/en/view/109822806) provides a description of how to safely shut down the Software Controller using a SITOP UPS.

8.3 BIOS update

For correct operation, update the BIOS to the latest BIOS version specified in SiePortal (https://support.industry.siemens.com/cs/ww/en/view/109763408).

For detailed information on how to update BIOS, see section Quick start guide and SIMATIC IPC – BIOS update (https://support.industry.siemens.com/cs/ww/en/view/109757305).

BIOS settings after updating the BIOS of the IPC

After you have updated the BIOS, make sure you reapply the mandatory and recommended BIOS settings. If the boot menu screen (GRUB) does not appear after the BIOS Update, proceed as follows.

1. Go to BIOS Setup Boot→EFI.
2. Check, if the boot option "GRUB2" is in the first position of the boot order.
3. If it is not in the first position, move the boot option "GRUB2" to the first position.

If the boot option cannot be moved to the first position because the entries are grayed out, proceed as follows:

1. Go to Boot→Add Boot Options and check the state.
2. If the state is [Auto], change it to [First].
3. Move the boot option "GRUB2" to the first position in BIOS Setup Boot→EFI.

NOTE

Boot option "GRUB2"

You may have to boot Windows once and then return to BIOS Setup before the boot option "GRUB2" will be shown under the available boot options.

8.4 Firmware update of I/O modules

Introduction

During operation, it may be necessary to update the firmware (for example, due to functional enhancements).

NOTE

Firmware update of I/O modules

You can update central and distributed I/O modules.

Requirement

- You have downloaded the file(s) for the firmware update from the Siemens Industry Online Support (https://support.industry.siemens.com/cs/ww/en/ps).

  On this web site, select: Automation technology > Automation systems > Industrial Automation Systems SIMATIC > PLC > Software Controller > S7-1500 Software Controller.

  From there, navigate to the specific type of module that you want to update. To continue, click the link for "Software downloads" under "Support". Save the desired firmware update files.
- Before installing the firmware update, ensure that the modules are not being used.

Options for the firmware update

A firmware update is performed using STEP 7 (online) or the Web server.

Installation of the firmware update

⚠ WARNING

Impermissible plant states possible

Due to the installation of the firmware update, the CPU enters STOP mode, which can impact 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.

Before installing the firmware update, ensure that the CPU is not executing any active process.

Procedure using STEP 7

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" command from the shortcut menu.
3. Select the "Firmware update" group in the "Functions" folder.
4. Click the "Browse" button in the "Firmware update" area to select the path to the firmware update files.
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 "Start update" button. If the selected file can be interpreted by the module, the file is downloaded to the module. If the operating mode of the CPU needs to be changed for this purpose, you will be prompted to do this by means of dialogs.

NOTE

Updating the firmware

The "Run firmware after update" check box is always activated.

Procedure using the Web server

The procedure using the Web server is described in the function manual for the Web server. You can find the function manual on the Internet (https://support.industry.siemens.com/cs/ww/en/view/59193560).

Reference

Further information on firmware updates can be found in the S7-1500 Automation System (https://support.industry.siemens.com/cs/ww/en/view/109977246) system manual and the STEP 7 online help.

8.5 Resetting the CPU

During a reset, the CPU is set to the "delivery state". This means that all data stored in the CPU is deleted.

The following reasons may require a data reset:

- A restart with the original data (cold restart)
- A reset of all internally persistent settings (for example, IP address) for a defined status
- Use of a cleaned state of the CPU for new projects

NOTE

SNMPv1 community values

If you have changed the SNMPv1 community values, the reset to factory function will not reset these values to their default values "public" or "private".

To reset the SNMPv1 community values to their default community values, use the "Format the CPU volume" command on the display. For more information on this command, refer to chapter Formatting the CPU volume (Page 191).

Reset options

You have the following options to reset the CPU.

- **Memory reset**: The CPU is reset to the project settings configured by default. You can run this function as follows:
  - In the CPU display (Page 188)
  - Via the mode selector of the utilized hardware platform (Page 191)
- **Factory reset**: The CPU is reset to the default factory settings. You can run this function as follows:
  - In the CPU display (Page 188)
  - Using STEP 7 (Page 190)

NOTE

Date and time

After the reset, the Windows time is applied as the local date and local time.

NOTE

Memory and factory reset for failsafe CPUs

For fail-safe CPUs, you can use the display to perform a memory reset and factory reset with the "Full access (no protection)" protection level. For these operations, you do not need to use the "Full access incl. fail-safe (no protection)" protection level.

- **Format the CPU volume**: The CPU volume is cleaned (Page 191). You run this function in the CPU display.

  With an F-CPU, this function is not available via the display.

Conditions for reset

For resetting the CPU, make sure that the following conditions are met:

- CPU in STOP mode
  The CPU must be in STOP mode to be reset.
- Sufficient retentive memory available
  When the retentive memory is filled to capacity (100MB), it is no longer possible to perform a memory or factory reset of the CPU. Make sure that there is free retentive memory space available before performing a memory reset using the display or STEP 7.

Reference

Additional information on the topic "Resetting to factory settings" can be found in the Structure and Use of the CPU Memory (https://support.automation.siemens.com/WW/view/en/59193101) function manual, section on memory areas and retentivity, and in the online help for STEP 7.

8.5.1 Reset using the display

The following procedures are available to reset the CPU to factory settings or to perform a memory reset using the display.

Procedure using the display

To reset the CPU using the display, follow these steps:

1. Open the CPU display.
2. Start the CPU (if CPU is in "Power Off" state).
3. Select the "Settings" menu.
4. Confirm your selection with "OK".
   The "Settings" menu opens.
5. Select "Reset".

6. Confirm your selection with "OK".
   The "Reset" item opens.

Figure 8-1 Reset options

7. Select one of the options to reset the CPU.
   The requested function opens.

Figure 8-2 Confirmation prompt prior to reset

8. Acknowledge the confirmation prompt with "OK".

Result

The CPU performs the reset. The RUN/STOP LED flashes yellow. When the RUN/STOP LED lights up yellow, the CPU has been reset and is in STOP mode. The corresponding event is entered in the diagnostics buffer.

The project is retained since the load memory is not erased.

8.5.2 Reset using STEP 7

The following procedures are available to reset the CPU to factory settings using STEP 7.

Procedure using STEP 7

To reset the CPU using STEP 7, follow these steps:

1. Make sure there is an online connection to the CPU that is to be reset to the factory settings.
2. Open the online and diagnostics view of the CPU.
3. Select the "Reset to factory settings" group in the "Functions" folder.
4. Select the "Keep IP address" option button if you want to keep the IP address or the "Reset IP address" option button if you want to delete the IP address.
5. Click the "Reset" button.
6. Acknowledge the confirmation prompt with "OK".

NOTE

To also delete and reset the IP address, execute the following commands on the target system:

- CPU_ResourceConfigurator.exe -s -v
- CPU_ResourceConfigurator.exe -r "C:\Program Files (x86)\Siemens\Automation\CPU 150xS\ResourceConfigurator\<json file with desired resource configuration>" -v
- Reboot the system

Result

The CPU is set to STOP mode and is reset to factory settings.

The project is retained since the load memory is not erased.

8.5.3 Resetting via the mode switch

Procedure using the mode selector

This procedure is possible only for operation on the CPU 1515SP PC(2) (F).

Make sure that the CPU is in STOP mode (the CPU display shows STOP mode or RUN/STOP LED lights up yellow).

NOTE

A memory reset of the CPU via the mode selector also deletes the CPU's IP address.

To reset the CPU memory 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 mode selector 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 switch.
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 the memory reset while the RUN/STOP LED flashes yellow. When the RUN/STOP LED lights up yellow, the CPU has been reset and is in STOP mode. The corresponding event is entered in the diagnostics buffer.

8.5.4 Formatting the CPU volume

The CPU volume is a non-volatile memory for configuration data, user programs and data, initial data, and archives. When these objects are downloaded to the CPU, they are first stored in the load memory. The load memory is located in the CPU volume in the mass storage of your PC.

During the setup, the load memory is formatted automatically and, as a result, all data and files from the prior installation are deleted.

If the CPU volume is damaged (for example, due to voltage failure while the CPU volume is being written) or is to be cleaned for a new use, you can format the CPU volume using the "Format the CPU volume" function in the CPU display.

NOTE

The "Format the CPU volume" function is not supported by F-CPUs.

Requirement

- A CPU volume is created in the current configuration.
- The user of the PC has administrator rights.

Procedure

To format the CPU volume, and thus the load memory of the CPU, using the CPU display, follow these steps:

1. Open the CPU's display using the shortcut menu command "Run as administrator".
2. Select the "Format the CPU volume" command in the "Settings > Reset" menu.

Figure 8-3 Formatting the CPU volume

3. Confirm with OK.

   Another confirmation message appears.

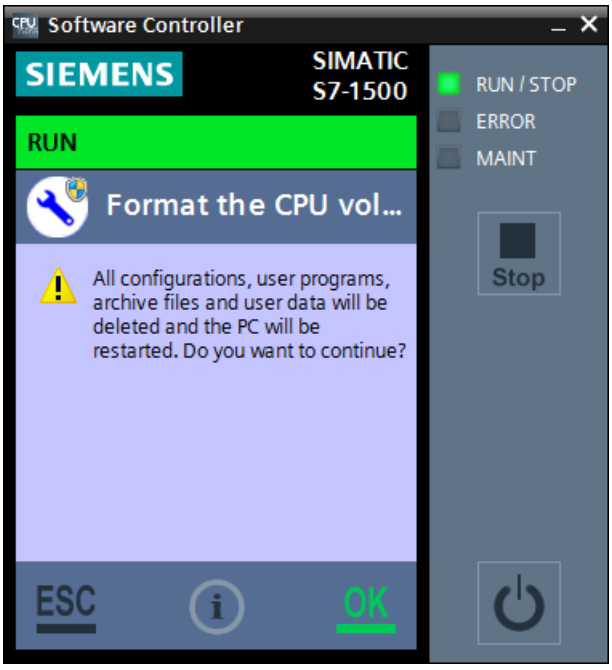


Figure 8-4 Confirming the CPU volume formatting

4. Confirm with OK.

NOTE

CPU in "POWER OFF" state

You can also execute this command when the CPU is in "POWER OFF" state.

NOTE

Assigned interfaces after formatting the CPU volume

Formatting the CPU volume also deletes the hardware configuration and the assigned interfaces. To keep the assigned interfaces after formatting the CPU volume, use Resource Configurator to reapply the previously applied JSON file.

Result

The CPU is stopped and shows the status of the formatting with the help of a progress bar. The formatting deletes the following data and values:

- The complete load memory
- Retentive data
- User programs and configurations
- Archives and user data
- Web server directories

The following internal CPU data is restored:

- Module name
- Index
- Assigned interfaces
- Retentive data memory
- Position of the mode selector
- Use of the LEDs

The startup type setting is retained. When you switch on the CPU the next time, the load memory is preset with default settings. The CPU is in STOP mode.

8.6 Backing up the image of the PC mass storage

Overview

Once you have configured the computer for your application, you can create an image of your system. An image can include the following:

- The CPU volume
- The Windows partitions and the CPU volume

You can use this image to restore your user-specific application to your system at a later time, if necessary. A system image is helpful for restoring all files and registry entries for your application.

You should back up an image of your configuration for these reasons:

- To save a fixed intermediate status of the configuration
- To create a backup of the current configuration in case of hardware problems and when the PC must be replaced
- To create a master image which can be restored on other PCs

  Note the Microsoft license condition for Windows in this regard.

NOTE

Pay attention to consistency

- The image must always be consistent with the installed version of the CPU.
- The images are dependent on the computer on which they were created. They cannot be used on different computer types.
- The mass storage on which the image is restored requires the same or more capacity than the mass storage card on which the image was created.

SIMATIC IPC Image & Partition Creator

Use the "SIMATIC IPC Image & Partition Creator" to back up your configuration.

"SIMATIC IPC Image & Partition Creator" is used to back up and restore files, directories, partitions, and entire hard drives. By creating backup images, "SIMATIC IPC Image & Partition Creator" prevents data loss caused, for example, by hardware failure, installation problems, operating errors, or external influences (viruses).

NOTE

Restoration of images on a larger mass storage

If you want to restore an image from a smaller mass storage on a larger mass storage, do not change the size of the partitions proportionally.

NOTE

Encrypted data is not supported

Image & Partition Creator does not support encrypted data. Before using Image & Partition Creator, decrypt the files, directories, partitions, or hard drive you wish to back up and restore.

Restoring images with Image & Partition Creator V3.6

If you are using Image & Partition Creator V3.6, the default restore option is to restore from volume to volume. To avoid booting problems after the restore, do not use this default restore type. Change from "Select volumes" to "Select disks" instead and restore as complete disks.

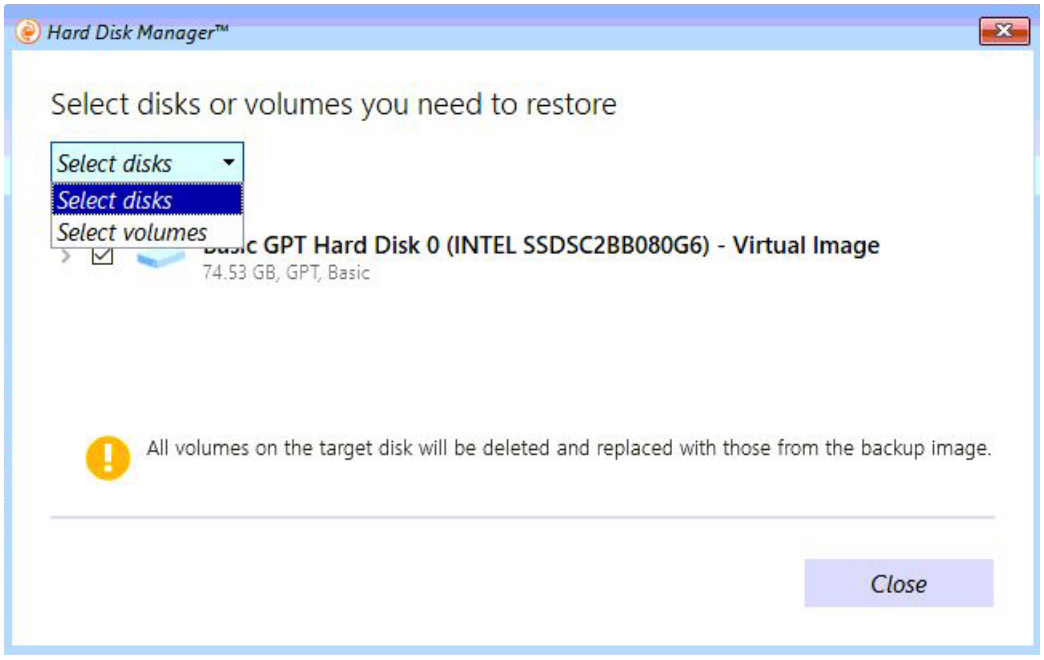


Figure 8-5 Changing the default restore type

After you have changed the restore type and clicked "Close", the following window appears. On this window, click "Restore now".

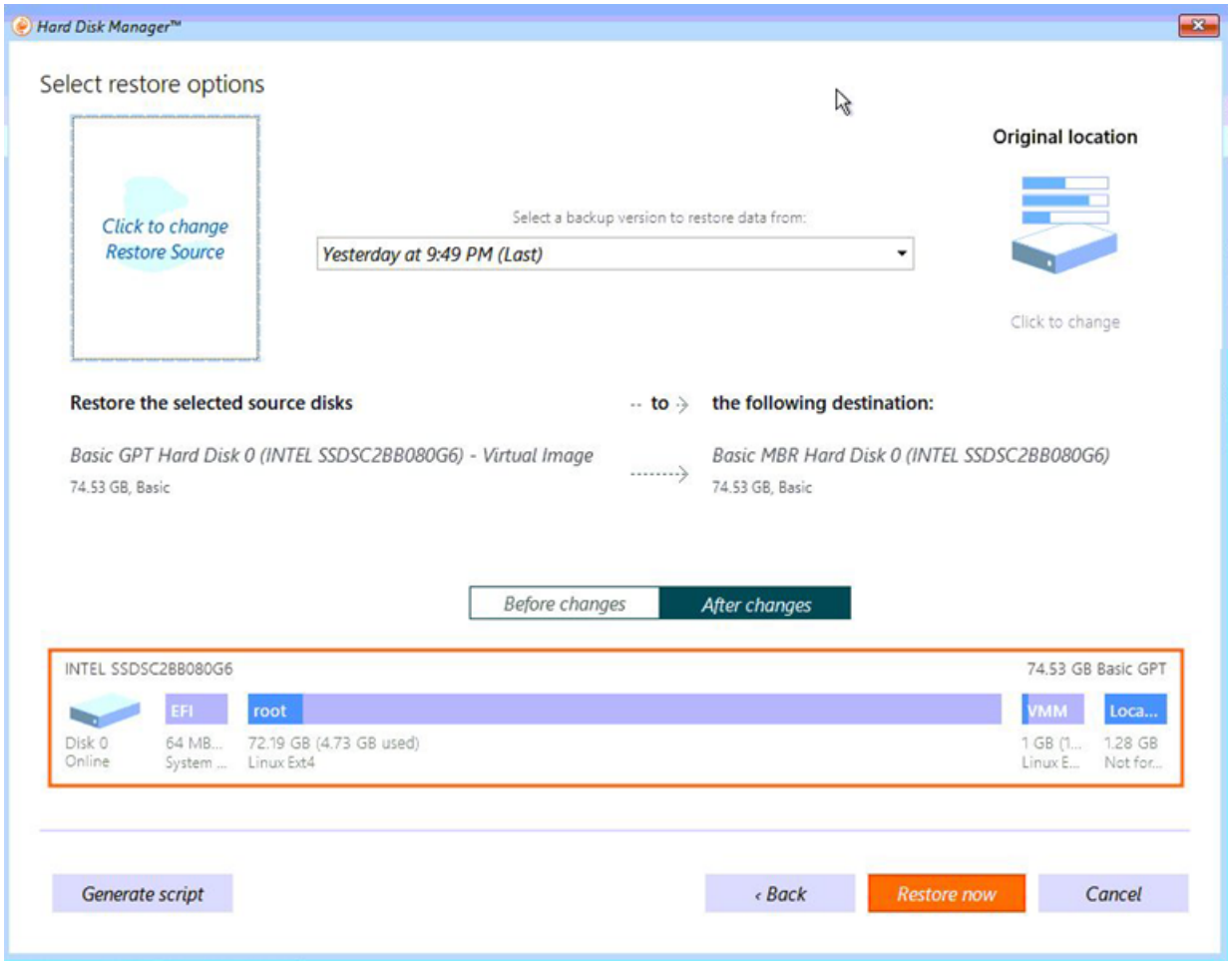


Figure 8-6 Disk to disk restore dialog

Reference

For additional information on backing up an image, see the documentation on the "SIMATIC IPC Image & Partition Creator" (https://support.automation.siemens.com/DE/view/en/21766418).

You also have access to topic-related FAQs (https://support.automation.siemens.com/DE/view/en/19422936/133000).

Backing up and restoring the installation on mass storage devices

You have the possibility to create a backup of your Software Controller installation from a mass storage device and to restore this backup on another mass storage device.

To avoid boot failures after an uninstallation or upgrade of the Software Controller, the utility BootSect.exe is automatically installed in the C:\Windows\System32\ directory during the installation of an IPC.

8.7 Special features

8.7.1 Use of bus adapters

The CPU 1505SP supports the following bus adapters:

Bus adapter	Article number
BA 2xM12	6ES7193-6AM00-0AA0
BA 2xRJ45	6ES7193-6AR00-0AA0
BA LC/RJ45	6ES7193-6AG20-0AA0
BA LC/FC	6ES7193-6AG40-0AA0
BA 2xSCRJ	6ES7193-6AP00-0AA0
BA SCRJ/RJ45	6ES7193-6AP20-0AA0
BA SCRJ/FC	6ES7 193-6AP40-0AA0
BA 2xLC	6ES7 193-6AG00-0AA0

8.7.2 Error messages during installation of drivers

All necessary drivers are installed automatically by default when the software for the CPU is installed. Additional dialogs and messages regarding installation of drivers do not appear. The supplied drivers are certified by Microsoft and have a digital signature that indicates Siemens as the supplier.

If warning messages concerning the driver software are displayed during installation, you must assume that the installation files have been altered.

Check whether the installation files used are identical to those on the installation DVD supplied by Siemens.

8.7.3 Special situations when downloading in STEP 7

No connection possible

In order to download the project to the target system, an online connection must be established.

If an online connection to the target system is not possible, check the interface settings, such as the IP address. You also have the option of establishing an online connection via the IE General interface.

Download aborts

If the download aborts for unidentifiable reasons, you may need to reset the CPU to factory settings using the display (Page 188).

8.7.4 Special situations when starting or stopping the CPU

Possible situations

The following special situations can occur when starting or stopping the CPU:

- The CPU indicates a "Fault" status.
- The CPU display cannot establish a connection to the CPU.
- The PC booted up in "Windows" mode.
- The CPU has been started or stopped using a command line command.

CPU in "Fault" state

"Fault" can occur in the following cases:

- While the CPU is starting

  The CPU remains in "Fault" state until the user selects one of the functions in the "Restore" menu.
- While the CPU is running

  The display changes automatically to the "Restore" menu. The CPU restarts automatically after 10 seconds in STOP mode.

No connection to the CPU

If the display cannot establish a connection to the CPU, the display automatically opens the "Restore" menu. You can choose from the following options:

- Restart PC

  The entire PC is restarted.

  Restart the PC using the "Windows and S7-1500 Software Controller" mode, otherwise the message "Wrong Boot Option" will be shown on the display.

- Terminate CPU

  The CPU is stopped. Retentive data is lost.

PC start in "Windows" mode

If you start the CPU display after the PC was booted in "Windows" mode, the display automatically opens the restore menu to restart the PC. The message "Wrong boot option" will be shown in the display.

Starting or stopping the CPU using command line commands

The CPU can be controlled in various ways. In addition to operation via the display application, it is also possible to control operation using command line commands. You can also automate the use of command line commands in batch files or scripts.

For an overview of available command line commands, see chapter Operation using the command line commands (Page 178).

8.7.5 CPU behavior on Windows shutdown

When you switch off your PC, the Windows operating system shuts down automatically, and all active applications are closed.

The following actions will shut down the Windows operating system:

- PC is switched off via the Start menu.
- PC is switched off with the on/off button.
- Uninterruptible power supply (UPS) (Page 183) triggers a shutdown.
- PC is shut down in the CPU's user program by means of the "SHUT_DOWN: Shutdown target system" instruction. The instruction is available in TIA Portal in the "Instructions" task card under Basic instructions > Program control > Runtime control.

  A restart is advisable, however, in the following situations:

  – An industrial UPS reports a power failure via a digital input.
  – Too many error OBs are called in the user program.
  – Windows stops responding or shows a "blue screen".

  You can find more information on the "SHUT_DOWN: Shut down target system" instruction in the STEP 7 online help.

When the Windows operating system shuts down, the CPU is stopped properly. The CPU stores the retentive data and all CPU-specific files.

When you restart the PC, the CPU starts as previously configured.

Reference

Additional information about the CPU behavior during starting or stopping can be found in section Manually starting and stopping the CPU via display (Page 166).

8.7.6 Windows error handling and operating the CPU after a Windows crash

Introduction

The CPU is a PC-based controller. It is installed for use on a PC with the Windows operating system. A crash of the Windows operating system may affect the operation of the CPU.

CPU reaction to a Windows crash

The CPU continues to run even when the operating system crashes. Configure Windows so that it automatically restarts after a crash. After most scenarios, the CPU remains in RUN mode and controls the automation process even during the crash. Because increased drive access by the operating system can occur during the Windows restart, the drive access of the CPU may become slower temporarily. Once Windows has been started up again, the user program of the CPU is notified about the restart of the operating system.

If Windows does not automatically restart after a crash, restart the PC with one of the following options:

- Use the instruction "SHUT_DOWN: Shutdown target system".
- Switch off the PC using the "Power" switch or by briefly removing the power supply (remove and insert the connector). The CPU is stopped. If you have configured retentive data storage in the onboard NVRAM of your PC, the retentive data is retained during this operation. If you have configured retentive data storage in the mass storage of your PC, the retentive data is deleted during this operation. The CPU starts in the unbuffered state.

NOTE

Diagnostics on Windows availability

A diagnostic buffer entry is generated when Windows starts, stops, or crashes, and a diagnostic interrupt (OB82) is started.

To get detailed information about the Windows status via the OB82, open the "RALRM" (SFB54) instruction.

It may be the case that Windows can no longer send a signal to the CPU in the event of a blue/"frozen" screen. OB82 is not called in this case and no diagnostic entry is created.

To obtain more information, call the "RDREC" instruction (SFB52) with a cyclic OB (for example, OB1).

You can find further information about the diagnostics and the instructions with the parameters in the Diagnostics (https://support.automation.siemens.com/WW/view/en/59192926) function manual and in the STEP 7 online help.

Windows error handling features

Windows error handling features such as recovery options, advanced startup settings, the "chkdsk" command, memory diagnostics and antivirus offline scan may only be used after the PC has been restarted in "Windows-only" mode.

For more information on how to restart Windows in "Windows-only" mode, see chapter Restarting Windows (Page 203).

8.7.7 Timeouts

The following processes on the PC can affect the Software Controller cycle:

- The PCI Express bus of the PC is shared by all applications on the PC. A high PCI Express bus load can therefore lead to runtime influences between applications. To keep the number of timeouts as low as possible, use a high send clock for isochronous mode, in particular, and avoid large loads (for example, 3D graphics).
- If you are using the Software Controller in isochronous mode, cycle times may be exceeded during Windows restarts. Check the return values of the isochronous SFCs (126 and 127).
- Windows restarts on a SIMATIC IPC with TPM module.

NOTE

Hiding TPM module in BIOS settings

Hiding the TPM module will decrease jitter on Windows restart. For this reason, we recommend hiding the TPM module on all IPCs supporting this option to avoid timeouts.

For more information on individual BIOS settings, refer to the BIOS settings mentioned in section Reference information for use with SIMATIC IPC (Page 235).

- Windows restarts on a SIMATIC IPC using System Management Interrupts (SMI).

8.7.8 Restarting Windows

Windows restart during operation of the Software Controller

If Windows does not start successfully after a restart, or if (HMI) communication with the Software Controller is disrupted, you can continue to operate the Software Controller for as long as necessary until a brief shutdown is possible from the point of view of your application. Remedy the situation by power cycling (off/on) the entire PC (Windows and Software Controller).

Depending on the state of the Windows system, proper restarting of Windows is not possible in rare cases. You should therefore avoid Windows restarts of a machine or plant during live operation.

Only Windows is restarted by default. Restarting Windows while the Software Controller is running might have a negative impact on the time response of the Software Controller.

If you reboot Windows during Software Controller operation, note the following:

- The PC does not start via the BIOS. Instead, only the Windows operating system is restarted.

  Some components require a system restart via the BIOS, for example, if the TPM module requests a restart. In this case, restart the complete system. You can find additional information in the section "Restarting the operating system and CPU (Page 205)".
- Increased jitter occurs during the Windows restart, for example, due to hardware with a TPM module.
- If the PC is switched off/restarted via iAMT (Intel Active Management Technology), the retentive data are lost.

NOTE

Ensuring real-time capability during the restart phase

To ensure real-time capability during the reboot phase of the system, the USB ports are disabled during the Windows reboot process. Input devices such as the mouse and keyboard that are connected via a USB port are also disabled.

If you use additional PCI/PCIe plug-in cards in the SIMATIC IPC, a Windows reboot may not be supported. Test the function before using it during live operation.

NOTE

Unsupported cases of Windows restarts

A Windows restart is not supported in the following cases:

- plc_priority is set to value 4 in the Resource Configuration json file.
- You use remote management, for example, iAMT, for your IPC.
- You have configured a different graphics card than the onboard Intel graphics card as the primary graphics card.

Use the instruction "SHUT_DOWN": Shut down target system" to reset a crashed Windows session only in the case of a blue screen.

Restarting system in "Windows-only" mode

The system needs to be restarted in "Windows-only" mode, if, for example, you want to run Windows error handling features. To restart the system in "Windows-only" mode, you have the following options:

Option 1:

1. Set the CPU to STOP mode.
2. Execute the command "CPU_Control /AllowReboot" in the command line editor ("cmd") or by using a batch file.
3. Restart Windows.

   Note: The CPU will also restart.
4. Select the "Windows-only" mode in the boot menu of the CPU shown during system boot.

Option 2:

1. Shut down Windows.
2. Power on the IPC again.
3. Select the "Windows-only" mode in the boot menu of the CPU shown during system boot.

Now you can use the desired Windows functionality.

To start Windows and the CPU again, reboot Windows and select the "Windows and CPU 150xS" mode in the boot menu of the CPU.

8.7.8.1 Restarting the operating system and CPU

To perform a complete restart of the PC with the operating system and CPU, follow these steps:

Shut down the PC using the appropriate command in the Windows Start menu. Restart the PC using the "Power" switch, or remove and insert the connector.

If neither the "Power" switch nor the connector is accessible due to the location of the PC, or if the PC must be restarted via a remote connection, the command line (Page 178) provides the possibility of completely restarting the PC. You must explicitly stop the CPU beforehand.

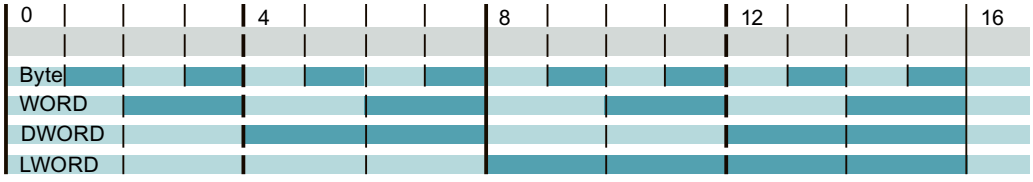
To restart the entire PC, create a small batch file with the following command sequence in the command line:

```
CPU_Control /AllowReboot
CPU_Control /PowerOffCPU
shutdown /r /t 1
```

This command sequence can be created as batch processing in a batch file.

8.7.9 Assignment of addresses with absolute addressing

To ensure optimum runtime when addressing tags, the tags must be located at addresses that match their length. In the figure below, this means either in the light blue or in the dark blue area.



- ≤ 1-byte tags (for example, Bool, BYTE, Char) can be created at any addresses.
- 2-byte tags (for example, WORD) must always be created at even addresses.
- 4-byte tags (for example, DWORD, Int, REAL) must always be created at addresses that can be divided by four.
- 8-byte tags (for example, LInt, ULInt, LWord, LReal, LTime, LDT, LTOD) must always be created at addresses that can be divided by eight.

8.7.10 "Autonegotiation" port setting

Optimizing port settings on the IO device and IO controller

During startup of the IO device, a check of the transmission medium and the duplex option takes place if the CU is wired. These checks take time. You can shorten the time the check requires with specific presets of these options. Make sure that the settings made correspond to the actual conditions (using the correct cables).

To synchronize the settings for the local port and partner port, clear the "Start autonegotiation" check box for the CPU under "Port options" for both ports.

If you have disabled the autonegotiation setting including autocrossing, this saves time that would otherwise be required to negotiate the transmission rate during startup.

Reference

You can find more information on the topic "Cabling rules with disabled autonegotiation" in the STEP 7 online help.

Protection

9

9.1 Overview of the protective functions of the CPU

Introduction

This section describes the functions for protecting the S7-1500 automation system against unauthorized access. The following functions are available:

- Configuring access protection
- Using complex passwords
- Using virus scanners and firewall
- Protection against unauthorized operation (deactivating or restricting remote access)
- Copy protection
- Know-how protection
- Using Windows user rights management
- Using allowlisting tools

Further measures for protecting the CPU

The following measures additionally increase protection against unauthorized access to functions and data of the CPU from outside and via the network:

- Deactivation of the Web server
- Deactivation of the OPC UA server (you can find additional information on the security mechanisms for OPC UA server in the Communication (https://support.automation.siemens.com/WW/view/en/59192925) function manual)
- Deactivation of the time synchronization via an NTP Server
- Deactivation of the time synchronization via Windows clock
- Deactivation of the PUT/GET communication

NOTE

Functions disabled by default

These functions are disabled by default. To use the functions, you must enable them in STEP 7.

Reference

For additional information on the protection functions of the S7-1500 automation system, see the section on protection in the S7-1500 Automation System (https://support.automation.siemens.com/WW/view/en/59191792) system manual.

9.2 General information on protection

Configuration for the Web server

A user with the name "Any" is created by default in the user list of the Web server. This user has minimal access rights such as read-only access to the introduction and home page. Because "Any" does not have a password assigned in STEP 7, pay close attention to the access rights you assign to this user. Individual authorizations, such as the option to change the operating mode, may represent a security risk.

To assign safety-related authorizations, configure a new user and always assign a password in STEP 7. Assign secure passwords to users during configuration. A secure password has the following characteristics:

- Is only used for a single application
- Is at least 10 characters long
- Consists of lower-case and upper-case letters
- Includes special characters and numbers (?!+%$1234...)

Whenever possible, select the option "Permit access only with HTTPS" as soon as you have assigned a password to at least one user.

Data blocks for PUT/GET instructions

The PUT/GET instructions are suitable for connections configured at one end or both ends.

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

Reference

You will find more information on the configuration of the Web server in the Web Server (https://support.industry.siemens.com/cs/ww/en/view/109977246) function manual.

You will find more information on the PUT/GET and NTP instructions in the Communication (https://support.automation.siemens.com/WW/view/en/59192925) function manual.

9.3 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.automation.siemens.com/WW/view/en/59192925) function manual.

9.4 Local user management

As of TIA Portal version V19 and Software Controller firmware version V30.1, S7-1500 Software Controllers, along with S7-1500 hardware CPUs, feature improved management of users, roles, and CPU function rights (User Management & Access Control, UMAC).

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:

Navigate to the "Security Settings > Users and roles" area in the project tree to manage users with their rights, for example, to control access rights.

The 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.

Reference

For detailed information on local user management, refer to the System manual S7-1500 automation system (https://support.automation.siemens.com/WW/view/en/59191792).

9.5 Access protection

9.5.1 Configuring access protection for the CPU in STEP 7

Introduction

The following section describes how to use the various access levels of the CPUs. The description applies to CPUs up to firmware version V30.0.

In later firmware versions, use the Local user management (Page 209) 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 offers four access levels to limit access to specific functions.

By setting up the access levels and the passwords for a CPU, you limit the functions and memory areas that are accessible without entering a password. The individual access levels and 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 10 characters long.
- Use different cases and characters: uppercase/lowercase, numbers, and special characters.

Access levels of the CPU

The following table provides an overview of the access levels of the CPU:

Access levels	Access restrictions
Full access including fail-safe (no protection)	Every user can change fail-safe blocks.
Complete access (no protection)	Every user can read and change the hardware configuration and the blocks. The writing to fail-safe modules is excluded.
Read access	With this access level, read-only access to the hardware configuration and the blocks is possible without entering a password, which means you can upload the hardware configuration and blocks to the programming device. In addition, HMI access and access to diagnostics data, display of offline/online comparison results, changing the operating state (RUN/ STOP), and setting time-of-day are possible. No blocks or hardware configuration can be downloaded into the CPU without first entering the password. It is also not possible to write test functions or perform firmware updates (online) without a password.

Access levels	Access restrictions
HMI access	This access level only allows HMI access and access to the diagnostics data without entering the password. Without entering the password, you can neither load blocks nor the hardware configuration into the CPU, nor load blocks and hardware configuration from the CPU into the programming device. It is also not possible to test functions, change the operating mode (RUN/STOP), perform a firmware update or display online/offline comparison status without a password.
No access (complete protection)	When the CPU has complete protection, no read or write access to the hardware configuration or 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.

Each access level allows unrestricted access to certain functions without entering a password, for example, identification using the "Accessible devices" function.

The default of the CPUs is "No access (complete protection)". In the default access level, the user is not permitted to read or change the hardware configuration or 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, for example, "Full access (no protection)"

Communication between the CPUs (via the communication functions in the blocks) is not restricted by the protection level of the CPU, unless PUT/GET communication is deactivated.

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 prevents unauthorized changes to the CPU by restricting download rights. However, blocks are not write- or read-protected. Use know-how protection to protect the code of blocks.

Assigning access protection parameters in STEP 7

To assign the access levels for the CPU, follow these steps:

1. Select the CPU.
2. Open the properties in the Inspector window.
3. Open the "Protection" entry in the area navigation.

   A table with the possible access levels appears in the Inspector window.

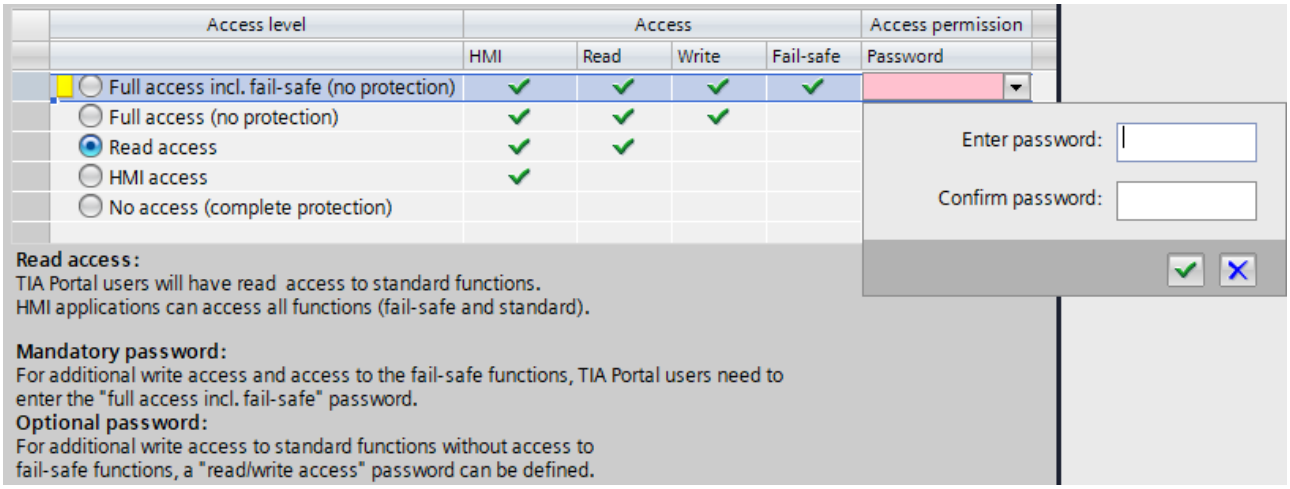


Figure 9-1 Possible access levels

4. Activate the desired protection level in the first column of the table. The green checkmarks in the columns to the right of the respective access level show you which operations are still available without entering the password.
5. In the "Enter password" field, specify a password for the selected access level. In the "Confirm password" field, enter the selected password again to protect against incorrect entries.

   NOTE

   Secure password

   Ensure that the password is sufficiently secure, in other words, that it does not follow a pattern that can be recognized by a machine.

   You must enter a password in the first row ("Full access" access level). This enables unrestricted access to the CPU for those who know the password, regardless of the selected protection level.
6. Assign additional passwords as needed to other access levels if the selected access level allows you to do so.
7. Download the hardware configuration to the CPU for the access level to take effect.

   The configured protection level and the password become effective as soon as the data is downloaded to the CPU. The CPU display indicates the current protection status with an additional icon in the status bar. The operation of the display is restricted depending on the selected protection level. For example, the mode selector or some of the submenus are deactivated.

Access level for F-CPUs

For the fail-safe CPUs, there is the additional access level "Full access incl. fail-safe (no protection)". For additional information on this access level, refer to the description in SIMATIC Industrial Software SIMATIC Safety - Configuring and Programming (https://support.industry.siemens.com/cs/ww/en/view/54110126).

NOTE

Resetting password for access protection for fail-safe CPUs

As of V30.0, there is no more PC Station available. Therefore, it is no longer possible to reset a password for access protection for fail-safe CPUs. However, an import of a .psc file will automatically remove this password.

Behavior of a password-protected CPU during operation

The CPU protection takes effect after the settings are downloaded to the CPU.

Validity is checked before the online function is executed. If the CPU is password-protected, a password prompt appears on the display.

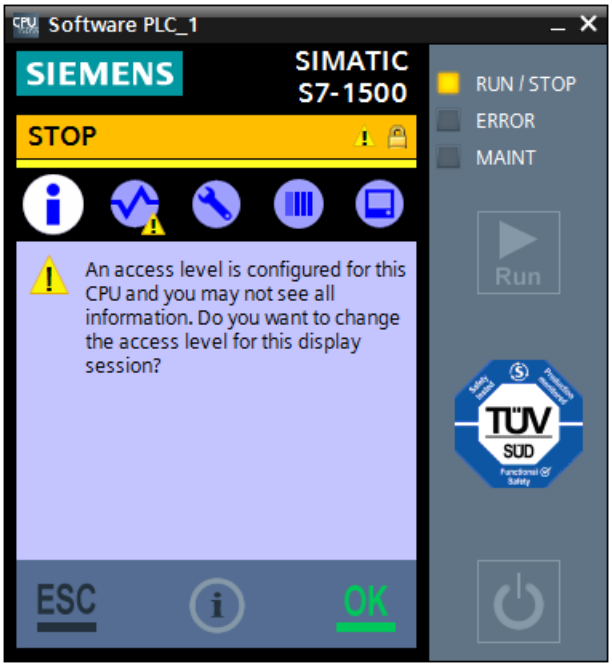


Figure 9-2 CPU display with password setup

Click "OK" to proceed straight to the password input page.

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.

Access authorization to the protected data is in effect for the duration of the online connection or until the access authorization is manually rescinded with "Online > Delete access rights".

Access to a password-protected CPU in RUN mode can be limited locally in the display so that it cannot be accessed even with a password.

9.5.2 Using the display to change the protection level for display access

Unlike the SIMATIC S7-1500 hardware CPU, the CPU cannot be protected from unauthorized access with a separate display password. Because the CPU can also be controlled by remote access, it uses the access protection passwords from STEP 7 to ensure access protection for the display.

Displaying access protection on the display

Once you have assigned the access protection parameters in STEP 7 and have downloaded the program to the CPU, the access protection takes effect.

The lock symbol in the status information of the CPU indicates the current protection level on the display.

The table below shows the meaning of the status information:

Status information	Meaning
	No access protection configured
	The CPU is in the configured protection level, which can be one of the following: • Write protection configured • Read/write protection configured • Complete protection (no access) configured
	The CPU is in one of the following, weaker protection levels because a password has been entered: • Write protection configured • Read/write protection configured • No access protection configured

Effect of access protection on the availability of display functions

The availability of display functions may be limited depending on the access protection of the CPU.

The table below provides an overview of the effects of access protection on the availability of display functions:

	Read-only	Read/write protection	Complete protection
LEDs	always active	always active	always active
"Power" button	always active	always active	always active
CPU status information	always active	always active	always active
Mode selector	active	inactive	inactive
"Overview" menu	always active	always active	always active
"Diagnostics" menu	active	active	Submenus inactive

"Settings" menu	read-only access	Submenus inactive	Submenus inactive
"Modules" menu	active	Submenus inactive	Submenus inactive
"Display" menu	always active	always active	always active
"Settings > Reset" menu	always active	always active	always active

NOTE

Displaying the value of the time zone with HMI access

The current local time and time zone under "Settings > Date & Time > General" are only shown on the display with access levels "Full access" and "Read access".

Changing protection level with the STEP 7 password

The parameterization of the access protection is done in STEP 7. The parameterized protection level can then be changed directly on the CPU display using a valid password.

To change the configured protection level directly in the display, follow these steps:

1. Open the display and select "Protection < Access level".
2. Decide whether you want to combine password and username (local user management) or only use password (legacy access control):

Figure 9-3 Changing password

3. Enter the password or username and password configured in STEP 7.
4. Confirm your entry with "OK".

   The password is checked.

Result

The requested protection level is activated.

The protection level is only valid for the defined time period, and for activities with the CPU display. You will receive an error message if the password is incorrect. The current protection level has not been changed. After confirming the error message, re-enter the password.

If you cancel the "Protection level" dialog with "ESC", the current protection level remains in effect.

NOTE

Using the user program to set additional access protection

In addition to restricting access to the display, you can also restrict access to a password-protected CPU in the user program using block SFC 110. You can find a description of this block in the STEP 7 online help under the keyword "ENDIS_PW: Limit and enable password legitimation".

If ENDIS_PW is executed immediately on IPCs without a "RUN/STOP" switch, disabling passwords as a result, access to STEP 7 can be blocked. To set up a period for entering passwords before passwords are disabled, delay the execution of ENDIS_PW with a time operation.

Reference

You can find additional information about access protection and an overview of the protection functions of the CPU in the S7-1500 Automation System (https://support.automation.siemens.com/WW/view/en/59191792) system manual.

9.5.3 Locking protection levels with the PLC program

Introduction

The instruction "Limit and enable password legitimization" (ENDIS_PW) is used to specify whether or not configured passwords are legitimized for the CPU. In this way, you can prevent legitimized connections, even if the correct password is known.

Inadvertent lockout

If passwords are set up (all protection levels) and the output parameters of the password of the block "Limit and enable password legitimation" are set to "Disallow in RUN", you will be completely locked out.

The output parameters of the block are retentive. This means that the parameter assignment is retained after "POWER OFF – POWER ON".

To disable the protection, delete the load memory via the display under Settings with "Format the CPU volume".

NOTE

Special features of an F-CPU

The function "Format the CPU Volume" is not available with fail-safe systems.

A Software Controller repair or reinstallation is required to reset the load memory or format the CPU volume of a fail-safe Software Controller.

IPCs without "RUN/STOP"

If ENDIS_PW is executed immediately on IPCs without a "RUN/STOP" switch, disabling passwords as a result, access to STEP 7 can be blocked. To set up a period for entering passwords before passwords are disabled, delay the execution of ENDIS_PW with a time operation.

If the period is not long enough, install an input module with a switch and a user program for disabling it.

If you have nevertheless locked yourself out, you will receive access to the CPU again by importing a configuration file without any password protection and "ENDIS_PW" protected blocks. Alternatively, you can format the CPU volume or completely reinstall the Software Controller. This option is available as of firmware V2.5.

For firmware prior to V2.5, you must uninstall the CPU and then reinstall it. A repair installation is not enough to reset the configured access protection using the ENDIS block.

9.6 Protecting blocks

Know-how protection protects the following blocks from unauthorized access:

- Blocks of the OB, FB, FC type
- Global data blocks

Know-how protection protects the code of these blocks from unauthorized reading and modification.

NOTE

Transferring protected block or library

If you transfer a protected block from a hardware controller to a project of a SIMATIC S7-1500 Software Controller or vice versa, the block must be compiled again. To do so, you need the password for the block that is to be compiled.

If you transfer a system library from a hardware controller to a project of a SIMATIC S7-1500 Software Controller, the library must be recompiled.

Possible actions

You can perform the following actions with a know-how-protected block:

- Copying and deleting
- Calling in a program
- Online/offline comparison
- Downloading

Readable data

If a block is know-how protected, only the following data are readable without the correct password:

- In/out parameters Input, Output, InOut, Return, Static, Temp
- Block title
- Block comment
- Block properties
- Global tags without information on the point of use

Reference

For additional information on protected blocks or copying protected blocks and libraries, refer to the STEP 7 online help.

9.7 Virus scanners and firewall

Operation on systems with virus scanner

The CPU and all associated components can be operated on systems with a virus scanner. The virus scanner used should give you the option to protect the runtime system.

The CPU has been tested with the following virus scanners:

- Windows Defender
- Symantec AntiVirus Corporate Edition
- Trend Micro Office Scan Corporate Edition
- McAfee VirusScan Enterprise

Operation on systems with firewall

The CPU and all associated components can be operated on systems with an activated firewall. For the CPU's default settings, the setup program will configure the firewall rules automatically. You must confirm the changes to the firewall rules during the installation.

For Open User Communication and Web server applications, application-specific IP ports can be used. The setup program does not open these IP ports by default, and as a result of these default settings, the firewall can prevent the connection. You must therefore configure the firewall rules for the following applications yourself:

- Open User Communication via Windows interface
- Web server via Windows interface (default: port 81 or port 343)

Configuring the firewall for Web server use

If you use a PC with an enabled firewall, you must configure the firewall for use of the Web server. In order to open the application-specific ports in the Windows firewall, create a new firewall rule for this purpose in the firewall settings.

To configure a new firewall rule, proceed as follows:

1. Select the "Advanced settings" command in the "Control Panel > Windows Firewall" menu.
   The "Windows Firewall with Advanced Security" dialog is opened.
2. Select the "Inbound Rules" entry.
3. Select the "New Rule" command in the "Actions" panel.
   The "New Inbound Rule Wizard" dialog opens.
4. Select the "Port" option.
5. Follow the steps in the dialog.
6. Confirm the configuration by clicking the "Finish" button.

9.8 Setting up copy protection

Application

The CPU has the same copy protection mechanisms as the S7-1500 Advanced Controller. You can link the copy protection to the serial number of the device and the mass storage.

Unlike the S7-1500 Advanced Controllers, the CPU only uses values for the serial number that are derived partly from the serial number of the PC motherboard and the PC mass storage. You can therefore only read the serial numbers at the corresponding locations on the display. Besides the serial number, the function for automatic insertion of the serial number during downloading is available.

Adding the serial number during download to a device

We recommend that you use the "Serial number is inserted when downloading to a device or a memory card" option for setting up copy protection during configuring.

Reading serial number from display

You can read the serial number from the display as follows:

- Serial number of the CPU: "Overview > PLC > Serial number"
- Serial number of the mass storage: "Overview > Load memory > Serial number"

Reference

You can find additional information on setting up the copy protection in the STEP 7 online help.

Interrupts, diagnostics, error and system messages 10

10.1 Status and error display of the CPU

Introduction

The status and error displays of the CPU are described below.

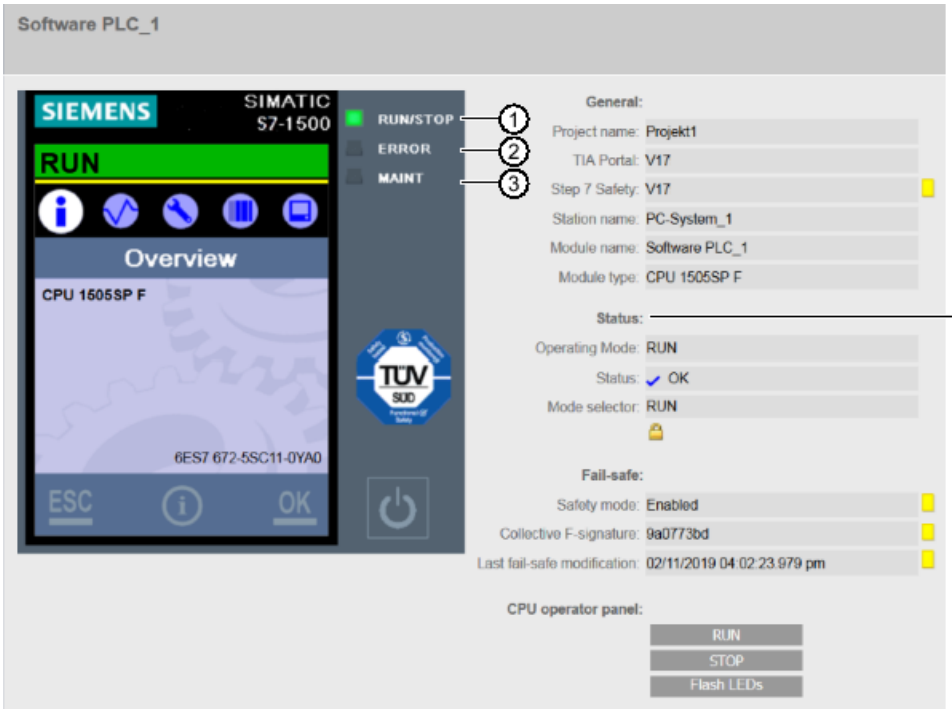
You will find additional information on "Alarms" in the STEP 7 online help.

You will find additional information on "Diagnostics" and "System messages" in the Diagnostics (https://support.automation.siemens.com/WW/view/en/59192926) function manual.

Status display

The status of the CPU is displayed at the following places:

- on the LED display
- in STEP 7
- on the start page of the CPU Web server



① RUN/STOP LED (yellow/green LED)
② ERROR LED (red LED)
③ MAINT LED (yellow LED)
④ Status display in words

Figure 10-1 Example status display of a fail-safe Software Controller (CPU 1505SP F)

NOTE

Example image

Note that the display image only serves as an example. The display differs depending on your used type of Software Controller.

Meaning of the LED displays

The CPU has three LEDs to indicate the current operating mode and diagnostic status. The following table below shows the meaning of the various color combinations of the RUN/STOP, ERROR and MAINT LEDs.

Table 10-1 Meaning of the LEDs

RUN/STOP LED	ERROR LED	MAINT LED	Meaning
LED off	LED off	LED off	POWER OFF, the DIAG LED display is not enabled.
LED off	LED flashes red	LED off	An error has occurred.
LED green	LED off	LED off	CPU is in RUN mode. There are no events, requirements, errors, etc.
LED green	LED flashes red	LED off	A diagnostics event is pending.
LED green	LED off	LED yellow	Maintenance demanded for the plant. The affected hardware must be replaced within a short period of time.
			Active Force job
			For fail-safe CPU: Safety mode is deactivated.
LED green	LED off	LED flashes yellow	Bad configuration
LED yellow	LED flashes red	LED off	A diagnostics event is pending.
LED yellow	LED off	LED flashes yellow	Firmware update successfully completed.
LED yellow	LED off	LED off	CPU is in STOP mode.
LED yellow	LED flashes red	LED flashes yellow	The user program causes an error.
			CPU is in FAULT status.
LED flashes yellow	LED off	LED off	CPU is performing internal activities during STOP, e.g. ramp-up after STOP.
			Loading the user program.
			A programmed breakpoint in the user program has been reached.

RUN/STOP LED	ERROR LED	MAINT LED	Meaning
 LED flashes yellow/green	LED off	LED off	Startup (transition from STOP → RUN).
 LED flashes yellow/green	 LED flashes red	 LED flashes yellow	Startup (CPU booting).
			Test of LEDs during startup, inserting a module.
			LED flashing test.

10.2 Export of diagnostic information

Customer Support offers help in critical cases. For a thorough analysis of your situation, Customer Support needs detailed diagnostic information. You can export these service data with the SIMATIC Diagnostics Tool. The SIMATIC Diagnostics Tool gives you the option to collect diagnostic and system information. The SIMATIC Diagnostics Tool collects the information from a local computer, or from multiple networked computers via remote access.

The SIMATIC Diagnostics Tool is available as a download (https://support.automation.siemens.com/WW/view/en/65976201) on the Internet.

Required service data

The exported service data must include the following information:

- Product-specific data
- Internal error logging as binary code
- Diagnostics buffer entries
- Latest call list
- Memory dump (optional)
- Time stamp of the TIA Portal project

Additional information and download

For the download and additional information on handling the SIMATIC Diagnostics Tool, see the corresponding FAQ (https://support.automation.siemens.com/WW/view/en/65976201).

10.3 Diagnostics

10.3.1 Diagnostic information via the CPU display

10.3.1.1 "Overview" and "Diagnostics" menu

The following section provides an overview of the "Overview" and "Diagnostics" menus of the CPU. Both menus display important information about the properties of the CPU and modules.

NOTE

Example images

Note that the display images only serve as an example. The display differs depending on your used type of Software Controller.

"Overview" menu

The "Overview" menu contains information about the properties of the CPU.

NOTE

Using the DataMatrix code

Install the SIMATIC SUPPORT APP on your smart phone or tablet to use the QR code. The QR code gives you access to specific pages with product information, technical specifications or FAQ information in the Customer Support Portal.

To open the "Overview" menu, follow these steps:

1. Open the CPU display.
2. Start the CPU.
3. Select the "Overview" menu with the icon.
4. Select "PLC".

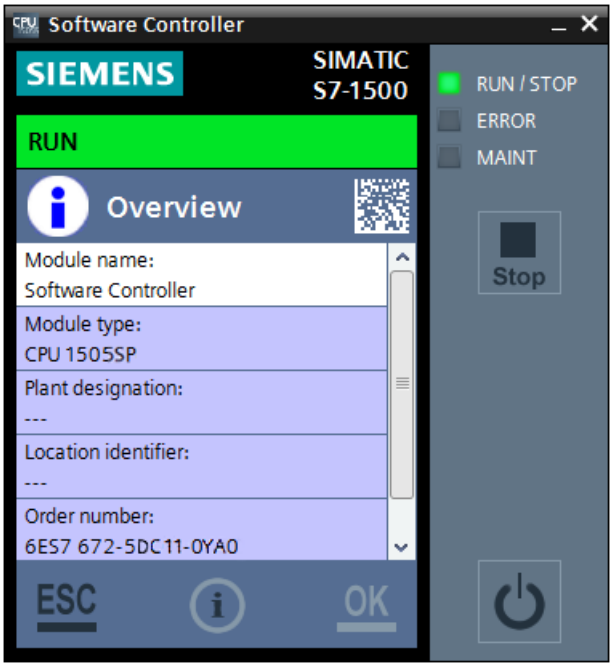


Figure 10-2 "Overview" menu

The "Overview" menu provides an overview of the product-specific data of the CPU:

- Module name: Name from the hardware configuration in STEP 7
- Module type: CPU 1505SP, CPU 1507S or CPU 1508S
- Plant designation (HID): No entry if no configuration has been downloaded. If a configuration has been downloaded, the configured value is displayed.
- Location identifier (LID): No entry if no configuration has been downloaded. If a configuration has been downloaded, the configured value is displayed.
- Article number: Article number of the CPU
- Serial number: Serial number of the mass storage and the PC platform
- Software version: Product version of the CPU

The product-specific data of the CPU in the "Overview" menu is dependent on the downloaded configuration. If a new configuration is downloaded, the values change accordingly.

"Diagnostics" menu

The "Diagnostics" menu contains information about diagnostics alarms, the diagnostics description, and the display of alarms.

To open the "Diagnostics" menu, follow these steps:

1. Open the CPU display.
2. Start the CPU.
3. Select the "Diagnostics" menu with the icon.

Figure 10-3 "Diagnostics" menu

10.3.1.2 Display of alarms

"Alarms" menu in the CPU display

The "Alarms" menu displays the latest error information. Alarms indicate events and states that occur in the system, in the process, or on the operator unit itself. A state is reported when it occurs.

By means of the system diagnostics, you can create blocks that analyze errors in the system and generate alarms with an error description text and an indication of the error location. These alarms are defined per component with alarm capabilities (for example, channel errors or rack errors) and are limited to 255 alarms per component with alarm capability.

Alarms can be displayed on the CPU display, in STEP 7, and via the Web server.

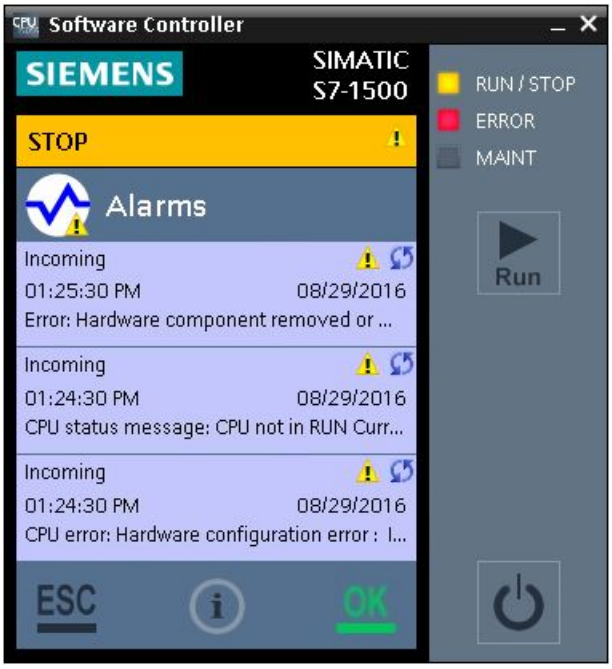


Figure 10-4 "Alarms" menu

Alarm events

The following alarm events can occur for an alarm:

- Incoming
- Outgoing
- Acknowledge

Alarm events are stored in an internal buffer.

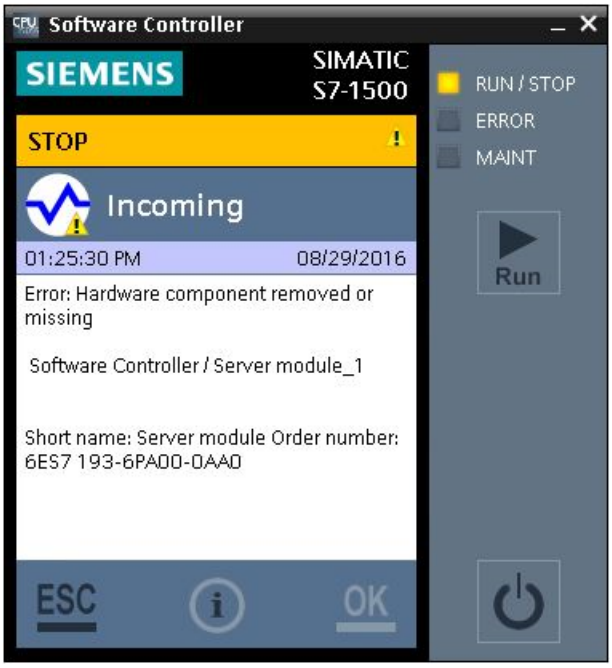


Figure 10-5 Detailed entry

10.3.1.3 Display of the diagnostics buffer entries

"Diagnostics buffer" menu in the CPU display

The diagnostics buffer is used as a log file for the diagnostics events that have occurred on the controller and the modules assigned to it. These are entered in the order of their occurrence, with the latest event shown at the top.

The diagnostics buffer entries can be displayed on the CPU display, in STEP 7, and via the Web server.

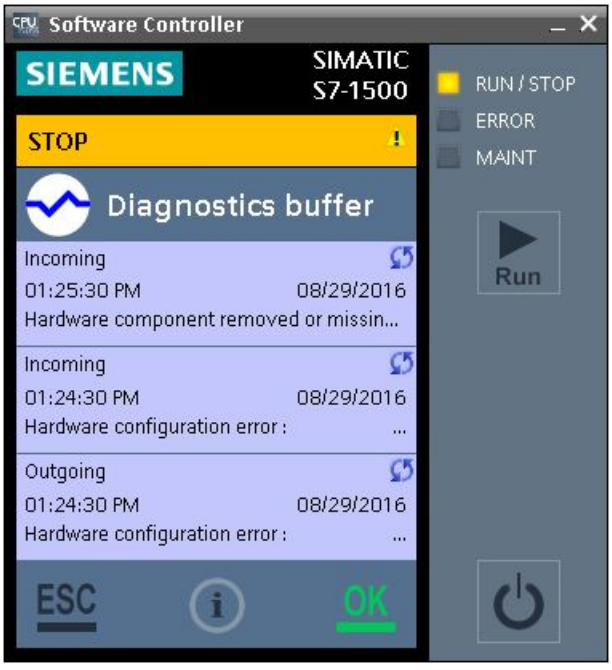


Figure 10-6 "Diagnostics buffer" menu

Diagnostics events

The entries available in the diagnostics buffer include:

- Internal and external errors on a module
- System errors
- Operating mode transitions (for example, from RUN to STOP)
- Errors in the user program
- Removal/insertion of modules

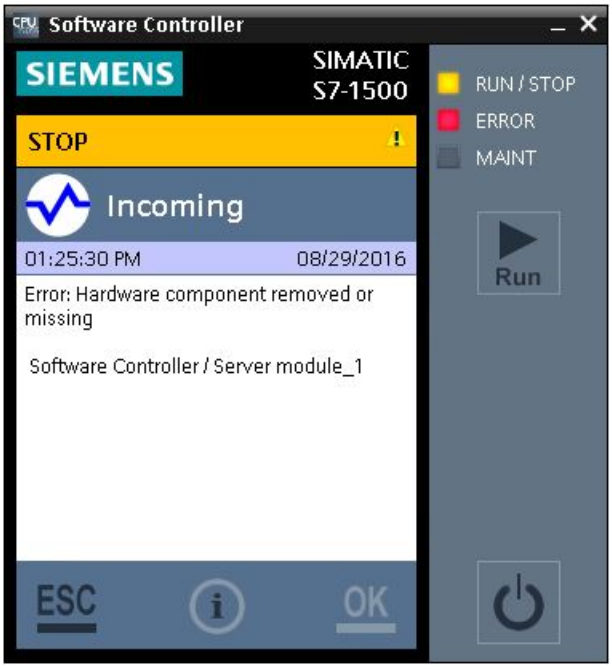


Figure 10-7 Detailed diagnostics buffer entry

The content of the diagnostics buffer is retained in the retentive memory in case of a memory reset of the CPU. The diagnostics buffer makes it possible to evaluate CPU errors or events even after an extended period to determine the cause of a STOP or trace and assign the occurrence of particular diagnostics events.

10.3.2 Diagnostics information using STEP 7

Options for identifying diagnostics information

When the online connection to the CPU is established in STEP 7, the diagnostics status of the CPU and its lower-level components is determined, as well as its operating mode.

You have various options in STEP 7 for identifying diagnostics information:

- Accessible devices
- Devices and networks
- Online & Diagnostics
- "Diagnostics" tab in the Inspector window
- CPU diagnostics buffer
- "Online tools" task card

Reference

You can find further information about diagnostics in the Diagnostics (https://support.automation.siemens.com/WW/view/en/59192926) function manual and in the STEP 7 online help.

10.3.3 Diagnostics information using the Web server

System diagnostics using the CPU Web server

The CPU has an integrated Web server that enables, among other things, the display of system diagnostics information via PROFINET.

You use an Internet browser on any web client, such as a PC, multi panel, or smartphone, to access:

- Module data
- User program data
- Diagnostics data of the CPU

This means access to the CPU is possible without STEP 7 installed.

The Web server offers web pages with reduced complexity which have been optimized for devices with small screens and low computing power.

The following diagnostics options are available with the integrated Web server:

- Start page with general CPU information
- Identification information
- Contents of the diagnostics buffer
- Module information
- Messages (without acknowledgment option)
- Information about communication
- Topology

Reference

You can find additional information about the "Web server" topic in the Web server (https://support.industry.siemens.com/cs/ww/en/view/109977246) function manual.

Technical Data

A

Article number

The CPU 1505SP, 1507S and CPU 1508S are PC-based controllers of the SIMATIC S7-1500 Software Controller family.

Technical specifications

The following table provides you with an overview of the supported CPUs:

CPU	Article number	Technical specifications
CPU 1505SP	6ES7672-5DC12-0YA0	CPU 1505SP (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-5DC12-0YA0/td)
CPU 1505SP F	6ES7672-5SC12-0YA0	CPU 1505SP F (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-5SC12-0YA0/td)
CPU 1505SP T	6ES7672-5VC12-0YA0	CPU 1505SP T (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-5VC12-0YA0/td)
CPU 1505SP TF	6ES7672-5WC12-0YA0	CPU 1505SP TF (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-5WC12-0YA0/td)
CPU 1507S	6ES7672-7AC02-0YA0 (DVD) 6ES7672-7AC02-0YG0 (Download)	CPU 1507S (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-7AC02-0YA0/td)
CPU 1507S F	6ES7672-7FC02-0YA0 (DVD) 6ES7672-7FC02-0YG0 (Download)	CPU 1507S F (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-7FC02-0YA0/td)
CPU 1508S	6ES7672-8AC02-0YA0 (DVD) 6ES7672-8AC02-0YG0 (Download)	CPU 1508S (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-8AC02-0YA0/td)
CPU 1508S F	6ES7672-8FC02-0YA0 (DVD) 6ES7672-8FC02-0YG0 (Download)	CPU 1508S F (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-8FC02-0YA0/td)
CPU 1508S T	6ES7672-8TC02-0YA0 (DVD) 6ES7672-8TC02-0YG0 (Download)	CPU 1508S T (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-8TC02-0YA0/td)
CPU 1508S TF	6ES7672-8UC02-0YA0 (DVD) 6ES7672-8UC02-0YG0 (Download)	CPU 1508S TF (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-8UC02-0YA0/td)

Reference information for use with SIMATIC IPC

B

Power management settings of IPCs

With the default SIMATIC power management profile, the Windows power management functionality is deactivated.

NOTE

Do not change the SIMATIC power management profile on your IPC.

Any further power management settings specific to individual IPCs can be found in the following chapters of the IPC concerned.

BIOS downloads for SIMATIC IPCs

For a list of BIOS downloads for SIMATIC IPCs, SIMATIC Tablet PCs, SIMATIC Field PGs, SINUMERIK PCU and SIMOTION P320 and their latest BIOS version, along with the predecessor versions, see BIOS downloads (https://support.industry.siemens.com/cs/ww/en/view/109763408).

B.1 SIMATIC IPC227G / IPC277G (PRO)

If you are using these IPCs, note the following reference information for your device:

	Property	Notes
Hardware version	IPC227G: FS ≥ AA IPC277G: FS ≥ AA	The hardware version can be found on the name-plate of your SIMATIC IPC.
BIOS version	V28.01.11	
	Mandatory BIOS settings: • Power→CPU Configuration→Intel (VMX) Virtualization Technology = Enabled	
	Recommended BIOS Settings: • Power→Advanced CPU Control→CPU Power Level = Stable Performance • Security→Current TPM device = Hidden (not detected if no TPM available)	
	Hiding TPM module Hiding the TPM module will decrease jitter on Windows restart. For this reason, we recommend hiding the TPM module to avoid timeouts.	
Operating systems	Windows 10 Enterprise LTSC 2019 Windows 10 Enterprise LTSC 2021	
Boot method	UEFI boot with GPT partitioning	
Graphics driver		
LED use	IPC227G: Supported, configurable IPC277G: Not supported	
Mass storage		

	Property	Notes
Using onboard interfaces for PROFINET:		
PN / IE (LAN) X1	Yes (either X1 or X2 at a time)	To be configured in Resource Configuration file use type = "Intel Advanced Ethernet Controller"
PN / IE (LAN) X2	Yes (either X1 or X2 at a time)	
PN / IE (LAN) X3	not supported	

NOTE

Automatic restart after Windows crash

Note that IPC 227G and IPC 277G do not support an automatic restart of Windows after a crash of the operating system.

For this reason, perform the following action before possible crashes of the operating system can occur:

- Configure Windows so that it remains in error state after an operating system crash.

To be able to use the operating system functionalities again, perform a manual restart of the complete system.

Reference to IPC operating instructions

You can find the operating instructions of these IPCs under the following links:

- IPC227G (https://support.industry.siemens.com/cs/ww/en/view/109823984)
- IPC277G (https://support.industry.siemens.com/cs/ww/en/view/109824433)
- IPC277G PRO (https://support.industry.siemens.com/cs/ww/en/view/109972230)

Availability of NVRAM

NOTE

NVRAM module

You can plug NVRAM separately after ordering an IPC.

If you remove or add NVRAM after installation of the Software Controller, then adapt the "nvram_usage" parameter to "false" or "true" in the Resource Configuration file according to your TIA Portal project and apply the new configuration with the following commands before downloading the project to the CPU:

CPU_ResourceConfigurator -s

CPU_ResourceConfigurator -r <resource configuration json file>

Updating BIOS

NOTE
BIOS update
To guarantee correct operation, update the BIOS to the specified version or higher. For detailed information on how to update the BIOS, see SIMATIC IPC – BIOS update (Page 184).

NOTE
BIOS settings lost after BIOS update
The BIOS update will reset the BIOS to its default settings. After you have updated the BIOS, configure the correct BIOS settings again.

B.2 SIMATIC IPC427E / IPC477E (PRO)

If you are using these IPCs, note the following reference information for your device:

	Property	Notes
Hardware version	IPC427E: FS ≥ AA IPC477E: FS ≥ AA	The hardware version can be found on the name-plate of your SIMATIC IPC.
BIOS version	V21.01.18	
	Mandatory BIOS settings: • Power→CPU Configuration→Intel (VMX) Virtualization Technology = Enabled	
	Recommended BIOS settings: • Power→Power and Performance→CPU-Power Management Control→CPU Power Level = Determ-inism Optimized • Security→TPM Availibility = Hidden (not detected if no TPM available)	
	Hiding TPM module Hiding the TPM module will decrease jitter on Windows restart. For this reason, we recommend hid-ing the TPM module to avoid timeouts.	
Operating systems	Windows 10 Enterprise LTSC 2019 Windows 10 Enterprise LTSC 2021	
Boot method	UEFI boot with GPT partitioning	
LED use	IPC427E: Supported, configurable IPC477E (PRO): Not supported	
NVRAM use	Supported, 135 KB can be used for user data	
Mass storage		
Using onboard interfaces for PROFINET:		
PN / IE (LAN) X1	Not supported	
PN / IE (LAN) X2	Yes	To be configured in Resource Configuration file use type="Intel Standard Ethernet Controller"
PN / IE (LAN) X3	Yes	

NOTE

Automatic restart after Windows crash

Note that the IPC 477E does not support an automatic restart of Windows after a crash of the operating system.

For this reason, perform the following action before possible crashes of the operating system can occur:

- Configure Windows so that it remains in error state after an operating system crash.

To be able to use the operating system functionalities again, perform a manual restart of the complete system.

Reference to IPC operating instructions

You can find the operating instructions of these IPCs under the following links:

- IPC427E (https://support.industry.siemens.com/cs/ww/en/view/109742190)
- IPC477E (https://support.industry.siemens.com/cs/ww/en/view/109749206)
- IPC477E PRO (https://support.industry.siemens.com/cs/ww/en/view/109749400)

Updating BIOS

NOTE

BIOS update

To guarantee correct operation, update the BIOS to the specified version or higher. For detailed information on how to update the BIOS, see SIMATIC IPC – BIOS update (Page 184).

NOTE

BIOS settings lost after BIOS update

The BIOS update will reset the BIOS to its default settings. After you have updated the BIOS, configure the correct BIOS settings again.

Windows-only reboot

NOTE

X1 not supported for Windows-only reboot with IPC427E and IPC477E

If you want to use the Windows-only reboot functionality (rebooting Windows while the Software Controller keeps running), the usage of the X1 interface is not supported.

B.3 SIMATIC IPC647E / IPC847E

If you are using these IPCs, note the following reference information for your device:

	Property	Notes
Hardware version		The hardware version can be found on the name-plate of your SIMATIC IPC.
Operating systems	• Microsoft Windows 10 Enterprise LTSC 2019 • Microsoft Windows 10 Enterprise LTSC 2021	
Boot method	UEFI boot with GPT partitioning	
Graphics driver		
LED use	Not supported	
Mass storage		Unsupported configurations: Configurations with additional HW RAID controller
Using onboard interfaces for PROFINET:		
PN / IE (LAN) X1	Not supported	
PN / IE (LAN) X2	Yes	To be configured in Resource Configuration file use type="Intel Standard Ethernet Controller"
PN / IE (LAN) X3	Yes	

NOTE

Blue screen

Configure Windows so that there is no automatic restart in the event of a blue screen. You will find this setting under the Windows Advanced System Settings. Reboot the entire PC system in case of a blue screen.

If Windows is configured to remain in blue screen, disable the TCO Timer in the BIOS settings as mentioned in the recommended BIOS settings:

Advanced→PCH-IO Configuration→Enable TCO Timer→**Disabled**

If you do not disable the TCO Timer in the BIOS settings, then Windows will restart the complete system after a while.

NOTE

System reboot time

In rare cases, rebooting an IPC with more than one mass storage device connected to it may take longer than expected.

BIOS settings

During installation, the following mandatory and recommended BIOS settings will be configured automatically. The BIOS settings serve as a reference for verifying the correct settings or in case a manual configuration of BIOS becomes necessary. The settings listed below are valid for BIOS V25.02.14.

Mandatory BIOS settings

- Advanced → PCH-IO Configuration → SATA and RST Configuration → SATA Mode Selection = AHCI

  The default value of "SATA Mode Selection" is "Intel RST Premium with Intel Optane System Acceleration". However, the Software Controller requires AHCI for installation.

  Note: Do not change the SATA Mode Selection to AHCI directly. To change SATA Mode Selection to AHCI, follow the instructions in section "Changing SATA Mode Selection to AHCI".

- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) Speed Shift Technology = Disabled
- Advanced → CPU Configuration → Intel (VMX) Virtualization Technology = Enabled

Recommended BIOS settings

- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) SpeedStep(tm) = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → C states = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → Turbo Mode = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → HDC Control = Disabled
- Advanced → CPU Configuration → Hyper-Threading = Disabled
- Advanced → PCH-IO Configuration → Enable TCO Timer = Disabled
- Security → TPM Availability = Hidden

Updating BIOS

NOTE

BIOS update

To guarantee correct operation, update the BIOS to the specified version or higher. For detailed information on how to update the BIOS, see SIMATIC IPC – BIOS update (https://support.industry.siemens.com/cs/ww/en/view/109757305).

NOTE

BIOS settings lost after BIOS update

The BIOS update will reset the BIOS to its default settings. After you have updated the BIOS, configure the correct BIOS settings again.

If a blue screen appears after you have reconfigured the BIOS and restarted, proceed as follows:

1. Open the BIOS and change the SATA Mode Selection to "Intel RST Premium with Intel Optane System Acceleration".
2. Restart the PC in "Windows-only" mode to enable the AHCI driver mode.

   To enable the AHCI driver mode, proceed as follows:

   - Run the command line as administrator.
   - Run the command "sc config storahci start= boot".
3. Restart the PC.
4. Open the BIOS again and change the SATA Mode Selection to AHCI.
5. Restart the PC in either "Windows-only" or "Windows and CPU 150xS" mode.

Reference to IPC operating instructions

You can find the operating instructions of these IPCs under the following links:

- IPC647E (https://support.industry.siemens.com/cs/ww/en/view/109825870)
- IPC847E (https://support.industry.siemens.com/cs/ww/en/view/109825871)

Instruction "SHUT_DOWN: Shutdown target system"; MODE = 5

IPC647E and IPC847E do not support the use of the instruction "SHUT_DOWN: Shutdown target system" in MODE = 5 to restart Windows in case of a crash/blue screen.

B.4 SIMATIC IPC627E / IPC677E

If you are using these IPCs, note the following reference information for your device:

	Property	Notes
Hardware version		The hardware version can be found on the name-plate of your SIMATIC IPC.
Operating systems	• Microsoft Windows 10 Enterprise LTSC 2019 • Microsoft Windows 10 Enterprise LTSC 2021	
Boot method	UEFI boot with GPT partitioning	
Graphics driver		
LED use	Supported	
NVRAM use	Supported, 135 KB can be used for user data	
Mass storage		Unsupported configurations: IPCs with additional HW RAID controller
Using onboard interfaces for PROFINET:		
PN / IE (LAN) X1	Not supported	
PN / IE (LAN) X2	Yes	To be configured in Resource Configuration file use type="Intel Standard Ethernet Controller"
PN / IE (LAN) X3	Yes	

NOTE

Valid IPC configurations for CPUs 1508S T/TF

The CPUs 1508S T/TF can be installed on an IPC627E and IPC 677E but only support a subset of available configurations. Information on the available configuration can be found in the ordering information under the following link (https://support.industry.siemens.com/cs/ww/en/view/109827480).

NOTE

Blue screen

Configure Windows so that there is no automatic restart in the event of a blue screen. You will find this setting under the Windows Advanced System Settings. Reboot the entire PC system in case of a blue screen.

If Windows is configured to remain in blue screen, disable the TCO Timer in the BIOS settings as mentioned in the recommended BIOS settings:

Advanced→PCH-IO Configuration→Enable TCO Timer→**Disabled**

If you do not disable the TCO Timer in the BIOS settings, then Windows will restart the complete system after a while.

NOTE

System reboot time

In rare cases, rebooting an IPC with more than one mass storage device connected to it may take longer than expected.

BIOS settings

During installation, the following mandatory and recommended BIOS settings will be configured automatically. The BIOS settings serve as a reference for verifying the correct settings or in case a manual configuration of BIOS becomes necessary. The settings listed below are valid for BIOS V25.02.14.

Mandatory BIOS settings for IPCs with Intel processors

Mandatory BIOS settings for IPCs with Intel i7 8700 processors for Software Controllers 1508S T and 1508S TF:

- Advanced → PCH-IO Configuration → SATA and RST Configuration → SATA Mode Selection = AHCI

  The default value of "SATA Mode Selection" is "Intel RST Premium with Intel Optane System Acceleration". However, the Software Controller requires AHCI for installation.
- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) Speed Shift Technology = Disabled
- Advanced → CPU Configuration → Intel (VMX) Virtualization Technology = Enabled

Recommended BIOS settings with Intel processors

Recommended BIOS settings for IPCs with Intel i7 8700 processors for Software Controllers 1508S T and 1508S TF:

- Advanced → Power and Performance → CPU - Power Management Control → Power & Performance Scenario = Max Performance
- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) SpeedStep(tm) = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → C states = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → Turbo Mode = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → HDC Control = Disabled
- Advanced → Power and Performance → GT - Power Management Control → Maximum GT Frequency = 100MHz

  Note that Maximum GT Frequency is only available from BIOS version V25.02.14 onwards. For this reason, make sure that your BIOS is up to date.

  For more information on optimum real-time behavior, refer to section "Optimizing real-time behavior".
- Advanced → CPU Configuration → Hyper-Threading = Disabled

- Advanced → PCH-IO Configuration → Enable TCO Timer = Disabled
- Security → TPM Availability = Hidden

NOTE

Optimizing real-time behavior

For all CPU 1508 based Software Controllers installed to 627E/677E devices with an Intel i7-8700 processor, you can configure the hypervisor to lower the impact of Window's activities on the Software Controller's real-time behavior by setting "plc_priority" to Level 4.

For more information on "plc_priority" Level 4, refer to section Parameters (Page 93).

Mandatory BIOS settings for IPCs with all other types of processors

Mandatory BIOS settings for IPCs with all other processor types and all Software Controller types:

- Advanced → PCH-IO Configuration → SATA and RST Configuration → SATA Mode Selection = AHCI

  The default value of "SATA Mode Selection" is "Intel RST Premium with Intel Optane System Acceleration". However, the Software Controller requires AHCI for installation.
- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) Speed Shift Technology = Disabled
- Advanced → CPU Configuration → Intel (VMX) Virtualization Technology = Enabled

Recommended BIOS settings for IPCs with all other types of processors

Recommended BIOS settings for IPCs with all other processor types and all Software Controller types:

- Advanced → Power and Performance → CPU - Power Management Control → Power & Performance Scenario = Max Performance
- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) SpeedStep(tm) = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → C states = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → Turbo Mode = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → HDC Control = Disabled
- Advanced → CPU Configuration → Hyper-Threading = Disabled
- Advanced → PCH-IO Configuration → Enable TCO Timer = Disabled
- Security → TPM Availability = Hidden

Updating BIOS

NOTE

BIOS version

To guarantee correct operation, update the BIOS to the specified version or higher. For detailed information on how to update the BIOS, see SIMATIC IPC – BIOS update (https://support.industry.siemens.com/cs/ww/en/view/109757305).

NOTE

BIOS settings lost after BIOS update

The BIOS update will reset the BIOS to its default settings. After having updated the BIOS, configure the correct BIOS settings again.

If a blue screen appears after you have reconfigured the BIOS and restarted, proceed as follows:

1. Open the BIOS and change the SATA Mode Selection to Intel RST Premium with Intel Optane System Acceleration.
2. Restart the PC in "Windows-only" mode to enable the AHCI driver mode.

   To enable the AHCI driver mode, proceed as follows:

   - Run the command line as administrator.
   - Run the command "sc config storahci start= boot".
3. Restart the PC.
4. Open the BIOS again and change the SATA Mode Selection to AHCI.
5. Restart the PC in either "Windows-only" or "Windows and CPU 150xS" mode.

Reference to IPC operating instructions

You can find the operating instructions of these IPCs under the following links:

- IPC627E (https://support.industry.siemens.com/cs/ww/en/view/109825869)
- IPC677E (https://support.industry.siemens.com/cs/ww/en/view/109824273)

Instruction "SHUT_DOWN: Shutdown target system"; MODE = 5

IPC627E/IPC677E do not support the use of the instruction "SHUT_DOWN: Shutdown target system" in MODE = 5 to restart Windows in case of a crash/blue screen.

B.5 SIMATIC BX-39A / PX-39A (PRO)

If you are using these IPCs, note the following reference information for your device:

	Property	Notes
Hardware version	BX-39A: FS ≥ AA PX-39A: FS ≥ AA	The hardware version can be found on the rating plate of your SIMATIC IPC.
Operating systems	Windows 10 IoT Enterprise Version 21H2	
Boot method	UEFI boot with GPT partitioning	
LED use	Supported, configurable	
NVRAM use	Supported, 135 KB can be used for user data	
Mass storage	Supported	Operating system and Software Controller must be installed on same NVMe device (Drive1 or Drive2).
Using onboard interfaces for PROFINET:		
PN / IE (LAN) X1	Not supported	
PN / IE (LAN) X2	Supported	
PN / IE (LAN) X3	Supported	
PN / IE (LAN) X4	Supported	

NOTE

Automatic restart after Windows crash

Note that the PX-39A does not support an automatic restart of Windows after a crash of the operating system.

For this reason, perform the following action before possible crashes of the operating system can occur:

- Configure Windows so that it remains in error state after an operating system crash.

To be able to use the operating system functionalities again, perform a manual restart of the complete system.

BIOS settings

During installation, the following mandatory and recommended BIOS settings will be configured automatically. The BIOS settings serve as a reference for verifying the correct settings or in case a manual configuration of BIOS becomes necessary. The settings listed below are valid for BIOS V29.01.07.

NOTE

BIOS version

To guarantee correct operation, update the BIOS to the specified version or higher. For detailed information on how to update the BIOS, see SIMATIC IPC – BIOS update (Page 184).

Mandatory BIOS settings for IPCs with Xeon 11555, Xeon 11155, Xeon 11865 processors:

- Advanced → System Agent (SA) Configuration → VMD Configuration → Enable VMD Controller = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → Power & Performance Scenario = Stable Performance
- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) SpeedStep(tm) = Enabled
- Advanced → Power and Performance → CPU - Power Management Control → Intel(R) Speed Shift Technology = Enabled
- Advanced → Power and Performance → CPU - Power Management Control → Turbo Mode = Enabled
- Advanced → System Agent (SA) Configuration → Above 4GB MMIO BIOS assignment = Disabled
- Advanced → CPU Configuration → Intel (VMX) Virtualization Technology = Enabled
- Advanced → CPU Configuration → CPU Flex Ratio Override = Enabled
- Security → TPM Availability = Hidden

Recommended BIOS settings for IPCs with Xeon 11555, Xeon 11155, Xeon 11865 processors:

- Advanced → Power and Performance → CPU - Power Management Control → C states = Disabled
- Advanced → Power and Performance → CPU - Power Management Control → HDC Control = Disabled
- Advanced → CPU Configuration → Hyperthreading = Disabled
- Power → USB Ports Wake up during S5 = Disabled

  If this setting is enabled, then rebooting Windows while the Software Controller is running is not supported.

NOTE

Support of Intel Celeron processors

Note that IPCs of both BX-39A and PX-39A with Intel Celeron 6600HLE processors are not supported.

Reference to IPC operating instructions

You can find the operating instructions of these IPCs under the following links:

- BX-39A (https://support.industry.siemens.com/cs/ww/en/view/109813517)
- PX-39A (https://support.industry.siemens.com/cs/ww/en/view/109814324)
- PX-39A PRO (https://support.industry.siemens.com/cs/ww/en/view/109815541)

Availability of NVRAM

NOTE

NVRAM module

You can plug NVRAM separately after ordering an IPC.

If you remove or add NVRAM after installation of the Software Controller, then adapt the "nvram_usage" parameter to "false" or "true" in the Resource Configuration file according to your TIA Portal project and apply the new configuration with the following commands before downloading the project to the CPU:

CPU_ResourceConfigurator -s

CPU_ResourceConfigurator -r <resource configuration json file>

Index