

SIEMENS

SIMATIC

S7-1500 Software Controller CPU 1505SP (F), CPU 1507S (F) and CPU 1508S (F) SIMATIC Industrial OS Version 30.1




Operating Instructions

Documentation guide	1
Security information	2
Industrial cybersecurity	3
Product overview	4
Installing	5
Commissioning	6
Operation	7
Maintenance	8
Protection	9
Interrupts, diagnostics, error, and system messages	10
Technical Data	A
Reference information for use with SIMATIC IPC	B
Additional information	C

Legal information

Warning notice system

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

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


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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Table of contents

1	Documentation guide	7
1.1	S7-1500/ET 200MP Documentation Guide	9
1.1.1	S7-1500 / ET 200MP Documentation Guide	9
1.1.2	SIMATIC Technical Documentation	10
1.1.3	Tool support	12
2	Security information	14
2.1	Security settings for IPCs	14
2.2	Notes on data protection	14
2.3	Change of the operating mode with critical actions	14
2.4	Information about third-party software updates	14
2.5	Notes on protecting root rights	15
2.6	Additional security information	15
3	Industrial cybersecurity	16
3.1	Cybersecurity information	16
3.2	Security update notification	17
3.3	Basic information on industrial cybersecurity	17
3.3.1	Definition of industrial cybersecurity	17
3.3.2	Objectives of industrial cybersecurity	17
3.4	Holistic security concept and security strategies	18
3.4.1	Holistic "Defense in Depth" security concept	18
3.4.2	Security management	18
3.5	Operational application environment and security assumptions	20
3.5.1	Intended use	20
3.5.2	Requirements for the operational application environment and security assumptions	21
3.6	Security properties of the devices	22
3.7	Secure operation of the system	22
3.7.1	Hardening measures	22
3.7.2	Secure configuration	22
3.7.3	Access control	23
3.7.4	Handling of sensitive data	23
3.7.5	Regular firmware updates	23
3.7.6	Notifications about security gaps	23
3.7.7	Data backup	24
3.7.8	Security checks	24
3.7.9	Secure decommissioning	24
3.7.9.1	Securely removing data	25
3.7.9.2	Recycling and disposal	26
3.8	Secure operation of the engineering software	26

3.9	Secure operation of the CPUs.....	26
3.9.1	Secure configuration.....	26
3.9.2	User management and access control.....	26
3.9.2.1	Administration of user accounts.....	26
3.9.2.2	Assigning secure passwords.....	27
3.9.2.3	Password management.....	27
3.9.2.4	Setting protection levels.....	28
3.9.2.5	Certificate management.....	28
3.9.3	Protection functions.....	28
3.9.4	Web server.....	28
3.9.5	Secure communication/OPC UA.....	28
3.9.6	Sensitive data.....	29
3.9.7	Backups.....	29
3.9.8	Additional measures for network security.....	29
3.9.9	Remote access to CPU.....	30
3.9.9.1	Using a Web server.....	30
3.9.10	Recording security events.....	30
3.9.11	Syslog messages.....	31
3.9.11.1	Transfer the syslog messages to a syslog server.....	33
3.9.11.2	Structure of the Syslog messages.....	36
4	Product overview.....	39
4.1	Introduction to PC-based control.....	39
4.2	Overview of functions.....	40
4.3	Functions.....	44
4.3.1	Memory concept of the CPU.....	44
4.3.1.1	CPU memory areas.....	44
4.3.1.2	Storage of retentive data.....	46
4.3.2	Interface types.....	48
4.3.3	PROFINET IO.....	49
4.3.4	PROFenergy.....	49
4.3.5	Web server of the CPU.....	50
4.3.5.1	Overview.....	50
4.3.6	Fail-safe.....	51
5	Installing.....	52
5.1	System requirements.....	52
5.2	Installing the Software Controller.....	52
5.3	Updating/upgrading the Software Controller.....	58
5.4	Uninstalling the Software Controller.....	59
6	Commissioning.....	61
6.1	First commissioning.....	61
6.2	Resource Configurator.....	62
6.2.1	Example of a Resource Configuration file.....	64
6.2.2	Error handling.....	76

6.3	Exporting and importing configuration files.....	79
6.3.1	Command prompt.....	79
6.3.2	Exporting configuration files.....	80
6.3.3	Importing configuration file.....	82
6.3.4	Printing configuration information.....	86
6.3.5	Error handling.....	86
6.4	Shutdown and startup.....	87
6.4.1	Behavior of Software Controller when shutting down IndOS.....	89
6.5	Communication.....	92
6.5.1	Communication with CPU using bridging.....	92
6.5.2	Communication with CPU using IP routing.....	94
7	Operation.....	96
7.1	Operation using command line commands.....	96
7.2	Operating modes.....	98
7.2.1	Basic principles.....	98
7.2.2	Operating mode transitions.....	99
8	Maintenance.....	100
8.1	BIOS update.....	100
8.2	Firmware updates of I/O modules.....	101
8.3	Resetting the CPU.....	103
8.3.1	Reset using STEP 7.....	103
8.4	Special features.....	104
8.4.1	Special situations when downloading in STEP 7.....	104
8.4.2	Timeouts.....	104
8.4.3	Assignment of addresses with absolute addressing.....	104
8.4.4	"Autonegotiation" port setting.....	105
8.5	Backup and restore.....	105
8.5.1	SIMATIC IPC Image & Partition Creator.....	105
9	Protection.....	110
9.1	Overview of the protective functions of the CPU.....	110
9.2	General information on protection.....	111
9.3	Protection of confidential configuration data.....	111
9.4	Local user management.....	112
9.5	Access protection.....	112
9.5.1	Configuring access protection for the CPU in STEP 7.....	112
9.5.2	Locking protection levels with the PLC program.....	116
9.6	Protecting blocks.....	117
9.7	Virus scanners and firewall.....	118
9.8	Setting up copy protection.....	118

10	Interrupts, diagnostics, error, and system messages.....	119
10.1	Status and error display of the CPU.....	119
10.2	Export of diagnostic information.....	122
10.3	Diagnostics.....	122
10.3.1	Diagnostics information using STEP 7.....	122
10.3.2	Diagnostics information using the Web server.....	123
A	Technical Data.....	124
B	Reference information for use with SIMATIC IPC.....	125
B.1	Permitted commands and parameters.....	125
B.2	SIMATIC IPC227G / IPC277G (PRO).....	128
B.3	SIMATIC IPC427E / IPC477E (PRO).....	129
B.4	SIMATIC BX-39A / PX-39A (PRO).....	130
C	Additional information.....	132
C.1	Siemens Industry Online Support.....	132
C.2	Industry Mall.....	132
	Index.....	133

Documentation guide

Purpose of the documentation

These operating instructions supplement the system manual of the S7-1500 automation system as well as the function manuals. Cross-system functions are described in the system manual.

The information provided in these operating instructions and the system manual enables you to commission the Software Controller.

Basic knowledge required

The following knowledge is required to understand the documentation:

- General knowledge of automation technology
- Knowledge of the SIMATIC industrial automation system
- Knowledge of working with STEP 7
- Knowledge of working with Linux

Validity of the documentation

This documentation is valid for the products.

Software Controller	Article number
CPU 1505SP CPU 1505SP F	cannot be ordered, since only available preinstalled on a CPU 1515SP PC2 (F)
CPU 1507S CPU 1507S F	6ES7672-7AD02-0YG0 6ES7672-7FD02-0YG0
CPU 1508S CPU 1508S F	6ES7672-8AD02-0YG0 6ES7672-8FD02-0YG0

Notes

Also observe notes marked as follows:

NOTE

A note contains important information on:

- The product described in the documentation
 - The handling of the product
 - The part of the documentation to which you should pay particular attention
-

Definitions and naming conventions

The following terms are used in this documentation:

- **CPU or Software Controller:** These terms refer to the CPU1505SP (F), CPU 1507S (F) and the CPU 1508S (F).
- **STEP 7:** We refer to the configuration and programming software as "STEP 7" in this documentation as a synonym for the version "STEP 7 V19 (TIA Portal)".
- **PC:** This term designates a SIMATIC IPC and includes the following Open Controllers.
 - CPU 1515SP PC2
 - CPU 1515SP PC2 F

ID link for the digital nameplate



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

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

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

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

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

1.1 S7-1500/ET 200MP 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 200MP systems.

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>)

SIMATIC S7-1500 comparison list for programming languages

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

You can find the comparison list on the Internet

(<https://support.industry.siemens.com/cs/ww/en/view/86630375>).

1.1.2 SIMATIC Technical Documentation

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

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

Overview of the SIMATIC Technical Documentation

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



Industry Online Support International

(<https://support.industry.siemens.com/cs/ww/en/view/109742705>)

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



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



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

Retention of the documentation

Retain the documentation for later use.

For documentation provided in digital form:

1. Download the associated documentation after receiving your product and before initial installation/commissioning. Use the following download options:
 - Industry Online Support International: (<https://support.industry.siemens.com>)
The article number is used to assign the documentation to the product. The article number is specified on the product and on the packaging label. Products with new, non-compatible functions are provided with a new article number and documentation.
 - ID link:
Your product may have an ID link. The ID link is a QR code with a frame and a black frame corner at the bottom right. The ID link takes you to the digital nameplate of your product. Scan the QR code on the product or on the packaging label with a smartphone camera, barcode scanner, or reader app. Call up the ID link.
2. Retain this version of the documentation.

Updating the documentation

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

1. Download the current version as described above via the Industry Online Support or the ID link.
2. Also retain this version of the documentation.

mySupport

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

Registration	You must register once to use the full functionality of "mySupport". After registration, you can create filters, favorites and tabs in your personal workspace.
Support requests	Your data is already filled out in support requests, and you can get an overview of your current requests at any time.
Documentation	In the Documentation area you can build your personal library.
Favorites	You can use the "Add to mySupport favorites" to flag especially interesting or frequently needed content. Under "Favorites", you will find a list of your flagged entries.
Recently viewed articles	The most recently viewed pages in mySupport are available under "Recently viewed articles".
CAX data	The CAX data area gives you access to the latest product data for your CAX or CAE system. You configure your own download package with a few clicks: <ul style="list-style-type: none"> • Product images, 2D dimension drawings, 3D models, internal circuit diagrams, EPLAN macro files • Manuals, characteristics, operating manuals, certificates • Product master data

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

Application examples

The application examples support you with various tools and examples for solving your automation tasks. Solutions are shown in interplay with multiple components in the system - separated from the focus on individual products.

You can find the application examples on the Internet.

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

1.1.3 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>).

See also

PRONETA Professional (<https://support.industry.siemens.com/cs/ww/en/view/109781283>)

Security information

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 125](#)).

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 root rights

A user with root rights has extensive access and manipulation possibilities on the system. A root user has, for example, the right to change the operating state of the CPU, even if the root user is not a member of the "software_controller_operators" group.

Therefore, make sure that the root rights are 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 Additional security information

SIMATIC Industrial OS (IndOS) is a Linux-based (Debian) operating system. The following security information additionally applies to users of SIMATIC Industrial OS.

Access to the PC

A user has extensive access and manipulation possibilities on the system.

Therefore, make sure that the PC is adequately protected in physical terms to prevent unauthorized changes.

Rights for operating the Software Controller

Do not change the access rights for files provided by Siemens, such as the Linux tools for the Software Controller. The Linux tools are executable with standard user rights in the "software_controller_operators" group.

Linux security issues

The security issues of the Linux operating system are the responsibility of the user.

SIMATIC IPC - Security Guidelines for Linux systems

In the following configuration example, recommendations are given for necessary settings in order to minimize risks for IPCs in industrial environments:

Configuration example (<https://support.industry.siemens.com/cs/ww/en/view/109768383>)

Industrial cybersecurity

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. In the following sections, measures for the entire system and individual components are recommended to protect against 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 holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept.

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

For more information on protective industrial cybersecurity measures for implementation, please 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 at all times, 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 "Search in knowledge base" option.
4. Select the "Other types" option from the filter menu for "Type," and then choose "Download" and "Product note".
5. Select the document from which you want to create notifications.
6. For information on setting up an email notification, refer to the video "Individual notifications and filters" (https://cache.industry.siemens.com/dl/dl-media/691/90000691/att_1036866/v1/How-to_Videos-SIOS_EN/story_html5.html?lang=en).

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:

- Trouble-free operation and ensuring the availability of industrial plants and production processes
- Preventing threats to people and production through cybersecurity attacks
- Protection of industrial communication against espionage and manipulation
- Protection of industrial automation systems and components against unauthorized access and data loss
- Practical and cost-effective concept for securing existing plants and devices without their own security functions
- Use of existing, open, and proven industrial security 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 Holistic security concept and security strategies

3.4.1 Holistic "Defense in Depth" security concept

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

Productivity and know-how are protected on 3 levels:

Plant security

Plant security uses various methods to ensure a secure physical access of people to critical components. This begins 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.

More information

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 for basic security measures to protect machine and plant operation in an industrial environment.

3.4.2 Security management

The ISO 27001 and IEC 62443 standards call for a "holistic" approach in IT and 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 employees with all the necessary resources and training to fully support these objectives

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 RSS feed (<https://www.siemens.com/global/en/products/services/cert.html>) for vulnerabilities. Register with mySiePortal (<https://sieportal.siemens.com/en-ww/home>) and create filters to be notified when important information is published. 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 communicates the provision of security updates, the total discontinuation of a product and cancellation of product support.

Employee awareness

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

- Secure handling of USB devices
- Encrypted communication
- Use of VPN
- Rules for passwords and use of access
- Setting up two-factor authentication
- Education on dangers caused by malware, phishing, social engineering, and others

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 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.

It is recommended to:

- 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

In short: 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. Mitigation measures should be selected on the basis of a cost/benefit analysis and classification of the 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

Continuous monitoring of the cybersecurity situation through:

- Setting anomaly references and creating allow and deny lists based on normal network communication and production machine behavior
- Establishment of an intrusion detection system (IDS) that generates alarms when unusual behavior occurs in the network
- Introduction of a Security Incident 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:

- Conducting a threat and risk assessment (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

Information about network security can be found in the whitepaper "Industrial Network Security Architecture", available in 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

Physical corporate security can be ensured through the following measures:

- 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

Physical production security can be ensured through the following measures, among others:

- 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.

3.7 Secure operation of the system

- 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, 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:

- A "secure configuration" where only necessary software components and services are installed or activated for proper operation.
- "Access control", where 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.

- One possible risk is unauthorized access to the network.
- Another risk is unauthorized access to programs.

To minimize risks, only the necessary services should be activated for all automation components.

- Consider all activated services (especially Web servers, FTP, remote maintenance etc.) 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 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 TIA Portal).
- Refer to the information about password management in the section Protection (Page 110) and in the STEP 7 online help (TIA Portal).

3.7.4 Handling of sensitive data

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

Also see the section Sensitive data (Page 29).

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.

There are two ways of being automatically informed about firmware updates:

- Use "Enable notification" and "Add to mySupport favorites" functions, see section Security update notification (Page 17).
- Consult the firmware collection on SIOS. To do this, register in the download section on mySiePortal (<https://sieportal.siemens.com/en-ww/home>).

Also, observe the basic security information in the section Cybersecurity information (Page 16).

3.7.6 Notifications about security gaps

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.

Siemens ProductCERT

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

You can find the documents for SIMATIC on the following Siemens AG Web page: Siemens ProductCERT and Siemens CERT

(<https://www.siemens.com/global/en/products/services/cert.html>)

Enter "SIMATIC" in the search box "Search Security Advisories".

On this page, you will also find all necessary information about handling vulnerabilities.

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities

3.7 Secure operation of the system

- 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) standard
 - Measures
 - Availability
 - Etc.
 - Report possible vulnerabilities yourself at (<https://www.siemens.com/global/en/products/services/cert.html>)
- Set up an RSS feed to receive notifications about security-related topics.

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 must 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 the CPU volume and reset the CPU to factory settings.

For information on how to format the CPU volume, refer to section "Formatting the CPU volume".

For information on how to reset the CPU to factory settings, refer to section "Resetting the CPU".

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 the 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 the is 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 112) 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 passwords, do not use passwords (or part of passwords) that you have already used before.
- 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.
- Use passwords that are longer than the required minimum length and use a combination of upper and lower case and special characters.

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

Components and functions with password protection

The following table gives you an overview of all 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/59193560)
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.
- For user management and access control, use the Local user management (Page 112).
- Using a password provider: In STEP 7, you can set up a password provider.
- Alternatively, commercially available password management programs can be used.

3.9 Secure operation of the CPUs

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 110) and the STEP 7 online help (TIA Portal).

3.9.2.5 Certificate management

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 110).

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:

- Access via the secure transmission protocol "HTTPS" using the CA-signed Web server certificate
- User authorization you can configure by means of user list
- Activation for specific interfaces

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) function manual, 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 110)
Data deemed sensitive by the operator	Backups, other configuration data, analysis data	Section Exporting and importing configuration files (Page 79)

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 110).
- 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 section "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 memory

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.

These security events 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 (by instruction or 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 \geq 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 31](#)).

Connection to a SIEM system

A SIEM system (Security Information and Event Management) is used for real-time analysis of security event logs. It can, for example, be installed 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 recording of safety-related 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.

In addition to syslog, messages regarding installation, upgrades, uninstallation, changes in CPU state and resource configuration etc. are also logged in the IndOS logging journal "journalctl".

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

In order to be able to accept the incoming syslog messages, a SIEM-system must understand the syslog protocol according to RFC 5424. Otherwise, the SIEM system cannot accept or process the incoming messages.

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.

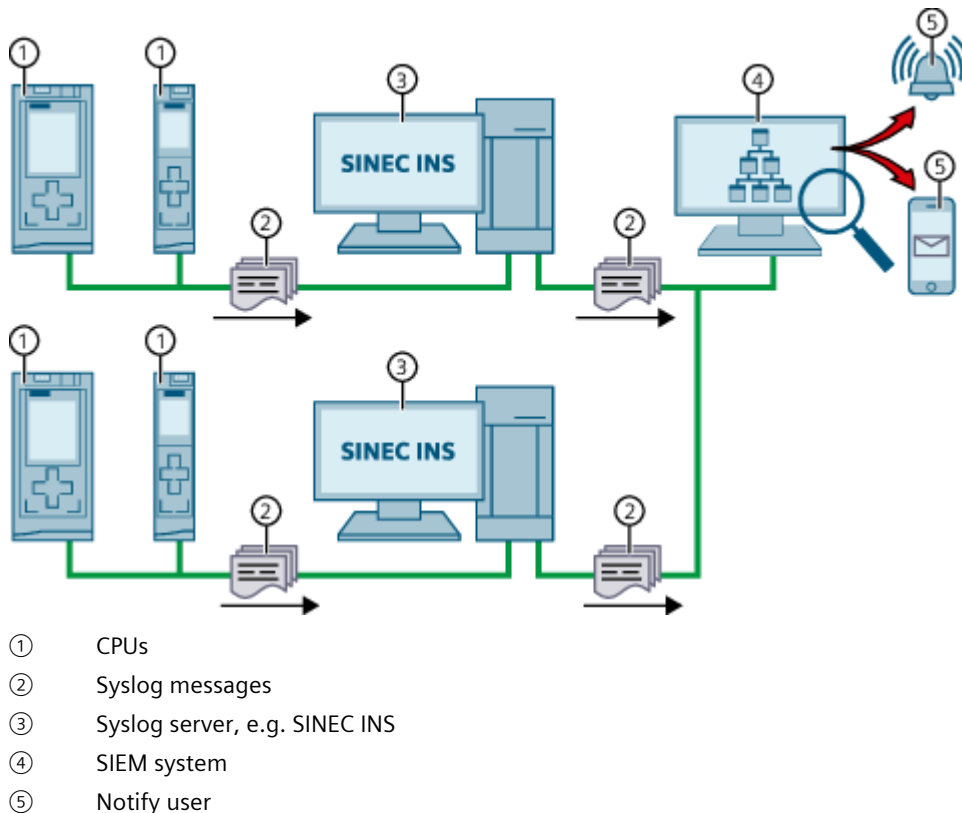


Figure 3-1 Forwarding and processing of syslog messages

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 36).

3.9.11.1 Transfer the syslog messages to a syslog server

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 "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 one of the following port numbers depending on the transport protocol used:
 - Standard TCP port for TLS: 6514
 - Standard UDP port: 514

Result: You have configured the transfer of syslog messages to a syslog server.

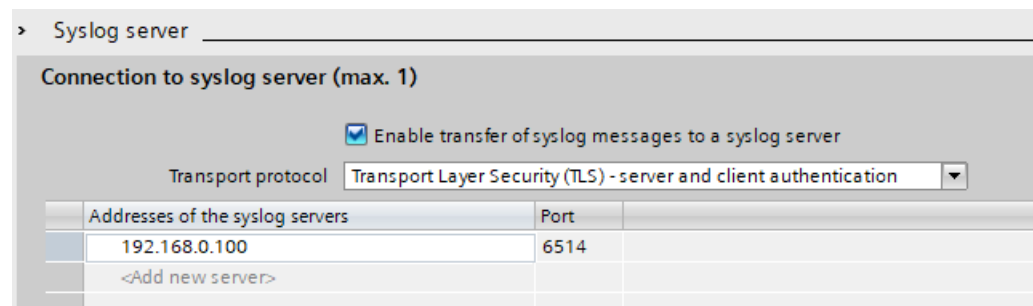
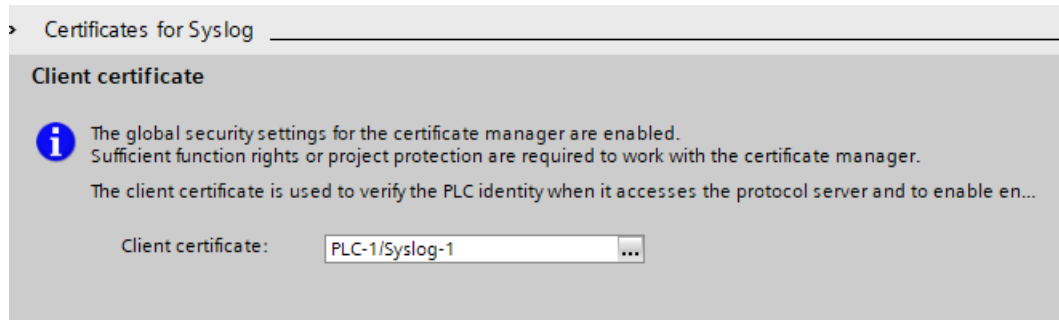


Figure 3-2 Transfer of syslog messages to a syslog server configured

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. In the "Client certificate" field, select the desired certificate.



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 "Protection & Security > Syslog" > "Certificates for Syslog".
3. In the "Trusted servers" area, specify whether the connected syslog server should 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 3-4 Example: HEADER of the syslog message of a CPU

The following table describes the parameters in the prescribed order.

Parameter	Description
PRI	<p>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: $PRI = Facility \times 8 + Severity$ 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.</p>
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:

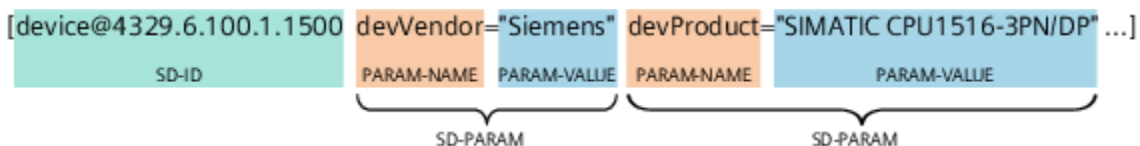


Figure 3-5 Example: SD ELEMENT of the syslog message of a CPU

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

4.1 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 and 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 in order 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.

You use the same programming languages, program structure, and programming interface (STEP 7) 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.

NOTE

Available operating systems

The present manual describes Software Controllers using the Industrial OS operating system. The latest manual for Software Controllers using Windows is available on the Internet (<https://support.industry.siemens.com/cs/ww/en/view/109817941>).

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 Resource Configurator and STEP 7

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, IndOS.

- 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 and Open Controller with this option) possible in case of a power failure

Communication

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

- IndOS-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
 - PROFlenergy
 - Media redundancy
 - I-Device
 - Isochronous mode
 - MRP/MRPD
- Communication (SIMATIC Communication, Open User Communication, OPC UA) with IndOS 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 and 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, backing up and restoring the CPU configuration, 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, and external encoders.
- 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 tracks
- Measuring inputs

Advanced synchronization functions:

- Synchronization with specification of the synchronous position
- Actual value coupling
- Shifting of the master value at following axis
- Camming

Other functions:

- Cyclic specification of motion vector from the application (MotionIn interface)
- Technology object for control of kinematics with up to 4 interpolating axes, for example, Cartesian gantry, 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 is generated automatically and displayed by:

- Programming device
- PC
- HMI
- Web server

System diagnostics is 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
Allows you to securely protect algorithms 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. To assign separate rights to different user groups, you use authorization levels.
- Integrity protection
The system protects the data transferred to the CPU from unauthorized manipulation. The CPU reliably detects altered or external transmission of engineering data.
- 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 Memory concept of the CPU

4.3.1.1 CPU memory areas

Introduction

This section describes the structure of the CPU memory.

Memory areas

The CPU uses the mass storage of the PC on which it is installed. The following figure shows the partitions (sda) on the PC:

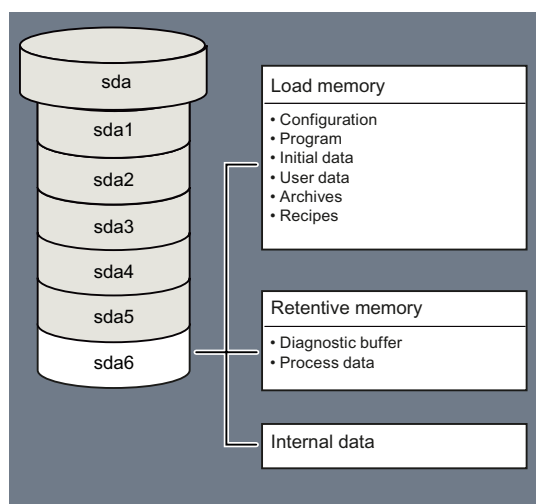


Figure 4-1 Partitions on the PC

NOTE

Disk naming

Note that for the IPC227G, IPC277G, BX-39A and PX-39A the disk name is "nvme0n1". The naming for the individual partitions is nvme0n1p1 to nvme0n1p6.

For more information on the different partitions, see chapter Installing the Software Controller ([Page 52](#)).

Work memory

The RAM of the PC is used for the work memory. When the CPU starts, the SIMATIC hypervisor exclusively allocates a portion of the RAM memory. 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.

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. You can store retentive data 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 system stores data defined as retentive in retentive memory. The system retains this data beyond a power-off or power failure.

If you are using PC mass storage, use a UPS 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 on 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 available 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 Resource Config JSON file (Page 64).

If "Saving retentive data: PC mass storage" is selected, the complete data storage can be kept retentive. To ensure complete backup of the retentive data in case of a power failure, refer to the description in section Shutdown and startup (Page 87).

Reference

For additional information about the memory structure and the basic meaning of these memory areas, refer to the function manual Structure and Use of the CPU Memory (<https://support.industry.siemens.com/cs/ww/en/view/59193101>). This documentation also describes how you obtain information about the memory utilization using STEP 7.

4.3.1.2 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 onboard NVRAM

The following data is saved:

- The current data from data blocks, bit memory, timers, counters and technology objects that is marked as retentive in 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 Software Controller 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.

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.

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. To protect the file system, use a UPS ([Page 87](#)) or activate the usage of NVRAM.

Deleting the data

To delete the data from the CPU, use the "--MemoryReset" command of the s7_cpu_control tool.

Storage in NVRAM

The storage of 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

You must order NVRAM with the SIMATIC IPCs. With the latest BX-39A, PX-39A, IPC227G and IPC277G devices, the NVRAM modules can be ordered separately and mounted afterwards. If you mount an NVRAM device after installation of the Software Controller, you must reinstall the Software Controller.

The reference information of the product information includes information on which IPCs support NVRAM.

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.

4.3.2 Interface types

Below you find an overview of the interfaces used by the IndOS PC:

- CPU 1505SP:
 - A PROFINET onboard interface of CPU 1515SP PC2.
Isochronous data exchange via Isochronous Real Time (IRT) is possible
- CPU 1507S:
 - Two 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:
 - Two 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.

4.3.3 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 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.

4.3.4 PROFlenergy

PROFlenergy

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

Additional information

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

4.3.5 Web server of the CPU

4.3.5.1 Overview

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 under IndOS 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 118](#)).

Web browsers

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 (Version 11.0)
- Microsoft Edge (Version 100.0)
- Mozilla Firefox (Version 90.0)
- Google Chrome (Version 100.0)
- Opera (Version 85.0)
- Mobile Safari and Chrome for iOS (12.5.1)
- Android Browser (7.x, 8.x and 10.x)
- Chrome for Android (7.x, 8.x and 10.x)

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 without 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 selector, the position of the mode selector 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 CPU specifications.
- "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" topic in the Web server (<https://support.industry.siemens.com/cs/ww/en/view/59193560>) function manual.

4.3.6 Fail-safe

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-CPU's

(<https://support.industry.siemens.com/cs/ww/en/view/109478599>).

Installing

5.1 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 125](#)).

Category	Requirement
Operating system	SIMATIC Industrial OS (IndOS) V3.4.2 or later. SIMATIC Industrial OS (IndOS) V4.x versions are not supported.
Operator interface	Color monitor, keyboard and mouse or other pointing devices (optional)
Communication interface	One or more communication interfaces for communication with STEP 7 or other S7 applications or for communication with distributed I/O
Supported Software Controllers	CPU 1507S (F) and CPU 1508S (F)
Open Controller	CPU1505SP (F) also supports the ET 200SP Open Controller (CPU 1515SP PC2).
Supported SIMATIC IPCs	See section Reference information for use with SIMATIC IPC (Page 125)
Supported TIA Portal versions	as of V19
BIOS settings	For information on where to find these settings in the BIOS, see section Reference information for use with SIMATIC IPC (Page 125).

5.2 Installing the Software Controller

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 together with the hardware.

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

	CPU 1507S	CPU 1507S F	CPU 1508S	CPU 1508S F
IPC227G	✓	✓	--	--
IPC277G (PRO)	✓	✓	--	--
IPC427E	✓	✓	✓	✓
IPC477E (PRO)	✓	✓	✓	✓
BX-39A	✓	✓	✓	✓
PX-39A (PRO)	✓	✓	✓	✓

Requirements

Observe the following requirements for the installation:

- PC must meet the System requirements (Page 52)
- The latest BIOS version installed on PC
- The BIOS must be in UEFI mode (except for CPU1515SP PC2 where legacy mode is used)
- IndOS must have already been installed
- User has root privileges
- The system time and date is set to the current time and date
Use the "date" command before installing the Software Controller to check whether the date is correct. If the date is not correct, use the "date +%Y%m%d -s "currentdate"" command to set the correct date (for example, date +%Y%m%d -s "20211004")

Observe the following requirements during installation:

- The installation is not interrupted by manual operations or power failure.
In case of an interruption during installation, uninstall the Software Controller and then reinstall it.

NOTE

Installation location

It is only possible to install the Software Controller to the disk where IndOS is installed, even if there are other disks available in the system.

NOTE

Reinstallation of IndOS

If you reinstall IndOS with an already installed Software Controller on it, uninstall the Software Controller manually before reinstalling IndOS.

If you are unable to uninstall the Software Controller, clear the data on the RAW partition (Partition 6). You can clear the data from Partition 6 by using, for example, the following command:

```
dd if=/dev/zero of=/dev/sda6 or dd if=/dev/zero of=/dev/nvme0n1p6
```

Additional requirement for users of GNOME desktop environment

If PCs using GNOME desktop environment are kept idle for a configured period of time, IndOS goes into an unrecoverable suspension state.

To avoid this scenario, disable auto-suspension. To disable auto-suspension, proceed as follows:

Open the command terminal and run the following commands with root privileges:

- `$ gsettings set org.gnome.settings-daemon.plugins.power sleep-inactive-ac-timeout 0`
- `$ gsettings set org.gnome.settings-daemon.plugins.power sleep-inactive-battery-timeout 0`

Edit the default of "/etc/gdm3/greeter.dconf" as root and uncomment the following configurations from the end of configuration.

```
# Automatic suspend
# =====
[org/gnome/settings-daemon/plugins/power]
# - Time inactive in seconds before suspending with AC power
# 1200=20 minutes, 0=never
```

5.2 Installing the Software Controller

```
sleep-inactive-ac-timeout=0
# - What to do after sleep-inactive-ac-timeout
# 'blank', 'suspend', 'shutdown', 'hibernate', 'interactive' or 'nothing'
sleep-inactive-ac-type='nothing'
# - As above but when on battery
sleep-inactive-battery-timeout=0
sleep-inactive-battery-type='nothing'
```

To apply this configuration run as root:

```
dpkg-reconfigure gdm3
```

This command causes GNOME Display Manager (GDM) to reload its configuration upon the next logout or reboot.

Industrial OS service stick

The Software Controller installer script (install.sh) depends on components stored on the Industrial OS service stick. Therefore, before you start installing the Software Controller, carry out the following steps first:

- Insert the Industrial OS service stick into your target device
- Open the Linux terminal on your target device
- Enter the following command to update your system:
`sudo apt update`

NOTE

Remote repository

If you have set up a remote repository, the installation also considers the packages from the remote repository.

Software Controller setup

All necessary installation packages for installing the Software Controller are included in the compressed install script "install.sh". The install script contains the following Debian packages:

- vmm-installer.deb
- swcpu-installer.deb
- simatic-vmm-vnic.deb
- s7vmm-dev.deb
- swcpu-hooks.deb
- man-pages.deb

Apart from the install script "install.sh", there is also the following "uninstall.sh" script for uninstalling the Software Controller.

For information on how to uninstall the Software Controller, refer to section Uninstalling the Software Controller ([Page 59](#)).

Installation start

To extract the setup, enter the following command in the command prompt (the example uses the CPU 1507S and the IndOS installation default settings):

```
root@localhost:/home/pt# tar xvf  
CPU1507S-30.01.00.00-XXX_setup.tar.gz
```

To start the Software Controller setup, go into the extracted folder. Run the "install.sh" script by entering the following command (the example uses the CPU 1505SP):

```
root@localhost:~/CPU1505SP-30.01.00.00-XXX_setup# ./install.sh
```

NOTE

Location of installation script "install.sh"

For the installation to be successful, run the "install.sh" installation script from the setup directory where the script is located.

NOTE

License Agreement and Security Information

Before you can proceed with the installation, confirm the following:

- License Agreement of Siemens AG
 - Security Information
 - Open Source and Third Party License
-

After the confirmations, the Debian package for the SIMATIC Hypervisor is installed to the system. This package prepares the environment by shrinking the disk and creating new partitions for the SIMATIC Hypervisor and the Software Controller to be installed. Afterwards the Software Controller Debian package and associated drivers are installed to the system.

Installation log messages

During installation, the system writes log messages such as username, Software Controller variant, version and event/command information into "journalctl".

Silent installation

You can also carry out a silent installation by using the "./silent_install.sh" command.

Automatic configuration of BIOS settings

If you install the Software Controller on BX-39A / PX-39A (PRO) IPCs, the mandatory and recommended BIOS settings will be set automatically during installation. The following installation dialog prompts you to allow an automatic selection of the correct BIOS settings:

```
Do you want to allow Setup Installer to configure BIOS settings  
automatically?
```

If you select "y", the system will do several reboots and apply the correct BIOS settings. The system restarts and displays information regarding the BIOS attributes. After the restart, the Software Controller installation continues automatically.

Automatic configuration of BIOS for backup/restore or cloning scenarios

The automatic configuration of BIOS settings is also useful if you want to clone master copy image of your device to deploy the functionality onto further devices. If you want to automatically configure the BIOS settings with an installed Software Controller disk image, you will find the installed "efiutils" folder in the file system. If you want to automatically configure the BIOS settings without an installed Software Controller disk image, you will find the "efiutils" folder inside your installation media.

To automatically configure the mandatory and recommended BIOS settings, follow the instruction below.

NOTE

Note that the automatic configuration of BIOS settings will overwrite previous BIOS settings.

NOTE

If you install the Software Controller using `silent_install.sh`, the "efiutils" folder might not be installed to the system. In that case, use the "efiutils" folder from the compressed binary file containing the installer of the Software Controller.

When you apply changes to the BIOS settings as a security requirement, certificates are used.

NOTE**Use your own certificate**

We highly recommend that you use your own certificates. As a certificate creation mechanism, you can use OpenSSL.

An example command would be as follows:

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

Scenario 1: If you want the BIOS settings to be applied automatically on the new device where the master copy image will be restored including a Software Controller installation, copy your certificate and key file into:

```
/mnt/swcpu_mount/SWCPU/etc/efiutils/efitemp/efi/EFI/temp/
```

Scenario 2: If you want the BIOS settings to be applied automatically on the new device where the master copy image will be restored without including a Software Controller installation, copy your certificate and key file into: <InstallationMedia
efiutils/efitemp/efi/EFI/temp/cert/

NOTE

The certificate file must be for both cases named as "tmpcert.crt" and the key file must be named as "tmpkey.pem".

Then, for both scenarios, proceed as follows:

1. Navigate to the "efiutils" folder.
2. Run the "prepare.sh" script as `sudo`.

After successful execution of the script, create the disk image. The next time the system is booted from the mass storage device to be cloned, the BIOS settings will be applied automatically. Now you can create the master copy of the device using an imaging tool.

NOTICE
Booting after creation of master copy
Do not boot from the mass storage device to be cloned until the master copy has been created.

After the installation

After the packages are installed, a reboot is required to ensure that all system related changes are applied.

Select "y" for automatically reboot the system and to complete the installation.

After the installation is completed, the disk partitions for IPC427E / IPC477E have the following structure:

pt@localhost:~\$ lsblk	
Partition	Description
sda	
- sda1	EFI system partition
- sda2	
- sda3	
- sda4 -- sokol	IndOS root file system - "sokol" encrypted partition
- sda5	CPU data partition; mount point: /mnt/swcpu_mount
- sda6	CPU volume

For IPC227G, IPC277G, BX-39A and PX-39A, the partition naming is as follows:

root@localhost:/home/pt# lsblk	
Partition	Description
nvme0n1	
- nvme0n1p1	EFI system partition
- nvme0n1p2	
- nvme0n1p3	
- nvme0n1p4 -- sokol	IndOS root file system - "sokol" encrypted partition
- nvme0n1p5	CPU data partition; mount point: /mnt/swcpu_mount
- nvme0n1p6	CPU volume

For more information on the CPU memory area, see chapter CPU memory areas ([Page 44](#)).

After the installation finishes, the system is configured with the basic hardware configuration and the Software Controller is in STOP mode. If your hardware requirements differ from the basic configuration, update the configuration accordingly in Resource Configurator. To be able to switch the Software Controller to RUN, carry out a CPU-only download in TIA Portal. For information on how to use Resource Configurator, see chapter Resource Configurator ([Page 62](#)).

Generating hash values for installed files

You can check files that are installed by Software Controller for manipulation. To do so, compare the hash values of the installed files with the original hash values stored in the hash file. The hash file is part of the setup as provided from the Siemens Customer Support web site.

To generate the hash value for an installed file, use the following command under IndOS:
"sha256sum <file name>"

NOTE

Make sure that you keep the hash file in a secure place.

5.3 Updating/upgrading the Software Controller

To update or upgrade an already installed Software Controller, extract the new installer. Run `install.sh` with root privileges or by using the `sudo` command.

NOTE

Before you can start the update or upgrade, confirm the License Agreement and Security Information.

To proceed with the update or upgrade, the CPU must be powered off.

```
root@localhost:/home/pt/CPU1507S-30.01.00.00-07.01.00.15_setup# sudo ./install.sh
SWCPU Installation started...
VMM and CPU RAW Partitions already exist!
The system will be updated soon!
CPU needs to be powered off. Would you like to continue? (y/n)y
```

After successful update or upgrade, a reboot is required for the installation to be completed.

```
root@localhost:/home/pt/CPU1507S-30.01.00.00-07.01.00.15_setup# sudo ./install.sh
SWCPU Installation started...
VMM and CPU RAW Partitions already exist!
The system will be updated soon!
CPU needs to be powered off. Would you like to continue? (y/n)y
CPU is being powered off...
```

After finishing the update or upgrade, the user project, retentive data and configuration data are still available.

NOTE**Updating IndOS operating system**

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

NOTE**Handling of V30.0 projects on a Software Controller V30.1**

If a Software Controller V30.1 is running on an IPC with a downloaded V30.0 project, reinitialize the system with the following commands before downloading a V30.1 project to the IPC:

- "CPU_Resourceconfigurator -s"
 - "CPU_Resourceconfigurator -r" <resource configuration json file>
-

5.4 Uninstalling the Software Controller

Requirements

To uninstall the Software Controller, root privileges are required.

Uninstallation start

The Software Controller installer provides a script called "uninstall.sh". Use this script to start the uninstallation process.

NOTE**Mount point of Software Controller**

Before you uninstall the Software Controller, make sure that the mount point of the Software Controller (usually "/dev/sda5") is not in use by other processes.

To start the uninstallation, enter the following command (the example uses the CPU 1505SP):
~/CPU1505SP-30.01.00.00-XXX_setup# ./uninstall.sh

After the uninstallation

After successful uninstallation, reboot the system. After the reboot, all Software Controller related components are removed from the system.

NOTE**BIOS settings**

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

Disk partitions after uninstallation and reboot

After uninstallation and reboot, the disk partitions should have the following structure:

Partition	Description
sda1 / nvme0n1p1	EFI system partition
sda2 / nvme0n1p2	
sda3 / nvme0n1p3	
sda4 / nvme0n1p4	IndOS root file system

Verification of remaining disk partitions

You can verify the remaining disk partitions by running the following command:

fdisk -l

After running this command, only the following disk partitions remain:

- sda1 / nvme0n1p1
- sda2 / nvme0n1p2
- sda3 / nvme0n1p3
- sda4 / nvme0n1p4

NOTE

Disk partition sda6

If partition sda6 still remains after uninstallation, it has no effect on IndOS other than sda6 not being utilizable by IndOS.

The existence of the sda6 partition has no effect on the reinstallation of the Software Controller. The same partition will be occupied by the next installation.

If you do not intend to install the Software Controller again, proceed as follows:

- Delete sda6
 - Extend the root partition to be able to utilize this area
-

Commissioning

6.1 First commissioning

Commissioning

The following checklist guides you through the steps necessary for first commissioning.

Step	Procedure	Further information
1.	Install Software Controller V30.1 IndOS following the installation process as described in section Installing (Page 52).	Section Installing the Software Controller (Page 52)
2.	Create a TIA Portal project.	STEP 7 online help
3.	Create a Configuration file compatible to your TIA Portal project.	Section Example of a Resource Configuration file (Page 64)
4.	Assign an IP address to the SIMATIC RT-VMM Network Adapter.	Paragraph "Network interface card" in section Resource Configurator (Page 62)
5.	Execute s7_resource_configurator via command line interface.	Section Resource Configurator (Page 62)
6.	Reboot the device for the configuration changes to take effect (Software Controller is accessible via a physical interface or over SIMATIC RT-VMM Network Adapter interface).	Section Resource Configurator (Page 62)
7.	Download user program onto device via TIA Portal connection.	STEP 7 online help
8.	Switch Software Controller to RUN either via TIA Portal connection or the s7_cpu_control tool.	Section Operation using command line commands (Page 96)

NOTE

Bridging the physical and SIMATIC RT-VMM Network Adapter interfaces

If you want to bridge the physical interface and the SIMATIC RT-VMM Network Adapter interface, the bridge must have an IP address which is in the same subnet as SIMATIC RT-VMM Network Adapter.

6.2 Resource Configurator

Resource Configurator configures all system resources which are necessary for operating the Software Controller. Resource Configurator is part of the Software Controller installer. The tool is automatically installed on the target device. Resource Configurator does not have a graphical user interface but is a command line tool executable on the IndOS terminal.

You can use the IndOS terminal to carry out the following actions:

- Install
- Update
- Backup
- and configure the Software Controller

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

Resource Configurator and its dependent files are located under the Software Controller data partition.

```
pt@localhost:/mnt/swcpu_mount/SWCPU/bin$ lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE  MOUNTPOINTS
sda         8:0    0   28G  0 disk
├─sda1      8:1    0   256M  0 part  /efi
├─sda2      8:2    0     1M  0 part
├─sda3      8:3    0     1G  0 part
├─sda4      8:4    0    24G  0 part
├─┬soko1   252:0  0    24G  0 crypt /
├─sda5      8:5    0     1G  0 part  /mnt/swcpu_mount
└─sda6      8:6    0    1.7G  0 part
pt@localhost:/mnt/swcpu_mount/SWCPU/bin$
```

Figure 6-1 Data partitions

During the setup, the Software Controller creates a partition containing the Software Controller data and mounts it under `/mnt/swcpu_mount`.

The command line tool is located under the following mount point:

- `/<mount_point>/SWCPU/bin/`

The Resource Configurator dependent Configuration file ("Resource Configuration file") is located under:

- `/<mount_point>/SWCPU/etc/resource_configurator/`

The last successfully applied resource assignment Configuration file is located under:

- /etc/successful_config/

NOTE

File transfer to other target devices

If the target IPC has the same article number as the source IPC, you can also transfer "successful_config" files stored under this location to other devices and use these files as input to execute Resource Configurator.

Executing Resource Configurator

After completing the Software Controller installation, the Software Controller is configured with the basic hardware configuration and in STOP mode. If the hardware requirements differ from the basic configuration, update the configuration in Resource Configurator. To be able to switch the Software Controller to RUN, carry out a CPU-only download in TIA Portal.

During operation, execute Resource Configurator manually via command line to apply your configuration changes as desired. The following figure shows the help screen, which is visible via the "--help" command.

```

root@localhost:/mnt/swcpu_mount/SWCPU/bin# ./s7_resource_configurator --help
Copyright © Siemens AG, 2023
Command Line Configuration utility of S7-1500 Software Controller

Usage:
./s7_resource_configurator --resource-config <json-file> [--force-reboot] [--verbose]
./s7_resource_configurator --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:
./s7_resource_configurator -r /<path>/Resource_Assignment.json
./s7_resource_configurator --resource-config /<path>/Resource_Assignment.json --force-reboot --verbose
./s7_resource_configurator -s -f -v
    
```

Figure 6-2 Help screen

Resource configurator will take the following parameters as input.

- "-r, --resource-config=FILE" (mandatory)

Other parameters:

- "-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 IndOS to reboot automatically after successful execution of Resource Configurator to make the changes effective. Alternatively, you can manually reboot the system later.

The following figure shows the result after successful operation.

```
pt@localhost:~$ s7_resource_configurator -r /home/pt/IPC_basic_configuration.json -v
Executing -> Resource Configurator...
Article number from JSON : AUTO
Article number from SMBIOS: 6AG4141-5BC50-3JA0
Corresponding PCI_MAP file: PCI_MAP_6AG4141-XXX5X-XXXX.json
NVRAM Available : NO
Executing -> Update VMM configuration...
Executing -> Update config area...
Executing -> Save Successful Configuration...
SUCCESSFUL!
REBOOT THE SYSTEM FOR CHANGES TO BE APPLIED!
pt@localhost:~$
```

Figure 6-3 Successful operation

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

Multiple calls of Resource Configurator

Resource Configurator can also be called multiple times in a row. Provided configuration changes are applied according to the provided Resource Configuration file.

Changing the "nvram_usage" and "interfaces" entries erases the Software Controller's load memory while changing the "led_usage" and "start_cpu_on_pc_boot" entries does not erase the Software Controller's load memory.

6.2.1 Example of a 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.

NOTE

Changing the hardware configuration in TIA Portal

In rare cases, changing the hardware configuration in TIA Portal, e.g. changing the Software Controller version, and downloading the project to a device, which already contains a TIA Portal project, might fail.

In such cases, use the following commands to remove the currently downloaded project from the target device, before downloading the project containing the changed hardware configuration:

- "s7_resource_configurator -s"
 - "s7_resource_configurator -r" <resource configuration json file>
-

Example of a resource Configuration file

The following figure shows a configuration file with an example basic configuration. Use this file to change the values to your actual 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"
    }
  ]
}
```

The following figure shows a Configuration file with an example of an IE General external card configuration.

```
{
  "content_id": "resource_assignment",
  "article_number": "6AG4141-7BJ50-5AA0",
  "led_usage": true,
  "nvram_usage": false,
  "start_cpu_on_pc_boot": false,
  "interfaces": [
    {
      "name": "X2",
      "hw_identifier": 64
    },
    {
      "name": "X102",
      "hw_identifier": 72,
      "type": "Intel i210 or Compatible"
    }
  ]
}
```

The following figure shows a Configuration file with an example of an CP 1625 external card configuration.

```
{
```

```

"content_id": "resource_assignment",
"article_number": "6AG4141-7BJ50-5AA0",
"led_usage": true,
"nvram_usage": false,
"start_cpu_on_pc_boot": false,
"interfaces": [
{
"name": "X2",
"hw_identifier": 64
},
{
"name": "X102"
"hw_identifier": 72,
"type": "CP 1625"
}
]
}

```

NOTE**Structure of a Configuration file**

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

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 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.

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"  
  }  
]
```

"content_id"

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

"article_number"

Change "article_number" to the article number of your device. The article number must match the article number of the IPC selected in TIA Portal.
If you set the value to "auto", Resource Configurator automatically uses the correct device article number.

NOTE

Automated setting of article numbers

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

"led_usage"

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 Configuration file, "true" already is the default value.

The parameter "led_usage" corresponds to the "Hardware LED" section of TIA Portal:

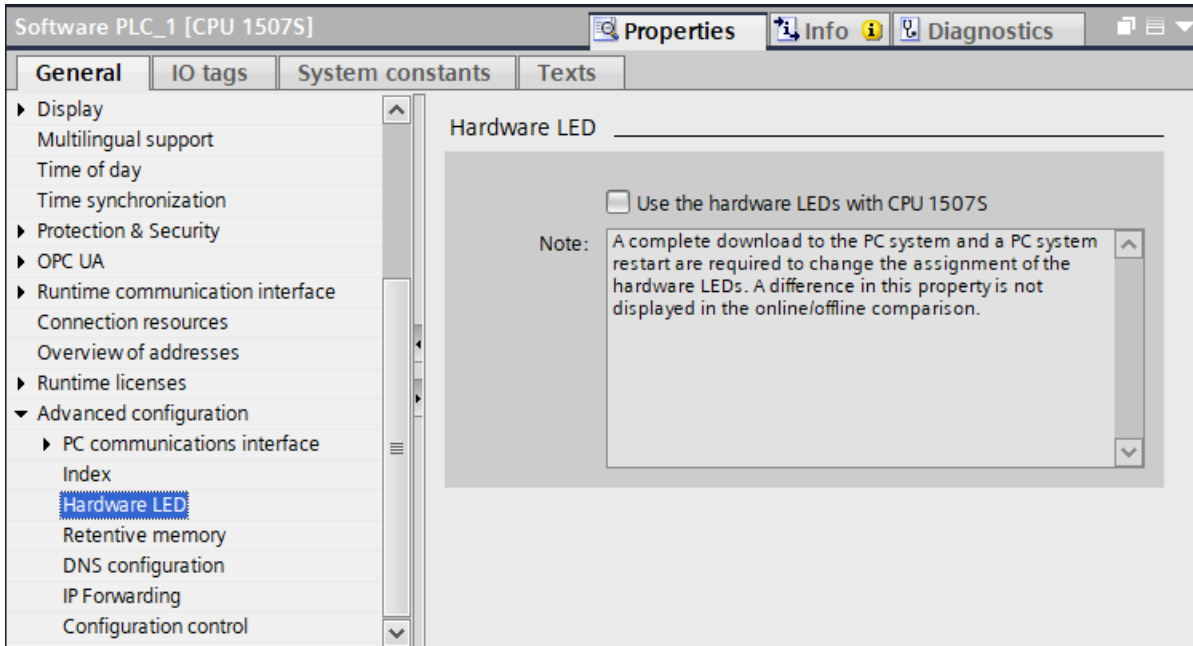


Figure 6-4 Hardware LEDs

"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.

The parameter "nvram_usage" corresponds to the "Retentive data memory" section of TIA Portal:

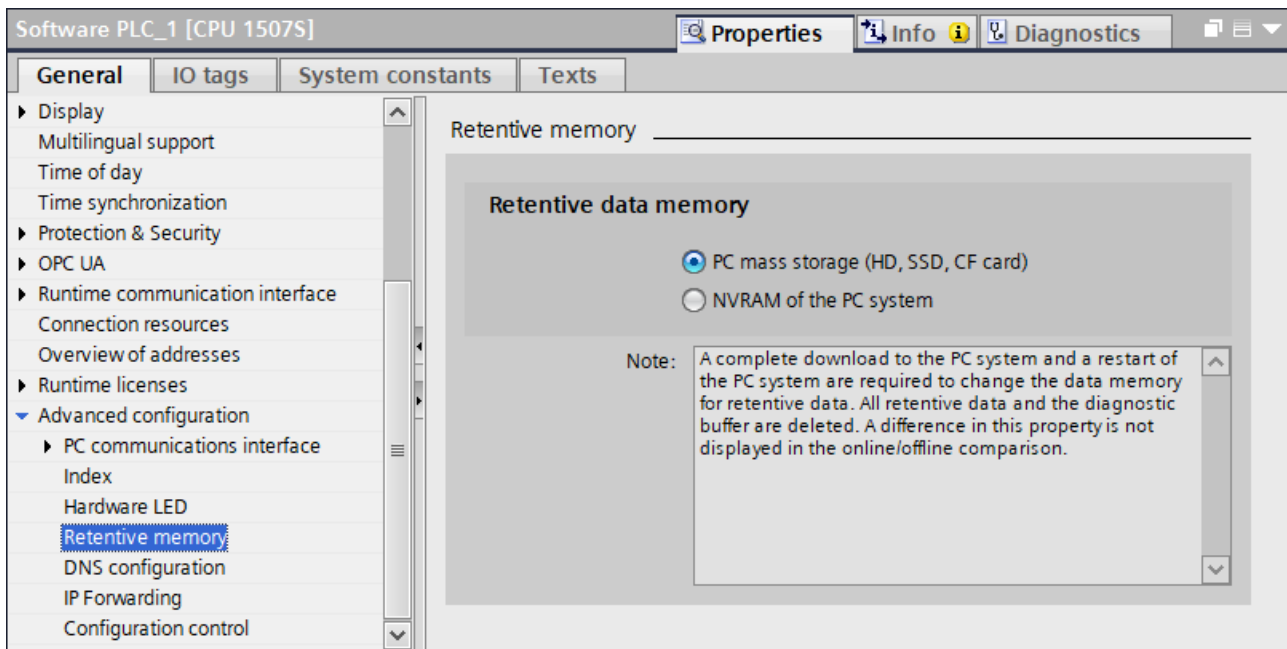


Figure 6-5 Retentive memory

"start_cpu_on_pc_boot"

If you want to start the Software Controller automatically after booting the PC, 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 s7_cpu_control tool. Otherwise, the CPU download fails.

"interfaces"

In the "interfaces" section, you assign the interface parameters for the Software Controller.

"name" and "type"

Set "name" to the name of the interface assigned to the Software Controller (for example, X2).

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 a IPC427E TIA Portal project to a BX-39A).

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

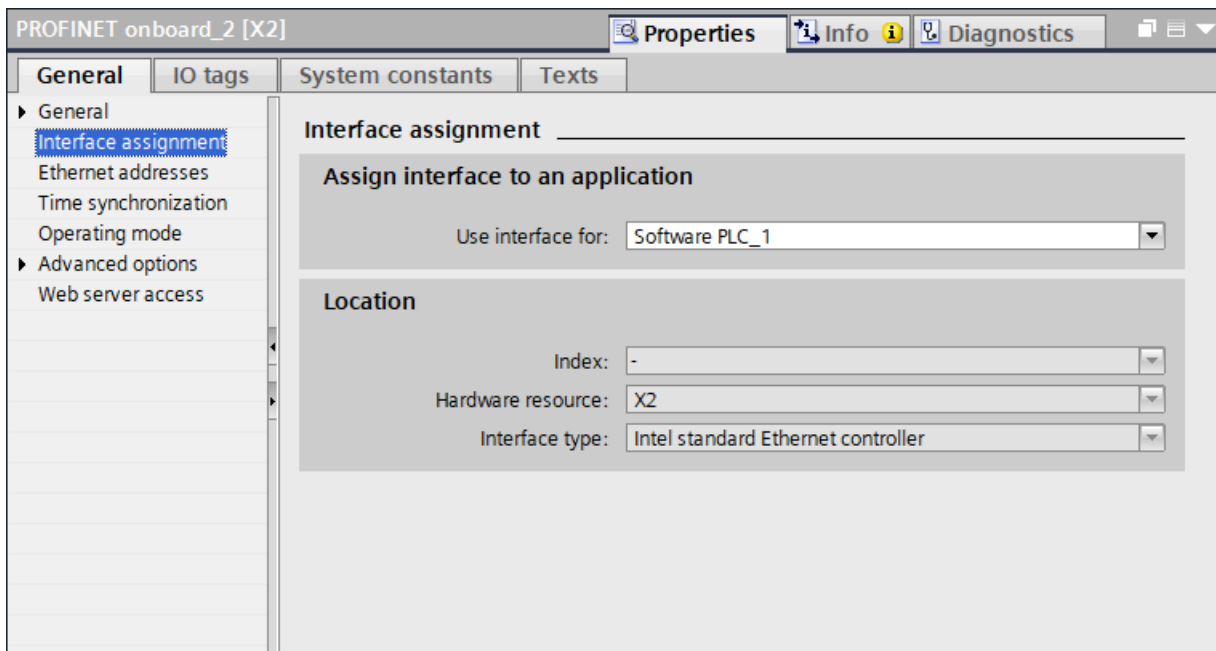


Figure 6-6 Interface assignment

NOTE

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

The following table shows which CPU interfaces and types you can use on which device.

Device	CPU interface	Interface type
Open Controller CPU 1515SP PC2	X1	
IPC227G / IPC277G (PRO)	X1, X2	Intel Advanced Ethernet Controller
IPC427E / IPC477E (PRO)	X2, X3	Intel Standard Ethernet Controller
BX-39A / PX-39A (PRO)	X2,	Intel Standard Ethernet Controller

Device	CPU interface	Interface type
BX-39A / PX-39A (PRO)	X3, X4	Intel Advanced Ethernet Controller
IE General card	X101, X102 ...	Intel i210 or compatible
CP 1625 card	X101, X102 ...	CP 1625

"hw_identifier"

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:

Name	Type	Hardware identi.	Used by	Comment
Local-PROFINET_onboard_2~Port_1	Hw_Interface	65	Software PLC_1	
Local-PROFINET_onboard_2	Hw_Interface	64	Software PLC_1	

Figure 6-7 Hardware identifier

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

- The interfaces defined in the 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

The combination X3 + X4 is not supported.

NOTE

PROFIBUS interfaces

The Software Controller V30.1 does not support PROFIBUS with SIMATIC IPCs.

NOTE**Hardware ID 59**

HW ID 59 belongs to the PC communication interface. Since IndOS does not have a PC Station interface, you cannot use HW ID 59 for a Software Controllers running on IndOS.

Network interface card

NOTE

If you assign a new network interface card to the Software Controller, the name of the SIMATIC RT-VMM Network Adapter changes, e.g. enp0sf1. The SIMATIC RT-VMM Network Adapter IP address is no longer available. The s7_cpu_control tool can no longer communicate over the SIMATIC RT-VMM Network Adapter interface.

To avoid this scenario, after the installation of the Software Controller setup is completed, you have the following possibilities:

- Assign a new IP address (for more information on how to assign IP addresses, see chapter Operation using command line commands)
or
- Write a udev rule to give a permanent name to the SIMATIC RT-VMM Network Adapter interface according to its MAC address

To write a udev rule, proceed as follows:

1. Add a file with the file extension .rules (for example, "10-network.rules") to folder "/etc/udev/rules.d"
2. Write the following rule into the file:
SUBSYSTEM=="net", ACTION=="add",
ATTR{address}=="MAC_ADDR_OF_VMM_NETWORK_ADAPTER",
NAME="VMM_NETWORK_ADAPTER_NAME"

The following example shows the rule with an example MAC address and SIMATIC RT-VMM Network Adapter interface name added to it:

```
SUBSYSTEM=="net", ACTION=="add", ATTR{address}=="28:63:36:78:b4:2d",  
NAME="enp0s3f1"
```

3. Save the file and reboot the system.
4. Use the "ip a" command to check, if the new SIMATIC RT-VMM Network Adapter interface name has been added.

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:
<mount_point>/SWCPU/etc/resource_configurator/.

```
{
  "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"
    }
  ]
}
```

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 delivered via setup and stored in the following default path:

<mount_point>/SWCPU/etc/resource_configurator/.

```
{
  "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

A basic configuration is applied during installation by default. If you require a different configuration, reconfigure the system. As an example, we consider this following scenario. You want to use the additional external card CP 1625. You create your custom resource assignment file by modifying the existing one or by copying it with a different name.

During installation, user groups are automatically created. The system administrator must add users to the appropriate user group(s) using the -add command.

- For a standard Software Controller, the root and the users belonging to the "software_controller_operators" group can execute the tool.
- For a fail-safe Software Controller, only users belonging to the "failsafe_operators" group can execute the tool.

The following shows an example of a customized configuration:

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

Then execute Resource Configurator by providing this file as an input. Finally, reboot the system for the changes to take effect.

```
pt@localhost:~$ s7_resource_configurator -r /home/pt/IPC_basic_configuration.json -v
Executing -> Resource Configurator...
Article number from JSON : AUTO
Article number from SMBIOS: 6AG4141-5BC50-3JA0
Corresponding PCI_MAP file: PCI_MAP_6AG4141-XXX5X-XXXX.json
NVRAM Available : NO
Executing -> Update VMM configuration...
Executing -> Update config area...
Executing -> Save Successful Configuration...
SUCCESSFUL!
REBOOT THE SYSTEM FOR CHANGES TO BE APPLIED!
pt@localhost:~$
```

Figure 6-8 Apply changes

If you apply the same configuration more than once, the following message appears:
"Hardware configuration is up to date. No changes will be applied!"

```
pt@localhost:~$ s7_resource_configurator -r /home/pt/IPC_basic_configuration.json -v
Executing -> Resource Configurator...
HARDWARE CONFIGURATION IS UP TO DATE!
NO CHANGES WILL BE APPLIED!
pt@localhost:~$
```

Figure 6-9 Configuration is up to date

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.

Delete configuration

To delete the configuration, use the "set-initial" command. This command deletes the previously loaded project. You can use either of the two following commands:

- `s7_resource_configurator -s -v`
- `s7_resource_configurator --set-initial -verbose`

The following images shows the application of the "set-initial" command.

```
pt@localhost:~$ s7_resource_configurator -s -v
Executing -> Resource Configurator...
Article number from JSON : AUTO
Article number from SMBIOS: 6AG4141-5BC50-3JA0
Corresponding PCI_MAP file: PCI_MAP_6AG4141-XXX5X-XXXX.json
NVRAM Available : NO
Executing -> Update VMM configuration...
Executing -> Update config area...
Executing -> Save Successful Configuration...
SUCCESSFUL!
REBOOT THE SYSTEM FOR CHANGES TO BE APPLIED!
pt@localhost:~$
```

Figure 6-10 Delete configuration

6.2.2 Error handling

Configuration errors

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

```
pt@localhost:~$ s7_resource_configurator -r /home/pt/IPC_basic_configuration.json -v
Executing -> Resource Configurator...
Wrong hardware identifier: 65
Wrong attribute in JSON file!
FAILED!
```

Figure 6-11 Configuration error while parsing Configuration file

Resource Configurator shows a status message about the operation result. If an error occurs, use the `--verbose` parameter (`-v`) to collect detailed information about the error reason.

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 error reason. A return value of "0" means that no error appeared, and the operation was successful.

The following list gives an overview of possible error reasons:

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	File not in JSON format
ERR_LOAD_CFG_FILE_FAILED	Error while loading linux cpu config file
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
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 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	This device does not support PLC priority
ERR_UNSUPPORTED_SPU_CONFIG	This device does not support Safety Processing Unit
ERR_RM_ALL_AHCI_FAILED	Removing an 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

Error message	Meaning
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 Exporting and importing configuration files

6.3.1 Command prompt

The tool for importing and exporting configuration files is called S7 CPU Configuration Tool.

This command line executable tool is located under:

`<mount_point>/SWCPU/bin/`

You can automate the usage of the tool via scripting.

Command prompt

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

```
pt@localhost:~$ s7_cpu_configuration --help
Copyright © Siemens AG, 2023
Command line tool for File Import/Export operations of S7 - 1500 Software Controller

Usage:
./s7_cpu_configuration [PARAMETERS]...

Parameters:
-h, --help           Print Help
-v, --verbose        Set Verbose Logging
-V, --version        Print Version
-p, --print          Print Configuration
--ramdisk            Working directory will be changed to /run for current execution
-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

Example:
./s7_cpu_configuration --import <path>/ExportedFile.psc --verbose
./s7_cpu_configuration --import <path>/ExportedFile.psc --retain --verbose
./s7_cpu_configuration -e <path>/ExportedFile.psc -v
./s7_cpu_configuration --import <path>/ExportedFile.psc --ramdisk
./s7_cpu_configuration -e <path>/ExportedFile.psc --ramdisk
./s7_cpu_configuration --import <path>/ExportedFile.psc --print <path>/ExportedFile.psc
./s7_cpu_configuration --clear

NOTE:
When using export/import with retain, the user is asked for a password
Password:*****

Return code: 0x0.
```

Figure 6-12 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 verbose logging on. 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`
The command changes the working directory from `/tmp` to `/run` for the current execution.
- `--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.
- `--retain` or `-r`
The command adds retentive data to the `.psc` file.

NOTE

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

1. Import the `.psc` file without the `--retain` command
2. Import the `.psc` file with the `--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 (`s7_cpu_configuration --clear`).

6.3.2 Exporting configuration files

Export operation

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.
2. You have created and applied a TIA Portal project to the CPU.
3. You have executed `s7_cpu_configuration` with the `--export` parameter via the command line interface.
4. The `.psc` file is created in this step.

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.

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

1. Run the `./s7_cpu_configuration --export <path>` 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.

The following image shows the export of an example file (`./s7_cpu_configuration --export /path/to/project.psc`).

```
pt@localhost:~$ s7_cpu_configuration --export /home/pt/exported_project.psc
Exporting memory card file is starting...
Memory card file successfully generated in /home/pt/exported_project.psc
Exporting memory card file is finished successfully...
SUCCESSFUL!
Return code: 0x51A3.
```

Figure 6-13 Successful configuration export

NOTE

Usage of paths

The export function does not work with relative paths. Do not use relative paths but use absolute paths instead.

Exporting CPU configuration including retentive data

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

1. Run the "`s7_cpu_configuration --export <filepath> --retain`" command in the command prompt and add the following commands:
"`s7_cpu_configuration --export <filepath> --retain`" or "`s7_cpu_configuration --e<file path> --r`"
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.

```
pt@localhost:~$ s7_cpu_configuration --export /home/pt/export_retain.psc -v -r
Enter the password for retain, empty password is not acceptable
Password:
Exporting memory card file is starting...
Generation Metafile.xml is starting...
Successfully generated Metafile.xml.
Exporting retentive data is finished...
Mounting Load storage area is starting...
Successfully mounted Load Storage area.
Exporting process of OMSSTORE is starting...
Successfully exported OMSSTORE from loadstorage area.
Exporting process of VoT is starting...
Successfully exported VoT from loadstorage area.
Exporting process of ODK is starting...
Successfully exported ODK from loadstorage area.
Unmounting load storage area is starting...
Successfully umounted Load Storage area.
Memory card file generation is starting...
PCSystem.zip successfully generated...
retain.zip successfully generated...
Memory card file successfully generated in /home/pt/export_retain.psc
Exporting memory card file is finished successfully...
SUCCESSFUL!
Return code: 0x51A3.
```

Figure 6-14 Retentive data export

6.3.3 Importing configuration file

Import operation

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

1. A Software Controller V30.1 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 `s7_cpu_configuration` with the `--import` parameter via the command line interface.
5. You have switched the Software Controller to POWER ON.
6. The Software Controller can be operated using the imported configuration.

Importing CPU configuration

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

You use the `s7_cpu_control` tool to change the operating state to POWER OFF, before executing the import command.

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

1. Power off the Software Controller using the command `./s7_cpu_control --PowerOffCPU`.
2. Run the `./s7_cpu_configuration --import /path/to/project.psc` command in the command prompt.
3. Wait for execution.
4. After the confirmation that the operation was successful use the command `./s7_cpu_control --PowerOn`.
5. Use the command `./s7_cpu_control --Run` to put the Software Controller into RUN.

The following shows an example configuration import for a standard Software Controller.

```
pt@localhost:~$ s7_cpu_control --GetStatus
Current State: ST0P
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --PowerOff
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_configuration --import /home/pt/psc_files/FileImport_IPC_427E_Addition.psc
Importing memory card file is starting...
Importing memory card file is finished successfully...
SUCCESSFUL!
pt@localhost:~$ s7_cpu_control --PowerOn
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --Run
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --GetStatus
Current State: RUN
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ █
```

Figure 6-15 Example configuration import for standard Software Controller

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

1. Power off the Software Controller using the command `./s7_cpu_control --PowerOffCPU`.
2. Run the `./s7_cpu_configuration --import /path/to/project.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. Confirm the collective fail-safe signature by using the `s7_cpu_control` tool and running the command `./s7_cpu_control --ConfirmCollectiveFSignature -Signature <signature>`
6. Use the command `./s7_cpu_control --Run` to put the Software Controller into RUN.

```

pt@localhost:~$ s7_cpu_control --GetStatus
Current State: STOP
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --PowerOff
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_configuration --import /home/pt/psc_files/F_NonPMS_NonPro_Add.psc
Importing memory card file is starting...
Collective F-Signature: 9A0773BD
Importing memory card file is finished successfully...
SUCCESSFUL!
pt@localhost:~$ s7_cpu_control --PowerOn
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --ConfirmCollectiveFSignature -Signature 9A0773BD
Current Collective F-Signature: 9A0773BD
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --Run
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ s7_cpu_control --GetStatus
Current State: RUN
Command sent SUCCESSFULLY to SWCPU
pt@localhost:~$ █

```

Figure 6-16 Example configuration import for fail-safe Software Controller

NOTE**Usage of paths**

The import function does not work with relative paths. Do not use relative paths but use absolute paths instead.

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 by executing the command `./s7_cpu_control --PowerOffCPU`.
2. Run the `./s7_cpu_configuration --import <filepath>` command to import the configuration without retentive data.
3. Wait for execution.
4. After the confirmation that the operation was successful, execute the command `./s7_cpu_control --PowerOnCPU` to power on the CPU.
5. Power off the CPU by executing the command `./s7_cpu_control --PowerOffCPU`.
6. Run the `s7_cpu_configuration --import <file path> --retain` command to import the configuration including the retentive data.
7. Wait for execution.
8. After the confirmation that the operation was successful, execute the command `./s7_cpu_control --PowerOnCPU` to power on the CPU.
9. Use the command `./s7_cpu_control --Run` to put the Software Controller into RUN state.

```
pt@localhost:~$ s7_cpu_configuration --import /home/pt/export_retain.psc -v -r
Enter the password for retain, empty password is not acceptable
Password:
Importing memory card file is starting...
Extraction process of memory card file is started...
Extraction process of memory card file is finished successfully.
Extraction process of retain.zip in memory card file is finished successfully.
Extraction process of PCSystem.zip in memory card file is finished successfully.
Extracting .psc file is finished successfully.
Path of extracted .psc folders are :
/tmp/psc_extraction_folder_2023-11-16_12:37:09/PCSystem/1/SIMATIC.S7S
Mounting Load storage area is starting...
Successfully mounted Load Storage area.
The SIMATIC.S7S/OMSSTORE folder successfully deleted
The ODK1500S folder successfully deleted
The SIMATIC.S7S folder is successfully replaced
Importing retentive data is finished successfully...
Unmounting load storage area is starting...
Successfully unmounted Load Storage area.
Collective F-Signature: 9A0773BD
Importing memory card file is finished successfully...
SUCCESSFUL!
Return code: 0x51A3.
```

Figure 6-17 Retentive data import

NOTE**Import limitations for CPU 1508S (F)**

Importing a .psc file created in TIA Portal to a CPU 1508S (F) is not possible.

Import attempts may result in a defect state of the CPU. To repair this situation, uninstall and then reinstall the Software Controller.

To also use the import functionality with a CPU 1508S (F), proceed as follows:

1. Download your project to the target IPC and verify that it is running.
 2. Create a .psc file using the export command of the s7_cpu_configuration tool.
 3. While importing, use the .psc file that is created in step 2.
-

6.3.4 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 ".s7_cpu_configuration --print /path/to/project.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.

The following image shows an example command line output.

```
pt@localhost:~$ s7_cpu_configuration --print /home/pt/export_retain.psc
Metafile
Component
  Index="1"
  Name="CPU1507SF"
  Id
  TypeId="17752839"
  Author="localhost.localdomain/pt"
  Comment="Exported on Thu Nov 16 12:31:40 2023"
  TextList
  Software
  IuM
  Manufacturer="Siemens"
  OrderId="6ES7 672-7FC02-0YA0"
  SoftwareRevision="V 30.1.0"
  FunctionDesignation
  LocationDesignation
  InstallationDate="2023-11-14T10:45:00"
  AdditionalInfoText
  CollectiveFailsafeSignature="0x9A0773BD"
Return code: 0x51A3.
```

Figure 6-18 Example of printed configuration metadata

6.3.5 Error handling

Error messages

S7 CPU Configuration Tool 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 error reason. A return value of "0" means that no error appeared, and the operation was successful.

The following list gives an overview of possible error reasons:

Message	Code
SUCCESS	0x0
FAILSAFE_SUCCESS	0x51A3

Message	Code
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_CPU_TYPE_NOT_MATCH	0x80040338
ERR_RETAIN_ENCRYPTION_FAILED	0x80040339
ERR_RETAIN_DECRYPTION_FAILED	0x8004033A
ERR_GENERIC_FAIL	0x8004033F

6.4 Shutdown and startup

Software Controller start after booting PC

For IndOS, you do not determine the starting behavior of the Software Controller in TIA Portal but in the Resource Configuration file of Resource Configurator.

For information on how to start the Software Controller after booting the PC, refer to section Resource Configuration file ([Page 64](#)).

Software Controller mode after booting PC

The mode the Software Controller is in, after powering on the Software Controller, is set in the "Startup" section of TIA Portal.

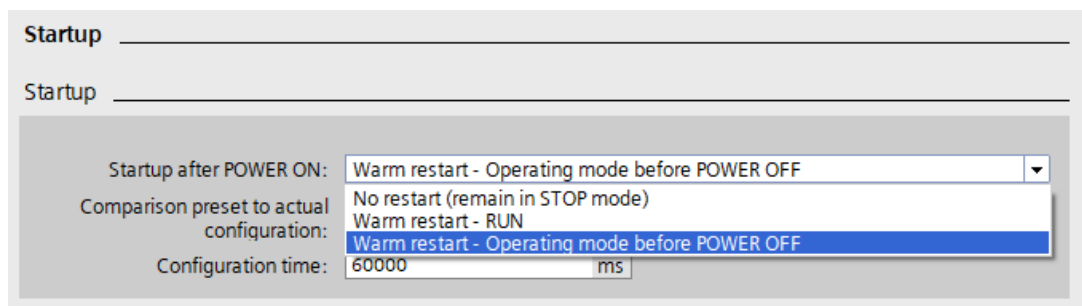


Figure 6-19 Startup

Option "No restart (remain in STOP mode)"

If you use this option and initiate a restart for IndOS, the Software Controller powers off and IndOS restarts the PC. Retentive data stored in PC mass storage or NVRAM is kept.

After restart, use the "Bootling of the PC" option "IndOS and S7-1500 Software Controller" in the GRUB screen menu. After system start, the Software Controller is powered on but is in STOP mode. All retentive data is available again.

Options "Warm restart - RUN" and "Warm restart - Operating mode before POWER OFF"

If you use one of these options and initiate a restart for IndOS, the Software Controller powers off and IndOS restarts the PC. Retentive data stored in PC mass storage or NVRAM is kept.

After restart, use the "Booting of the PC" option "IndOS and S7-1500 Software Controller" in the GRUB screen menu. After system start, the Software Controller is in RUN or assumes its previous state before POWER OFF. All retentive data are available again.

NOTE

Software Controller operating mode

You can check the operating mode of the Software Controller using the `s7_cpu_control` tool.

Reference

You can find additional information on setting the startup type in the STEP 7 online help.

Rebooting PC

IndOS does not support IndOS-only restarts. When restarting IndOS, the complete PC including the Software Controller is stopped and shut down and the system is restarted.

NOTE

IndOS shutdown behavior

If the Software Controller shuts down ungracefully, retentive data is lost. An ungraceful shutdown of the Software Controller can have the following reasons:

- A restart or shutdown of the Software Controller takes too long due to an interruption
 - The Software Controller is not reachable from IndOS due to a connectivity problem
 - The PCI configuration has changed, for example, by plugging or unplugging a network interface card, leading to a name change of the virtual Ethernet interface
-

NOTE

Rebooting or shutting down IndOS and the Software Controller

When rebooting or shutting down IndOS and the installed Software Controller, the following log message might sporadically appear:

"Failed unmounting /mnt/swcpu_mount".

Note that this occurrence has no negative functional impact on the system.

NOTE

Software Controller cycle time during system boot

Note that the cycle time of the Software Controller may increase during the boot of the system when IndOS and the Software Controller are starting.

For more information on the cycle time of CPUs, refer to the Cycle and Response Times (<https://support.industry.siemens.com/cs/ww/en/view/59193558>) function manual.

SFC 97 SHUT_DOWN instruction

You can shut down the PC from the Software Controller'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.

NOTE

Supported SHUT_DOWN modes

For IndOS, only the instruction "SHUT_DOWN: Shutdown target system"; MODE = 2 is supported.

When you use this instruction, the Software Controller restarts. IndOS is not shut down. All retentive data is saved.

Using an optional uninterruptible power supply (UPS)

IndOS supports the use of a UPS (for example, SITOP or other devices). To be able to use a UPS, proceed as follows:

1. Connect the UPS to the PC via USB.
The UPS notifies IndOS. 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.
2. Enter the command "s7_cpu_control --PowerOffCPU" in the shutdown script of the UPS.

6.4.1 Behavior of Software Controller when shutting down IndOS

Shutting down IndOS

You can shut down IndOS using the following actions:

- In case of graphical user interface, switch off the PC by clicking the corresponding button
- Shut down the PC via the command-line command "shutdown"

When you restart the PC, the Software Controller starts as previously configured.

NOTE

Preventing immediate system reboots after IndOS fatal system errors and freeze scenarios

To prevent an immediate reboot of the system which may lead to losing retentive data of the Software Controller, proceed as follows:

1. Remove the "99-watchdog.conf" file from the following path:
"usr/lib/systemd/system.conf.d"
 2. Run the following command: update-initramfs -u
 3. Reboot IndOS
-

Loss of retentive data when shutting down and restarting IndOS

If the following three conditions are met, retentive data might be lost after shutting down and restarting IndOS:

- You have configured retentive data
- You have set a password for the "No access" protection level or configured User Management & Access Control (UMAC)
- You have downloaded project data to the CPU

To avoid a loss of retentive data, use one of the following two workarounds.

Workaround 1

Use the `s7_cpu_control` tool and the password (and username for UMAC) to shut down the Software Controller, before shutting down and restarting IndOS.

Workaround 2

Save the password hash which belongs to the specified protection level in the TIA Portal project. For legacy protection, write a shell script to save the password hash to the internal graceful shutdown script of the Software Controller. For UMAC protection, write a shell script with the password itself and username.

NOTE

Security

We strongly recommend that you use the password hash (for UMAC, the password itself) of protection level "HMI access" for better security.

Also make sure that only root users can execute the shell script that you wrote.

After finishing the operation, the user should change to a standard user account for higher security.

The following workaround applies, if you are using the legacy "No access" protection level. To make sure that the Software Controller shuts down gracefully during a reboot of IndOS, you need to add additional information to the following configuration file:

`/etc/swcpushutdowncredentials.conf`

Reading and writing in this file requires root privileges. If you are using UMAC (User Management & Access Control) (Page 112), you also need to make sure that the 'expect' package is installed. For installing this package, use the following command: `apt-get install expect`

Configuration for legacy protection

If legacy protection is enabled on the device, enter the hash value of the relevant password for "HASH_OF_LEGACY_PASSWORD".

```
# For LEGACY utilization,  
# please edit only HASH_OF_LEGACY_PASSWORD value  
HASH_OF_LEGACY_PASSWORD="10074a6c83a03f68e8506087b91b3e7fe49a9dc9"
```

Figure 6-20 Legacy protection

Configuration for UMAC protection

If UMAC protection is enabled on the device, enter the values

"PLAINTEXT_OF_UMAC_USERNAME and PLAINTEXT_OF_UMAC_PASSWORD" as plaintext.

```
# For UMAC utilization,  
# please edit only PLAINTEXT_OF_UMAC_USERNAME and PLAINTEXT_OF_UMAC_PASSWORD values  
PLAINTEXT_OF_UMAC_USERNAME="userfail"  
PLAINTEXT_OF_UMAC_PASSWORD="Fail1234."
```

Figure 6-21 UMAC protection

After these steps, the password hash (for UMAC: password and user name) is saved to the internal graceful shutdown script of the Software Controller. The script is part of the installer package. The script is installed automatically.

NOTE

Password changes

Note that when changing the password in the TIA Portal project, you must run the same script using the hash of the new password.

If the password has not been changed, it is sufficient to only run the script once.

6.5 Communication

6.5.1 Communication with CPU using bridging

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

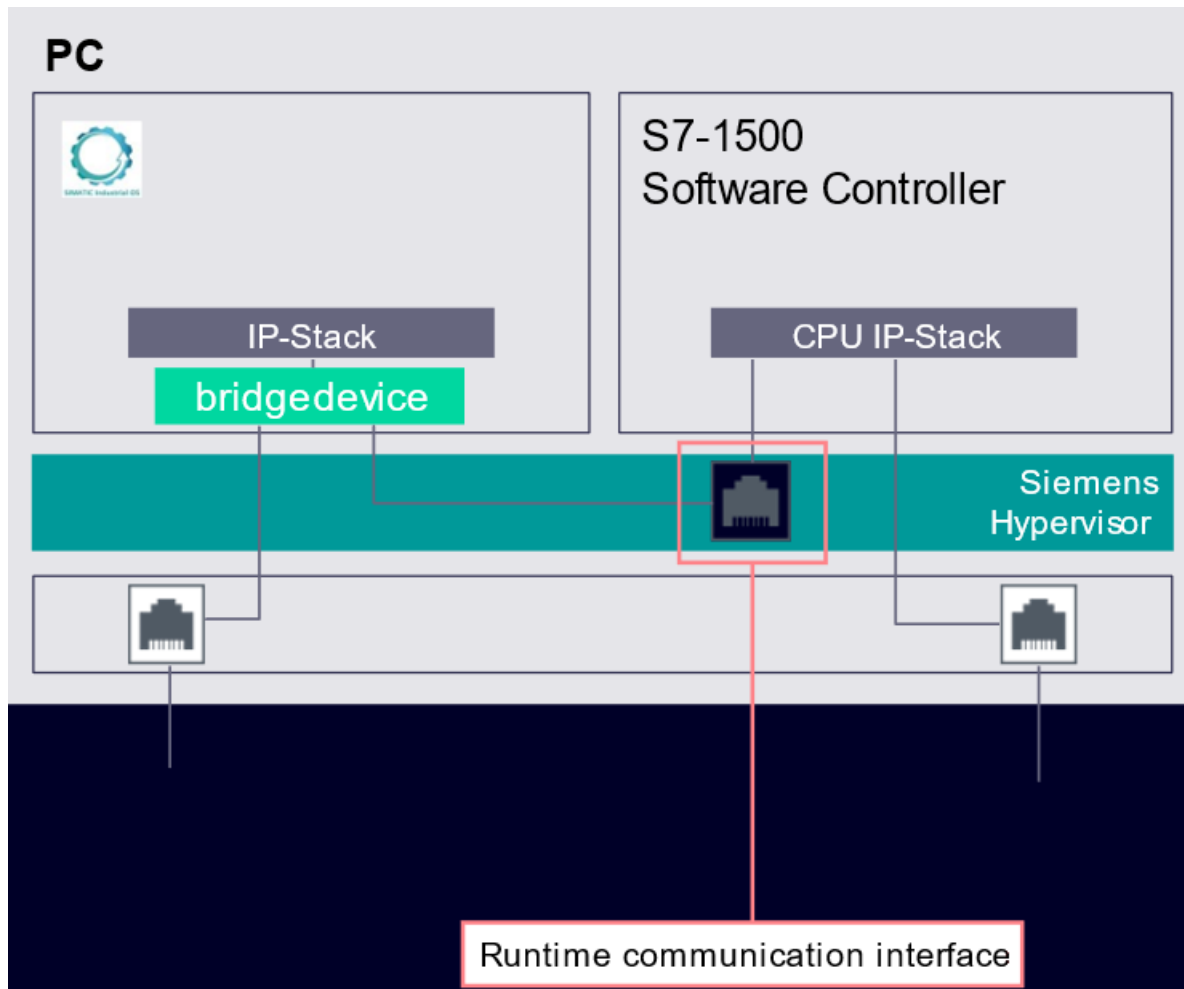


Figure 6-22 Communication with the CPU using bridging

The Siemens RT VMM Network adapter is bridged to one of the physical network interfaces with IndOS.

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 IndOS and the runtime communication interface are in the same IP subnet.

For bridging, proceed as follows:

1. If multiple CPU installations shall be used in one network:
 - make sure that the runtime communication interfaces of all CPUs have a unique MAC address within the network
 - if necessary, change the MAC addresses using the IP Config command line tool
2. 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.

3. Assign an IP address to the new IndOS bridging interface.
4. Assign an IP address to the CPU runtime communication interface in TIA Portal matching the network of the IndOS bridging interface for:
 - using STEP 7 online functions (when used on the same IPC)
 - downloading the configuration with IP address set
5. 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 runtime communication interface and SIMATIC RT-VMM Network Adapter use random MAC addresses from a defined range so that no conflicts are to be expected.
- The MAC address of the SIMATIC RT-VMM Network Adapter may be reused by IndOS for the bridging interface. The MAC address of the bridging interface might then be identical with the MAC address of the bridging interface or of the runtime communication interface of other CPUs. Thus, it can happen that the MAC address of the bridging interface is not unique within the network.
- If the runtime communication interface of more than one CPU within the same network accidentally uses the same MAC address, you need to assign unique MAC addresses to each of the interfaces.

To change the MAC address of the runtime communication interface use the IP Config command line tool and:

- create a new random address
- assign an own address (obtained from the relevant authority)

6.5.2 Communication with CPU using IP routing

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

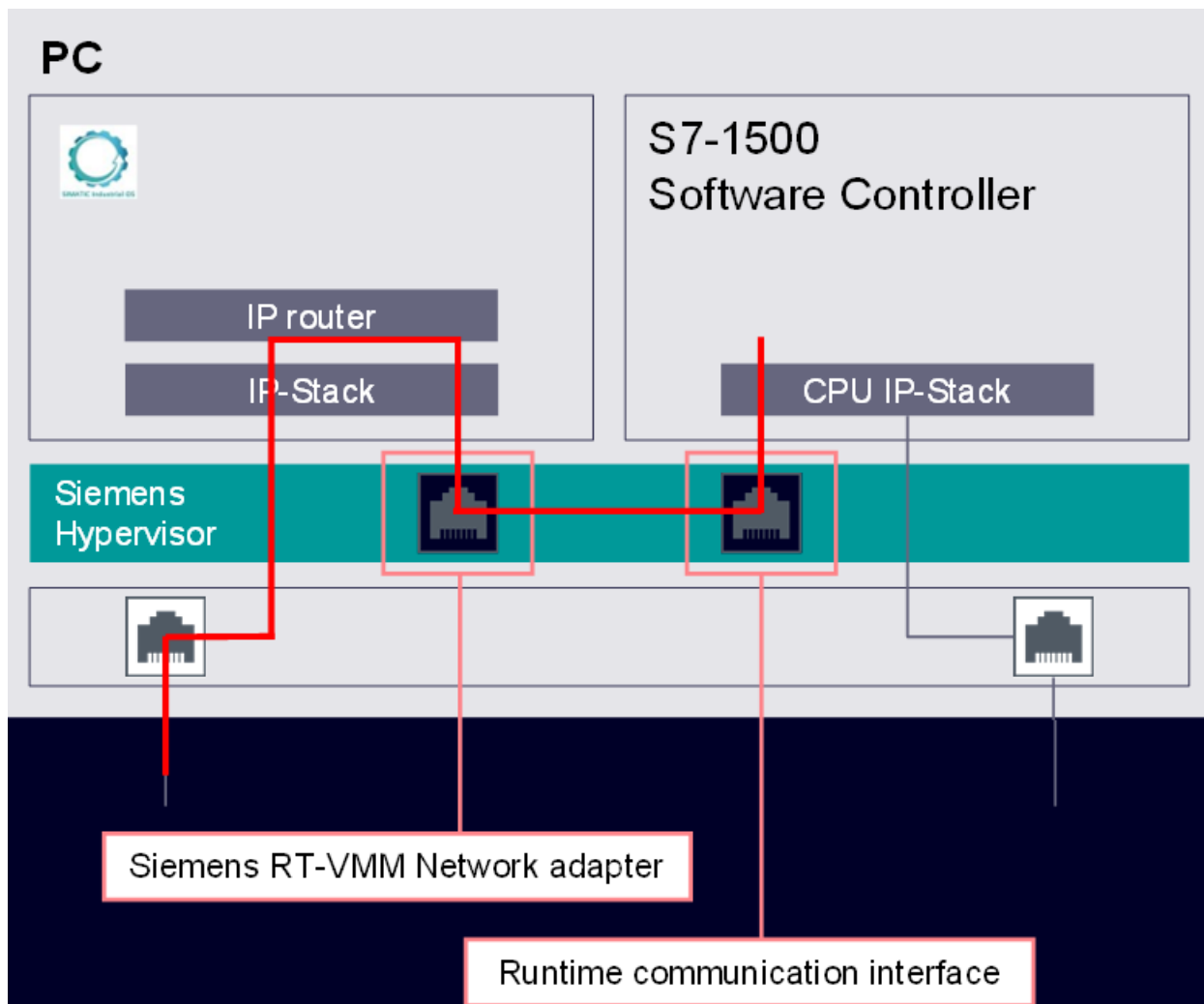


Figure 6-23 Communication with the CPU using IP routing

IP Routing is used to make a connection to a physical network interface using IndOS 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 it to the CPU (for example, using X2 or file import)
- Set the IP address for the SIMATIC RT-VMM Network Adapter
- Configure the IndOS 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.

Operation

7.1 Operation using command line commands

If the internal communication via the virtual Ethernet interface is established, you can control the CPU with the `s7_cpu_control` tool via command-line commands.

NOTE

Remote access from another device

The `s7_cpu_control` tool can run remotely on another device. To prevent external influence on the CPU, protect the TCP port with the port number "2024" in the firewall settings.

Requirement

The fifth partition is mounted in the file system.

Procedure

To use the `s7_cpu_control` tool, proceed as follows:

Execute the command `./s7_cpu_control`:

```
root@localhost:/mnt/swcpu_mount/SWCPU/bin# ./s7_cpu_control
```

NOTE

Call infotext in the command line

If you do not specify a parameter after the `./s7_cpu_control` command, a list with permitted commands and a description opens.

To change the operating state of the CPU, enter the required command:

```
./s7_cpu_control <Command>
```

Check the operating state of the CPU after each command input with the command `-- GetStatus`. This operation checks the actual execution result.

The following image shows a command sent to the CPU.

```
root@localhost:/mnt/swcpu_mount/SWCPU/bin#
root@localhost:/mnt/swcpu_mount/SWCPU/bin# ./s7_cpu_control --STOP
Command sent SUCCESSFULLY to SWCPU
root@localhost:/mnt/swcpu_mount/SWCPU/bin# ./s7_cpu_control --Getstatus
Current State: STOP
Command sent SUCCESSFULLY to SWCPU
root@localhost:/mnt/swcpu_mount/SWCPU/bin#
root@localhost:/mnt/swcpu_mount/SWCPU/bin#
```


Commands to control the CPU

The following table provides an overview of the command line commands supported by the CPU:

Command	Explanation
--PowerOnCPU	Starts the CPU in "STOP" mode. For more information on the transitions between the different operating modes, see section Operating mode transitions (Page 99).
--PowerOffCPU	Shuts down the CPU. Note that when powering off the CPU while the retentive memory is filled to capacity (100MB), an error message appears prompting you to restart Linux. Make sure that there is free retentive memory space available, before powering off the CPU. For more information on IndOS shutdown behavior, see section Shutdown and startup (Page 87).
--Run	Sets the CPU to "RUN" operating mode.
--Stop	Sets the CPU to "STOP" operating mode.
--GetStatus	Shows the operating mode of the CPU.
--MemoryReset	Resets the CPU memory.
--FactoryReset	Resets the CPU to factory settings.
--IP:	Identifies and stores the IP address of the runtime communication interface. Execute this command if the IP address already assigned has changed due to a download via STEP 7. Note: If you change the IP address, use the s7_cpu_control tool once with the new IP address. This approach allows you to make sure that the new IP address is saved successfully. Otherwise, retentive data is lost after IndOS reboot. If the new IP address is saved successfully, the following example message appears: Successfully saved IP address as 192.168.73.84
--GetSerialNumber	Displays the serial number of the CPU.
--username together with --pwd	Used for the commands requiring a password legitimization, for example: root@localhost:~# s7_cpu_control --username userfailsafe -run --pwd Password:

NOTE

Changing the operating mode of a CPU

Users added to the user group "software_controller_operators" in the computer administration allows you to change the operating state of a CPU. The user who executes this command must be part of this user group.

As of V30.1 installation, user groups are automatically created. The system administrator must add users to the appropriate user group(s).

The command can also be executed when a protection level is configured for the CPU.

Parameters of the s7_cpu_control tool

The following table provides an overview of the s7_cpu_control tool parameters:

Parameter	Explanation
--Force	Skips the warning and sets the CPU to the "STOP" operating mode.
--DumpServiceData	Saves service data to a etc/swcpu folder. Returns a success message.
--DumpServiceData=/etc/myFolder	Saves service data to a etc/myFolder. Returns a success message.
--DumpServiceData=SomeInvalidPath	The s7_cpu_control tool returns the following error message "Failed to save servicedata".

7.2 Operating modes

7.2.1 Basic principles

Introduction

Operating modes describe the states of the CPU. You can set the following operating modes via the Web server, the s7_cpu_control tool or STEP 7.

- RUN
- STOP

In these operating modes, the CPU can communicate, for example, via the PN/IE interface. Status LEDs indicate the current operating mode.

Reference

You can find additional information in the STEP 7 online help.

7.2.2 Operating mode transitions

Operating modes and operating mode transitions

The following figure shows the operating modes and the operating mode transitions:

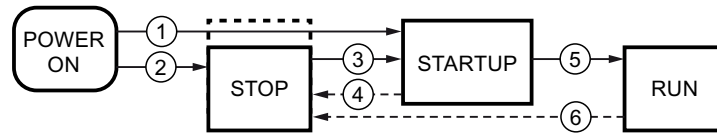


Figure 7-1 Operating modes and operating mode transitions

No.	Operating mode transitions	Conditions
①	POWER ON → STARTUP	After switching on, the CPU goes to "STARTUP" mode if: <ul style="list-style-type: none"> The hardware configuration and program blocks are consistent. The start-up type "Warm restart - RUN" is set or the start-up type "Warm restart - mode before POWER OFF" is set and RUN mode was active before POWER OFF. Non-retentive memory is cleared. 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: <ul style="list-style-type: none"> The hardware configuration and program blocks are not consistent or The "No restart" startup type is set Non-retentive memory is cleared. 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: <ul style="list-style-type: none"> The hardware configuration and program blocks are consistent. The CPU is set to "RUN" by the programming device. Non-retentive memory is cleared. 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: <ul style="list-style-type: none"> 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 the "RUN" mode in the following cases of "START-UP": <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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.

Maintenance

8.1 BIOS update

BIOS settings after updating the BIOS of the IPC

After you have updated the BIOS, make sure that 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 "VMM" is first in the boot order.
3. If the boot option "VMM" is not first in the boot order, move the boot option "VMM" 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 "VMM" to the first position in BIOS Setup Boot → EFI.

NOTE

"VMM" boot option

You may have to boot the IndOS operating system once and then return to BIOS Setup before the boot option "VMM" will be shown under the boot options.

8.2 Firmware updates 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 the firmware of an I/O module centrally or distributed.


Requirement

- You have downloaded the file(s) for the firmware update from the Customer Support (<https://support.industry.siemens.com/cs/ww/en/ps>) web site.
On this web site, select: Automation technology > Automation systems > SIMATIC industrial automation system > Controllers > SIMATIC S7 modular controllers > SIMATIC S7-1500.
From there, navigate to the specific type of module that you want to update. To continue, click on 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

You can carry out the firmware update in STEP 7 (online) or via the Web server.

Installation of the firmware update

 WARNING
Impermissible plant states possible Due to the installation of the firmware update, the CPU enters the STOP mode. The STOP mode 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, make sure that the CPU is not executing any active process.

Procedure using STEP 7

To carry out an online firmware update in STEP 7, proceed as follows:

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. To select the path to the firmware update files, click the "Browse" button in the "Firmware update" area.
5. Select the matching firmware file.
The table in the firmware update area lists all modules for which an update is possible with the selected firmware file.
6. Click the "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

For further information on the procedure, refer to the STEP 7 online help.

8.3 Resetting the CPU

During a reset, the CPU is set to the "delivery state". This means that information stored on the CPU, such as retentive data, is deleted.

The following reasons may require a data reset:

- A restart with the original data (cold restart)
- Reset all internally persistent settings (for example, IP address) for a defined status
- Use a cleaned state of the CPU for new projects

Reset options

To reset the CPU, you have the following options:

- **Memory reset:** The CPU is reset to the project settings configured by default. You can execute this functionality via the "--MemoryReset" command of the s7_cpu_control tool. A general reset only clears the work memory of the CPU.
- **Factory settings:** CPU is reset to the default factory settings. You can execute this functionality in STEP 7 or via the "-- FactoryReset" command of the s7_cpu_control tool.

NOTE

STOP mode required

The CPU must be in STOP mode to be reset.

8.3.1 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".

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.

8.4 Special features

8.4.1 Special situations when downloading in STEP 7

No connection possible

To download the project to the target system, establish an online connection.

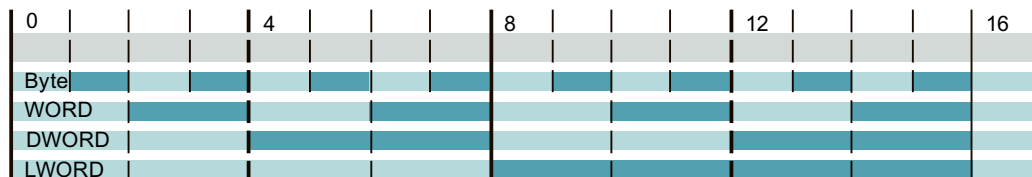
If an online connection to the target system is not possible, check the interface settings, such as the IP address.

8.4.2 Timeouts

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).

8.4.3 Assignment of addresses with absolute addressing

To ensure optimum runtime during access to 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.

8.4.4 "Autonegotiation" port setting

Optimizing port settings on the IO device and IO controller

The transfer medium and the duplex option are checked during startup of the IO device for control unit wiring. 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, the time for negotiating the transmission rate during startup is saved.

Reference

You can find more information on the topic "Cabling rules with disabled autonegotiation" in the STEP 7 online help.

8.5 Backup and restore

Once you have configured the computer for your application, you can create an image of your system. You can use this image to restore your user-specific application to your system at a later time, if necessary.

You should back up an image of your configuration for the following reasons:

- To save a fixed intermediate status of the configuration.
- Create a backup of the current configuration in case of hardware problems and when the PC must be replaced.
- Create a master image which can be restored on other PCs.

8.5.1 SIMATIC IPC Image & Partition Creator

"SIMATIC IPC Image & Partition Creator" is used to back up and restore files, directories, partitions and entire hard drives. "SIMATIC IPC Image & Partition Creator" prevents data loss caused by:

- Hardware failure
- Installation problems
- Operating errors
- External influences (viruses)

NOTE

Restoration of images on a larger CFast card

If you want to restore an image from a smaller CFast card on a larger CFast card, do not change the size of the partitions proportionally.

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.

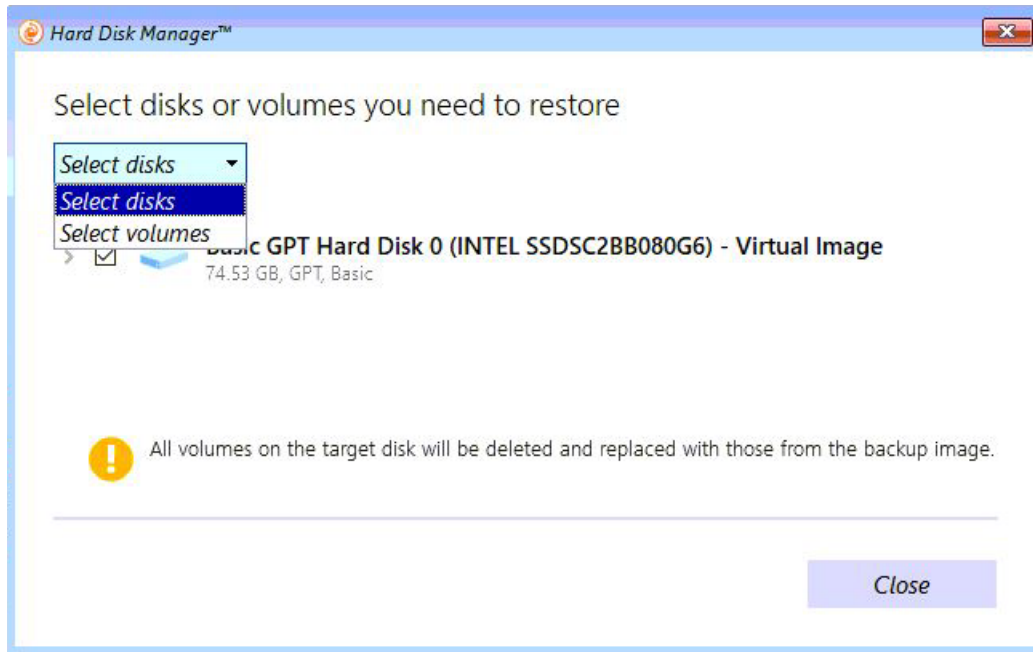


Figure 8-1 Changing the default restore type

After changing the restore type and clicking "Close", the following window appears. On this window, click on "Restore now".

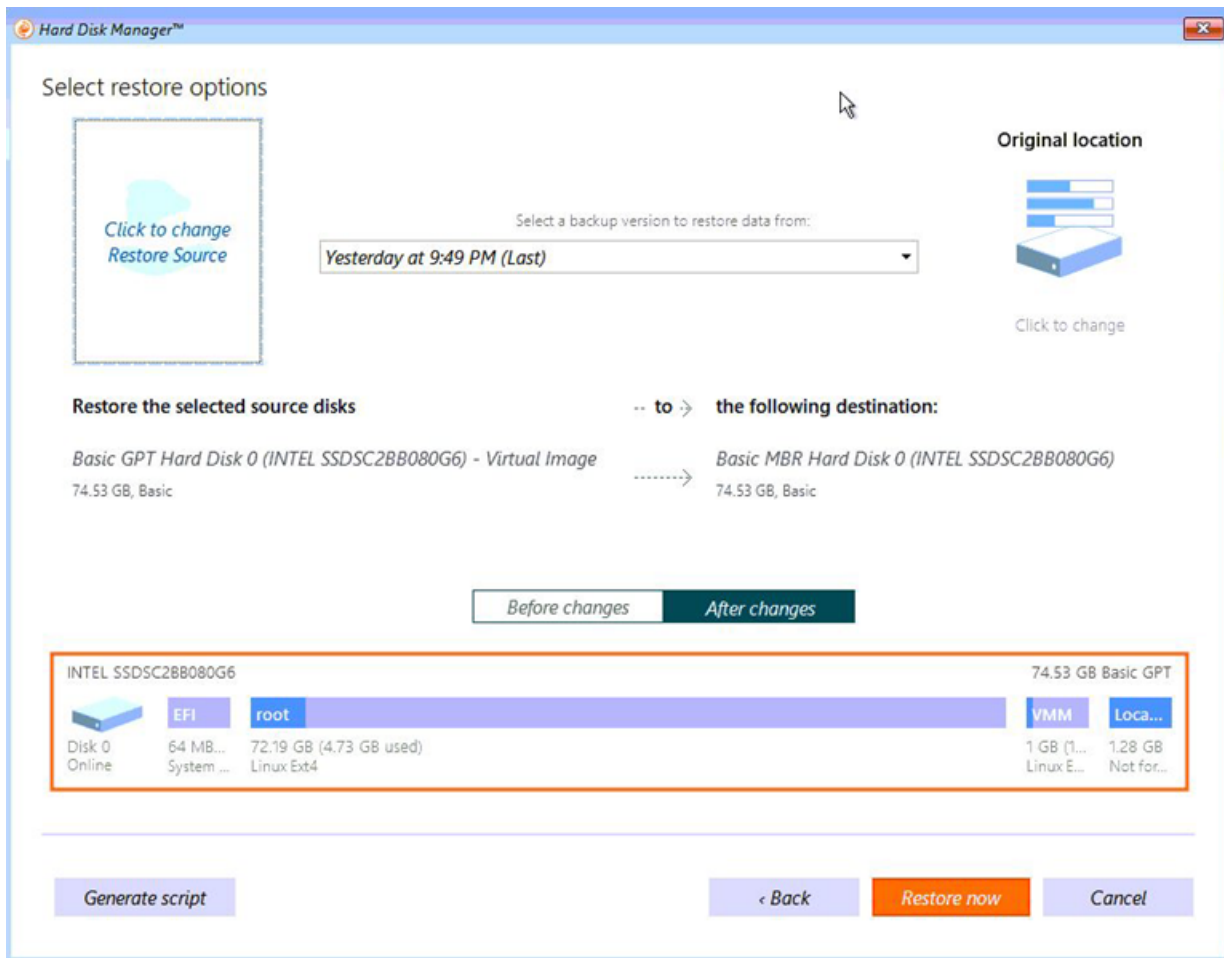


Figure 8-2 Disk to disk restore dialog

After finishing the restore, the following message appears.

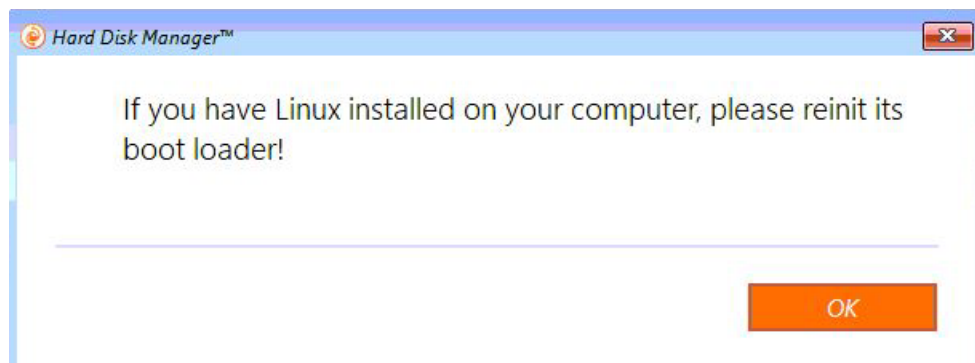


Figure 8-3 Reinit Linux boot loader

To confirm and reinitialize the Linux boot loader, click OK.

Restoring images with Image & Partition Creator V3.5 and V3.6

Image & Partition Creator V3.5 and V3.6 do not preserve symbolic links.

For this reason, there is a separate script (`after_disk_restore.sh`) provided in the Software Controller setup bundle. After a disk restore or clone operation in Image & Partition Creator, run this script to fix symbolic links.

Automatic default option

If you use the script without providing any arguments, the automatic option is selected by default. You should use the automatic option, if you did not create any separate partition independently from IndOS and the Software Controller.

The following image is an example for running the script without providing any argument:

```
root@localhost:~# ./after_disk_restore.sh
SUCCESS!
```

Figure 8-4 Script without providing any argument

Using the '-a' option

The behavior of the '-a' option is the same as the automatic default option. If you use '-a', you set the auto mode and the Software Controller is installed on the fifth partition of the boot disk.

```
root@localhost:~# ./after_disk_restore.sh -a
SUCCESS!
```

Figure 8-5 Automatic option

Using the '-m' option

Use the '-m' option together with the full path of the Software Controller disk partition, if you want to provide the Software Controller partition manually.

The following image is an example for running the script using the '-m' argument:

```
root@localhost:~# ./after_disk_restore.sh -m /dev/sdb5
SUCCESS!
```

Figure 8-6 Manual option

Using the '-f' option

If you use the '-f' option, the system reboots automatically after the execution to apply the changes. Alternatively, you can use the '-a' option together with the '-f' option to enable the automatic option and an automatic reboot. If you want to use the '-m' option following by an automatic reboot, use '-m' and '-f'.

The following image is an example for running the script using the '-f' argument:

```
root@localhost:~# ./after_disk_restore.sh -f
SUCCESS!
```

Figure 8-7 Force option

The following image is an example for running the script using the '-m' and '-f' arguments:

```
root@localhost:~# ./after_disk_restore.sh -m /dev/sdb5 -f
SUCCESS!
```

Figure 8-8 Manual and force options

Using the '-h' option

The '-h' option displays the help screen:

```
root@localhost:~# ./after_disk_restore.sh -h

Siemens AG Copyright © 2021

'after_disk_restore.sh' is a Bash script that must be executed after
disk restore or clone operations by automatically or manually.

If no argument is given to the script, it will run in automatic mode.
Alternatively, '-a' argument could be given as another option to enable
automatic mode. In this case, the fifth partition of the disk is selected
where SWCPU is installed. If any partition is not created manually and
the existing partitions are created during IndOS and SWCPU installation
processes, the automatic option would be preferred. Otherwise, the manual
option is recommended. If the manual option is selected, '-m' argument
must be given and the disk partition where SWCPU is installed must be
given as a next argument. A reboot is required to apply these changes.
Therefore, only at the end of the successful operation, the reboot will
be triggered according to the result of user input. On the other hand,
if '-f' argument is given, a reboot will be done immediately without
asking user.

Please check the following examples:

Usage of automatic option           : after_disk_restore.sh
Alternative usage of automatic option : after_disk_restore.sh -a
Usage of automatic option with a force option : after_disk_restore.sh -a -f
Usage of manual option              : after_disk_restore.sh -m /dev/sdXY
Usage of manual option with a force option : after_disk_restore.sh -m /dev/sdXY -f
```

Figure 8-9 Help screen

After running the script, reboot the system to apply the changes.

Protection

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 allowlist tools

Further measures for protecting the CPU

The following measures additionally increase the 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 time synchronization via an NTP Server
- Deactivation of the PUT/GET communication

NOTE

Functionalities disabled by default

These functionalities are deactivated by default. To use the functionalities, you 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 manual (<https://support.industry.siemens.com/cs/ww/en/view/59191792>).

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 the user "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 more than 8 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.automation.siemens.com/WW/view/en/59193560>) 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 function manual

(<https://support.automation.siemens.com/WW/view/en/59192925>).

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 S7-1500 System Manual (<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 112](#)) 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.

To limit access to specific functions, the CPU offers different access levels.

Access levels and CPU passwords limit the functions and memory areas that are accessible without password. The individual access levels as well as the entry of their associated passwords are specified in the object properties of the CPU.

Rules for passwords

Ensure that passwords are sufficiently secure. Passwords must not follow a machine-recognizable pattern.

Apply the following rules:

- Assign a password that is at least 8 characters long.
- Use different cases and characters: uppercase/lowercase, numbers, and special characters.

Access levels of the CPU

The following table provides you with 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 of fail-safe modules is excluded.
Read access	<p>With this access level, read-only access to the hardware configuration and the blocks is possible without entering a password. This means you can upload the hardware configuration and blocks to the programming device.</p> <p>In addition, the following is possible:</p> <ul style="list-style-type: none"> • HMI access • Access to diagnostics data • Display of offline/online comparison results • Changing the operating state (RUN/ STOP) • Setting time-of-day <p>However, you cannot download blocks or hardware configuration into the CPU without password.</p> <p>In addition, the following is not possible without a password: Writing test functions and firmware updates (online).</p>
HMI access	<p>With this access level only HMI access and access to diagnostics data is possible without the password.</p> <p>Without password, the following is not possible:</p> <ul style="list-style-type: none"> • Load blocks and hardware configuration into the CPU • Load blocks and hardware configuration from the CPU into the programming device • Test functions • Changing the operating mode (RUN/STOP) • Firmware update • Display of online/offline comparison status
No access (complete protection)	<p>When the CPU has complete protection, the following is not possible:</p> <ul style="list-style-type: none"> • Read or write access to the hardware configuration and the blocks • HMI access • Server function for PUT/GET communication (is disabled in this access level and cannot be changed) <p>Authentication with the password will again provide you full access to the CPU.</p>

An enumeration of which functions are available in the different access levels is available in the "Setting options for the protection" entry in the STEP 7 online help.

NOTE

Forced shutdown of the CPU

If you use the command `.ls7_cpu_control --poweroffcpu --force` in the `s7_cpu_control` tool to force a shutdown of the CPU, a password for the access level "No access (complete protection)" must have been specified before (if configured in TIA Portal).

Note that using the `--force` command to shut down the system might lead to a loss of retentive data, even if a password has been specified.

Properties of the access levels

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, it is not allowed to read or change the hardware configuration and the blocks. To obtain access to the CPUs, use an alternative parameter assignment in the properties of the CPU:

- A password for the protection level "No access (complete protection)"
- A different protection level, for example, "Full access (no protection)"

Communication between the CPUs (via the communication functions in the blocks) is not restricted by the access level of the CPU, unless PUT/GET communication is deactivated in the "No access" (complete protection) access level.

Entry of the right password allows access to all the functions that are allowed in the corresponding level.

NOTE

Configuring an access level does not replace know-how protection

Configuring access levels offers a high degree of protection against unauthorized changes on the CPU via network access. Access levels are used to restrict the rights to download the hardware and software configuration to the CPU. However, blocks are not write- or read-protected. To protect the code of blocks, use know-how protection.

Behavior of functions with different access levels

The STEP 7 online help includes a table listing the online functions available in the various access levels.

Assigning access protection parameters in STEP 7

NOTE

Parameter assignment for access protection for the entire PC system

Unlike for a hardware CPU, parameter assignment for access protection is not done directly in the CPU's properties. This ensures that consistent protection level passwords are configured for all of a PC system's components.

To assign the access levels for the CPU, follow these steps:

1. Select the PC system that is assigned to the CPU.
2. Open the properties of the PC system in the Inspector window.

- Open the "Protection" entry in the area navigation.

A table with the possible access levels appears in the Inspector window.

Access level	Access				Access permission
	HMI	Read	Write	Fail-safe	Password
<input type="radio"/> Full access incl. fail-safe (no protection)	✓	✓	✓	✓	
<input type="radio"/> Full access (no protection)	✓	✓	✓		
<input checked="" type="radio"/> Read access	✓	✓			
<input type="radio"/> HMI access	✓				
<input type="radio"/> No access (complete protection)					

Read access:
TIA Portal users will have read access to standard functions.
HMI applications can access all functions (fail-safe and standard).

Mandatory password:
For additional write access and access to the fail-safe functions, TIA Portal users need to enter the "full access incl. fail-safe" password.

Optional password:
For additional write access to standard functions without access to fail-safe functions, a "read/write access" password can be defined.

Enter password:

Confirm password:

Figure 9-1 Possible access levels

- 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.
- In the "Password" column, specify a password for the selected access level. In the "Confirmation" column, enter the selected password again to protect against incorrect entries.
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.
- Assign additional passwords as needed to other access levels if the selected access level allows you to do so.
- Download the hardware configuration to the CPU, so that the access level will take effect.
The configured protection level and the password become effective as soon as the data is downloaded to the CPU.

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>).

Forgotten or lost access level passwords

If you have forgotten or lost an access level password in case of an activated access protection, proceed as follows.

Options standard CPUs

For standard CPUs, chose one of the following possibilities:

- In the Resource Configurator, use the "-s, --set-initial" command to reset the hardware configuration and reconfigure your configuration. Then download a project without access level passwords.
- Import a suitable project (.psc file) without access level passwords.
- Reinstall the Software Controller.

Options for fail-safe CPUs

- Import a suitable project (.psc file) without access level passwords.
- Reinstall the Software Controller.

9.5.2 Locking protection levels with the PLC program

Introduction

To specify if passwords are legitimized for the CPU, you use the instruction "Limit and enable password legitimization" (ENDIS_PW). In this way, you can prevent legitimized connections, even if the correct password is known.

Inadvertent locking

If passwords are set up (all protection levels) and the output parameters of the password of the block "Limit and enable password legitimization" are set to "Disallow in RUN", you will be completely blocked.

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, enter the command-line command [\(Page 96\)](#) "/MemoryReset".

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 is 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 firewall

You can operate the CPU and all associated components on systems with activated firewall. Configure the firewall rules manually.

For Open User Communication, you can use application-specific IP ports. These ports are not enabled by default by the setup program. Due to the default settings, the firewall can thus prevent the connection. Therefore, configure the firewall rules for the Open User Communication yourself.

Configuring the firewall for Web server use

If you use a PC with an enabled firewall, you must configure the firewall for the use of the Web server. To open the application-specific ports in the firewall, create a new firewall rule for this purpose in the firewall settings.

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. The values are derived partly from the serial number of the PC motherboard and the PC mass storage. The serial numbers can therefore only be read at the corresponding points in the Web server or in the online diagnostics in STEP 7. 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 following option for setting up copy protection during in the configuration: "Serial number is inserted when downloading to a device or a memory card"

Reading out the serial number

You can read the serial numbers in the Web server on the "Diagnostics" web page under "Identification".

Reference

You can find additional information on setting up the copy protection in the STEP 7 online help.

Interrupts, diagnostics, error, and system messages

10.1 Status and error display of the CPU

Introduction

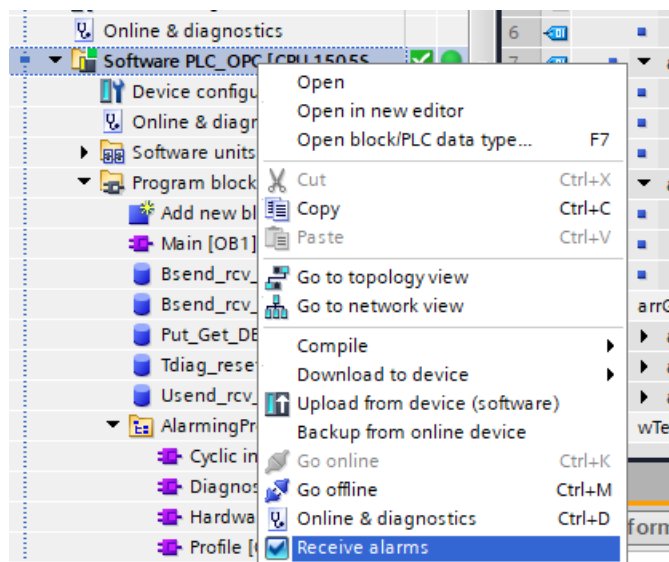
The status and error displays of the CPU are described below.

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 manual (<https://support.automation.siemens.com/WW/view/en/59192926>) function manual.

Acknowledge alarms

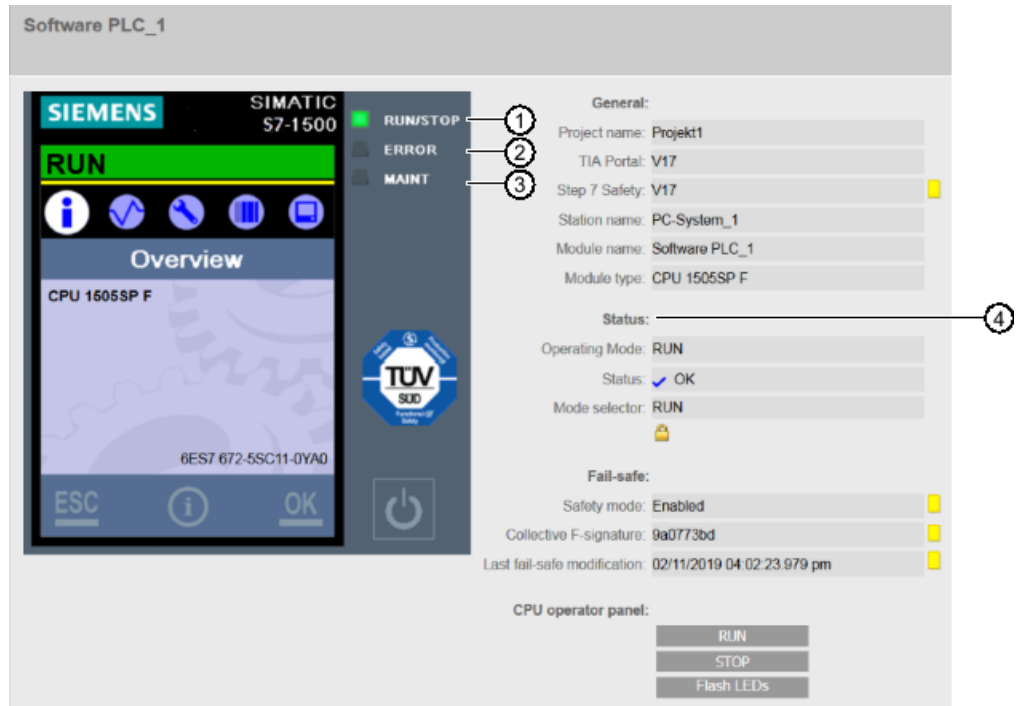
To be able to acknowledge alarms from TIA Portal for individual devices, proceed as follows:
In TIA Portal, activate the check box "Receive alarms" for the device, the alarms should be acknowledged for:



Status display

The status of the CPU is displayed at the following places:

- In STEP 7
- On the LEDs of the PC
- 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

Meaning of the LED displays

To indicate the current operating mode and diagnostic status, the CPU has three LEDs. The following table 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.
 LED green	 LED flashes red	 LED off	A diagnostics event is pending.

RUN/STOP LED	ERROR LED	MAINT LED	Meaning
 LED green	 LED off	 LED yellow	Maintenance demanded for the plant. The affected hardware must be replaced within a short period of time.
 LED green	 LED off	 LED flashes yellow	Maintenance required for the plant. The affected hardware must be replaced within a reasonable time period.
 LED green	 LED flashes red	 LED off	An error has occurred.
 LED yellow	 LED flashes red	 LED off	
 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 defective
 LED flashes yellow	 LED off	 LED off	CPU is performing internal activities during STOP, e.g. ramp-up after STOP. Loading the user program.
 LED flashes yellow	 LED off	 LED off	CPU is in HOLD state. A programmed breakpoint in the user program has been reached.
 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 by remote access even from several computers connected by a network.

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 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.

10.3.2 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.automation.siemens.com/WW/view/en/59193560>) function manual.

Technical Data

Technical specifications

You can find the latest technical data under the following link on the Siemens Industry Online Support.

CPU	Article number	Technical specifications
CPU1505SP	cannot be ordered, since only available preinstalled on a CPU 1515SP PC2 (F)	CPU 1515SP PC2 (https://support.industry.siemens.com/cs/ww/en/pv/6ES7677-2DB43-0GB0/td?dl=en)
CPU1505SP F		CPU 1515SP PC2 F (https://support.industry.siemens.com/cs/ww/en/pv/6ES7677-2SB43-0GB0/td?dl=en)
CPU 1507S	6ES7672-7AD02-0YG0	CPU 1507S (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-7AD01-0YG0/td?dl=en)
CPU 1507S F	6ES7672-7FD02-0YG0	CPU 1507S F (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-7FD01-0YG0/td?dl=en)
CPU 1508S	6ES7672-8AD02-0YG0	CPU 1508S (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-8AD01-0YG0/td?dl=en)
CPU 1508S F	6ES7672-8FD02-0YG0	CPU 1508S F (https://support.industry.siemens.com/cs/ww/en/pv/6ES7672-8FD01-0YG0/td?dl=en)

Reference information for use with SIMATIC IPC

B.1 Permitted commands and parameters

To configure and operate the CPU, different commands and parameters are available for the respective tools. This section lists the commands and parameters of the individual tools.

Commands and parameters in the s7_cpu_control tool

To be able to use the commands, start the s7_cpu_control tool with ".s7_cpu_control", for example:

```
root@localhost:/mnt/swcpu_mount/SWCPU/bin# .s7_cpu_control --MemoryReset
```

Command	Explanation
--PowerOnCPU	Starts the CPU in "STOP" mode.
--PowerOffCPU	Shuts down the CPU. For more information on IndOS shutdown behavior, see section Shutdown and startup (Page 87).
--Run	Sets the CPU to "RUN" operating mode.
--Stop	Sets the CPU to "STOP" operating mode.
--GetStatus	Shows the operating mode of the CPU.
--MemoryReset	Resets the CPU memory.
--FactoryReset	Resets the CPU to factory settings.
--IP:	Identifies and stores the IP address of the runtime communication interface. Execute this command if the IP address already assigned has changed due to a download via STEP 7.
--username together with --pwd	Used for the commands requiring a password legitimization, for example: root@localhost:~# s7_cpu_control --run --username userfailsafe --pwd
--pwd (without username for legacy access control complete protection)	Using a password command without username, for example: root@localhost:~# s7_cpu_control --get status --pwd

To be able to use the parameters, start the s7_cpu_control tool with ".s7_cpu_control".

Parameter	Explanation
--Force	Skips the warning and sets the CPU to the "STOP" operating mode
--DumpServiceData	Saves service data to a etc/swcpu folder. Returns a success message.
--DumpServiceData=/etc/myFolder	Saves service data to a etc/myFolder. Returns a success message.
---DumpServiceData=SomeInvalidPath	The s7_cpu_control tool returns the following error message "Failed to save servicedata".

B.1 Permitted commands and parameters

The following table shows additionally command line commands that are available for F-CPU:

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

Parameters in the Management Tool for MAC Addresses

To be able to use the parameters, start the Management Tool with ".ls7_vnic_macconfig".

Parameter		Explanation
-m	-mount-path	Parent directory of "SWCPU"
-t	--target	Specifies the interface whose MAC address has changed <ul style="list-style-type: none"> • IndOS: SIMATIC RT-VMM Network Adapter • Software Controller: Runtime communication interface
-a	--mac-addr	Assigns new MAC address
-d	--default-mac	Assigns default value for MAC address

Parameters in the IPConfig Tool

To be able to use the parameters, start the IPConfig Tool with `./s7_vnic_ipconfig`. The parameters are case-sensitive.

Parameter		Explanation
-n	--nic	Name of the IndOS runtime communication interface via which the request is sent. To display the name, list all interfaces using the command "ip addr". root@debian:/mnt/SWCPU/bin# ip addr The interface with a MAC address between "28-63-36-78-B0-00" and "28- 63-36-78-BF-FF" is the runtime communication interface.
-m	--mac	MAC address of the runtime communication interface from the CPU. Use the Management Tool for MAC Addresses with the parameter "-m" to display the MAC addresses of the interfaces. root@debian:/mnt/media/SWCPU/bin# ./s7_vnic_macconfig -m
-s	--setip	IP address assigned by the CPU for the runtime communication interface.
-t	--setmask	Network mask assigned by the CPU for the runtime communication interface.
-g	--setgw	Gateway that is assigned by the CPU for the runtime communication interface.

NOTE

Assigning IP addresses

IP address assignment to SIMATIC RT-VMM Network Adapter can be done by generic Linux commands such as "nmcli" or by editing the network file located under /etc/NetworkManager. `s7_vnic_ipconfig` can also be used.

For the Software Controller side of vNIC, `s7_vnic_ipconfig` must be used.

After running the `s7_vnic_ipconfig` tool to assign an IP address to the runtime communication interface of the CPU, check the operation result.

To make sure that assigning the IP address was successful, check if the assigned IP address is reachable by using the ping command.

NOTE

Assigning IP address in RUN operating state

If you use the `s7_vnic_ipconfig` tool to assign a new IP address while the CPU is in RUN, make sure that the option "IP address is set directly at the device" is set in TIA Portal.

If this option is not set, the GetStatus command will be "Failed" in the IPC Config Tool. When pinging the new IP address, the error message "Destination Host Unreachable" appears.

Command line parameters valid for all tools

The following table shows commands which can be used for all tools.

Parameter	Explanation
--Help	Displays the info text in the command line editor
--Version	Displays the versions of the tool

NOTE

Version numbers

The version numbers of individual tools might be different from the firmware version of the Software Controller. You can find the Software Controller firmware version under `/mnt/swcpu_mount/SWCPU/version_info`.

The version number stored in the `version_info` file (for example, 21.09.00.00_54 .01.00.07) is an internal version number which corresponds to the official Software Controller version (for example, 21.9).

B.2 SIMATIC IPC227G / IPC277G (PRO)

If you are using these PCs supported by the CPU, 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 rating plate of your SIMATIC IPC.
BIOS version	V28.01.06	
	Recommended BIOS Settings:	
	<ul style="list-style-type: none"> • 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 IndOS restart. For this reason, we recommend hiding the TPM module to avoid timeouts.	
Operating systems	SIMATIC Industrial OS V3.4.2	
Boot method	UEFI boot	
Graphics driver		
LED use	IPC227G: Supported, configurable IPC277G: Not supported	
Mass storage		
Using onboard interfaces for PROFINET:		
PN / IE (LAN) X1	Yes (either X1 or X2 at a time)	To be configured in Resource Configuration file
PN / IE (LAN) X2	Yes (either X1 or X2 at a time)	
PN / IE (LAN) X3	not supported	

NOTE**IndOS fatal system error (kernel panic) or freeze scenarios on an IPC227G**

If an IndOS fatal system error or system freeze occurs on an IPC227G, the IPC will remain in this error state.

To set the system to automatically recover after such an error, proceed as follows:

1. Open the following file: `/etc/sysctl.conf`
2. Add the following line to the file: `kernel.panic = 30`
3. Reboot the system.

B.3 SIMATIC IPC427E / IPC477E (PRO)

If you are using these PCs supported by the CPU, 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 rating plate of your SIMATIC IPC.
BIOS version	V21.01.18	
	Recommended BIOS Settings:	
	<ul style="list-style-type: none"> • Power → Power and Performance → CPU-Power Management Control → CPU Power Level = Determinism Optimized • Security → Current TPM device = Hidden (Not Detected, if no TPM available) 	
	Hiding TPM module Hiding the TPM module will decrease jitter on IndOS restart. For this reason, we recommend hiding the TPM module to avoid timeouts.	
Operating systems	SIMATIC Industrial OS V3.4.2	
Boot method	UEFI boot	
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
PN / IE (LAN) X3	Yes	

B.4 SIMATIC BX-39A / PX-39A (PRO)

If you are using these PCs supported by the CPU, note the following reference information for your device:

	Property	Notes
Hardware version	BX39A: FS ≥ AA PX39A: FS ≥ AA	The hardware version can be found on the rating plate of your SIMATIC IPC.
BIOS version	V29.01.03	
	Mandatory BIOS settings: <ul style="list-style-type: none"> Advanced → System Agent (SA) Configuration → VMD Setup Menu → Enable VMD Controller = Disabled Advanced → System Agent (SA) Configuration → Above 4GB MMIO BIOS Assignment = Disabled Setup Utility → Security → Trusted Platform Module (TPM) = Hidden Note: If no TPM is available in the system, then this setting is not relevant. Recommended BIOS settings: <ul style="list-style-type: none"> Advanced → Power and Performance → CPU-Power Management Control → Power & Performance Scenario = Max Performance Advanced → Power and Performance → CPU-Power Management Control → Intel Speedstep = Disabled Advanced → Power and Performance → CPU-Power Management Control → Intel Speed Shift Technology = Disabled Advanced → Power and Performance → CPU-Power Management Control → HDC Control = Disabled Advanced → Power and Performance → CPU-Power Management Control → C States = Disabled Note: These mandatory and recommended BIOS settings will be set automatically during installation. For more information on these automatic settings during installation, refer to chapter Installing the Software Controller (Page 52) .	
Operating systems	SIMATIC Industrial OS V3.4.2	
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 to 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

IndOS fatal system error (kernel panic) or freeze scenarios on a BX-39A

If an IndOS fatal system error or system freeze occurs on a BX-39A, the IPC will remain in this error state.

To set the system to automatically recover after such an error, proceed as follows:

1. Open the following file: **/etc/sysctl.conf**
 2. Add the following line to the file: **kernel.panic = 30**
 3. Reboot the system.
-

Additional information

C.1 Siemens Industry Online Support

You can find current information on the following topics quickly and easily here:

- **Product support**
All the information and extensive know-how on your product, technical specifications, FAQs, certificates, downloads, and manuals.
- **Application examples**
Tools and examples to solve your automation tasks – as well as function blocks, performance information and videos.
- **Services**
Information about Industry Services, Field Services, Technical Support, spare parts and training offers.
- **Forums**
For answers and solutions concerning automation technology.
- **mySupport**
Your personal working area in Industry Online Support for messages, support queries, and configurable documents.

This information is provided by the Siemens Industry Online Support in the Internet (<https://support.industry.siemens.com>).

C.2 Industry Mall

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

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

Index

A

Access levels, [113](#)
Access protection, [112](#)

B

BIOS, [53](#)

C

CFast card, [105](#)
Commands, [125](#)
Communication, [40](#)
CP 1625, [48](#), [62](#)
CPU Control Tool, [96](#)
 Remote access, [96](#)
CPU memory area, [46](#)
Cycle time, [88](#)

D

Diagnostics, [41](#)
 Web server, [41](#)
 LEDs, [120](#)
 Status display, [120](#)
 Exporting data, [122](#)
 Information about STEP 7, [122](#)
 Web server, [123](#)

E

Error messages, [77](#), [86](#)

F

Factory settings, [97](#), [103](#), [103](#), [125](#)
Fail-safe CPUs, [113](#), [115](#)

G

GNOME, [53](#)

GRUB screen, [87](#)

H

Hash value
 for installed files, [58](#)
 for passwords, [90](#)

I

Integrated security, [42](#)
Intel i210, [62](#)
Interfaces, [48](#), [70](#)
Introduction, [39](#)
IP address, [97](#), [103](#), [125](#), [127](#)
IPConfig Tool, [127](#)

K

Know-how protection, [118](#)

L

LEDs, [68](#), [120](#)
Linux, [15](#)
Load memory, [45](#)

M

MAC address, [126](#), [127](#)
Management Tool for MAC Addresses, [126](#)
Mass storage, [47](#)
Motion control functions, [42](#)
Mount points
 Resource Configurator, [62](#)

N

Naming conventions, [8](#)
Network interface card, [72](#)

NTP Server, [110](#), [111](#)

NVRAM, [45](#), [48](#), [69](#)

O

Open Controller, [40](#), [52](#), [73](#)

P

Password, [111](#), [112](#), [114](#), [116](#)

Password provider, [43](#)

PCI Express, [104](#)

Properties

Of the Software Controller, [40](#)

Properties of PROFINET IO, [49](#)

Protection levels, [113](#)

PUT/GET instructions, [111](#), [111](#)

R

Remote repository, [54](#)

Retentive memory , [45](#)

S

Security functions, [110](#)

Notes, [111](#)

Access protection using STEP 7, [112](#)

Protecting blocks, [117](#)

Service stick, [54](#)

Setting up copy protection, [118](#)

Setup, [54](#)

SFC 97 SHUT_DOWN, [89](#)

SIMATIC Diagnostics Tool, [122](#)

Status display, [120](#)

Symbolic links, [108](#)

T

Technical properties, [40](#)

Technology functions, [41](#)

Tools

CPU Control Tool, [96](#)

SIMATIC Diagnostics Tool, [122](#)

CPU Control Tool, [125](#)

Management Tool for MAC Addresses, [126](#)

IPConfigTool, [127](#)

Trace, [41](#)

U

UPS, [47](#), [89](#)

USB, [89](#)

V

Validity, [7](#)

W

Web browser, [50](#)

Web browsers, [50](#)

Work memory, [44](#)