SIEMENS

SINUMERIK / SIMOTION / SINAMICS
Motion Control Industrial Security

Configuration Manual

05/2017
6FC5397-5EP40-6BA0

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens AG
Division Digital Factory
Postfach 48 48
90026 NÜRNBERG
GERMANY

Document order number: 6FC5397-5EP40-6BA0
℗ 04/2017 Subject to change

Preface

SINUMERIK documentation

The SINUMERIK documentation is organized into the following categories:

- General documentation/catalogs
- User documentation
- Manufacturer/service documentation

Additional information

You can find information on the following topics at the following address (https://support.industry.siemens.com/cs/de/en/view/108464614):

- Ordering documentation/overview of documentation
- Additional links to download documents
- Using documentation online (find and search in manuals/information)

If you have any questions regarding the technical documentation (e.g. suggestions, corrections), please send an e-mail to the following address (mailto:docu.motioncontrol@siemens.com).

mySupport/Documentation

At the following address (https://support.industry.siemens.com/My/ww/en/documentation), you can find information on how to create your own individual documentation based on Siemens' content, and adapt it for your own machine documentation.

Training

At the following address (http://www.siemens.com/sitrain), you can find information about SITRAIN (Siemens training on products, systems and solutions for automation and drives).

FAQs

You can find Frequently Asked Questions in the Service&Support pages under Product Support (https://support.industry.siemens.com/cs/de/en/ps/faq).

SINUMERIK

You can find information about SINUMERIK at the following address (http://www.siemens.com/sinumerik).

SIMOTION

You can find information about SIMOTION at the following address (https://www.siemens.com/simotion).

SINAMICS

You can find information about SINAMICS at the following address (https://www.siemens.com/sinamics).

Target group

This documentation is intended for manufacturers of machine tools / production machines, particularly:

- Planners and project engineers
- IT departments of end users and OEMs

The following knowledge is a prerequisite for implementing the described security concepts:

- Administration of the IT technologies familiar from the office environment
- Configuration of the SINUMERIK/SIMOTION/SINAMICS products used

Benefits

The "Industrial Security" documentation contains the necessary measures and information for planning and configuring systems or plants. The documentation serves as a reference manual and guideline. This documentation cannot and does not want to suggest that there is 100% security because the current threat scenario is much too diverse and complex.

This documentation includes all of the necessary measures that should be taken into account for configuring systems in a secure environment. This documentation is intended to support machine manufacturers in safely operating their controls or plants. You, as operator, are responsible for implementing the security measures.

Technical Support

Country-specific telephone numbers for technical support are provided in the Internet at the following address (https://support.industry.siemens.com/sc/ww/en/sc/2090) in the "Contact" area.

Table of contents

Fundamental safety instructions

1

1.1 General safety instructions

⚠ WARNING

Danger to life if the safety instructions and residual risks are not observed

If the safety instructions and residual risks in the associated hardware documentation are not observed, accidents involving severe injuries or death can occur.

- Observe the safety instructions given in the hardware documentation.
- Consider the residual risks for the risk evaluation.

⚠ WARNING

Danger to life or malfunctions of the machine as a result of incorrect or changed parameterization

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameterization (parameter assignments) against unauthorized access.
- Respond to possible malfunctions by applying suitable measures (e.g. EMERGENCY STOP or EMERGENCY OFF).

1.2 Industrial security

Note

Industrial security

Siemens provides products and solutions with industrial security 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 security concept. Siemens products and solutions only represent one component of such a concept.

The customer is responsible for preventing unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit:

Industrial security (http://www.siemens.com/industrialsecurity).

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at:

Industrial security (http://www.siemens.com/industrialsecurity).

⚠ WARNING

Danger to life as a result of unsafe operating states resulting from software manipulation

Software manipulations (e.g. viruses, trojans, malware or worms) can cause unsafe operating states in your system that may lead to death, serious injury, and property damage.

- Keep the software up to date.
- Incorporate the automation and drive components into a holistic, state-of-the-art industrial security concept for the installation or machine.
- Make sure that you include all installed products into the holistic industrial security concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.

What is industrial security? 2

Definition of industrial security

Generally, industrial security is understood to be all of the measures for protecting against the following:

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

Objectives of industrial security

The objectives of industrial security encompass:

- Fault-free operation and guaranteeing of availability of industrial plants and production processes
- Preventing hazards to people and production
- Protection of industrial communication from espionage and manipulation
- Protection of industrial automation systems and components from unauthorized access and loss of data
- Practicable and cost-effective concept for securing existing systems and devices that do not have their own security functions
- Utilization of existing, open, and proven industrial security standards
- Fulfillment of legal requirements

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

Why is industrial security so important? 3

3.1 Networking and wireless technology

Overview

There are many new trends which affect industrial security:

- Cloud computing in general
  The number of network connections across the world is constantly increasing. This enables innovations such as cloud computing and the applications that go hand in hand with it. In conjunction with cloud computing, there has been a massive increase in the number of mobile devices, such as cell phones and tablet PCs.
- Wireless technology
  On the other hand, the increasing use of mobile devices has only become possible thanks to the ubiquitous availability of mobile networks. Wireless LAN is also becoming increasingly available.
- Worldwide remote access to plants, machines and mobile applications
- The "Internet of things"
  Millions of electronic devices are becoming network-capable and are communicating via the Internet, such as onboard computers in cars, which transmit warranty information to dealers, or water meter sensors that transmit water consumption data to municipal water suppliers via radio.

However, in order for everything from cloud computing to sensors to function disturbance-free, you require a reliable network infrastructure and applications that are well protected against attacks from malware and hackers.

3.2 Possible corporate security holes

Possible security holes or weak points

The security chain of a company is only as strong as its weakest link. Security holes can exist at numerous points. The following list gives only a few examples:

- Employees / external companies
- Production plants
- Network infrastructure
- Data centers / PC workstations
- Laptops/tablets
- Printers
- Smartphones/smartwatches
- Mobile data storage media

For this reason, a holistic approach is required to deal with the issue of security. Coordinated guidelines and regulations are required that cover all areas: Devices, systems, processes and employees.

The topic of data security and access protection (security) is becoming more and more important in industrial environments. The following technologies results in higher requirements placed on protecting and securing industrial plants and systems:

- The ongoing networking of complete industrial plants and systems
- The vertical integration and networking of various company levels
- New techniques, e.g. remote maintenance and/or remote access

The threats are diverse and the consequences are far-reaching:

Possible threats:

Potential threats come from the industry environment and involve the topic of confidentiality, integrity and availability. Examples of threats include the following:

- Espionage of data, recipes, etc.
- Sabotage of production plants
- System stoppage, e.g. due to virus infection and malware
- Manipulation of data or application software
- Unauthorized use of system functions

Possible effects of a security incident

- Loss of intellectual property
- Loss of production or reduced product quality
- Negative company image and economic damage

- Catastrophic environmental influences
- Danger to people and machines

Security measures in automation and drive technology 4

Siemens automation and drive technology concerns itself with security aspects at the following levels:

- **Application security** refers to products and functions that take into consideration the needs of industrial security in the field of automation. This involves particular consideration of the application and task at hand, as well as the people performing the actions in an automated plant. This allows industrial security to be easily implemented in production processes.
- **Security support** provides support during the analysis, planning, implementation, testing and optimization of industrial security - by means of specialists with special knowledge of networks and the industry. These services lead to the highest possible level of industrial security and operating capacity of the production plant.
  Siemens offers comprehensive customer support based on the "Implement Security" service: With this service you can implement protective measures to increase the security level of plants and production facilities. You can find more information about the entire "Implement Security" portfolio on the Internet (https://www.industry.siemens.com/services/global/en/portfolio/plant-data-services/industrial_security).

Security measures

With increasing digitalization, comprehensive security in the automation system is becoming ever more important. For this reason, industrial security is a core element of every product that can be networked.

As manufacturer of automation and drive products, Siemens supports secure operation for its customers by **integrating security into its products**:

- All of the measures involving automation and drive technology are stored in the **Product Lifecycle Management (PLM) process**, which is certified by the German Technical Inspectorate (TÜV) based on IEC 62443-4-1.
- Analytically potential attack threats are detected and evaluated using **Threat and Risk Analyses (TRA)**. Identified critical threats are implemented in the product as necessary basic functions, based on the motto "Security by Design".
- Siemens regularly performs **code analyses** in order to identify and correct possible errors at an early stage during the formal check.
- In its products and its manufacturing process, Siemens has implemented **measures to secure integrity** to indicate any changes to the integrity.
- Siemens constantly checks the measures relating to **hardening**:
  - Operating systems are configured in such a way that **points of attack** (e.g. via ports, unneeded services) are **minimized**.
  - Siemens **tests its products** to detect weak points at an early stage.
  - Siemens offers a specific **hotfix/patch management**.

As manufacturer of automation and drive products, Siemens supports secure operation for its customers by **securing the development infrastructure and supply chain**:

- The Siemens ProductCERT (https://www.siemens.com/cert/en/cert-security-advisories.htm) (**C**yber **E**mergency **R**eadiness **T**eam) is the central department for security-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development work with consulting and other services. **ProductCERT** provides information about current threats and vulnerabilities as well as the appropriate countermeasures.
- Industrial security is a dynamic and complex subject that requires continuous monitoring and adaptation of new security measures. Information on how Siemens protects its products and solutions against cyber attacks and how industry profits from the competence of Siemens can be found on the Internet (https://www.industry.siemens.com/topics/global/en/industrial-security/always-active).

As manufacturer of automation and drive products, Siemens supports secure operation for its customers through direct support of integrators and operating companies **by providing patches, security components and the appropriate services**:

- SIEMENS offers monitoring through a **SIEM system** to monitor residual risk. SIEM stands for Security Information and Event Management and has become an established term in IT security. Such systems are able to identify and evaluate security-relevant events and notify the administrator.

Siemens Industrial Holistic Security Concept™

Siemens places great emphasis on protecting the integrity and guaranteeing the confidentiality of the processed data for its own products. Intellectual property and know-how of the Siemens products are also in focus.

To achieve this, the Siemens Industrial Holistic Security Concept (SI HSC) is applied which protects development departments and production plants (see the following diagram). Multi-level security systems and basic security improvements of the IT infrastructure are implemented. In parallel, process improvements have been introduced and training in security awareness provided in the development and production. These measures are being performed continuously by Siemens and clearly demonstrated by the security levels reached.

SI HSC also benefits the customers who Siemens has selected as partners for their industrial solutions, or who want to orientate themselves on the concept. Siemens suppliers are also considered with regard to security so that Siemens already applies the same security standards when purchasing as for the manufacture of its own products.

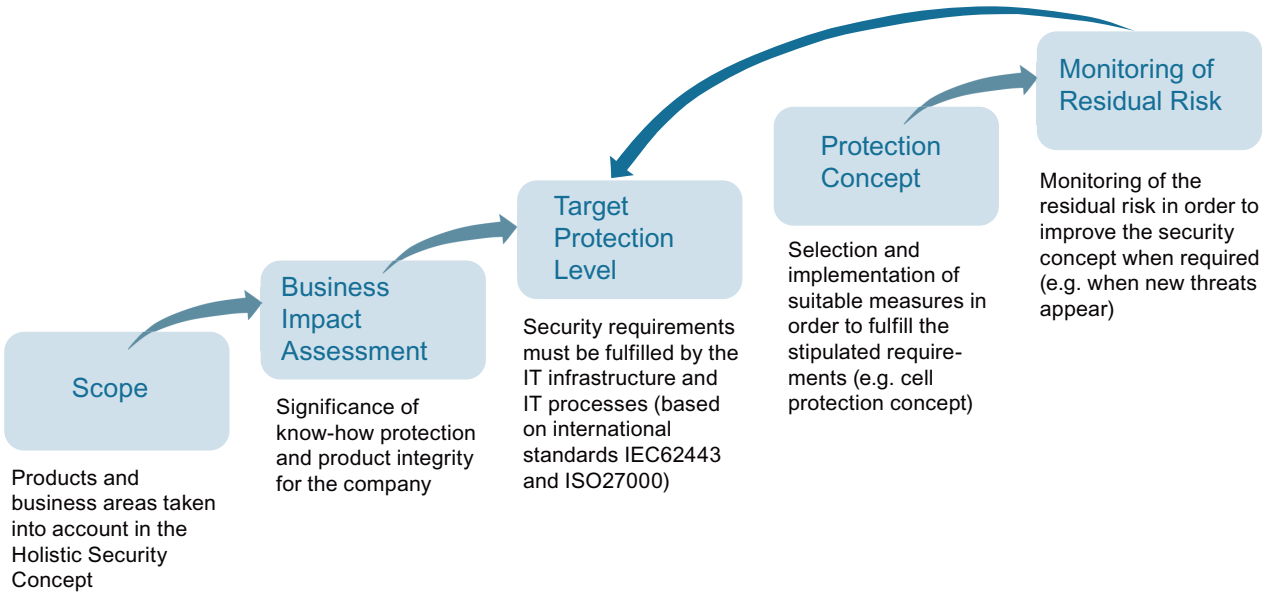

Figure 4-1 SI HSC security management process

Standards and regulations

Siemens complies with the valid standards and regulations in the industrial security area throughout the entire development process:

- ISO 2700X: Management of information security risks
- IEC 62443: IT security for industrial higher-level control systems – network and system protection

Security management

5

The security management process as a basis

Protect your system and your company. Security management according to IEC 62443 and ISO 27001 forms the basis for the successful implementation of industrial security.

The security management process is shown in the following:

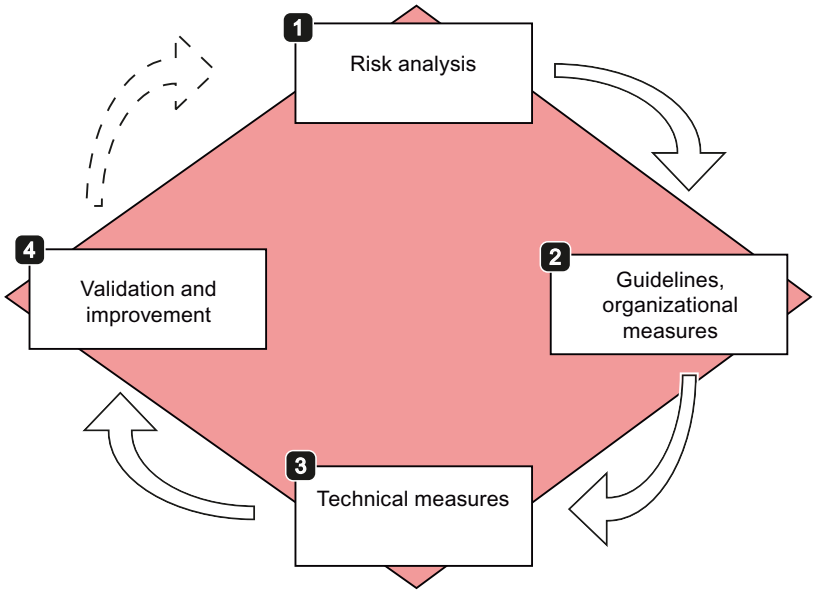

Figure 5-1 Security management process

1. Carry out a risk analysis. Determine all possible risks and define countermeasures for reducing the risk to an acceptable level. In detail, a risk analysis encompasses the following steps:
   - Identification of threatened objects
   - Analysis of value and potential for damage
   - Threat and weak point analysis
   - Identification of existing security measures
   - Risk evaluation
2. Define guidelines and introduce coordinated, organizational measures. To this end, the awareness of the importance of industrial security must be borne by all levels of the company. In addition, define guidelines and processes in order to achieve a uniform procedure and to support compliance with the defined industrial security concept.

3. Introduce coordinated technical measures. You can find a list of general measures that help to protect your plant against threats in Section General security measures (Page 21). You can find measures recommended for SINUMERIK, SIMOTION and SINAMICS environments in Section Product-specific security measures (Page 35).
4. A security audit must ensure that all of the measures have been implemented and that they have also eliminated or reduced the identified risks.

Note

Continuous process

Due to constantly changing security threats, **this process must be continuously repeated** in order to guarantee the security of your plant. For this reason, the security management process must be seen as a continuous process.

General security measures

6

In this section you will learn about the general security measures you can take in order to protect your system from threats. All of the measures are recommended.

Additional specific security measures for SINUMERIK, SIMOTION and SINAMICS products can be found in Section Product-specific security measures (Page 35).

To protect industrial plants and systems comprehensively against cyber attacks, measures must be applied simultaneously at all levels. From the operational up to the field level – from access control to copy protection. For this purpose, we use "Defense in Depth" as a general protection concept, according to the recommendations of ISA99 / IEC 62443, the leading standard for security in industrial automation.

Figure 6-1 Defense in depth strategy

A defense in depth model has a three level structure:

- Plant security
  Plant security represents the outermost protective ring. Plant security includes comprehensive physical security measures, e.g. entry checks, which should be closely coordinated with protective measures for IT security.
- Network security
  The measures, grouped under the keyword "Network security", form the core of the protective measures. This refers to the segmentation of the plant network with limited and secure communication between subnetworks ("secure islands") and the interface check with the use of firewalls.
- System integrity
  "System integrity" represents the combination of two essential protection aspects. PC-based systems and the control level must be protected against attacks. Steps include the following measures:
  - Integrated access protection mechanisms in the automation components to prevent unauthorized changes via the engineering system or during maintenance
  - The use of antivirus and whitelisting software to protect PC systems against malware
  - Maintenance and update processes to keep the automation systems up-to-date (e.g. patch management, firmware updates, etc.)

6.1 Plant safety

Unauthorized persons may be able to enter the production site/building and damage or alter production equipment as a result of gaps in a company's physical security. Confidential information can also be lost. This can be prevented if both the company's site and the production areas are protected accordingly.

6.1.1 Physical protection of critical production areas

Company security

The company's physical security can be ensured via the following measures:

- Closed off and monitored company premises
- Entry control, keys / card readers and/or security personnel
- Escorting of external personnel by company employees
- Security processes in the company are taught and followed by all employees

Physical production security

The physical security of a production location can also be ensured via the following measures:

- Separate access control for critical areas, such as production areas
- Installation of critical components in lockable control cabinets / switching rooms including monitoring and alarm signaling options
- Configuration of the radio field to restrict the WLAN range so that it is not available outside the defined areas (e.g. factory building).
- Guidelines that prevent the use of third-party data storage media (e.g. USB sticks) and IT devices (e.g. notebooks) classified as insecure on systems.

Further information

Further information on integrated Siemens security solutions can be found on the Siveillance page (https://www.buildingtechnologies.siemens.com/bt/global/en/security-solution).

6.2 Network security

Network security includes all measures taken to plan, implement and monitor security in networks. This includes the control of all interfaces, e.g. between the office network and plant network, or remote maintenance access via the Internet.

6.2.1 Network segmentation

6.2.1.1 Separation between production and office networks

One important protective measure for your automation or drive system is the strict separation of the production networks and the other company networks. This separation creates protection zones for your production networks.

Note

The products described in this manual must only be operated in defined protection zones.

Separation by means of a firewall system

In the simplest scenario, separation is achieved by means of an individual firewall system which controls and regulates communication between networks.

Separation via a DMZ network

In the more secure variant, the coupling is established via a separate DMZ network. In this case, direct communication between the production network and the company network is completely prevented by firewalls and only takes place indirectly via servers in the DMZ network.

Note

The production networks should also be divided into separate automation cells in order to protect critical communication mechanisms.

General security measures

Observe the general security measures even within protection zones, for example:

- Virus scanner (Page 32)
- Reduction of attack points (Page 29)

6.2.1.2 Network segmentation with SCALANCE S

Siemens provides SCALANCE S security modules to meet network protection and network segmentation requirements. Further information on SIEMENS SCALANCE S can be found on the Internet (http://siemens.com/scalance-s).

SCALANCE S security module

SCALANCE S security modules with Security Integrated provide:

- Stateful inspection firewall
  In order to implement user-specific control and logging, firewall rules can also be specified that only apply to certain users.
- VPN via IPsec (data encryption and authentication)
  This establishes a secure tunnel between authenticated users whose data cannot be intercepted or manipulated. The most important aspect is the protection against external access via the Internet.
- NAT/NATP (address translation)
- Router functionality (PPPoE, DDNS) for broadband Internet access (DSL, cable)
- SCALANCE S623 with additional VPN port (DMZ) enables the secure connection of an additional network for service and remote maintenance purposes. S623 also permits the secure, redundant connection of subordinate networks by means of routers and firewall redundancy.
- SCALANCE S615 has five Ethernet ports with which different network topologies can be protected by means of a firewall or Virtual Private Network VPN (IPsec and OpenVPN), and security concepts implemented flexibly.

Requirement

NOTICE
Data misuse Long distances between the device to be protected and the upstream security modules represent an invitation for data misuse. • Note that upstream security modules, such as SCALANCE S, must be installed close to the device to be protected in a locked control cabinet. This ensures that data cannot be manipulated here without notice.

Principle

The following application example shows cell segmentation by several SCALANCE S modules, each of which is upstream of the automation cells. The data traffic to and from the devices within automation cells can be filtered and controlled with the SCALANCE S firewall. If required, the traffic between the cells can be encrypted and authenticated. Secure channels and client access from the PCs to the cells can be established via SOFTNET Security Client, VPN client software for PCs.

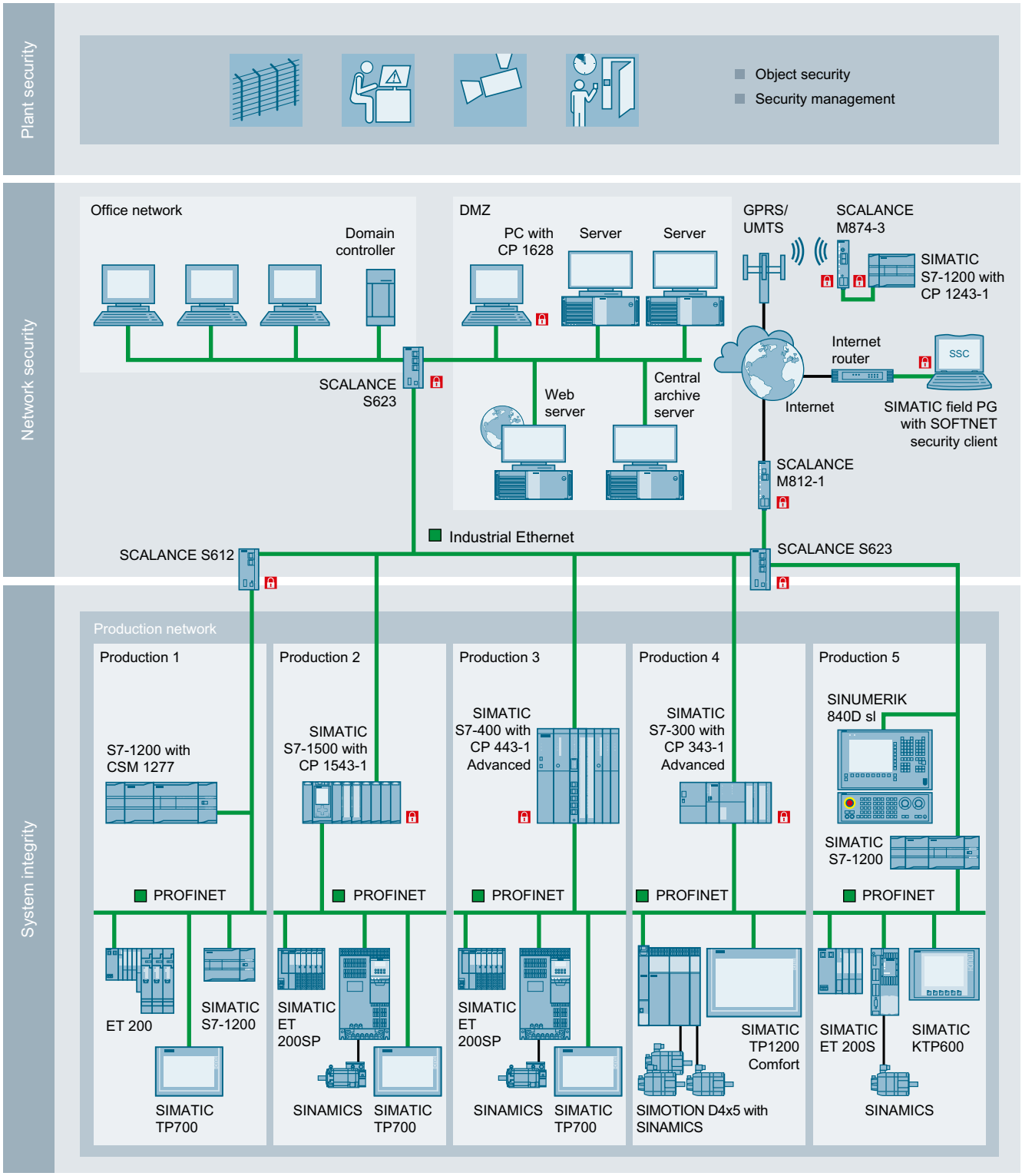

Figure 6-2 SCALANCE S application example

VPN access

Note

Note that a SCALANCE S security module must always be used for VPN access.

6.3 System integrity

System integrity

System integrity encompasses all of the measures to protect automation and drive systems – along with control components, SCADA and HMI systems – that have to be protected against unauthorized access and malware.

6.3.1 System hardening

6.3.1.1 Reduction of attack points

Services and ports

Activated services and ports represent a risk. To minimize the risk, only the necessary services for all of the automation components should be activated. Ensure that all activated services are taken into account (especially Web servers, FTP, remote maintenance, etc.) in the security concept.

A description of the ports used can be found in Section Product-specific security measures (Page 35) or in the Manuals and Function Manuals of the respective products.

User accounts

Any active user account that allows access to the system is thus a potential risk. Therefore, take the following security measures:

- Reduction of configured/activated user accounts to the actually needed minimum
- Use of secure access data for existing accounts. This also involves assigning a secure password.
- Regular checks, especially of the locally configured user accounts
- Regular change of passwords

PC in the industrial environment

PCs used in the industrial environment must comply with the generally valid security recommendations. Therefore, take the following measures:

- The PC used is set up and administered by appropriate departments, regularly checked and patched, and therefore kept at state-of-the art technology. This means that the software and operating systems, which are supported and maintained by the manufacturer, are installed.
- Regular installation of security updates and patches for the installed operating system (see Section Windows patch management (Page 33))
- The PC being used must have a current virus scanner that is regularly updated.
- Alternatively, you can apply whitelisting (Page 33) and network segmentation (Page 24) techniques.
- If possible, the PC should have a configuration without administrator rights.
- If possible, the PC should not be used for other tasks, e.g. in the office network. This is part of the separation of networks dealt with in Section "Separation between production and office networks (Page 24)".
- If you leave the PC to perform other tasks, always activate lock mode of the operating system. This will prevent other people from reading the screen contents. Other unauthorized access to the PC must be prevented.

Data storage

Note

When you store security-relevant data on your PC, you are responsible for secure data storage.

These include, for example, the following measures:

- Consequent marking of your documents according to confidentiality levels by introducing a document classification.
- Protection of your encrypted storage locations, such as sharepoints, against manipulation.
- If absolutely necessary, only store your confidential or security-relevant data encrypted on your PC / systems or the network.
  Security-relevant data includes sensitive data, such as archives, passwords, or executable files (*.exe).
- Regularly back up your security-relevant data, and carefully protect it against loss and manipulation.

Transporting data

Note

Apply the following measures when transporting data:

- Always encrypt your emails if you send confidential and/or security-relevant data by email.
- If you wish to transport confidential and/or security-relevant data on a data storage medium (USB flash drive, hard disk, etc.), carefully investigate as to which data storage media are considered secure. A regular virus check must be carried out for these data storage media. Always save your data on local data storage media so that the data is encrypted.

These measures are especially important for sensitive data, such as archives, passwords, or executable files (*.exe).

Passwords

NOTICE

Data misuse caused by using passwords that are not secure enough

Data can be easily misused by using passwords that are not secure enough. Passwords that are not secure enough can be easily hacked into.

- Therefore, change the default passwords during the commissioning and adapt them at regularly defined intervals.
- Always keep your passwords secure, and ensure that only authorized persons have access to these passwords.

Note

Assigning secure passwords

Observe the following rules when creating new passwords:

- When assigning new passwords, make sure that you do not assign passwords that can be guessed, e.g. simple words, key combinations that can be easily guessed, etc.
- Passwords must always contain a combination of upper-case and lower-case letters as well as numbers and special characters. Passwords must comprise at least eight characters. PINS must comprise an arbitrary sequence of digits.
- Wherever possible and where it is supported by the IT systems, a password must always have a character sequence as complex as possible.

The German Federal Office for IT Security (BSI) (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/GSK_15_EL_EN_Draft.pdf?__blob=publicationFile&v=2) provides additional rules for creating secure passwords

Programs are available that can help you to manage your passwords. Using these programs, you can encrypt, save and manage your passwords and secret numbers – and also create secure passwords.

Product security notifications

Note

Complying with product security notifications

Threats are extremely diverse in nature and are continually changing. As a consequence, always keep yourself up-to-date on a regular basis through the Industry Online Support (https://support.industry.siemens.com/sc/ww/en/sc/2090) regarding whether there are new and relevant product security notifications for your particular products. Comply with the instructions provided in the product security notifications.

6.3.1.2 Virus scanner

An anti-virus program, virus scanner or virus protection program is a software that can detect, block and, if required, eliminate computer viruses, computer worms or Trojans horses.

In principle, virus scanners can only detect known malware (viruses, worms, Trojans, etc.) or harmful logic and therefore cannot provide protection against all viruses or worms. For this reason, virus scanners can only be considered as a complement to general precautionary measures.

The use of a virus scanner must not impact the production operations of a plant. As the last consequence, this will lead to even a virus-infected computer not being permitted to immediately shut down if this would cause the control of the production process to be lost.

NOTICE
Data misuse when using online virus scanners If you use an online virus scanner, then security-relevant or confidential data can get into the wrong hands and be misused. • Do not check any security-relevant or confidential data using an online virus scanner.

Note

Keep virus scanners up-to-date

Always ensure that the virus scanner database is always up-to-date.

Note

Do not install several virus scanners together.

You must always avoid installing several virus scanners together in one system.

Note

Operation in a local network

Always use a virus scanner when locally connecting with the plant or system network.

6.3.2 Whitelisting

The basic philosophy of whitelisting is that all applications are mistrusted, unless they have been classified as trustworthy after an appropriate check. This means that a whitelist is maintained in the system. This whitelist therefore contains all applications that have been classified as trustworthy and consequently can be run on your PC systems.

Whitelisting mechanisms provide additional protection against undesired applications or malware and unauthorized changes to installed applications or executable files (.exe, .dll).

6.3.3 Windows patch management

WSUS

The **WSUS** (Windows Server Update Service) system functionality provided by Microsoft is available for current Windows systems. WSUS supports administrators by providing Microsoft updates in large local networks. WSUS automatically downloads update packages (Microsoft update) from the Internet and offers them to the Windows clients for installation.

The fully automatic update process ensures that Microsoft security updates are always available on Siemens clients.

NOTICE
Security gaps for out-of-date operating systems Note that security updates, hotfixes, etc. are no longer supplied by Microsoft for operating systems < Windows 7. As a consequence, dangerous security gaps can occur with your operating system. • Therefore, use a whitelisting application.

Note

Before installing Microsoft Updates, note the following important points:

- Before installing the update, carefully check whether the current update is really compatible with your system. You are responsible for the installation of the update!
- Never establish a direct connection to the WSUS server in the Internet! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

Product software

Note

Out-of-date product software also represents a potential security gap for attacks. As a consequence, always install the latest product software versions.

Product-specific security measures

7

This Chapter describes additional product-specific security measures for SINUMERIK, SIMOTION and SINAMICS devices.

7.1 SINUMERIK

The following Chapter provides you with an overview of the security-related measures you can take to protect your SINUMERIK control from threats. As with the entire Manual, all of the measures are recommended. Detailed descriptions and procedures can be found in the corresponding SINUMERIK documentation.

7.1.1 Physical protection of the NCU

NOTICE
Misuse, manipulation and theft Modules, such as the NCU, are open equipment. If not protected, there is the risk of misuse by unauthorized personnel, manipulation or theft of data (e.g. CompactFlash Card). • As a consequence, always install NCUs in housings and locked control cabinets or in electrical rooms. Only appropriately trained and authorized personnel may access these housings, electrical cabinets and electrical rooms. • You can find further information on control cabinet installation of the NC in the "SINUMERIK 840D sl, NCU 7x0.3 PN" Manual.

7.1.2 Firewall and networking

NCU/PCU networking structure

The following graphic shows the networking of the control (NCU) and the PCU. X130 at the NCU and eth 1 at the PCU are used to establish a connection to the company network. A firewall protects these two interfaces against unauthorized access.

The NCU contains a packet filter functionality (firewall) that filters the connection to the factory network. This integrated firewall is preconfigured with optimum settings for the incoming and outgoing communication. The firewall is configured in such a way that access to the networks behind the firewall is blocked, and when several logon attempts are made from a certain IP address, this is identified, blocked and prevented. In this way, the control is protected against brute-force attacks.

The PCU has the firewall function provided by Windows.

NOTICE
Data misuse via an unprotected interface There is a risk of potential data misuse as the X120 interface is not protected by a firewall. The interface only provides the option of establishing a connection to the local plant/system network. • As a consequence, never connect this local network with the Internet/company network.

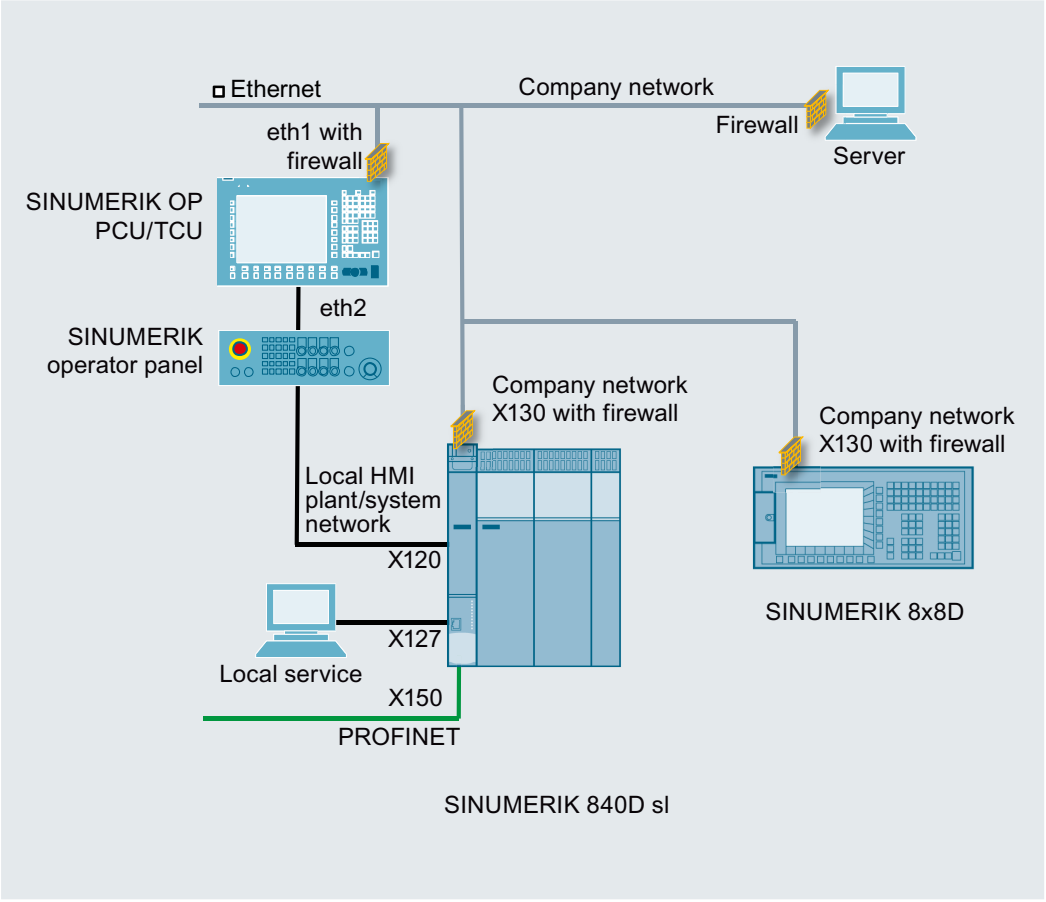

Figure 7-1 NCU/PCU networking

Firewall settings

Ethernet interface X130 of the NCU and the eth1 interface of the PCU are protected by a firewall for security reasons. If individual programs require access to a communication port for communication purposes, you can activate or deactivate the firewall via the HMI. Additional ports can be separately released.

Alternatively, you can configure the firewall via the "basesys.ini".

More detailed information on the configuration of the firewall and default settings can be found in the manuals:

- SINUMERIK Operate (IM9) (https://support.industry.siemens.com/cs/de/en/view/109481529)
- Diagnostics Manual (808D) (https://support.industry.siemens.com/cs/de/en/view/109736368)

7.1.3 Machine control panels - SINUMERIK (MCP/MPP)

Machine control panels (**M**achine **C**ontrol **P**anels and **M**achine **P**ush Button **P**anels) are available for user-friendly operation of SINUMERIK machine functions.

Note

Only operate the machine control panels (MCP/MPP) on an internal, local machine network and secure them against any possible external access.

7.1.4 System hardening

7.1.4.1 Deactivating hardware interfaces

Deactivating interfaces

Measure	Description
Deactivate/activate Ethernet interfaces in the BIOS of the PCU	You can activate or deactivate the Ethernet interfaces in the BIOS of the PCU. Detailed information on this topic can be found in the "SINUMERIK 840D sl PCU Base Software (IM8)" Manual, Section "BIOS settings".
Deactivating/activating USB interfaces	To prevent malware entering the control or the plant network via the USB interfaces, you can disable the USB interfaces of the NCU. Use the service command "sc_usb disable". Enter the relevant command on the Service Desktop in the "Run" dialog box or at the prompt. Use this function to make your system more secure and protect it from unwanted manipulation and malware. Detailed information can be found in the "SINUMERIK 840D sl PCU Base Software (IM8)" Manual, Section "Deactivating USB interfaces".

Deactivating ports

Measure	Description
Deactivating the PROFINET port for SINUMERIK 840D sl PLC	In STEP 7 HW Config, a PROFINET interface port of a SINUMERIK PLC can be deactivated (X150). It is activated by default. The SINUMERIK PLC cannot be accessed via a deactivated PROFINET interface port. Detailed information can be found in the "S7-300, CPU 31xC and CPU 31x: Technical Specifications" Manual, Section "Configuring the port properties". **No communication function.** Note that no communication functions, such as PG/OP functions, open IE communication or S7 communication (PROFINET IO), are possible via a deactivated port.
Deactivating a PROFINET port of SCALANCE X switch (possible as of the X200 series)	For secure operation, only one defined access point should be available to the network for diagnostics/maintenance. All of the other ports to the controls, devices, or switches (Scalance X) should be deactivated. This prevents unauthorized access. Detailed information can be found in the "Industrial Ethernet Switches, SCALANCE X-200" Configuration Manual, Section "Ports".

7.1.4.2 Communication services and used port numbers

SINUMERIK supports certain communication protocols. The address parameters, the relevant communication layer as well as the communication role and the communication direction are decisive for each protocol.

This information allows you to match the security measures for the protection of the automation system to the used protocols (e.g. firewall).

More detailed information on this topic is provided in the SINUMERIK Manual.

7.1.4.3 Whitelisting

SINUMERIK application example

Using the McAfee Application Control Software as example, a description as to how SINUMERIK PCU 50 with Windows XP can be "hardened" is provided. The licensed software can be used with the PCU 50 as a standalone version (Solidifier/Solidcore). The whitelisting software is directly purchased from the manufacturer.

A detailed description of this application can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/view/89027076).

Note

System hardening for software solutions

When using SINUMERIK Integrate software and other PC applications (e.g. Create MyConfig (CMC) or Access MyMachine (AMM)), make sure that the PC on which the software is used, always fulfills the requirements of industrial security.

These include, for example:

- Current Microsoft security updates
- Current virus scanner software
- Activated firewall, etc.

Further information can be found in Section System integrity (Page 29).

7.1.5 Virus protection

Within the context of constantly new warnings about computer viruses, the topic of virus protection on SINUMERIK controls with PCU50 (Microsoft Windows) is becoming increasingly important.

Note

Take necessary measures to protect against viruses

Take all the necessary measures for virus protection in the CNC environment. This also includes the proper handling of data storage media, USB sticks and network connections, precautionary measures when copying data and during software installations, etc.

You can find information on distributing the virus signatures in complex networks on the Internet (https://support.automation.siemens.com/WW/view/en/19577116).

7.1.5.1 Virus protection / memory card

The memory card must be handled with particular care for all SINUMERIK devices that use a memory card so that no malicious software is loaded to the system.

⚠ WARNING

Risk of death due to software manipulation when using exchangeable storage media

Storing files on exchangeable storage media poses an increased risk of infection, e.g. with viruses and malware. Incorrect parameter assignment can cause machines to malfunction, which can lead to injuries or death.

- Protect files stored on exchangeable storage media from malicious software using appropriate protection measures, e.g. virus scanners.

7.1.6 Security updates / patch management

For organizational reasons, it is not possible to provide the latest Windows security patch when a **PCU** is shipped. As a consequence, you must install current Windows security patches locally on site. This requires a secure connection to an update server, e.g. via a DMZ or a local WSUS server (see Chapter Windows patch management (Page 33)).

Possibly identified security weak points of the **NCU** are taken into account or corrected in the current CNC software version. We therefore recommend that whenever possible you always use the current CNC software version – or upgrade the control accordingly. Only in this way can you be certain that your control has the latest security version.

Use cases of security updates

A distinction is made between two SINUMERIK control use cases with Microsoft security updates:

- Security update before the first use in production
  Generally, a few months pass before being used in production by the end user (production in the Siemens plant, integration by the OEM, configuration and commissioning by end user). Therefore, new Microsoft security updates must be loaded by the end user at the latest at the start of use in the production.
- Security update during use in production
  We recommend that you regularly install the latest patches during maintenance intervals. The WSUS system functionality provided by Microsoft is available for this.

Note

Availability

The availability of Microsoft security updates is published via Microsoft Security Bulletins. The use of security updates is entirely up to the customer and is their sole responsibility. This can be realized based on the "evaluation of maximum severity" provided in the Microsoft Security Bulletin. Microsoft publishes information on security updates for the PCU and download links on the Internet (https://technet.microsoft.com/en-us/security/bulletins).

7.1.7 Passwords

NOTICE
Data misuse caused by using passwords that are not secure enough Data can be easily misused when passwords that are not secure enough are created. Passwords that are not secure enough can be easily hacked into. The default passwords for the basic commissioning procedure are listed in the documentation. • Therefore, change the preassigned default passwords during the commissioning and modify them at regularly defined intervals. • During commissioning, change the Linux password in addition to the NCK/HMI passwords. You can find additional information in the Commissioning Manual "NCU operating system".

7.1.7.1 Definition of access levels

Access to programs, data and functions is user-oriented and protected over seven hierarchical protection levels. These are divided into

- Three password levels for the machine manufacturer, commissioning engineer and user
- Four keyswitch positions for users

There are protection levels 1 to 7 (see table below); where

- 1 is the highest and
- 7 is the lowest level

HMI access rights

Protection level	Protected by	Area
1	Password: SUNRISE (default value)	Machine manufacturer
2	Password: EVENING (default value)	Service
3	Password: CUSTOMER (default value)	User
4	Keyswitch 3	Programmer, machine setter
5	Keyswitch 2	Qualified operator
6	Keyswitch 1	Trained operator
7	Keyswitch 0	Semi-skilled operator

Linux passwords / NCK

Level	User name	UID
(0)	siemens	101
1	manufact	102
2	service	103

Level	User name	UID
3	user	104
4	operator3	105
5	operator2	106
6	operator1	107
7	operator	108

Corresponding to the named user, there is always a Unix group with the same name (also with the GID to the UIDs). As user, you are always member of your own group and also in all "lower-level" groups. For example, "operator2" is a member of the "operator2", "operator1" and "operator" groups. The file access rights are mainly controlled via these groups.

Reference

You can find additional information on how you can change the passwords of the access levels along with other information on access levels for programs and softkeys and access rights for files in the manual "SINUMERIK Operate (IM9)", in chapter "General settings > Access levels".

7.1.7.2 CNC lock function

You can use the "CNC lock function" and the encrypted file that was created with SINUMERIK Integrate Access MyMachine (AMM) application to activate a lock date in the control. This allows the use of the machine to be limited to the time until the lock date is reached. The NC Start function of the control is locked when the lock date is exceeded.

The CNC lock function supports the business model with time-limited use. This protects against unauthorized use beyond the set interval.

Further information on the CNC lock function and on the creation of a lockset file can be found on the Internet:

- "SINUMERIK Integrate Access MyMachine /P2P (PC)" Operating Manual (https://support.industry.siemens.com/cs/de/en/view/109744806)
- "Basic Functions" Function Manual (https://support.industry.siemens.com/cs/de/en/view/109481523), Section "P4: PLC for SINUMERIK 828D > CNC lock function"

7.1.7.3 Deleting the preinstalled SSH key

Application

Removing the SSH key preinstalled by Siemens reduces the risk of data misuse. However, in order to ensure sufficient access to the system, you can define and install your own SSH key.

Service command

The service command 'sc' is a tool used for performing a range of service tasks on a SINUMERIK NCU:

Syntax:	sc clear preinstalled-keys
Alternative names:	---
Authorization level	service

This command deletes all of the SSH keys preinstalled by Siemens on the control. When called from the service system, the keys on the CompactFlash card are affected, and not the SSH keys on the service system itself.

Reference

Further information can be found in the "SINUMERIK 840D sl Operating System NCU (IM7)" Commissioning Manual and on the Internet (https://support.industry.siemens.com/cs/de/en/view/109481527).

7.1.7.4 PLC web server

In the delivered state, the PLC has no password and the Web server of the PLC is not activated.

Note

- If you activate the PLC Web server in the S7 project, you must define an appropriate user and an associated password for it. Create a secure password. When creating a new password, carefully follow the information provided in SectionReduction of attack points (Page 29).
- Only use the HTTPS protocol to establish communication confidentiality and integrity.

Further information on the PLC Web server can be found in the "SIMATIC S7-300 Web server" Function Manual on the Internet (https://support.industry.siemens.com/cs/de/en/ps/faq).

7.1.7.5 Access levels for softkeys

The display and operation of softkeys can be suppressed by both the OEM and the user. This allows the operating software to be specifically adapted to the required functional scope and therefore be configured as transparently as possible. To prevent access to functions in the operating software, or to restrict the possibility of operator errors, restricts the functional system scope.

Note

Applicability of modified access levels for softkeys

The setting of specific access levels for softkeys on a PCU only affects the respective PCU softkeys themselves. To implement access rights on the NCU, both the manufacturer and the user must use the appropriate mechanisms and set the rights accordingly, see Section "Access levels for programs" in the "SINUMERIK Operate (IM9)" Manual.

7.1.7.6 BIOS and AMT access protection

In order to prevent unauthorized access to the BIOS of the PCU 50 and the SIMATIC IPCs, make sure that you use a very secure BIOS password (see Section Reduction of attack points (Page 29))

Further information

Further information on BIOS settings of the PCU 50 can be found in the "PCU Base Software (IM8)" Manual.

Setting the password for AMT (Intel® Active Management Technology)

The Active Management Technology (AMT) function is used for the remote management of the PCU. For remote management, generally suitable protective measures must be taken (such as network segmenting) in order to guarantee secure operation of the plant.

For security reasons, AMT is deactivated when a PCU is delivered. When you activate AMT the first time in the BIOS setup, assign a strong password to prevent misuse of the remote management.

Further information on the AMT function of the PCU as well as the procedure for changing the password can be found in the SIMATIC IPC Manuals in Section "Active Management Technology (AMT)".

7.1.7.7 Password protection for Create MyConfig (CMC)

NOTICE
Data misuse due to incorrect assignment of rights Access data, such as preconfigured passwords for access to controllers, can fall into the wrong hands. • For that reason, set up organizational measures to ensure that only authorized persons are given access to these files.

Note

Password protection for linked external files

The protection mechanisms integrated into CMC (password protection) are ineffectual for linked external files that are integrated into the CMC context.

Note

Password protection of logbooks

Make sure that the password protection of logbooks is only simple read protection.

Note

Protecting CMC packages from reimporting

Note that CMC packages have to be protected by password against being reimported.

- For that reason, always set up a password against reimporting when you assign a password for a new project.

7.1.8 Know-how protection

The protection of technological knowledge against unauthorized access is bundled in the SINUMERIK Integrate "Lock-it!" module.

This includes copy protection as well as the safe storage of data with company know-how, such as through the use of encrypted cycles.

7.1.8.1 SINUMERIK Integrate Lock MyCycle

Using the "SINUMERIK Integrate Lock MyCycle" (cycle protection) function, cycles can be encrypted and then stored protected in the control. The cycles are encrypted outside the control using the SINUMERIK Integrate Access MyMachine/P2P program.

For cycles with cycle protection, execution in the NC is possible without any restrictions.

In order to protect the manufacturer's know-how, any type of view is inhibited for cycles with cycle protection.

You can find an application example for cycle protection for SINUMERIK on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109474775).

Reference

Detailed information on cycle protection can be found in the "Commissioning CNC: NCK, PLC, Drive" Commissioning Manual, in Section "Lock MyCycles - Cycle protection".

7.1.8.2 SINUMERIK Integrate Lock MyPLC

With the aid of block properties, you can protect the blocks created in the SIMATIC PLC from unauthorized changes, for example.

The block properties should be edited when the block is open. In addition to properties that can be edited, data that is only displayed for your information is also displayed in the respective dialog field: It cannot be edited.

A block that has been compiled using this option does not allow you to view the instruction section. The interface of the block can be viewed, but not changed.

Reference

Detailed information on block protection can be found in the "SIMATIC Programming with STEP 7" Manual, Section "Block properties".

Note

The integrated CP in the SINUMERIK 840D sl does not support the "Module access protection / protection level" option.

Encryption of blocks

As of STEP 7 version 5.5 SP3 and the CNC system software for 840D sl / 840D sl V4.5 SP2, you can create encrypted block protection for functions and function blocks in the offline and online view. You can use this function to encrypt your blocks and protect the block code against external access.

The option "SINUMERIK" and, if required, "SIMATIC" must be selected for the encryption with SINUMERIK.

A detailed procedure of how to encrypt your blocks can be found on the Internet (https://support.automation.siemens.com/WW/view/en/45632073).

7.1.8.3 OPC UA

OPC UA (Unified Architecture) is a standardized, industrial communication protocol for access to control data, e.g. by higher-level control systems. Variables of a SINUUMERIK 840D sl and SINUMERIK 828D can be read and written to via this communication protocol using the SINUMERIK Integrate Access MyMachine /OPC UA software option.

NOTICE

Date misuse resulting from an insecure connection to the client

There is a danger of data misuse due to an unencrypted connection to the OPC UA client.

- Therefore, always encrypt your connection to the OPC UA client.
- Information on the encryption of the data connection can be found in the "Basic Software and Operating Software" Commissioning Manual in Subsection "SINUMERIK Integrate Access MyMachine /OPC UA".

NOTICE

Data misuse due to incorrect user administration / rights assignment

A significant security risk can ensue through incorrect user administration and faulty right assignment. Users can access data or actions for which they have not been authorized.

- As a consequence, always very carefully consider which users are assigned which rights. As administrator, you are responsible for professional user administration and assignment of rights.

Note

Selecting a secure password

Always set a secure password for your connection to the OPC UA client! Further information on selecting a secure password can be found in Section Reduction of attack points (Page 29).

7.1.8.4 SIMATIC Logon

User administration and traceability

The SIMATIC Logon option package is used to set up access rights for products and libraries in STEP 7. These projects can therefore only be accessed by an authorized group of people. SIMATIC Logon can be used in conjunction with SINUMERIK STEP 7.

More detailed information can be found in Chapter Secure access control with SIMATIC Logon (Page 57).

7.1.9 Data backup

There are different archive forms and archiving methods in the SINUMERIK for the different components.

Time of the data backup

The following times are recommended for performing a data backup:

- After commissioning
- After changing machine-specific settings
- After the replacement of a hardware component
- Before and after a software upgrade
- Before the activation of memory-configuring machine data

Further information can be found in the "Commissioning CNC: NC, PLC, Drive" Commissioning Manual.

Note the general information on secure data storage with regard to archives in Section Reduction of attack points (Page 29).

NOTICE
Misuse of confidential data on the control system On the control system, there is a risk of confidential data being misused. • As a consequence, it is not permissible to load confidential data to the control (e.g. using the "SINUMERIK Integrate Access MyMachine/P2P" software). • Always store confidential data in an encrypted form locally on an encrypted storage location in the network.

7.1.10 SINUMERIK Integrate

7.1.10.1 Standalone (Intranet)

Access to the resources of the SINUMERIK Integrate server

Note

Access to the resources of the SINUMERIK Integrate server

Read and write access to the file system and resources of the operating system (in particular to the Windows Registry) of the SINUMERIK Integrate server is only enabled for users with administrator rights. Make sure that these administrator IDs have sufficiently strong passwords (Page 29).

NOTICE
Data manipulation possible Within the production/machine network (Intranet), there is a risk that a hacker can access the file system of the SINUMERIK Integrate Servers or the variance SINUMERIK Integrate clients. There, the hacker can manipulate various system components (e.g. the content of databases). As a consequence, attackers can change tool data, NC programs, machine archives – or the system structure itself, for example. SINUMERIK Integrate cannot prevent this type of attack. • As a consequence, as the person responsible for the machine network, it is imperative that you take the appropriate industrial security measures for the production/machine network. Siemens AG does not accept any liability in this regard.

Use of open programming interfaces

NOTICE

Data misuse by using open programming interfaces

There is a potential risk of data misuse when using open programming interfaces.

- Therefore, when using open programming interfaces, use **only** clients that communicate with SINUMERIK Integrate via **current authentication mechanisms** (SHA-256) and **secure communication paths** (TLS). This applies in particular to all clients that run on versions of the Microsoft™ Windows XP before SP 3 or Microsoft™ Windows NT operating systems.

System hardening

System hardening is the removal of all software components and functions that are not absolutely required by the desired application to fulfill the intended task.

System hardening of third-party software: Microsoft™ Internet Information Server, Microsoft™ SQL Server, browsers (Microsoft™ Internet Explorer, Mozilla Firefox)

SINUMERIK Integrate requires software from third parties: For example, the Microsoft™ Internet Information Server, Microsoft™ SQL Server products and various browsers. They must be hardened according to the latest technology. In particular, restrict access to the Microsoft™ SQL Server to the local host and protect access with a password. Encrypt access to the database. In addition, you should only use current browsers for communication with the SINUMERIK Integrate server. Secure communication cannot be guaranteed when using outdated browsers (SSL instead of TLS).

System hardening of neighboring products to SINUMERIK Integrate: For example, tool setting station, Teamcenter, AUVESY™ VersionDog

SINUMERIK Integrate communicates with neighboring software products, e.g. tool setting stations, Teamcenter and VersionDog. They must be hardened according to the latest technology so that there are no negative effects via this communication path.

Network file exchange via common drives

Note

Network file exchange via common drives (Server Message Block, SMB)

If you use SMBs for exchanging files with SINUMERIK Integrate functions, only use standard authentication mechanisms (user name / password). It is recommended to restrict access for each user. Data storage on shared drives should be kept to a minimum.

Data backup

For data backup on machine tools, see Section "Data backup (Page 48)". Also back up the server side. Relevant are the configuration and contents of the Microsoft SQL Server database, the SINUMERIK Integrate server and the following SINUMERIK Integrate applications:

- MMT
- SFT RM
- MMP
- AMC
- AMP

The following times are recommended for the data backup:

- After commissioning
- When changing the hardware configuration
- After replacing the hardware
- Before and after upgrading the software

Communication security for SINUMERIK Integrate applications

The communication between the SINUMERIK Integrate server and various client forms (such as MMT or browsers) is preconfigured with HTTP. The required configuration should provide support for service technicians trained specially for SINUMERIK Integrate. It is recommended that communication is switched over to HTTPS if possible; a separate certificate is required for this. It should be noted that HTTPS is not possible for all client/server combinations.

7.1.10.2 Cloud operation (ASP)

If the AMM and AMC applications are used in cloud operation, the Siemens AG as operator ensures the security of the SINUMERIK Integrate server. Customers only have to ensure the security of the infrastructure on the machine side.

Firewall of the machine network

In contrast to standalone operation, a connection to the cloud server outside the machine and company networks is required when using the SINUMERIK Integrate AMM and AMC applications. The associated firewalls must enable the required ports. However, only the required ports should be opened. Further information on the required firewall settings can be found in the SINUMERIK Integrate Installation Manual, Section "System requirements".

Phishing for passwords

The term "phishing" describes the threat of "using bait to fish for passwords" in e-mails, via counterfeit links or even text messages (e.g. SMS). What are known as "phishers" attempt to obtain data via serious or official-looking e-mails and websites. With the aid of malware, they exploit weak points, e.g. in the operating system or Web browser.

"Phishers" could attempt to obtain login data, which would allow them to carry out actions within SINUMERIK Integrate in the name of the user. Hackers could, for example, falsify e-mails and websites from SIEMENS and thus gain access to confidential information from SINUMERIK Integrate users. The users are then prompted, for example, to enter the access data in a form and then send it to their SINUMERIK Integrate organization.

Note

You should observe the following when you encounter suspicious e-mails:

- Be on your guard when you receive e-mails from someone you do not know, especially if the e-mails include links and attachments. Never open suspicious attachments and do not click on any links in the e-mail.
- Carefully check the sender’s complete e-mail address.
- Check the integrity of the links embedded in the e-mail (e.g. by moving the mouse over the link). Tell-tale signs are spelling mistakes or where links contain a confusing company name.
- If in doubt, never divulge any confidential information.

Handling of confidential information

The communication route between the company's firewall and the SINUMERIK Integrate server is protected against malicious attacks by secure communication protocols (TLS). Third parties cannot eavesdrop on the transferred information or change it. Also note the company-specific guidelines for the transfer of confidential information via AMM and AMC.

7.2 SIMOTION

7.2.1 Overview

SIMOTION security measures

The following section provides an overview of the Industrial Security features available for SIMOTION (Motion Control) in order to protect your plant against threats.

Security functions

- There is only compiled code on the controller by default. For this reason, no upload and consequently no re-engineering is possible.
- No modifications can be made to the configuration without the matching engineering project.
- Know-how protection for source programs with password and encryption.
- Applicative copy protection for the configuration on the control system.
- Detection of source code manipulation with the SIMOTION SCOUT engineering system.
- Activation/deactivation of unused functions (Web server, ports).
- Use of the SIMATIC Logon for access to a project only with the appropriate rights.
- Virus scan and security updates for SIMOTION PC-based controllers (SIMOTION P).

A production plant is typically divided into several different network segments. These "segments" are components that have the required security functions connected upstream. They are shown with a padlock symbol in the overview graphic.

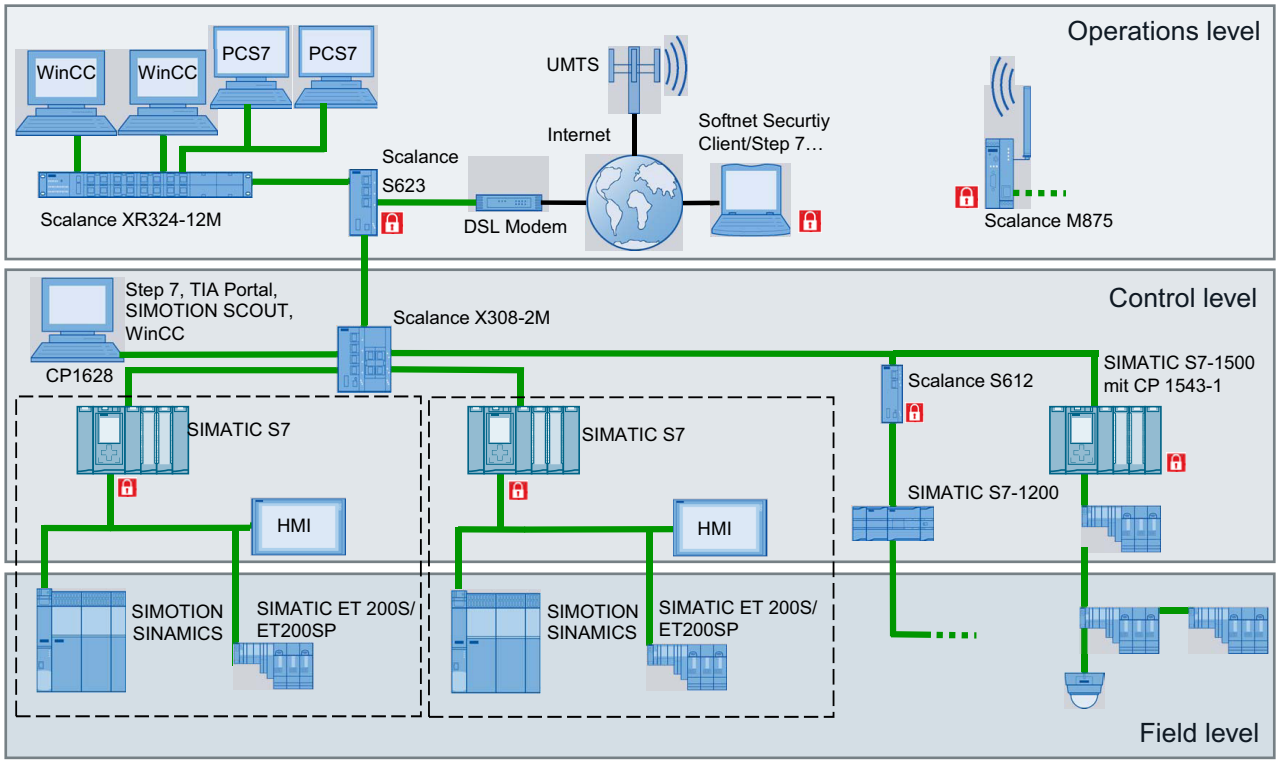

Figure 7-2 Display of a typical production plant with protected areas

Reference

Detailed descriptions and further procedures can be found in the corresponding SIMOTION documentation.

7.2.2 System hardening

7.2.2.1 Port security

Deactivating hardware ports

As of version 4.4, individual hardware ports of PROFINET interfaces (e.g. X150 interface ports) can be set to **Disable** in the engineering system (HW Config) for SIMOTION devices. This prevents devices being connected without permission and also increases security in terms of third-party access to the system. You should therefore deactivate unused ports.

Note

A SIMOTION device can no longer be accessed via a deactivated PROFINET interface hardware port.

The engineering system and the PN stack ensure that at least one port on each interface is not set to **Disable** to prevent users locking themselves out. The default setting is **Automatic settings**.

Reference

A detailed overview of the logical Ethernet ports and protocols used for SIMOTION can be found in the "Communication with SIMOTION" System Manual, Chapter "Used services".

7.2.2.2 Virus scan, Windows security patches, SIMOTION P

General information on virus scanners

Once an industrial PC system is connected to the Internet, either directly or via an internal company network, there is a danger that it can become infected with a virus. However, malicious software is not only able to reach the system via the Intranet/Internet, but also, for example, via a removable storage device (such as a USB memory stick) attached to the system for backing up data.

SIMOTION P320 virus scanner

A virus scanner that runs on Microsoft Windows, as used in office or home computers, has a deep impact on a system's processes. There are, for example, processes such as real-time scans or regular system scans. Such interventions can cause performance issues for the system, and as a result, for the SIMOTION Runtime software. Although the SIMOTION Runtime software runs in a real-time environment, it still depends on the available system resources.

Note

Because of the resulting performance impairments, the installation and use of a standard virus scanner on a SIMOTION P320 during system runtime is not permitted.

Using a virus scanner

As a standard virus scanner cannot be used for SIMOTION P320, an alternative procedure is followed. The virus scanner is installed to a separately bootable Windows PE operating system. It is started, for example, from a CD or a USB storage device and then performs a virus scan.

Note

FAQ Service & Support portal

More information on using a virus scanner on a SIMOTION P320 can be found in the FAQ "How can a virus scanner be used on a SIMOTION P3x0?" (https://support.automation.siemens.com/WW/view/en/59381507) which is available as a download from the Service & Support portal.

7.2.3 Secure project storage

Project data storage in SIMOTION SCOUT

All relevant data, configurations and programs are stored in the project. Only the programs and libraries encrypted via the know-how protection can be stored in a project. To protect the entire project, you should protect the project data with conventional office solutions, e.g. password-protected archives or encrypted hard disks.

File structure

The SIMOTION SCOUT project data can come in the following formats:

Engineering data (ES)

- Standard storage: File structure in project trees
  STEP 7 and SIMOTION SCOUT objects in the project directory. These objects are not secure and can be edited by anyone if there is no know-how protection for programs and libraries or external file encryption is used. Programs in this context programs are synonymous with units, which can contain the programs, function blocks and functions.
- XML data
  Project data created via an XML export/import. The know-how protection is retained.

Runtime data (RT) - data on the CF card

- ZIP archive of the SIMOTION project (not binary).
  The project archive is stored on the memory card of the respective SIMOTION controller (CFAST, CF card, MMC). The archive can be transferred, e.g. via SIMOTION SCOUT or using standard methods (FTP transfer).
- Binaries (zipped, unzipped)
  Binaries contain the compiled, executable project with the configurations and applications. Changes cannot be made during runtime without the SIMOTION SCOUT project because the project is stored as binary data on the SIMOTION controller.

The following figure shows an example of possible project data storage with display of the protected data.

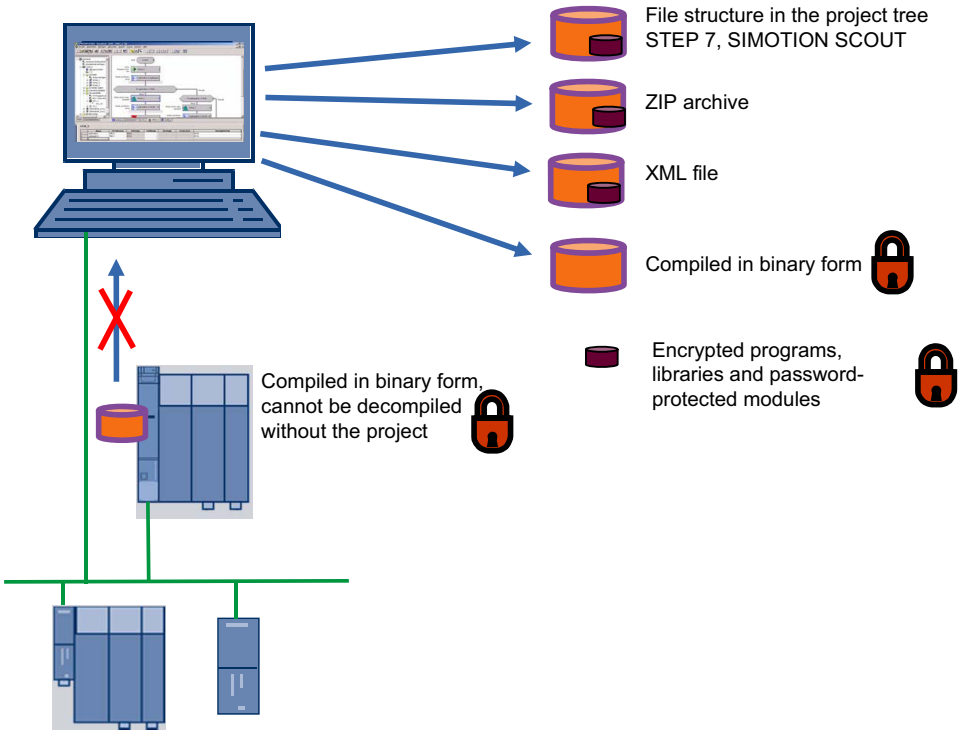

Figure 7-3 SIMOTION SCOUT project data storage

7.2.4 Know-how protection

7.2.4.1 Secure access control with SIMATIC Logon

User administration and traceability

The SIMATIC Logon option package is used to set up access rights for products and libraries in STEP 7. These projects can therefore only be accessed by an authorized group of people. SIMATIC Logon can be used in conjunction with SIMOTION SCOUT.

SIMATIC Logon supports the following functions:

- Assignment of individual authorization levels to users or user groups for the execution of specific actions (e.g. read, write, transfer blocks).
- Logging of online activities and logon actions on the computer. Access and changes in the project are reproducible.
- Assignment of authorization to users / user groups only for a limited time.
- Password aging strategies

Change log

A change log can be recorded when the access protection is activated. This includes, for example:

- Activation
- Deactivation
- Configuration of access protection and the change log
- Opening and closing of projects and libraries including their download to the target system as well as activities to change the operating state

7.2.4.2 Know-how protection in engineering

Know-how protection types

The know-how protection in SIMOTION SCOUT prevents unauthorized viewing and editing of your programs or parameters directly in the drive unit. Multiple logins are possible. The standard login can be set for the engineering session.

A distinction is made between two types of know-how protection:

- Know-how protection for programs and libraries
- Know-how protection for drive units (as of SINAMICS V4.5)

A login and a password have to be set under **Project > Know-how protection**. The know-how protection for the program is activated via the **Set** menu command. The programs contained in the project are still visible to the user in this session, but the program names are displayed with a padlock symbol.

Programs and libraries

The know-how protection protects the programs and libraries in your project. Unauthorized viewing and editing of your programs is prevented when the know-how protection is activated. You can set the know-how protection for individual programs or for all programs in a project.

Access protection and encryption can be set in several levels for the following types of data:

- Programs (units in ST, MCC and LAD/FBD that contain programs, function blocks and functions)
- DCC charts
- Libraries

You can select three different security levels for the encryption:

- **Standard**
  Access only with user login and password (backward compatible with versions before V4.2).
- **Medium**
  Improved coding of the password (due to a new procedure, no backward compatibility without knowledge of the password).
  Programs and libraries can be recompiled at any time even without knowledge of the password.
- **High** (only for ST source files in libraries)
  Compilation is only possible after the password has been entered.
  Protected libraries can also be used after an export without knowledge of the password, because in this case the compilation result is also exported.
  - **An export without source texts is also possible when exporting libraries**
    Highest protection. Complete removal of the source texts in the engineering upon export. The export only contains the compilation result (recompilation no longer possible).

The block interfaces are always visible.

Drive units in SIMOTION SCOUT

The know-how protection for drive units only applies online and is used to protect intellectual property, in particular, the know-how of machine manufacturers, against unauthorized use or reproduction of their products.

A detailed description can be found in Chapter Write and know-how protection (Page 66).

7.2.4.3 Copy protection for the configuration on the control system.

Copy protection for SIMOTION projects

Measures can be taken to tie the configuration to the memory card or the controller. This prevents illegal duplication of the configuration.

The serial numbers of the CPU, memory card and DRIVE-CLiQ components in the application can be queried via system functions. This enables the machine manufacturer to create a block with an encryption algorithm which generates a key from the currently installed serial numbers during runtime and compares it with a machine key. Each machine configuration has a specific machine key which is generated by the machine manufacturer and stored in the application, and which can be entered by the end customer, for example, via the HMI, particularly during maintenance work.

In addition, special agreements can also be made regarding extended know-how protection and copy protection through the use of a SIMOTION Open Architecture technology package.

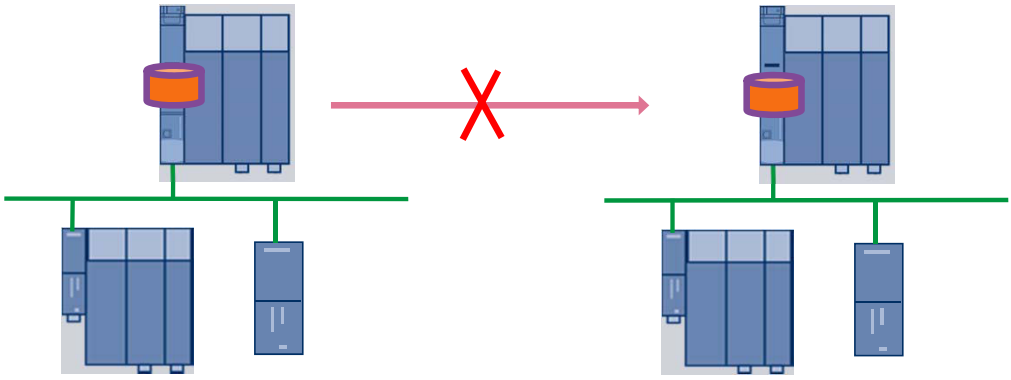

Figure 7-4 Copy protection of binary SIMOTION SCOUT projects

7.2.5 Offline/online comparison

Project comparison

You can use the SIMOTION SCOUT/STARTER **Project comparison** function (start this via the **Start object comparison** button) to compare objects within the same project and/or objects from different projects (online or offline).

The offline/online comparison is used to detect in detail any subsequent manipulations of the project data on the plant in comparison to your secured engineering data. Thus you check if any unauthorized third parties accessed the system.

The following comparisons are possible:

- Offline object with offline object from the same project
- Offline object with offline object from a different project
- Offline object with online object

The project comparison in SIMOTION SCOUT contains all objects in a project, such as SIMOTION devices, drive units, libraries, programs (units), technology objects, I/Os as well as the configuration of the execution system.

The offline/online comparison provides support for service jobs or for detecting changes to the project data.

It may, for example, be the case that inconsistencies are indicated when you switch to online mode in the project navigator, i.e. there are deviations between your project in SIMOTION SCOUT and the project loaded into the target system.

Possible causes can include, for example:

- A program has been changed
- The result of compiling a program is different
- There is a deviation on the global device variables

- The execution system has been changed
- The hardware configuration has been changed
- A library has been changed
- A configuration data item for an axis has been changed

The object comparison allows you to establish these differences and, if necessary, run a data transfer to rectify the differences.

Detailed offline/online comparison

You can determine specific differences between the offline and the online project by performing a complete project comparison. If there are discrepancies, you can determine the changes/ manipulation to the source code down to the program line level, when the additional information (source information) has also been stored on the target system during the download. This is also possible with the LAD/FBD and MCC graphical programming languages.

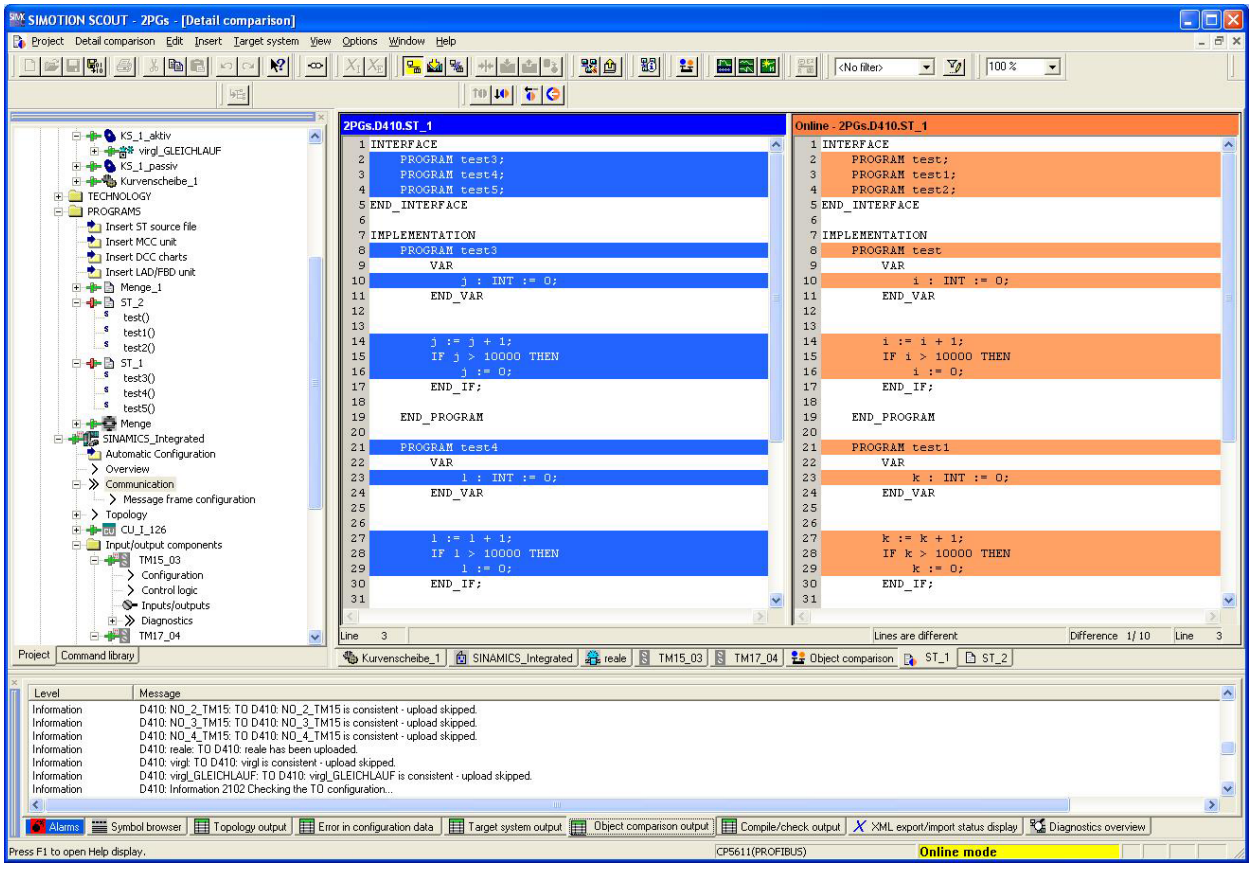

Figure 7-5 Example of ST detail comparison

7.2.6 SIMOTION IT Web server

Introduction

SIMOTION devices provide a Web server with preprepared standard websites. These websites can be displayed via Ethernet using a commercially available browser. Additionally, you have the option of creating your own HTML websites and incorporating service and diagnostic information. The web server can be deactivated. If the Web server is active, secure operation of the plant can be ensured via the integrated security concept and the user administration.

Deactivating/activating the Web server

The Web server with all functions and services can be activated or deactivated in the SIMOTION SCOUT or SIMOTION SCOUT TIA project under the hardware configuration of the controller. You can activate or deactivate individual functions.

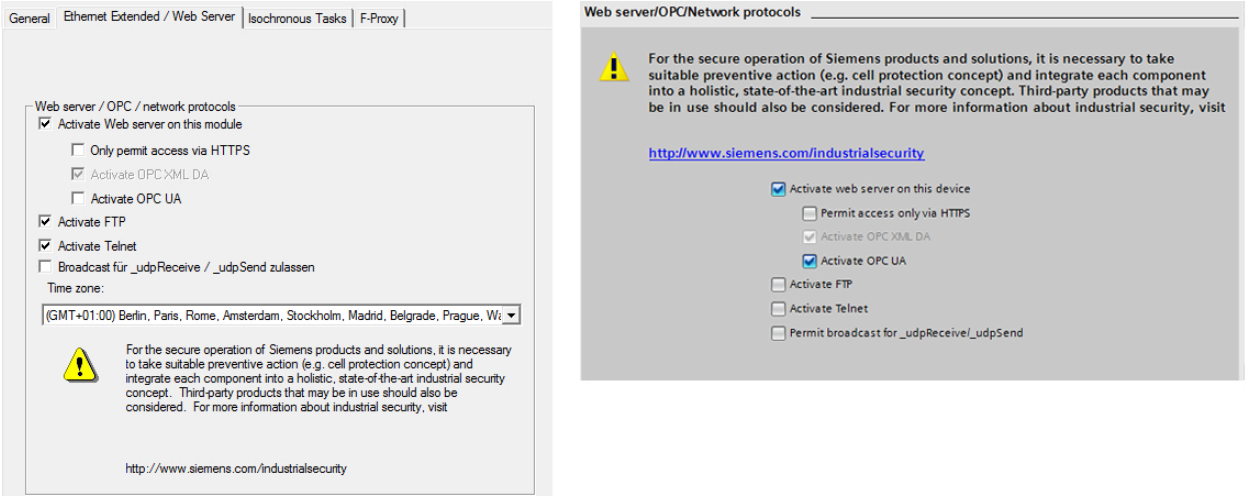

Figure 7-6 **Activating the SIMOTION IT Web server functions in SIMOTION SCOUT or SIMOTION SCOUT TIA**

Note

To activate the Web server, you must establish a user administration scheme with password-protected user access.

Security concept of HTTP/S, FTP and Telnet access on the Web server

As of version V4.4, access to the SIMOTION IT Web server is protected by a multi-level security concept.

The security status of the Web server is indicated by the security level on the website. This security level can have three different levels: Low, Normal, High

Security Level Low

The device is supplied with an empty user database. No projects exist yet. The security level is low to allow configuration of the device.

- In this state, access to the Web server as an anonymous user is possible to enable use of functions such as the project and firmware update or OPC XML.
- FTP and Telnet access are also possible.
- New users can be entered in the empty user database.

Security Level Normal

The controller has a user database. A project exists on the controller and HTTP, HTTPS, FTP, and Telnet are activated in the hardware configuration.

- User password authentication is mandatory for access to websites with sensitive content (e.g. firmware update, watch table, ...), FTP and Telnet.

As soon as a project has been loaded to the controller, Security Level Normal is active. If required, with an empty user database. Standard websites are still visible. All other websites can only be accessed with the necessary authentication.

Security Level High

High security with maximum access protection:

- HTTP, HTTPS, FTP and Telnet have been deactivated via the project in the hardware configuration. Access to the Ethernet via the various ports of the services is then no longer possible. The Web server cannot be used.

User management

SIMOTION IT uses a user database to safeguard access to a device. The groups are stored in the user database along with their assigned users. The defined user groups can be assigned access rights to the individual Web server websites. The Web server is accessed after the authentication.

Authentication

- There are users (USERs).
- Each user has a password. This is encrypted.
- Users belong to groups (GROUP).
- Websites, directories, and applications are protected by secure areas defined for each group.
- Only users that belong to the secure area can access the protected website.
- Each secure area has a group of users who have access authorization.
- A user can belong to different groups.

Encrypted data transfer (HTTPS)

The Web server can be accessed via an HTTP as well as an HTTPS connection. The Secure Socket Layer protocol (SSL) in HTTPS enables encrypted data transmission between a client (browser) and the SIMOTION controller (Web server). Secure transmission can be forced by deactivation of the HTTP port for security reasons.

Certificates must be generated and installed for encrypted communication between the browser and the Web server. A device comes supplied with a standard root certificate and a private key of the Web server as a file. These files should be replaced with your own to increase the security of HTTPS access to the device.

Key files

- Delivery state
  In order for you to be able to access the SIMOTION controller via the SIMOTION IT diagnostics standard websites (in their delivery state) via HTTPS, a root certificate and a private key are supplied as a file on the device.
- Create the SSL certificate yourself
  The cert.pl Perl tool can be used to generate the certificates required for customer plants (sites) and combine them into packages for loading.

There are two ways of acquiring your own server certificate (SSL certificate):

- Create a root certificate (self-signed) and a private key using a certificate software.
- Purchase a server certificate from a certificate authority.

Importing the SSL certificate into the browser

If you use SSL with your own certification authority, you will need to prepare your PCs for communication with the SIMOTION controller. To do this, the root certificate must be added to the list of certificates in your browser.

Reference

You will find a detailed description on the SIMOTION IT Web server in the following documentation:

- SIMOTION IT Diagnosis and Configuration (Diagnostics Manual)
- SIMOTION IT OPC UA (Programming Manual)
- SIMOTION IT Programming and Web Services (Programming Manual)
- SIMOTION IT Virtual Machine and Servlets (Programming Manual)

7.2.7 OPC UA server

Introduction

SIMOTION has implemented an OPC UA server with DA (Data Access).

OPC UA binary encoding is supported. Access to an arbitrary OPC UA client can be protected via authentication and encrypted data transfer.

Configuration

Note

Before connecting to the OPC UA server, ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

The OPC UA server can be activated or deactivated via HW Config from TIA Portal or STEP 7.

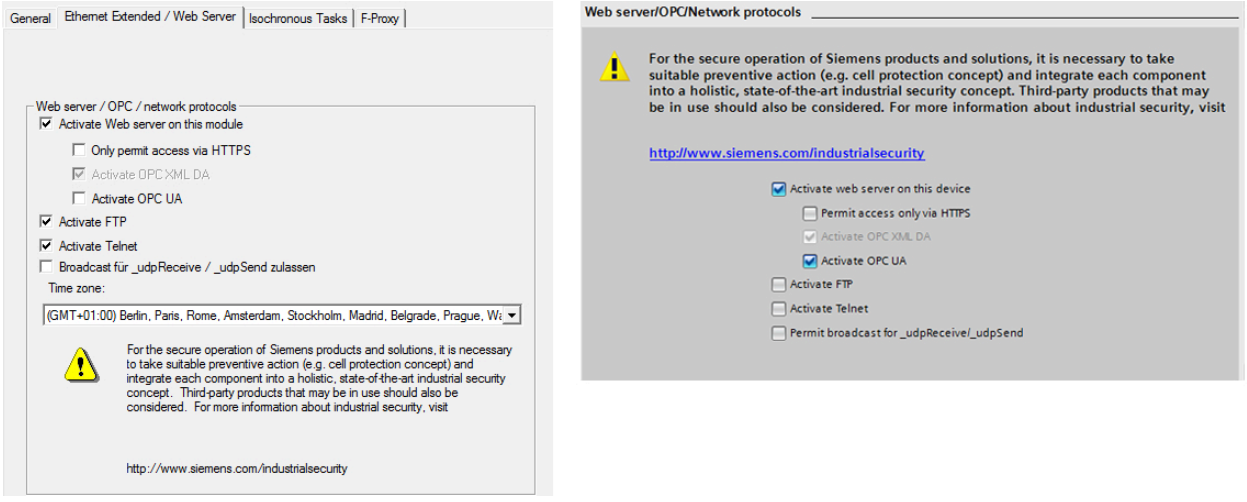

Figure 7-7 Activating the SIMOTION IT Web server functions in SIMOTION SCOUT or SIMOTION SCOUT TIA

Further settings are made via the SIMOTION IT Web server configuration masks:

- Enabling of the Ethernet interface and associated port of SIMOTION for the OPC UA access.
- Definition of the user name, password and user group as part of the user administration of the SIMOTION IT Web server.
- Handling of the certificates for the encryption of the data transfer.

Reference

You can find additional information about OPC UA in the SIMOTION IT OPC UA Programming Manual.

7.3 SINAMICS

7.3.1 Overview

The following section gives you an overview of the Industrial Security features for SINAMICS to protect your inverter from threats, and an overview of topics for which you should give special attention to Industrial Security:

- Write and know-how protection
- Parameters: Access levels + password
- Using the memory card
- Note on Safety Integrated
- Communication services and used port numbers
- Web server
- Information about individual interfaces
- SINAMICS Startdrive and STARTER
- SINAMICS Drive Control Chart (DCC)

As with the entire Manual, all of the listed measures are recommended. Detailed descriptions and procedures can be found in the corresponding SINAMICS documentation.

7.3.2 Network security

Note

Note that SINAMICS must only be used in a secure and trustworthy network with a firewall. Note the information on this topic in Section "Network segmentation (Page 24)".

7.3.3 Write and know-how protection

In order to protect your own projects against changes, unauthorized viewing or copying, SINAMICS converters have write protection and know-how protection functions.

Protection	Validity	Objective	Effect
Write protection	Online	Write protection is used to protect the parameterization from accidental changes by the user.	Adjustable parameters can be read, but cannot be written.
Know-how protection	Online	To protect intellectual property, especially the know-how of the machine manufacturers, against unauthorized use or reproduction of their products.	Adjustable parameters can neither be read nor written.

Further information

For detailed information on this topic, see the following references:

- SINAMICS S120 Function Manual, Drive Functions
  Sections "Write protection" and "Know-how protection"
- SINAMICS G Operating Instructions
  Sections "Write protection" and "Know-how protection"
- SINAMICS S and SINAMICS G List Manuals
  Section "Parameters for write protection and know-how protection"

7.3.4 Parameters: Access levels and password

The SINAMICS parameters are divided into access levels 0 to 4. With the aid of the access levels, you can specify which parameters can be modified
by which user or input/output device:

- For example, with the aid of parameter p0003, you can specify which access levels you can select with the BOP or IOP.
- Parameters of access level 4 are password-protected and only visible for experts.

Note

Special feature for the safety password

The safety password does not have the equivalent quality of a password (protection against unauthorized access, e.g. of an attacker), but rather that of write protection (e.g. protection against maloperation by authorized users).

The SINAMICS S and SINAMICS G List Manuals specify in which access level the parameter can be displayed and changed.

Further information

For detailed information on this topic, see the following references:

- SINAMICS S120 Function Manual, Drive Functions
  Section "Parameters"
- SINAMICS S120 Safety Integrated Function Manual
  Section "Handling the safety password"
- SINAMICS G Operating Instructions
  Section "Parameters"
- SINAMICS S and SINAMICS G List Manuals
  Section "Explanation of the list of parameters"

7.3.5 Using the memory card

The memory card must be handled with particular care for all SINAMICS devices that use a memory card so that no malicious software or erroneous parameterizations are spread between different commissioning PCs or inverters.

⚠ WARNING

Risk of death due to software manipulation when using exchangeable storage media

Storing files onto exchangeable storage media amounts to an increased risk of infection of the commissioning PCs, e.g. with viruses or malware. Incorrect parameter assignment can cause machines to malfunction, which can lead to injuries or death.

- Protect files stored on exchangeable storage media from malicious software using appropriate protection measures, e.g. virus scanners.

⚠ WARNING

Risk of death due to software manipulation when using exchangeable storage media

Storing the parameterization (incl. Safety Integrated parameterization) on exchangeable storage media carries the risk that the original parameterization (with Safety Integrated) will be overwritten, for example, by the memory card of another drive without Safety Integrated. Incorrect parameter assignment can cause machines to malfunction, which can lead to injuries or death.

- Ensure that only the memory card that belongs to the respective inverter is used.
- Ensure that only trained or authorized personnel have access to the enclosures, cabinets or electrical equipment rooms.

7.3.6 Note on Safety Integrated

To actually reduce the risk for machines and plants through the use of Safety Integrated functions, working with Safety Integrated functions requires special care for all SINAMICS devices that have it.

⚠ DANGER

Risk minimization through Safety Integrated

Safety Integrated can be used to minimize the level of risk associated with machines and plants.
Machines and plants can only be operated safely in conjunction with Safety Integrated, however, if the machine manufacturer adheres to the following rules:

- The machine builder (OEM) precisely knows and observes the technical user documentation, including the documented boundary conditions, safety information and residual risks.
- The machine or plant is carefully set up and configured and a thorough acceptance test must then be performed by qualified personnel and the results documented.
- All of the measures required in accordance with the machine/plant risk analysis are implemented and validated by the programmed and configured Safety Integrated functions or by other means.

The use of Safety Integrated does not replace the machine/plant risk assessment carried out by the machine manufacturer as required by the EC machinery directive.
In addition to using Safety Integrated functions, further risk reduction measures must be implemented.

7.3.7 Communication services and used port numbers

SINAMICS converters support specific communication protocols. The address parameters, the relevant communication layer, as well as the communication role and the communication direction are decisive for each protocol. You require this information to match the security measures for the protection of the automation system to the used protocols (e.g. firewall). The security measures are restricted to Ethernet and PROFINET networks.

For detailed information on this topic, see the following references:

- SINAMICS S120 Function Manual, Drive Functions
  Section "Communication services and used port numbers"
- SINAMICS G Function Manual, Fieldbuses
  Section "Ethernet and PROFINET protocols that are used"

7.3.8 Web server

The SINAMICS web server provides information on a SINAMICS device via its websites. This is accessed via an Internet browser.

Data transfer

In addition to the normal (unsecured) transmission (HTTP), the Web server also supports secure transmission (HTTPS). Secure transmission (https) is the recommended setting.

By entering "http://" or "https://" in front of the address of the drive, you can decide yourself whether normal or secure transmission is used to access the data.

For safety reasons, secure transmission can be forced by deactivation of the http port.

Access rights

The normal protection mechanisms of SINAMICS also apply for access via the web server, including password protection. Further protective mechanisms have been implemented especially for the Web server. Different access options have been set for different users, depending on the function. The parameter lists are protected so that only users with the appropriate rights can access or change the data.

Further information

For detailed information on this topic (e.g. the supported Internet browsers), see the following references:

- SINAMICS S120 Function Manual, Drive Functions
  Section "Web server"

7.3.8.1 Certificates for the secure data transfer

Protecting the HTTPS access

The "Transport Layer Security" (TLS) protocol enables encrypted data transfer between a client and the SINAMICS drive. HTTPS access between the browser and the drive is based on Transport Layer Security.

The encrypted variant of communication between the browser and the Web server using HTTPS requires the creation and installation of certificates (default configuration, self-created certificates or server certificates from a certification authority).

TLS

Transport Layer Security (TLS), more widely known under the predecessor designation Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure transfer of data in the Internet.

Key files

You need 2 key files (a public certificate and a private key) for the encryption method used by the Transport Layer Security.

Certificate handling

A master certificate and a private key as file on the device are supplied so that you can access the drive via https in the SINAMICS as delivered. How to establish an https connection with this data is described in the references under "Further information".

Further information

For detailed information on this topic, see the following references:

- SINAMICS S120 Function Manual, Drive Functions
  Section "Certificates for the secure data transfer"

7.3.9 Information about individual interfaces

X127 LAN (Ethernet)

The following restrictions apply for the LAN interface X127:

- Only local access possible
- No networking, only point-to-point connection permissible

X140 serial interface (RS232)

An external display and operator device for operator control/parameterization can be connected via the serial interface X140.

NOTICE
Access to the inverters only for authorized personnel Unauthorized persons may be able to damage or alter production equipment as a result of gaps in a company's physical security. Confidential information can also be lost or altered as a result of this. This can be prevented if both the company's site and the production areas are protected accordingly. • You can find information on suitable protective measures in Section "Physical protection of critical production areas (Page 23)".

X150 P1/P2 PROFINET

In accordance with the Defense in Depth concept (see Section "General security measures (Page 21)"), PROFINET must be isolated from the remaining plant network. Access to cables and possibly open connections must be implemented in a protected fashion, as in a control cabinet.

Further information

For detailed information on this topic, see the following references:

- SINAMICS S120 Manual Control Units and Control Elements
  Section on the respective interfaces
- SINAMICS S120 Function Manual, Drive Functions
- SINAMICS G Operating Instructions

7.3.10 SINAMICS Startdrive and TIA Portal

7.3.10.1 Danger to life caused by incorrect or changed parameterization

⚠ WARNING

Danger to life or malfunctions of the machine as a result of incorrect or changed parameterization

As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- Protect the parameter assignments against unauthorized access through "write protection".
- Respond to possible malfunctions by applying suitable measures (e.g. EMERGENCY STOP or EMERGENCY OFF).

See also

Write and know-how protection (Page 66)

7.3.10.2 SINAMICS Startdrive

Startdrive in the TIA Portal

SINAMICS Startdrive is an option package in the TIA Portal with which SINAMICS drives are commissioned. With regard to Industrial Security, the specifications for SINAMICS drives and for the TIA Portal must be taken into account.

In addition to the commissioning of single drives, drives on SIMATIC controllers such as the S7-1500 can also be configured. Information on how to proceed with SIMATIC controllers can be found in the TIA Portal online help at "Configuring networks".

Commissioning computer

Make sure that your commissioning computer runs in a secure environment and that the logon is protected via a secure password.

SINAMICS drives

The product-specific measures with regard to Industrial Security for SINAMICS drives can be found at SINAMICS (Page 66).

7.3.10.3 SINAMICS STARTER

Commissioning drives with STARTER

Drives of the MICROMASTER and SINAMICS families can be commissioned with STARTER. An integrated version of STARTER is contained in SIMOTION SCOUT. For information on SIMOTION SCOUT, see SIMOTION (Page 53).

Commissioning computer

Make sure that your commissioning computer runs in a secure environment and that the logon is protected via a secure password.

Security functions

- Know-how protection for the parameter assignment, scripts and DCCs and DCC libraries with password and encryption
- Copy protection for the configuration on the drive unit. The project can only be opened together with the original card.
- Detection of parameter manipulation with STARTER via the project comparison, see also Offline/online comparison (Page 60)
- Activation/deactivation of unused functions (Web server, ports), see also Web server (Page 69)
- Write protection for the parameter assignment, p-parameters are readable, but not writeable, protects against unintentional changes to the parameter assignment (only available online).

Know-how protection for drive units

In addition to the know-how protection for DCCs, DCC libraries and scripts, you can also protect the parameter assignment of your drive against unauthorized access via the know-how protection for the drive. The function is only available online. See also Write and know-how protection (Page 66).

Scripting

Scripts are used for automated execution in STARTER. You must therefore test the scripts before using them on machines.

⚠ WARNING

Risk due to incorrect configurations for automated operating actions

Scripting provides the extensive automation options that are required to be able to automate manual operator actions in the STARTER/SCOUT tools and therefore to optimize the time required for the recurring configuration of projects and tasks.

The script programmer and the script user are responsible for the operator actions implemented in scripting.

Incorrect configurations that are not discovered in tests can result in serious physical injury or death.

- Run systematic tests on new and modified scripts to verify and validate them.
- Before running a script, make sure it has the correct content. Verify and validate the results of script execution by tests on the machine.

As for DCC charts, scripts can also be protected via know-how protection.

7.3.11 SINAMICS Drive Control Chart (DCC)

7.3.11.1 Industrial Security with SINAMICS DCC

Overview

SINAMICS Drive Control Chart (DCC) offers a modular, scalable technology option, which has chiefly been developed for drive-related, continuous open-loop and closed-loop control engineering tasks.

With the Drive Control Chart Editor (DCC Editor) based on CFC, technology functions with DCC for SINAMICS drives can be configured graphically. The following figure illustrates the data flow of the configuration data when configuring with SINAMICS DCC and the ways to protect the configured/programmed DCC sources:

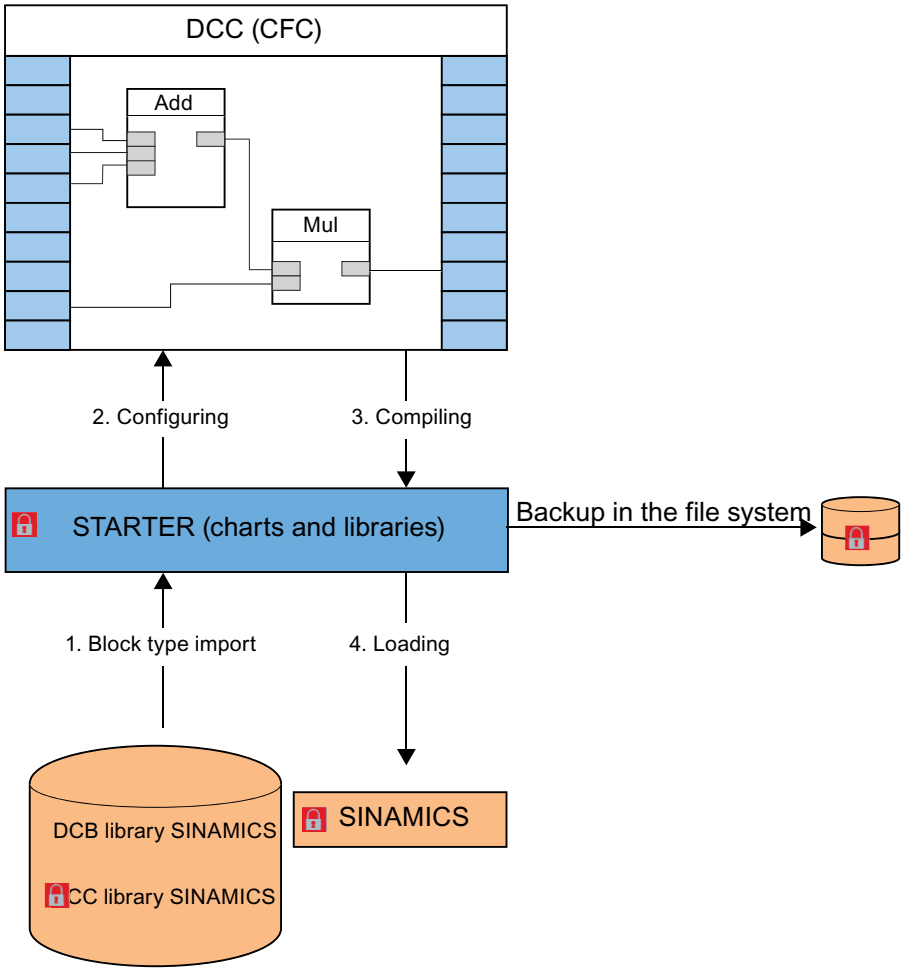

Figure 7-8 Flow of configuration data

Commissioning computer

Make sure that your commissioning computer runs in a secure environment and that the logon is protected via a secure password.

Using know-how protection

DCCs, DCC libraries, programs and backup files are subject to an increased risk of manipulation. Therefore, use the know-how protection, the write protection for drive units and the know-how protection for DCC charts and DCC libraries in STARTER, see also Use write and know-how protection (Page 76).

Information on know-how protection can also be found in the "Motion Control SINAMICS/ SIMOTION Editor Description DCC" Programming and Operating Manual.

Protecting backup files in the Windows file system

If you create backup files of charts or projects with Windows tools, you should also protect them with Windows tools against unauthorized access using secure passwords.

Note the information on SINAMICS and on the engineering systems

Also note the Industrial Security information for SINAMICS drives and engineering systems with which SINAMICS drives are commissioned. Particularly the information on network security is important, see also Network security (Page 24).

7.3.11.2 Use write and know-how protection

Prevent unauthorized changes by means of know-how protection

⚠ WARNING

Danger to life through manipulation of DCC charts and DCC libraries

The use of unprotected DCCs and DCC libraries entails a higher risk of manipulation of DCCs, DCC libraries and backup files.

- Protect important DCC charts and DCC libraries by using **know-how protection programs** or via the **know-how protection for drive units** in the SCOUT/STARTER. You can prevent manipulation by assigning a strong password.
- For **know-how protection programs** and **the know-how protection of drive units**, use passwords which include at least eight characters, upper and lower cases, numbers and special characters.
- Make sure that only authorized personnel can access the passwords.
- Protect the backup files on your file system using a write protection.

7.3.12 SINAMICS V20 Smart Access

The optional SINAMICS V20 Smart Access module gives you an intelligent solution for commissioning the SINAMICS V20 inverter.

SINAMICS V20 Smart Access is a web server module with integrated WLAN connectivity. It allows web-based access to the inverter from a connected device (conventional PC with WLAN

adapter, tablet or smartphone). This module is only intended for commissioning and therefore cannot be used with the inverter for the long term.

NOTICE

WLAN: Changing a default password

The misuse of passwords can also represent a considerable security risk.

- After the first login to SINAMICS V20 Smart Access using the default password, change the default password of SINAMICS V20 Smart Access.
- Assign a secure password. You can find information about this in the "SINAMICS V20 Inverter" Operating Instructions.

NOTICE

Unauthorized access to the inverter via the SINAMICS V20 Smart Access module

Unauthorized access to the SINAMICS V20 via the SINAMICS V20 Smart Access module as a result of cyber attacks could lead to interruptions of the process.

- Before you log in to the V20 websites, check the status LED on the SINAMICS V20 Smart Access module. If the status LED illuminates green or flashes, ensure that no unauthorized access has occurred. If unauthorized access has occurred, switch the SINAMICS V20 Smart Access module off and then on again via the on/off switch to restore the WLAN connection.

References

A

Additional general information about Industrial Security is available on the Internet.

- Industrial security (https://www.siemens.com/industrialsecurity)
- Implement security (https://www.industry.siemens.com/services/global/en/portfolio/plant-data-services/industrial_security)
- Operational Guidelines for Industrial Security (https://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf)

Additional product-specific information about Industrial Security is available on the individual product websites:

- SINUMERIK: SINUMERIK homepage (https://www.siemens.com/sinumerik)
- SIMOTION: SIMOTION homepage (https://www.siemens.com/simotion)
- SINAMICS: SINAMICS homepage (https://www.siemens.com/sinamics)

Product-specific manuals for the individual products can be found on the Internet:

- "SINUMERIK 840D sl NCU 7x0.3 PN" Manual (https://support.industry.siemens.com/cs/de/en/view/99922219)
- "Commissioning CNC: NC, PLC, Drive" Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109481519)
- "SINUMERIK 840D sl Operating System NCU (IM7)" Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109481527)
- "SINUMERIK 840D sl Base Software and HMI sl" Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109254363)
- "SINUMERIK Operate (IM9)" Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109481529)
- "PCU Base Software (IM10)" Commissioning Manual (https://support.industry.siemens.com/cs/de/de/view/109481697)
- "SIMOTION IT Programming and Web Services" Programming Manual (https://support.industry.siemens.com/cs/de/en/view/109476528)
- "SINAMICS S120 Drive Functions" Function Manual (https://support.industry.siemens.com/cs/de/en/view/109740020)
- SINAMICS S120 Safety Integrated Function Manual (https://support.industry.siemens.com/cs/de/en/view/109740018)
- SINAMICS S120/S150 List Manual (https://support.industry.siemens.com/cs/de/en/view/109739998)

Standards and regulations relating to Industrial Security are available on the Internet.

- IEC 62443

Glossary

AMC

Abbreviation for SINUMERIK Integrate Analyze MyCondition

AMD

Abbreviation for SINUMERIK Integrate Access MyData

AMM

Abbreviation for SINUMERIK Integrate Access MyMachine

AMP

Abbreviation for SINUMERIK Integrate Analyze MyPerformance

AMT

Abbreviation for Intel® Active Management Technology

Area of attack

The scope to which a system can be deprived of its protection so that it can be attacked.

Attack

An attempt to destroy a resource, to deprive it of its protection, to change it, to deactivate it, to steal it, to gain unauthorized access to it or to use it in an illegal way.

Authentication

Verification of the identity of a user, process or device, frequently as prerequisite for the permission to access resources in an information system.

Authorization

The right granted by a system entity to access a system resource.

Availability

Property to be accessible and usable when requested by an authorized entity.

Brute force

There are no efficient algorithms for solving many of the problems in computer science. The most natural and simplest approach to an algorithmic solution for a problem is to simply try out all possible solutions until the correct one is found. This method is called brute-force searching. One typical application is given again and again when it comes to listing an example of brute-force searching - the "cracking" of passwords. Passwords are often encrypted using cryptographic hash functions. Directly calculating the password from the hash value is practically impossible. However, a password cracker can calculate the hash values of numerous passwords. If a value matches the value of the stored password, then the password (or another, randomly matching password) has been found. In this case, brute force refers to the simple trial and error approach of entering every possible password.

Cloud computing

Cloud computing is the storage of data in a remote data center, and can also involve the execution of programs that are not installed on local computers, but rather in the (metaphoric) cloud.

Confidentiality

Property which ensures that the information is not made available or disclosed to unauthorized individuals, entities or processes.

Defense in depth

Potential cause of an undesirable incident which may result in damage to a system or organization.

Denial of service (DoS)

Denial of service (DoS) is the non-availability of an IT-based service that is normally available. Although there can be many reasons for such non-availability, the term "DoS" is generally used when infrastructure systems are overloaded. This can be the result of an unintentional overload or through a deliberate attack on a server, a computer or other components in a network.

DMZ

The demilitarized zone is an autonomous subnet that separates the local area network (LAN) from the Internet through firewall routers (A and B). The firewall routers are configured in such a way that they reject data packets for which there were no previous data packets. If a data packet is sent from the Internet to the server, it is therefore rejected by firewall router A. If, however, a hacker gains access to a server within the DMZ and sends data packets to the LAN in an attempt to analyze or hack it, these are rejected by firewall router B.

Firewall

Device to connect networks with one another, which restricts the exchange of data between two connected networks.

Hacker

Person involved in an intentional hacking activity. The reasons for these activities can be malicious or not malicious, or also remain within the limits of what is ethnically and legally acceptable.

Hardening

Procedure in which the security of a system is increased by reducing the area of attack.

IANA

The **I**nternet **A**ssigned **N**umbers **A**uthority (**IANA**) is a department of ICANN, and is responsible for assigning numbers and names in the Internet, especially IP addresses. It is one of the oldest institutions in the Internet.

Incident

One or more unwanted or unexpected events that impair the company operation and endanger the information security. The cause can be security holes, incorrect configurations or misconduct and their exploitation.

Industrial security

Measures to increase the industrial security standards of a plant. They protect against unauthorized access to higher-level control systems, industrial controls and PC-based systems of the plant as well as against cyber attacks.

Information security

Safeguards the confidentiality, integrity and availability of information.

Integrity

Property which guarantees that resources are free of error and complete.

IPsec (Internet Protocol Security)

IPsec is an expansion of the Internet protocol (IP) to include encryption and authentication mechanisms. This way, the Internet protocol can transport cryptographically secured IP packets via insecure public networks.

Malware

Malware is a general term for programs that have been developed to damage users. There are numerous types of malware, e.g. viruses, trojans, rootkits or spyware.

MMP

Abbreviation for SINUMERIK Integrate Manage MyPrograms

MMT

Abbreviation for SINUMERIK Integrate Manage MyTools

NAT (Network Address Translation)

NAT is a process used in IP routers that connect local networks to the Internet. Since, in general, Internet access is only via one IP address (IPv4), all other nodes in the local network require a private IP address. Private IP addresses can be used several times, but are not valid in public networks. For this reason, nodes with a private IP address cannot communicate with nodes outside the local network. In order for all computers with a private IP address to have access to the Internet, the Internet access router must replace the IP addresses of the local nodes with a separate, public IP address in all outgoing data packets. In order for the incoming data packets to be assigned to the correct station, the router saves the current TCP connections in a table. The NAT router "memorizes" which data packets belong to which TCP connection. This process is called NAT (Network Address Translation).

NCU

Central control module of a CNC control for NC, HMI, PLC and closed-loop control.

OpenVPN

OpenVPN is a program to establish a virtual private network (VPN) via an encrypted TLS connection. Libraries belonging to the OpenSSL program are used for encryption. OpenVPN uses either UDP or TCP for transferring data.

Patch management

Area of the system management whose tasks include the procurement, testing and installing of several patches (code changes) for an administered computer system or in such a system. At the same time, a subprocess of the Security Vulnerability Management whose tasks include the correction and containment of security holes for Siemens products by means of software corrections.

PCU

Highly integrated industrial PC for the user interface or system software and user interface of a CNC.

Phishing

Phishing is the attempt to obtain personal data of an Internet user via fake websites, e-mails or text messages in order to steal the user's identity.

Remote access

Use of systems which are within the perimeter of the security zone and that can be accessed from another geographical location with the same rights as if the systems were physically at the same location.

SCADA

Supervisory **C**ontrol **a**nd **D**ata **A**cquisition (**SCADA**) involves monitoring and controlling technical processes using a computer system.

Security

Safeguards the confidentiality, integrity and availability of a product, a solution or a service.

Security hole

Weak point in a computer system that allows an attacker to violate the integrity of the system. As a rule, this is the result of program errors or design defects in the system.

A weak point of a resource or operator element that can be exploited by one or more threats.

SIEM system

SIEM stands for Security Information and Event Management and has become an established term in IT security. Such systems are able to identify and evaluate security-relevant events and notify the administrator.

Switch

Network component for connecting several terminal devices or network segments in a local network (LAN).

Threat

Potential cause of an undesirable incident which may result in damage to a system or organization.

Threat and Risk Analysis

The TRA (Threat and Risk Analysis) is a Siemens-wide standardized method for use in the product, solution and service business, for product development, engineering or service projects. The method is intended to help those involved in the project to identify typical security defects and weak points, analyze the hazards that could exploit these defects and weak points, and evaluate the resulting risks.

TLS

Transport Layer Security (TLS), more widely known under the predecessor designation Secure Sockets Layer (SSL), is a hybrid encryption protocol for secure transfer of data in the Internet.

VPN (Virtual Private Network)

An encrypted connection of computers or networks via the Internet. It enables confidential data to be exchanged via public networks.

WSUS (Windows Server Update Services)

Windows Server Update Services (abbreviation WSUS) is the software component of the Microsoft (Windows) Server since Version 2003 which is responsible for patches and updates. It is the successor version of the Software Update Services software component.

Index

T

U

V

W

X