SIEMENS

SINUMERIK

SINUMERIK ONE
Industrial Cybersecurity

Configuration Manual

Valid for the SINUMERIK ONE control system
CNC software Version 6.23

01/2024
A5E51912408B AB

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E51912408B AB
Ⓟ 12/2023 Subject to change

Table of contents

Introduction

1

1.1 About SINUMERIK

From simple, standardized CNC machines to premium modular machine designs – the SINUMERIK CNCs offer the right solution for all machine concepts. Whether for individual parts or mass production, simple or complex workpieces – SINUMERIK is the highly dynamic automation solution, integrated for all areas of production. From prototype construction and tool design to mold making, all the way to large-scale series production.

Visit our website for more information SINUMERIK (https://www.siemens.com/sinumerik).

1.2 About this documentation

1.2.1 Purpose of the documentation

1.2.1.1 Target group

Overview

This documentation is intended for the following target groups:

- Planners and project engineers
- System integrators
- IT department of machine manufacturers (OEM) or end users

The target groups mentioned can use the information provided in this manual to securely configure and use the product.

In particular **system integrators** require the information to be able to derive specifications to define technical security designs. The following issue is of central importance:

- Identify a suitable secure product configuration as component of the system engineering in which the product will be integrated.
  This documentation includes references to security requirements as laid down in IEC 62443-4-2 at the component level. The security requirements of the particular implementation in the product are compared in Chapter Security functions of the product (Page 55). This comparison is intended to support system integrators to harmonize product-specific security functions with the technical security design of the system itself.

1.2.1.2 Data for the technical security design and the secure system configuration

The system integrator defines the technical security design of the system and a secure configuration of all system components.

As part of this task, a system integrator must clearly understand the security capabilities of the product, and the recommendations for a secure configuration of the product. A good understanding of the relevant configuration options can be gained by reading Chapter System overview (Page 45).

The security capabilities of the product were developed with reference to a specific intended operational environment, and must be integrated in an overall security concept, as described in Chapter Security assumptions for the intended operational environment (Page 52). Generally, the system is the main component of the intended operational environment for the product, which means that the system integrator must also ensure that the technical overall security design of the system complies with the assumptions described in Chapter Security assumptions for the intended operational environment (Page 52). This is absolutely necessary for the overall system security level, and if the system should not comply with assumptions, then this is taken into account in the TRA of the system.

Details about the security capabilities and the secure configuration for the product are provided in Chapter Security functions of the product (Page 55). The specific operating

instructions for the settings are not part of this manual; however, you can find these in the Commissioning Manuals for the relevant product and the current online help.

The recommendations in the specified chapter support system integrators when it comes to the following security tasks:

- Chapter Recommendations for secure operation and secure disposal (Page 95): Defining the security documentation for secure operation and secure disposal, which the system integrator hands over to customers.
- Chapter Procedure for managing security updates (Page 105): Defining the procedure for managing security updates
- Chapter Tips for security checks (Page 109): Performing security tests

1.2.2 Standard scope

Standard scope

This documentation only describes the functionality of the standard version. This may differ from the scope of the functionality of the system that is actually supplied. Please refer to the ordering documentation only for the functionality of the supplied drive system.

It may be possible to execute other functions in the system which are not described in this documentation. This does not, however, represent an obligation to supply such functions with a new control or when servicing.

For reasons of clarity, this documentation cannot include all of the detailed information on all product types. Further, this documentation cannot take into consideration every conceivable type of installation, operation and service/maintenance.

The machine manufacturer must document any additions or modifications they make to the product themselves.

Websites of third-party companies

This document may contain hyperlinks to third-party websites. Siemens is not responsible for and shall not be liable for these websites and their content. Siemens has no control over the information which appears on these websites and is not responsible for the content and information provided there. The user bears the risk for their use.

1.3 Documentation on the internet

1.3.1 Documentation overview SINUMERIK ONE

Comprehensive documentation about the functions provided in SINUMERIK ONE Version 6.13 and higher is provided in the Documentation overview SINUMERIK ONE (https://support.industry.siemens.com/cs/ww/en/view/109768483).

You can display documents or download them in PDF and HTML5 format.

The documentation is divided into the following categories:

- User: Operating
- User: Programming
- Manufacturer/Service: Functions
- Manufacturer/Service: Hardware
- Manufacturer/Service: Configuration/Setup
- Manufacturer/Service: Safety Integrated
- Information and training
- Manufacturer/Service: SINAMICS

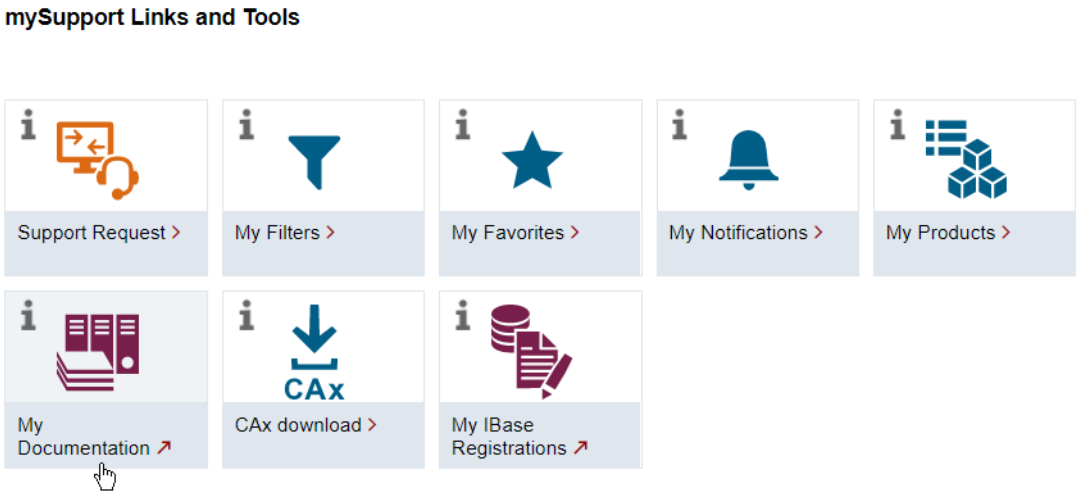
1.4 Feedback on the technical documentation

If you have any questions, suggestions, or corrections regarding the technical documentation published in the Siemens Industry Online Support, use the link "Give feedback" link which appears at the end of the entry.

1.5 mySupport documentation

With the "mySupport documentation" web-based system you can compile your own individual documentation based on Siemens content, and adapt it for your own machine documentation.

To start the application, click on the "My Documentation" tile on the "mySupport links and tools" (https://support.industry.siemens.com/cs/ww/en/my) portal page:



The configured manual can be exported in RTF, PDF or XML format.

Note

Siemens content that supports the mySupport documentation application can be identified by the presence of the "Configure" link.

1.6 Service and Support

Product support

You can find more information about products on the internet:

Product support (https://support.industry.siemens.com/cs/ww/en/)

The following is provided at this address:

- Up-to-date product information (product announcements)
- FAQs (frequently asked questions)
- Manuals
- Downloads
- Newsletters with the latest information about your products
- Global forum for information and best practice sharing between users and specialists
- Local contact persons via our Contacts at Siemens database (→ "Contact")
- Information about field services, repairs, spare parts, and much more (→ "Field Service")

Technical support

Country-specific telephone numbers for technical support are provided on the internet at address (https://support.industry.siemens.com/cs/ww/en/sc/4868) in the "Contact" area.

If you have any technical questions, please use the online form in the "Support Request" area.

Training

You can find information on SITRAIN at the following address (https://www.siemens.com/sitrain).
SITRAIN offers training courses for automation and drives products, systems and solutions from Siemens.

Siemens support on the go

With the award-winning "Industry Online Support" app, you can access more than 300,000 documents for Siemens Industry products – any time and from anywhere. The app can support you in areas including:

- Resolving problems when implementing a project
- Troubleshooting when faults develop
- Expanding a system or planning a new system

Furthermore, you have access to the Technical Forum and other articles from our experts:

- FAQs
- Application examples
- Manuals
- Certificates
- Product announcements and much more

The "Industry Online Support" app is available for Apple iOS and Android.

1.7 Using OpenSSL

This product can contain the following software:

- Software developed by the OpenSSL project for use in the OpenSSL toolkit
- Cryptographic software created by Eric Young.
- Software developed by Eric Young

You can find more information on the internet:

- OpenSSL (https://www.openssl.org)
- Cryptsoft (https://www.cryptsoft.com)

1.8 General Data Protection Regulation

Overview

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

For the SINUMERIK Operate, this means:

The product processes/saves the following personal data:

- FullName (optional): Only if user management is activated
- User name + password: Only if user management is activated
- UserID: nur bei aktivierter Benutzerverwaltung
- IP address
- Security events
- Time stamp

It does not involve data from the personal or private sphere.

The above data is required for the user log-in function. The storage of data is appropriate and limited to what is necessary, as it is essential for the identification of the authorized operator. (Mandatory here are: user name + password; the FullName is optional.)

The above-mentioned data cannot be stored anonymously or – with the exception of the user name – pseudonymously, as otherwise the purpose of identifying the operating personnel cannot be achieved.

Our products do not automatically delete the data mentioned above. The data and logs can be deleted manually by authorized personnel.

The above data is secured against loss of integrity and confidentiality by Industry State-of-the-Art Product Security mechanisms.

Security instructions 2

2.1 Fundamental safety instructions

2.1.1 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

Malfunctions of the machine as a result of incorrect or changed parameter settings

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

- Protect the parameterization against unauthorized access.
- Handle possible malfunctions by taking suitable measures, e.g. emergency stop or emergency off.

2.1.2 Warranty and liability for application examples

Application examples are not binding and do not claim to be complete regarding configuration, equipment or any eventuality which may arise. Application examples do not represent specific customer solutions, but are only intended to provide support for typical tasks.

As the user you yourself are responsible for ensuring that the products described are operated correctly. Application examples do not relieve you of your responsibility for safe handling when using, installing, operating and maintaining the equipment.

2.1.3 Cybersecurity information

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

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

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

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

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

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

Further information is provided on the Internet:

Industrial Security Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/108862708)

⚠ WARNING

Unsafe operating states resulting from software manipulation

Software manipulations, e.g. viruses, Trojans, 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 state-of-the-art, integrated industrial cybersecurity concept for the installation or machine.
- Make sure that you include all installed products in the integrated industrial cybersecurity concept.
- Protect files stored on exchangeable storage media from malicious software by with suitable protection measures, e.g. virus scanners.
- Carefully check all cybersecurity-related settings once commissioning has been completed.

What is industrial cybersecurity?

3

Definition of industrial cybersecurity

Generally, industrial cybersecurity 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 cybersecurity

The objectives of industrial cybersecurity encompass:

- Fault-free operation and guaranteeing of availability of industrial plants and production processes
- Preventing hazards to people and production due to cyber security attacks
- 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 cybersecurity 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.

3.1 Delimitation: Functional safety and industrial cybersecurity

Safety functions

Safety functions ensure the reliable functioning of safety-related components and functions, which must ensure that either the plant remains in a safe state or it is brought into a safe state if a fault occurs.

The highest priority is the prevention of systematic errors and the control of random errors or failures.

Functional safety guarantees the safety of persons and goods in the immediate vicinity of a component.

Security functions

Security functions and measures, on the other hand, maintain the expected system behavior by protecting against cyber attacks or unintended manipulation.

Cyber attacks and threats potentially leading to the failure of a component occur throughout the life cycle. For this reason security functions and measures must be regularly evaluated and adapted.

Why is industrial cybersecurity so important? 4

4.1 Trends with an impact on industrial cybersecurity

Global trends

There are many new trends which affect industrial cybersecurity. These effects underscore the relevance of security functions and measures.

- Cloud computing in general
  The number of network connections across the world is constantly increasing. This increasingly enables technologies such as cloud computing and the associated applications. 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. The development of new WLAN and mobile radio standards continues to advance.
- Worldwide remote access to plants, machines and mobile applications
- The Internet of Things (IoT)
  Millions of electronic devices are now network-capable and are communicating via the Internet.

To keep networked components and applications running smoothly, your plant needs a network infrastructure and applications that reliably protect against cyber attacks.

4.2 Possible corporate security vulnerabilities

Possible corporate security vulnerabilities

The security chain of a company is only as strong as its weakest link. Security vulnerabilities can occur in numerous places in an organization, such as:

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

A holistic approach is needed to identify security problems and find solutions. Binding guidelines and regulations must address all relevant areas of a company: Devices, systems, processes and employees.

4.3 Why is industrial cybersecurity so important?

The topic of data security is becoming increasingly important in the industrial environment, especially due to the worldwide increase in legal requirements for data protection.

Possible threats:

Potential security threats include confidentiality, integrity, and availability. Examples of threats are:

- Espionage of data
- Manipulation of data or software
- Sabotage of production plants
- System stoppage, e.g. due to virus infection or malware
- 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

General security measures in automation and drive technology

5

5.1 Security measures

Integration of security into the products

The following measures ensure the integration of security in current Siemens products for automation and drive technology:

- The requirements specified in IEC 62443-4-1 for the **product lifecycle management (PLM) process** are implemented. The implementation was certified by TÜV.
- **Code analyses** are used to identify and correct possible errors.
- Siemens implements **measures to secure integrity** in its products and its manufacturing processes.
- 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 checks its products for security weak points during development and performs appropriate **patch management**.
  - As manufacturer of automation and drive products, Siemens supports secure operation through direct support of system integrators and operating companies **by providing patches, security components and the appropriate services.**

Protection of the development infrastructure and supply chains

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

- 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 departments in the form of consulting and other services. **ProductCERT** provides information about current threats and vulnerabilities as well as the appropriate countermeasures.
- Industrial cybersecurity 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://new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html).

5.2 Defense in depth concept

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.

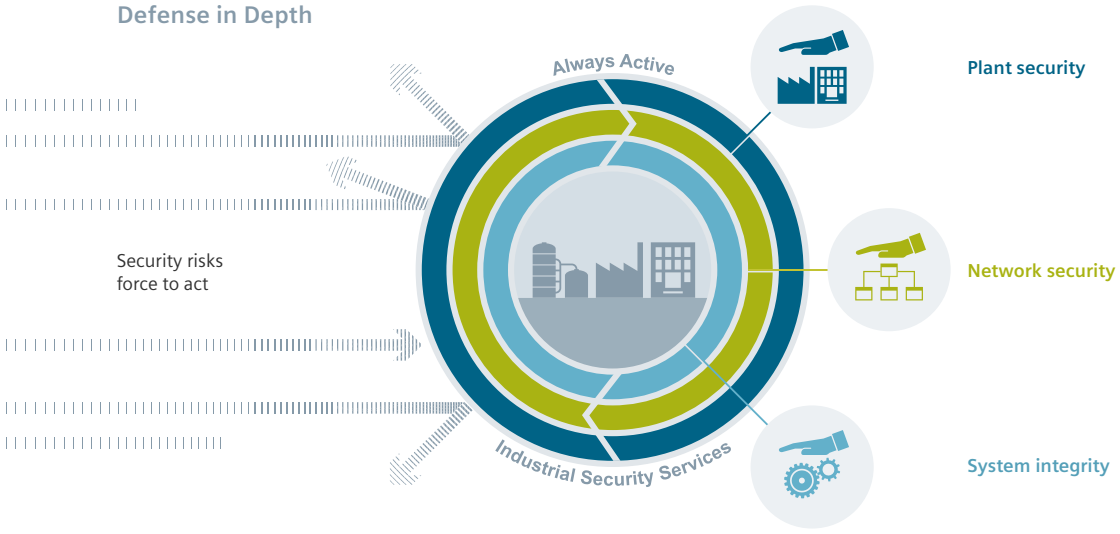


Figure 5-1 Defense in depth strategy

Further information on the defense in depth concept and the planning of a protection concept for industrial plants can be found on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/planning.html).

Protection levels

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 allowlisting 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.)

5.3 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.

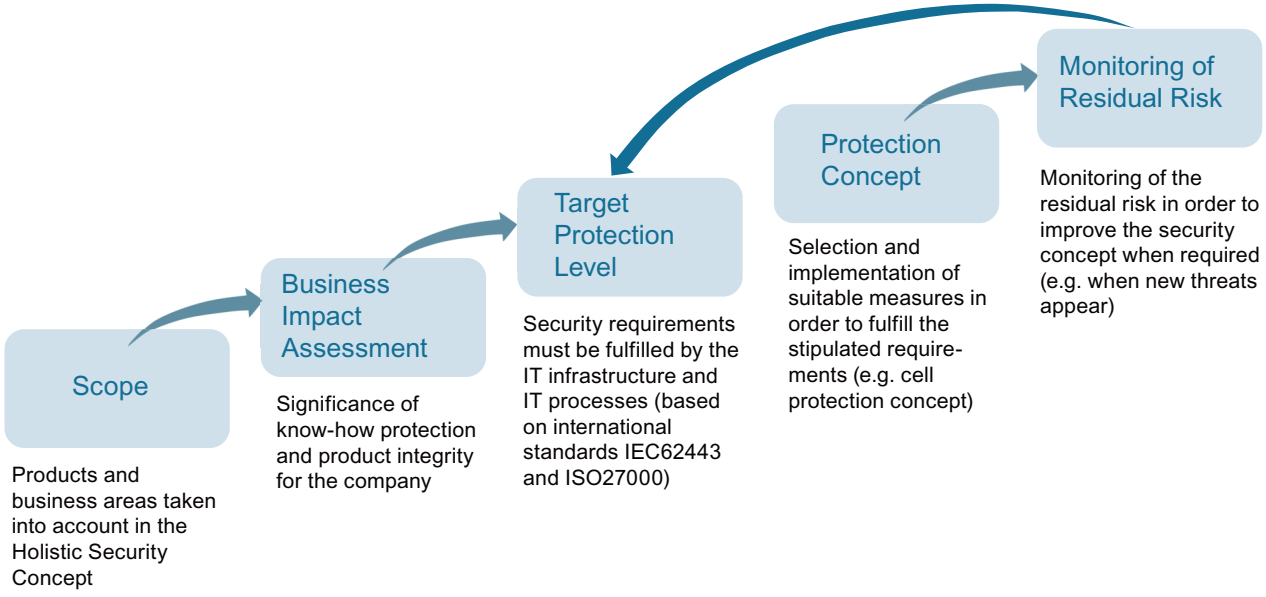


Figure 5-2 SI HSC security management process

5.4 Standards and regulations

Siemens takes the applicable industrial cybersecurity standards and regulations into consideration 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

More information on certifications and standards in the industrial cybersecurity field can be found on the Internet (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html):

5.5 Security management

Security management process according to IEC 62443 and ISO 27001 forms the basis for the successful implementation of industrial cybersecurity.

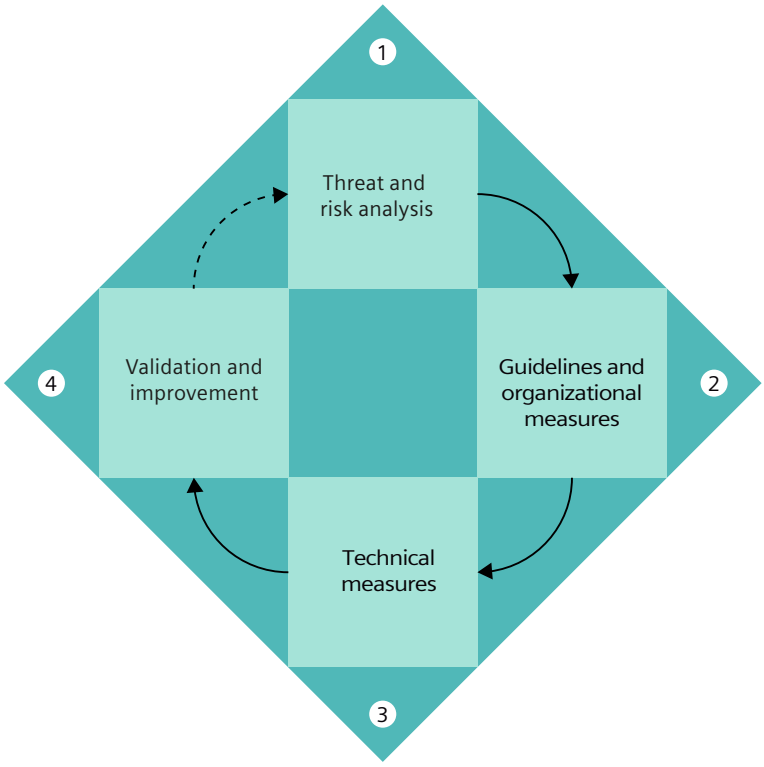


Figure 5-3 Security management process

Procedure

1. Perform a threat and risk analysis. Determine all potential risks and define countermeasures for reducing the risk to an acceptable level.
   A threat and risk analysis includes 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
   - Evaluation of effects with respect to protection goals: Confidentiality, integrity, and availability
2. Define guidelines and introduce coordinated, organizational measures.
   Establish awareness of the high relevance of industrial cybersecurity at all levels in the company. Define guidelines and processes for a consistent approach to security compliance.

3. Introduce coordinated technical measures.
4. Conduct a security audit to 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 ever-changing threat scenarios, this process must be constantly repeated. Implement the security management process as a continuous process.

5.6 Plant security

5.6.1 Overview

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.

5.6.2 Physical protection of critical production areas

The physical protection of critical production areas consists of 2 parts:

- Company security
- Production security

Company security

Company security must be ensured by taking the following measures:

- Closed off and monitored company premises
- Access control through locks, code cards, security personnel
- Escorting of external personnel by company employees
- Security processes in the company are taught and followed by all employees

Production security

For the products described in this manual, production security must be ensured by taking the following measures, for example:

- Separate access control for critical areas, such as production areas
- Installation of critical components in lockable control cabinets or in lockable electrical rooms (monitoring and alarm functions are recommended). Control cabinets must be equipped with a cylinder lock if the electrical room cannot be locked, or if components are installed outside a lockable electrical room. Do not use simple locks, such as universal, triangular/ square or double-bit locks.

- 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.

More information

More information on integrated Siemens security solutions can be found on this website (https://new.siemens.com/global/en/products/buildings/security/security-management.html).

5.7 Network security

5.7.1 Overview

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.

5.7.2 Network segmentation

5.7.2.1 Separation between production and office networks

The strict separation of production networks from the other company networks allows you to create protection zones for your production networks.

Note

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

Cell protection concept

The cell protection concept segments a production network into individual protection cells, between which all components communicate with each other in a secure manner. This is a way of restricting threats and security incidents to individual cells. Cell protection reduces the vulnerability of the entire production plant and thereby increases its availability.

General security measures

Implement the general security measures within protection areas.

More information is provided in Chapter "Reduction of the attack surface (Page 90)".

Firewall systems

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

DMZ network

A separate DMZ network provides a more secure pairing between production and office networks. Here, firewalls prohibit direct communication between production and office networks. Communication only takes place indirectly over servers in the DMZ network.

Note

Production networks should also be divided into individual protection cells in order to protect critical communication mechanisms.

5.7.2.2 Network segmentation with SCALANCE S

To meet the security requirements for network protection and network segmentation, Siemens offers SCALANCE S Industrial Security Appliances.

Requirement

Upstream SCALANCE S Industrial Security Appliances are housed in a secured control cabinet/ electrical room together with the components being protected. This ensures that data cannot be manipulated here unnoticed.

Description

SCALANCE S Industrial Security Appliances have the following features and characteristics:

- Stateful inspection firewall
  For user-specific control and logging, firewall rules can be specified that only apply to certain users.
- Data encryption and authentication
  Using VPN via IPsec, a VPN tunnel can be established for secure data transfer between authenticated users.
- Address translation with NAT/NAPT
- Router functionality for broadband Internet access
- Connection to the demilitarized zone (DMZ)
  Components such as the SCALANCE S623 have an extra VPN port for secure connection to the DMZ for service and remote maintenance.

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.

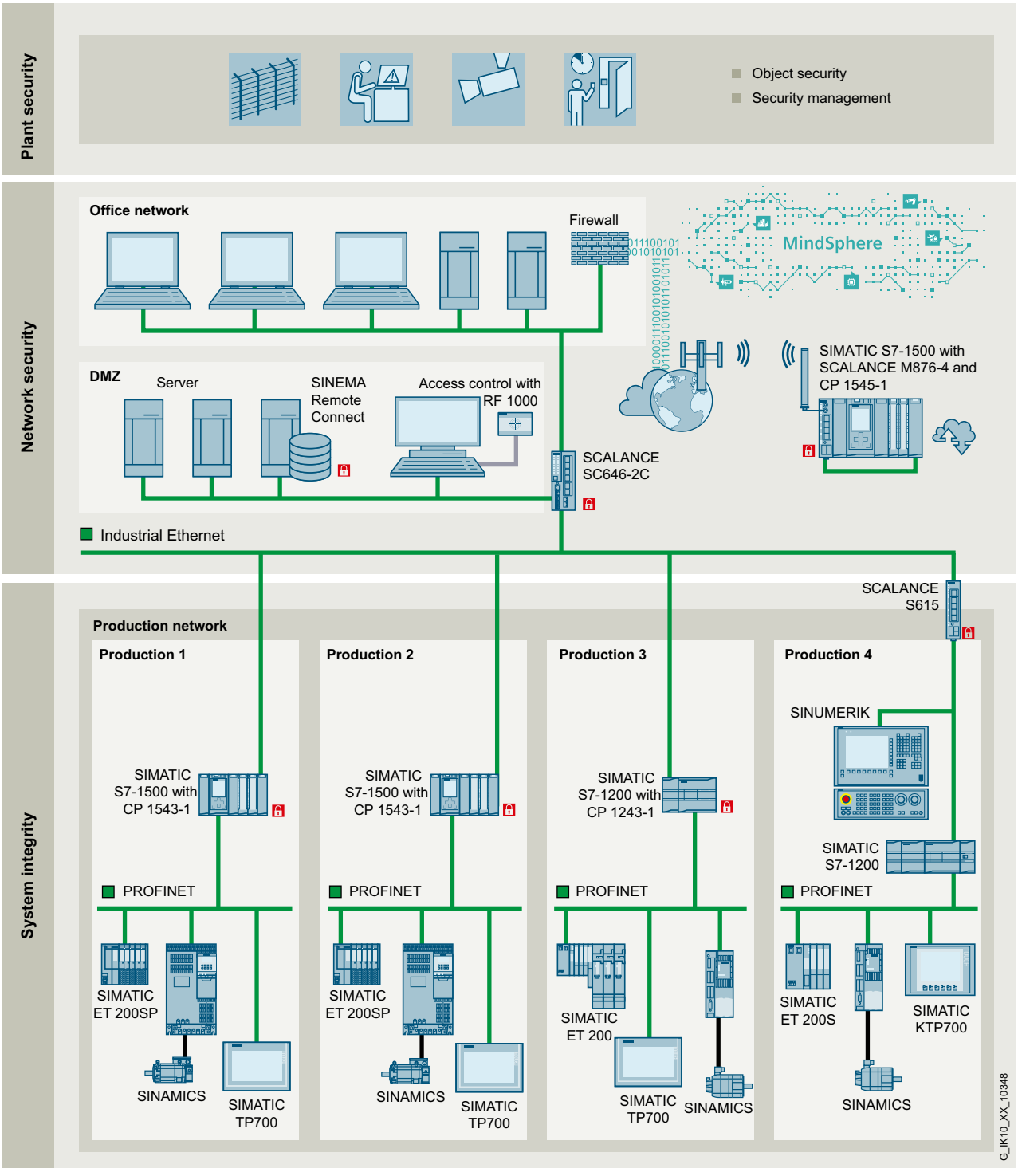


Figure 5-4 SCALANCE S application example

5.8 System integrity and authenticity

5.8.1 Overview

System integrity is understood to mean the "integrity" or "correctness" of the data or the correct response of the system. Thus, the following measures for protecting the system integrity should ensure that the data/functionality of the system cannot be manipulated by unauthorized persons or that manipulations can be detected.

Authenticity in the context of information security denotes the properties of genuineness, verifiability and trustworthiness. Authentication of the data source verifies that data can be assigned to a specified sender, which can be achieved using digital signatures.

5.8.2 System hardening

5.8.2.1 Services and ports

Recommendations

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.

More information

A description of all of the ports used can be found in the Equipment Manuals/Function Manuals of the respective products.

See also

Reduction of the attack surface (Page 90)

5.8.2.2 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

5.8.2.3 Operating units used in the industrial context

Recommendations

Operating units (such as PG/PCs, tablet PCs and smartphones) used in the industrial context must meet the generally applicable security requirements.

To minimize risk, take the following security measures:

- The deployed operating unit is set up, administered, regularly checked and patched by the appropriate departments. In terms of the secure configuration of an operating unit, this means:
  - Programs and operating systems are installed on the operating unit only if they are supported and regularly serviced by the manufacturer.
  - Security updates and patches for the installed operating system are regularly installed on the operating unit.
    You can find more information on patch management in Windows operating systems in Chapter "Windows patch management (Page 43)".
  - On the operating unit you can work with "Allowlists (Page 42)" and methods of the "Network segmentation with SCALANCE S (Page 35)" can be used. A virus scanner is additionally installed and regularly updated.
  - A firewall with appropriate settings is activated on the operating unit.
  - Non-volatile storage media (e.g. hard disks, SSD, eMMC) are encrypted to protect sensitive data against unauthorized access.
  - To prevent unintended changes to the configuration, only administrators should have admin rights to the operating unit.
- Only use the deployed operating unit in secured cells. The operating unit must not be used in the office network or via the Internet.
  You can find more information about the separation of the office and automation networks in Chapter "Network security (Page 34)".
- Secure PG/PCs against data theft using a lock or do not leave them unmonitored.

5.8.2.4 Store sensitive data securely

Examples of sensitive data stored on an operating unit include access data, project data and confidential data containing company secrets.

Ensure secure data storage when saving sensitive data on the operating unit.

To minimize risk, take the following security measures:

- Consequent marking of your documents according to confidentiality levels by introducing a document classification.
- Protect your encrypted storage locations against unauthorized access and manipulations.
- Regularly back up your sensitive data. Protect the backups against unauthorized access, loss and manipulation.

5.8.2.5 Transporting sensitive data securely

Take the following security measures when transporting sensitive data:

- Send sensitive data only via encrypted and signed emails or mobile data storage media, and only when absolutely necessary.
- If you wish to transport sensitive data on a storage medium such as a USB flash drive or hard disk, make sure that you only use storage media with an encryption function. The deployed storage media must be regularly checked for viruses.

5.8.2.6 Secure 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. Insecure passwords can easily be guessed or decoded. • Therefore, change the default passwords during the commissioning and adapt them at regularly defined intervals. • Also change passwords for functions that you yourself do not use to ensure that such unused functions are not misused. • 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. PINS must comprise an arbitrary sequence of digits.
- When assigning a password, always ensure you are adhering to the applicable company specifications, e.g. special password policy of the respective company.
- Observe that, in accordance with the applicable company specifications, passwords with the maximum required minimum length must be assigned.
- Wherever possible and where it is supported by the IT systems, a password must always have a character sequence as complex as possible.

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.

Further information on assigning secure passwords can be found in Chapter German Federal Office for Information Security (BSI) (https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html).

5.8.2.7 Virus scanner

Description

Antivirus programs and virus scanners are applications which detect, block and remove known computer viruses, computer worms, Trojan horses and other malware. Therefore, virus scanners do not protect against all malware and are only regarded as a supplement to general security 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.

Recommendations

Antivirus programs must not impair operation of the production plant.

Do not switch off an infected operating unit if that causes a loss of control of the production process.

To minimize risk, take the following security measures:

- Do not use online virus scanners:
  If you use an online virus scanner, confidential data can get into the wrong hands. Generally, therefore, do not use an online virus scanner.
- Up-to-date virus definitions:
  Make sure that the virus definitions in the database of your virus scanner are up to date at all times.
- Do not install multiple virus scanners:
  Avoid installing multiple virus scanners simultaneously on a single system.
- Connection to the production network:
  Only connect to the production network using an operating unit with virus protection.

Note

Recommendation

We expressly recommend the use of allowlists over virus scanners, since protection against malware is maintained even if there are no longer any updated virus patterns for the virus scanner used.
This ensures a longer lifetime for the operating system.

- Allowlists are only used on IPCs.
- There is no need to use allowlists on NCUs, since only signed software can be executed on them.

5.8.2.8 Allowlists

Allowlists are lists of applications that have been classed as trusted in a review.

These lists are used to decide which applications can be run on an operating unit. They provide protection against:

- Malware
- Unauthorized changes to installed applications and executable files (.exe, .dll)

5.8.2.9 Product security notifications

Recommendations

The threat scenarios for cyber attacks are diverse in nature and are continually changing.

For this reason, always use "Industry Online Support (https://www.siemens.com/de/de/produkte/services/digital-enterprise-services/industrial-security-services.html)" to keep yourself up to date about new and relevant product security notifications for your products. Comply with the instructions provided in the product security notifications.

Siemens ProductCERT (https://www.siemens.com/cert) (Cyber Emergency Readiness Team) is the central department for security-related incidents in the Siemens product and solution

environment. Siemens ProductCERT supports development departments in the form of consulting and other services. ProductCERT provides information about current threats and vulnerabilities as well as the appropriate countermeasures.

See also

Technical Support (https://support.industry.siemens.com/sc/ww/en/sc/2090)

5.8.3 Patch management

5.8.3.1 Windows patch management

Windows Server Update Services (WSUS)

NOTICE
Data manipulation through security vulnerabilities in the operating system Microsoft does not provide any automatic security updates, service packs or hotfixes for operating systems older than Windows 10. This can leave the operating system with dangerous security vulnerabilities. • If you are using an operating system older than Windows 10, take additional measures to protect the operating system. • If possible, always upgrade the operating system of your operating unit to the current version.

The **WSUS** (Windows Server Update Services) system functionality provided by Microsoft is available for Windows operating systems.

WSUS supports administrators by rolling out Microsoft updates in large local networks. WSUS automatically downloads update packages and offers them to the Windows clients for installation. The automated update process ensures that the latest system and security updates are installed on the Windows clients.

Before installing system and security updates, please note the following points:

- Perform a system backup.
- Administrators must ensure that system and security updates do not impair the operability of production plants.
- Do not establish a direct Internet connection to the WSUS server! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

More information

You can find more information about network segmentation in Chapter Network segmentation (Page 34).

5.8.3.2 Program updates in the TIA Portal

If you have installed the TIA Portal on your operating unit (PG/PC, Notebook), you can start a search for program updates in the TIA Portal at any time. New versions of individual TIA Portal applications are displayed and can be installed. Installing a new version also fixes security vulnerabilities.

Also activate automatic notifications to receive information about available program updates.

5.8.3.3 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.

System overview

6

6.1 System overview

SINUMERIK ONE offers modularity, openness, flexibility, and uniform structures for operation, programming and visualization. It provides a system platform with trend-setting functions for almost all technologies relating to metal processing and machining as well as robotics.

SINUMERIK ONE includes software for creating the machine control and the associated digital twin from an engineering system, thus supporting the seamless integration of hardware and software. The software and hardware innovations of SINUMERIK ONE and the possibility to create an end-to-end digital twin for products and production significantly accelerate machining processes.

SINUMERIK ONE is characterized by the following properties:

- A high degree of flexibility
- Excellent dynamic response and precision
- Optimum integration into networks

Benefits

- Outstanding performance and flexibility for multi-axis systems of mid to high complexity thanks to scalable hardware and software
- Seamless openness of the user interface, the PLC and the NC kernel so that you can integrate your specialist know-how
- Integrated safety functions for man and machine: SINUMERIK Safety Integrated
- Comprehensive range of products for integrating machine tools into communication, engineering and production processes
- Seamless engineering in all engineering phases of a plant or system through integration in the Totally Integrated Automation Portal (TIA Portal)

Field of application

SINUMERIK ONE can be used worldwide for turning, drilling, milling, grinding, laser machining, nibbling, punching, in tool and mold making, for high-speed cutting applications, for wood and glass processing, for handling operations, in transfer lines and rotary indexing machines, for mass production and Jobshop production environments.

The SINUMERIK ONE control system can also be used for robot applications and in medical technology.

SINUMERIK ONE is available as export version for use in countries where approval is required.

System configuration

SINUMERIK ONE combines CNC, HMI, PLC, closed-loop control and communication tasks in a single NCU (Numerical Control Unit). For operation, programming and visualization purposes, the corresponding operating software is already integrated in the CNC software for the NCU, and therefore runs on the high-performance NCU multi-processor module. A SIMATIC IPC for SINUMERIK can be used for increased performance in the operating area.

Up to 4 distributed operator panels can be operated on one NCU/PCU. The operator panel can be installed as a thin client at a distance of up to 100 m.

The following components can be connected to the NCU:

- SINUMERIK operator panel front with TCU 30.3 / SIMATIC IPC for SINUMERIK and Machine Control Panel / Machine Push Button Panel
- SIMATIC Thin Client (from firmware V2.0.1)
- SIMATIC CE panel
- SINUMERIK handheld units
- Distributed PLC I/O
  - SIMATIC, e.g. ET200SP and ET200MP
  - SINUMERIK via PROFIBUS DP: e.g. SINUMERIK I/O module PP 72/48D
  - SINUMERIK via PROFINET IO: e.g. SINUMERIK I/O modules PP 72/48D PN and PP 72/48D 2/2A PN
- SINAMICS S120 drive system
- Induction and synchronous feed, main spindle and direct-drive motors:
  - Feed motors: 1FT, 1FK
  - Main spindle motors: 1PH, 1FE, 2SP1
  - Direct-drive motors: 1FN3, 1FW6

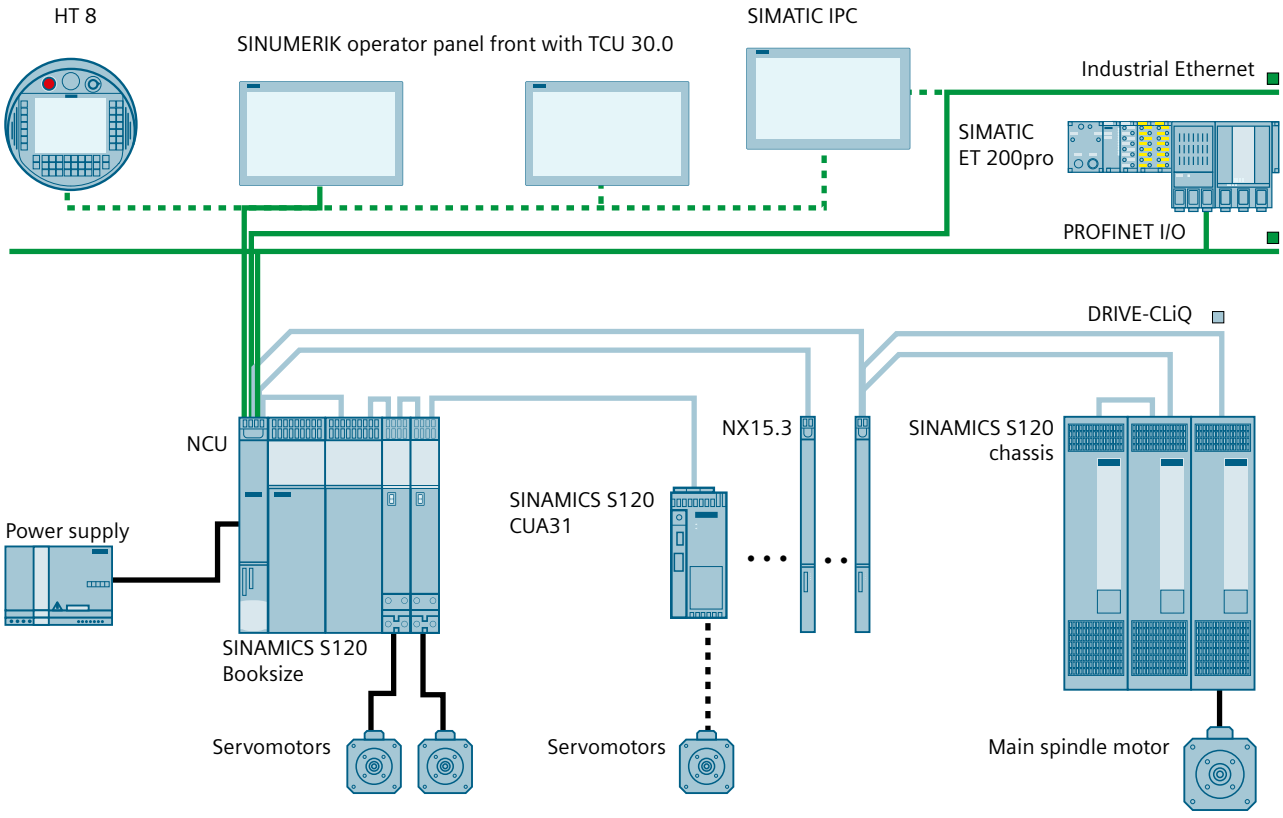


Figure 6-1 Typical topology of the SINUMERIK ONE complete system

6.2 Communication interfaces

The SINUMERIK ONE control offers a wide range of interfaces for different purposes and therefore also to segment networks.

SINUMERIK ONE interfaces

The following diagram provides an overview of the interfaces of SINUMERIK ONE and their function:

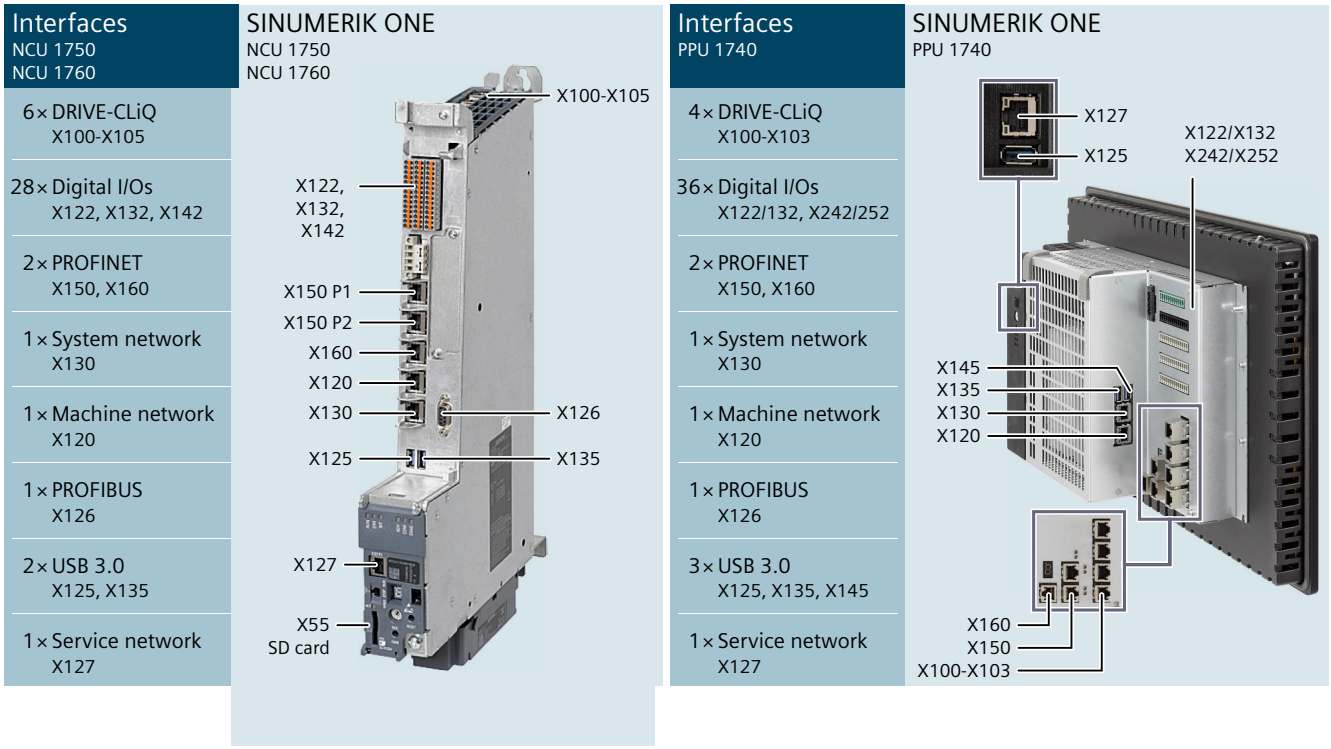


Figure 6-2 Overview of SINUMERIK ONE interfaces

Communication concept

The following diagram shows the interface and its segmentation regarding the various possible networks.

In the communication concept, we distinguish between the following networks:

- Field network (interface X126, X150):
  The field network should be an internal machine network, on which the PROFINET/PROFIBUS is used to connect sensors and actuators, including drives to the control. This network has very high expectations regarding deterministic and cyclic communication, and should not be available outside the machine.
  There is no firewall on the control side as this network is conceived as a pure internal network.
- Machine network (interface X120): This machine network is also an internal network; however, with lower requirements relating to the deterministic, as it is used to connect operating panels (IPCs/Thin Client Units, machine control panels etc.) and also possibly Edge devices. There is no firewall on the control side as this network is conceived as a pure internal network. When integrating an Edge device, the Edge device itself is used to disconnect the network.
- Company network (interface X130): X130 at the NCU and eth 1 at the IPC are used to establish a connection to the company network. A firewall protects these two interfaces against unauthorized access.
- System network (interface X160) and production network: The system network is the network within the production environment, which is typically used to connect various machines in a common production process. As a consequence, it is the first network that should be available outside the machine. Also here, high demands can be placed on the deterministic behavior. PROFINET is also used in this case. For lower requirements placed on the deterministic behavior, OPC UA can also be used. However, a protected network environment is expected that is not connected with an office network, or more importantly, not the Internet.

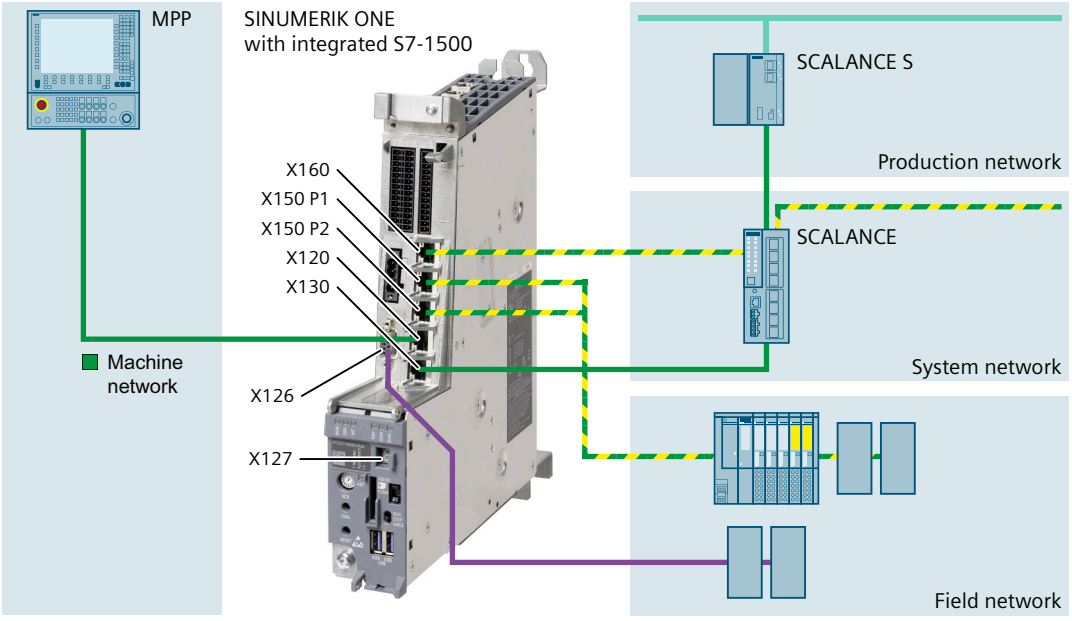


Figure 6-3 SINUMERIK ONE communication concept

6.3 Data flows and data memory

The following diagram provides an overview of the components of a SINUMERIK ONE system with the associated interfaces. The possible data flows (protocols) are shown for each interface. The colors indicate whether or not the communication connection can be encrypted and whether or not integrity protection is in place.

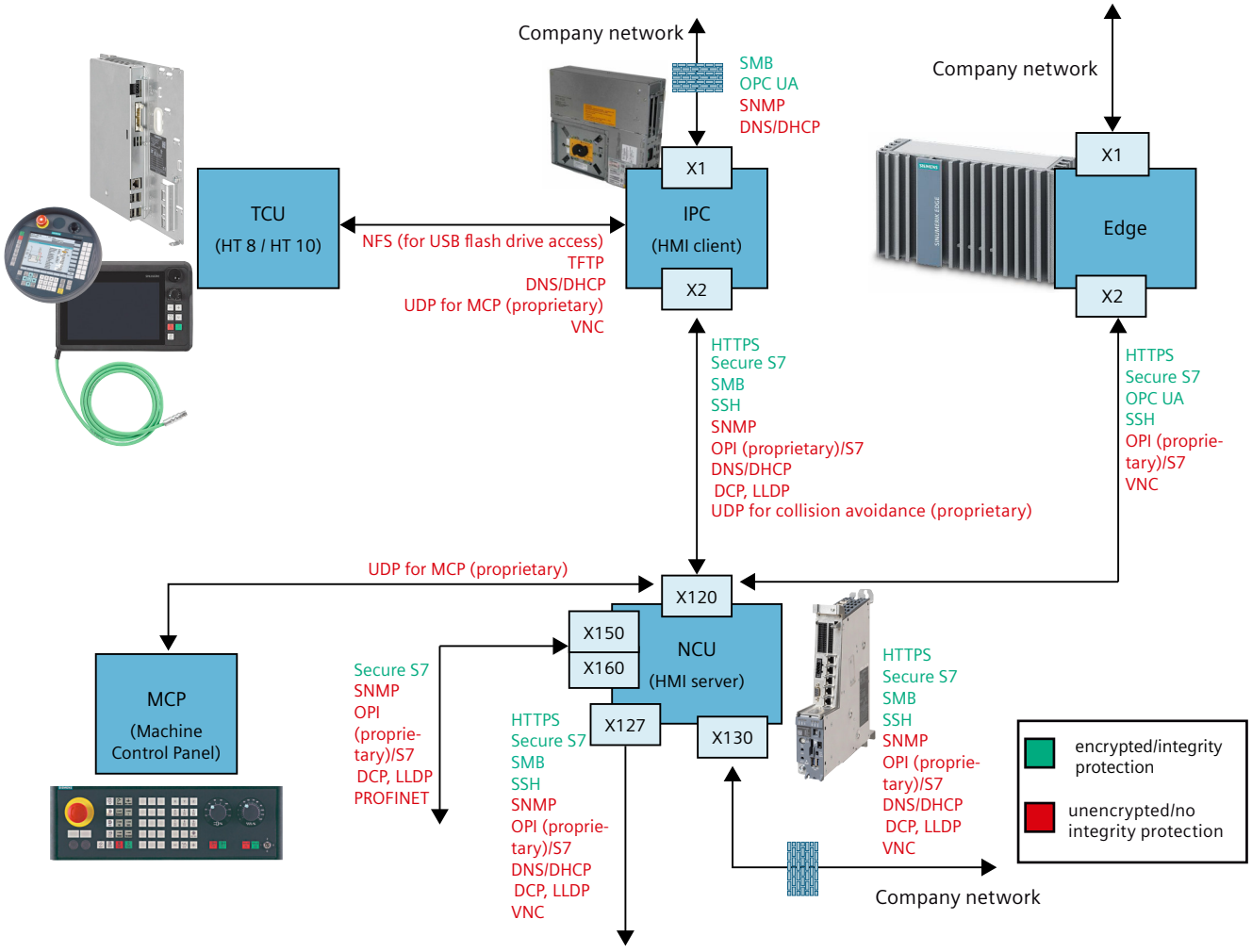


Figure 6-4 SINUMERIK ONE data flows and data memory

Note

Open User Communication

Note that it is possible to operate virtually any TCP/IP and UDP/IP protocol from the PLC program via all interfaces (X150, X160, X120, X130, X127). Protocols must be programmed in the PLC project before they can be used.

Intended operational environment 7

7.1 Description of the intended operational environment

A SINUMERIK ONE control system is part of a machine tool. This can also involve the control system of robots for handling or machining. This machine is typically part of a factory or a workshop. SINUMERIK ONE also offers a complete package for integrating one or several robots into SINUMERIK-controlled machine tools.

Possible additional components within the SINUMERIK system, such as thin client units and machine control panels, which are used for display, are generally arranged so that they can be accessed from the front side – while the rear side is in an enclosed housing. SINUMERIK ONE controls are also used in medical technology.

- From the operating environment it is therefore expected that a SINUMERIK ONE control system and any existing IPC **are exclusively operated indoors in a control cabinet or an enclosed housing** and are therefore not exposed to extreme climatic conditions.
- Further, it is assumed that **control cabinets or the enclosed housing is protected against unauthorized access**.
- It is also assumed that **organizational measures are firmly in place to ensure that only authorized personnel can access the machines**.

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 that can be securely locked. Implement appropriate monitoring and alarm systems. The control cabinets/electrical rooms must be locked using the appropriate cylinder locks. Do not use simple locks such as universal, triangular/square or double-bit locks. Only appropriately trained and authorized personnel may access these housings, cabinets or electrical rooms. • **More information** on the control cabinet installation of the NCU is provided in the corresponding Equipment Manuals for SINUMERIK ONE: "NCU1750" and "NCU1760".

7.2 Security assumptions for the intended operational environment

A SINUMERIK ONE control system is part of a machine. It is therefore assumed that this is protected by the general machine environment. This involves both physical access as well as network segmentation. It is also not assumed that a SINUMERIK ONE control is directly connected with the Internet or a part of an office network.

Table 7-1 Security assumptions for the intended operational environment

Assumption ID	Assumption	Responsible
AS-01	Only authorized personnel may physically access the SINUMERIK ONE system (control system IPC, TCU, MCP).	Machine builder and end user
AS-02	The internal networks of a SINUMERIK ONE control system (X120, X127, X150) are not available outside the machine. The physical access to these networks is also protected.	Machine builder
AS-03	The external networks (X130, X160) are connected with a protected production network. Further, there is no direct connection (without a security router, for example) to an office network or the Internet.	End user
AS-04	Secure environment with mobile data storage media (USB sticks): Protection against malware	End user
AS-05	Port 102 is closed at X130	Machine builder and end user

Protection objectives

8

8.1 Overview of protection objectives

The general objectives to protect product data and functions are as follows:

- Securing the **availability** of:
  - Functions of the production process
  - Functions of the safety-security mechanisms
  - System communication capability
- Non-disclosure of **confidential Information**, such as:
  - Passwords and private key
  - Machine builder / customer programs and expansions
  - Synchronized actions
  - Encrypted part programs
  - PLC programs
  - Encrypted cycles
  - Configurations and optimizations
  - Process data / log files
  - Licenses
- Protecting the **integrity** against unauthorized manipulation of:
  - Functions of the production process
  - Software Siemens / machine builder expansions
  - Firmware
  - Part programs / cycles
  - Machine parameters
  - Configurations and optimizations
  - Functions of security mechanisms
  - Machine builder / user data
  - Users, rights and groups
  - Passwords, private key and certificates
  - Process data / log files
  - Licenses

Security functions of the product

9

9.1 Overview

The implemented security functions of the product are described in this section. The security functions are intended to be able to evaluate and take into consideration the SINUMERIK ONE system capabilities when creating the security concept for the system.

The chapter encompasses statements on the following topic clusters:

- User management and access control (Page 59)
- Backup and restore (Page 69)
- Checking the system integrity (Page 72)
- Know-how protection (Page 81)
- Secure communication (Page 82)
- Firewall (Page 88)
- Reduction of the attack surface (Page 90)
- Plant security (Page 93)

Operation of the security functions

You will find many of the functions described here in SINUMERIK Operate in operating area "Setup" under the softkey "Security". To see the "Security" softkey, you require at least access level 3 (user).

You will find further descriptions of the security functions, the requirements, and the precise sequence of all worksteps in SINUMERIK Operate in the Commissioning Manual "Final commissioning steps" and the associated online help.

9.2 Role and access requirements for security functions

To use certain security functions of the SINUMERIK you need different roles or access levels. These requirements depend on whether you are working with or without active user management (Page 59). This table is intended to give you an overview of implemented security functions and their access requirements.

You can find the described security functions in SINUMERIK Operate via the "Setup" operating area using the "Security" softkey.

Requirements for access

Security function	WITH active user management	WITHOUT active user management
User management (Page 59)	You have the role "Security Admin" or access level 3 (end user).	You have access levels 1 (machine builder).
PLC security (Page 72)	You have the role "Security Admin" or access level 3 (end user).	You have at least access level 3 (end user).
HMI security (Page 83)	You have the role "Security Admin" or access level 3 (end user).	You have at least access level 3 (end user).
Security Eventlog (Page 85)	You have the role "Security Admin" or access level 3 (end user).	You have at least access level 3 (end user).
Trusted devices (Page 77)	You have the role "Security Admin" or access level 2 (service).	You have at least access level 3 (end user).

9.3 User management and access control

9.3.1 Types of supported access management systems

Supported access management systems

SINUMERIK supports two types of access management systems:

- The classic form of access management via group-based access levels (Page 57). This form is enabled by default when the system is shipped.
- The new SINUMERIK user management (Page 59). The user management enables personalized authorization. Via the new user management, you can assign role groups, user groups as well as create and manage users in your project. You can explicitly activate the new user management via the operating area "Setup" > "Security". User management is an optional security function. We recommend activating user management over the classic form of access level management.

9.3.2 Classic access management: Group-based access levels

SINUMERIK ONE offers the classic type of access management via group-based access levels as standard. The access levels allow access to the system and are available via SINUMERIK Operate. SINUMERIK ONE offers a central system access level. This is why all applications have the same access level at the same time. No session-based access levels are available.
The group-based access level remains active until you log off manually. After a system restart, the access level is retained.

The access concept controls access to functions and data areas. Access levels 1 to 7 are available, where 1 represents the highest level and 7 the lowest level. Access levels 1 to 3 are locked using a password and 4 to 7 using the appropriate key-operated switch.

Access level	Locked by	Area	Data class
1	Password: SUNRISE	Machine manufacturer	Manufacturer (M)
2	Password: EVENING	Service	Individual (I)
3	Password: CUSTOMER	User	User (U)
4	Key-operated switch setting 3	Programmer, machine setter	User (U)
5	Key-operated switch setting 2	Qualified operator	User (U)
6	Key-operated switch setting 1	Trained operator	User (U)
7	Key-operated switch setting 0	Semi-skilled operator	User (U)

A full description of the traditional group-based access levels is not part of this manual. Further and more detailed information on this subject can be found in the Commissioning

Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139).

9.3.3 Features and benefits of user management

The SINUMERIK user management differs from the classic system of access level management, and also offers numerous advantages - especially in the area of security:

Differences compared to the previous authorization by means of access levels

- **Personalized login**
  Every configured user can log in to the system in user management using his or her own user name and individual password. Since each user only knows his or her individual access data, this type of authorization is much more secure than authorization via access levels.
- **Configuring users, groups and roles**
  - The classic access levels of SINUMERIK (Manufacturer, Service, User, etc.) are still available in the form of roles. These roles can be assigned to users by the Security Admin in the form of user groups.
- **Introduction of two new roles:**
  - There is a **Security Admin role for the manufacturer** and a **Security Admin role for the user**.
    The purpose of these two new roles is to separate the rights for security configuration from functional configuration.
    These Security Admin roles are required to change security-relevant settings, but they have no functional rights (Key switch 0 role).
    Nevertheless, it is possible to assign both a Security Admin role and a SINUMERIK function role (Manufacturer, Service, User, etc.) to a user, so that a commissioning engineer can, for example, have the Security Admin role in addition to the Manufacturer role.
  - Another main advantage is that the security configuration on the end user side no longer needs to be changed, as it may be used by a larger number of people.
- **Key switch**: An anonymous login using the keyswitch is deactivated.
- **PI service:** PI service for logging in/out and changing the password no longer works if user management is activated.
  - For this purpose, there are new OA interfaces for login/logout/change password in user management.
- **Log in only from the paired IPC**: With user management activated, logging in from external HMIs - apart from the coupled IPC - is no longer possible.

Purpose and advantages of SINUMERIK user management

Activating the user management provides you with more security in user management and thus has numerous advantages:

- Protection of the system and data against unauthorized access (both internal and external)
  - Anonymous authorization methods, such as logging in via key switches, are no longer supported by the new user management. Each user authorizes himself uniquely via his domain, user name, and password
- Access management can be precisely controlled through the groups and roles. Roles can be assigned individually for each user.
- Only a trained security administrator familiar with the subject matter can create new users, assign groups to users and role groups to their project. Other users cannot and do not have to deal with user management, which prevents misuse and reduces susceptibility to errors. Login information is thus better protected from publication and tampering.
- Prompt blocking or deletion of users and authorizations when they are no longer needed (e.g. when a user leaves the company)

9.3.4 User management

9.3.4.1 Overview and definition

What is user management?

User management refers to various activities that involve managing the users of all systems and applications in a company or organization. Usually, the administrator is the one who performs these activities and/or coordinates them.

User management offers the following functions:

- Protection of IT systems and data against unauthorized access (both internal and external)
- Unique identification of each user (e.g. through a combination of user name and password)
- Changing the password when required
- Assignment of access authorizations to systems, services, and applications
- Prompt blocking or deletion of accounts and authorizations when they are no longer needed (e.g. when a user leaves the company)

Local and external user management

There are two ways in which the administrator can manage users:

- locally (internally)
- externally

With local user management, the administrator creates the users directly in the respective system.

With external user management, the various systems and applications are connected to an external user management system, such as an "Active Directory", where the users are managed centrally.

As an alternative to authorization by means of the previous access levels, the SINUMERIK system optionally features **local user management**.

9.3.4.2 Architecture of the user management

Procedure principle

User management in SINUMERIK ONE is performed for the system components involved based on 2 well-known principles:

- Desktop Single Sign-On (DSSO) principle
  The main components of the system are based on the "**Desktop Single Sign-On (DSSO) principle**". This means that the user authenticates himself once to a main component with a valid user name and password. The user management then provides feedback as to which groups the respective user belongs to. From this information, SINUMERIK can derive the information as to which role the user has.
  Both the login and the group assignment are globally valid for all main components (NCK, HMI OA application, SINUMERIK Operate, WinCC Unified). The assignment of groups to roles and thus to rights in the application is controlled by the application.
- Authentication Outside principle
  Some communication components, such as OPC UA, work with decentralized authentication (**Authentication Outside principle**). This means that local authentication in the component does not affect user management and vice versa.

Architecture of the user management NCU system

- On a pure NCU system, the user management is installed on the NCU itself.

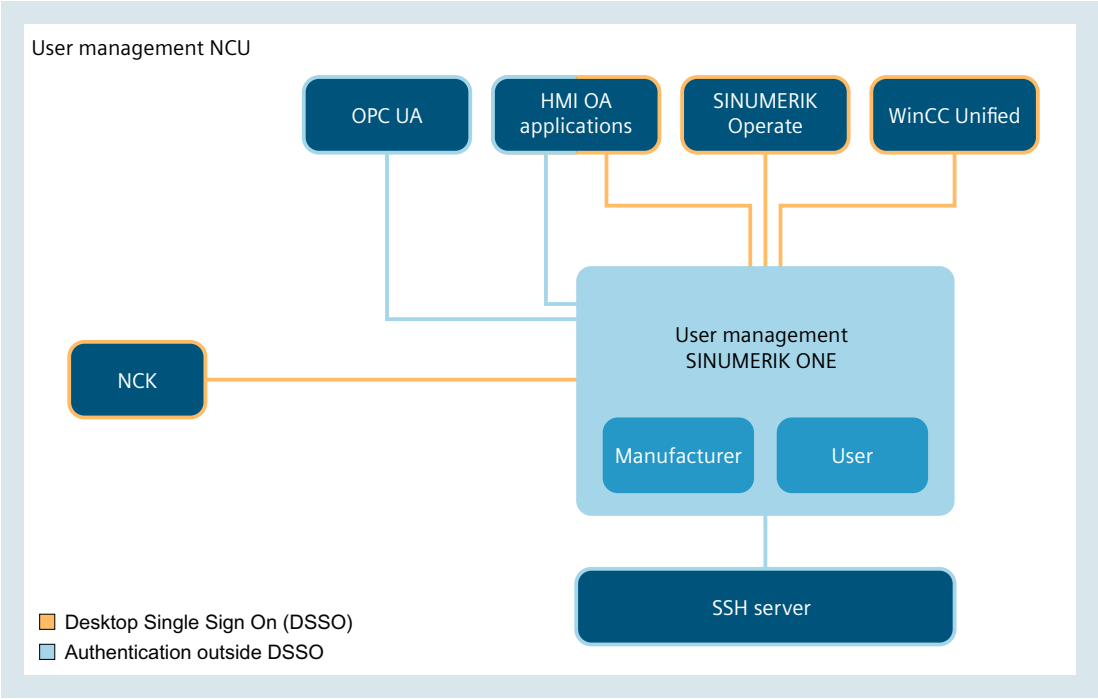


Figure 9-1 User management on the NCU

User management in the distributed system - NCU & IPC system

If an NCU and an IPC are installed, the user management is on the IPC. Because the IPC defines the roles and rights of the users for the NCU, a trusted connection between the two components is important to establish a secure system.

NOTICE
Misuse of data and system takeover resulting from replacement of the IPC In a distributed system, there is a risk of misuse of data and hostile system takeover if the IPC is replaced. To avoid this misuse of data, you should pair the NCU to the IPC before activating the user management and thus ensure a trusted connection between the two components.

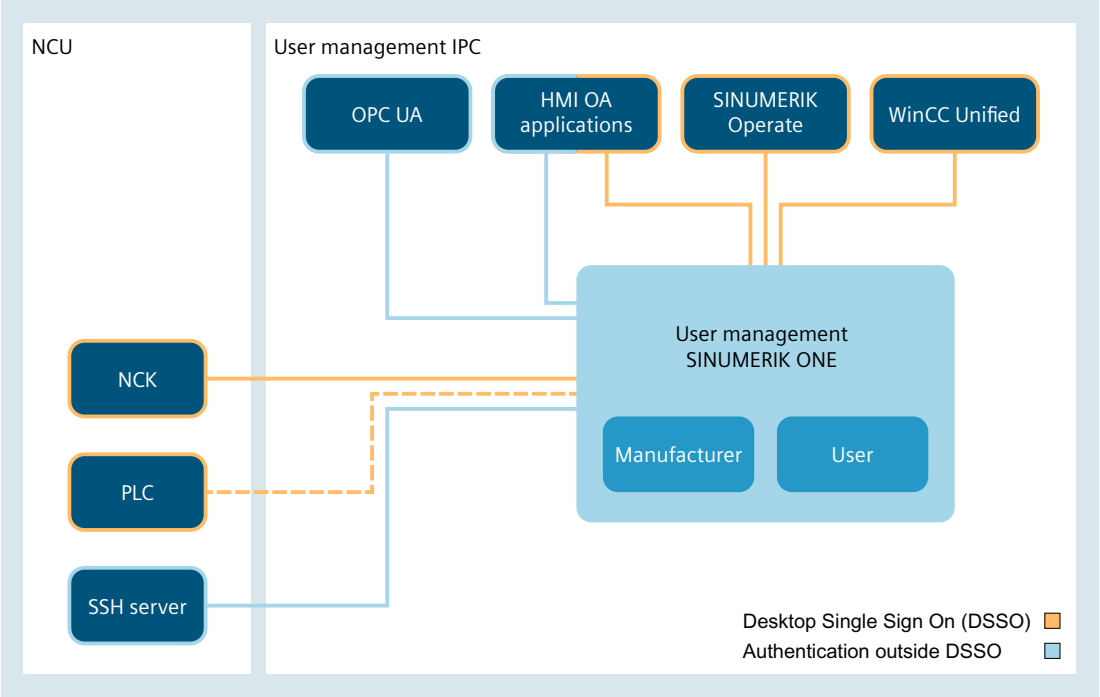


Figure 9-2 User management on the IPC

Domains

Two different domains are implemented in the user management at SINUMERIK ONE, each of which has different demands on the system:

- Manufacturer
- User

Each domain can separately define and assign its own administrators, groups, users, and permissions. When activating user management, a unique name must be assigned for the manufacturer domain and end user domain.

NOTICE
Each security administrator administers only his own domain Note that the respective security administrator - depending on the login - can and may only administer his own domain in each case. • The Security admin manufacturer can only administer the manufacturer domain. • The Security admin end user can only administer the end user domain. • We recommend that the Security admin of the manufacturer, after creating the manufacturer domain, creates a separate domain with users / roles / passwords for the end user. When the machine is handed over to the end user, this data can be transferred to the end user in confidence.

Note

When logging in, the domain must always be specified in addition to the user name and password. This ensures that the uniquely correct user always logs on to the correct domain. The selection of the last selected domain is saved.

9.3.4.3 Groups and role concept

SINUMERIK ONE user management distinguishes three types of groups:

Machine roles

- Machine roles form a group for aggregating machine-level roles across multiple applications of the machine.
- Only the Security Admin Manufacturer can create, modify and delete machine roles.
- For each machine role, the manufacturer can decide whether it can be assigned by the user.
- Machine roles have the advantage that the manufacturer often has a better overview of all components of a SINUMERIK system and their implemented assignment of rights. The end user then no longer has to deal with the assignment of rights for the individual components. This is done by the manufacturer.
- Machine roles inherit their function rights from one another.
  Users inherit the AccessLevel from the machine roles to which they belong. A user who belongs to multiple machine roles receives the highest AccessLevel contained in these roles. A higher AccessLevel always also includes the lower AccessLevels.
  A machine role can also include the Security Admin role and confer this role on the users in the machine role concerned. The "Security admin manufacturer" role can only be held by users from the manufacturer domain and the "Security admin end user" role can only be held by users from the end user domain. This means that no user can have both Security Admin roles.

User groups

- A user group is a group for the organizational grouping of users.
- Machine roles can be assigned to the user groups in SINUMERIK Operate.

Users

A user can then in turn become a member of one or more user group(s). Via the user's login, the user management can assign which rights/roles which user has at any time. Only those functions are then accessible to the user that were previously defined in the machine role via user management.

9.3.4.4 Role of the security admin

Description

For the activation and configuration of user management, at least one user must be named, who is formally assigned the **Security admin manufacturer** role. Within the scope of the user management, this user is authorized to carry out the entire configuration of the user management for the manufacturer and also on behalf of the end user. Consider the assignment of the Security Admin role carefully.

Who defines the Security Admin role?

The manufacturer is responsible for formally defining the administrator role. The manufacturer must also decide whether and to what extent the end user is allowed to access the administration functions.

NOTICE
Each Security Admin role administers only their own domain Note that the respective Security Admin role - depending on the login - can and may only administer their own domain. • The Security admin manufacturer can only administer the manufacturer domain. • The Security admin end user can only administer the end user domain. • We recommend that the Security admin of the manufacturer, after creating the manufacturer domain, creates a separate domain with users / roles / passwords for the end user. When the machine is handed over to the end user, this data can be transferred to the end user in confidence.

Predefined user names and passwords

In the delivery state of SINUMERIK Operate, the classic form of access level management is activated by default. User management must first be explicitly activated as a security function. No predefined user names and passwords are configured.

Administration functions

The following configuration functions are available to the Security admin manufacturer in the SINUMERIK user management:

- Activate user management and set up domain
  - Activate user management and set up manufacturer domain and end user domain
  - Deactivate user management
- Machine roles
  - Overview of machine roles
  - Create machine roles
  - Change machine roles
  - Delete machine roles

- User groups
  - Overview of user groups
  - Create user groups
  - Change user groups
  - Delete user groups
- Policies
  - Define password policy
- Users
  - Overview of users
  - Create users
  - Change users
  - Delete users
- Login/logoff
  - User login/user logoff
  - Change passwords (all other users are also able to change passwords)

Who-does-what matrix

To consistently apply the principle of least privilege, we recommend creating a who-does-what matrix before any user accounts are created. The necessary user accounts are then set up in user management according to the defined user profiles.

9.3.4.5 Activating and configurating user management

You can control the activation of the user management centrally via SINUMERIK Operate.

The sequence shown serves as guideline for sensible configuration. Deviations from the sequence are possible. A detailed description of all individual steps and setting options can be found in the manual and online help linked below.

Sensible order of configuring

1. Activate the user management function in SINUMERIK Operate via "Security > User management > Configuration". If user management is not activated, the classic SINUMERIK access management via access levels is active by default.
2. Define the name for the manufacturer domain.
3. Specify the user name and password for the Security admin manufacturer.
4. Define a name for the end user domain.
5. Specify the user name and password for the Security admin end user.
6. Activate user management.

7. Configure the user management for the "Manufacturer" domain. This includes the following individual steps:
   - Configuration of machine roles
   - Configuration of user groups and assignment of user groups to the machine roles
   - Creation of users
   - Assignment of the users to the user groups
8. Optionally configure the user management for the end user domain. This includes the following individual steps:

   Note

   What does the manufacturer do? / What does the end user do?

   We recommend that the manufacturer's Security Admin preconfigure a separate domain with user groups and users for the end user after creating the domains and activating the user management. When the machine is handed over to the end user, this data can be transferred to the end user in confidence.

   - Configuration of user groups and assignment of user groups to the machine roles
   - Creation of users
   - Assignment of the users to the user groups

More information

A description of all individual steps and setting options for user management in SINUMERIK Operate can be found at Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139) and in the SINUMERIK Operate online help.

9.3.4.6 Role and access requirements for security functions of user management

To be able to use the various subordinate security functions of the SINUMERIK user management, you need different roles/rights. These requirements depend on whether you are working with or without active user management. This table is intended to give you an overview of all implemented security functions of the user management and their access requirements.

You can find the described subordinate security functions in SINUMERIK Operate via the "Setup" operating area via the softkey "Security > User management".

Requirements for access

Security function / softkey	WITH active user management	WITHOUT active user management
Configuration	You have the role "Security admin manufacturer" or "Security admin end user".	You have access levels 1 (machine builder).
Machine roles	You have the "Security admin manufacturer" role. For other users, this softkey is not visible or the function cannot be used.	If user management is deactivated, this softkey is not visible or the function cannot be used.

Security function / softkey	WITH active user management	WITHOUT active user management
User groups	You have the "Security admin manufacturer" or "Security admin end user" role. The softkey is visible to other users; but read-only access only.	If user management is deactivated, this softkey is not visible or the function cannot be used.
Policies	You have the "Security admin manufacturer" or "Security admin end user" role. The softkey is visible to other users; but read-only access only.	If user management is deactivated, this softkey is not visible or the function cannot be used.
Users	You have the "Security admin manufacturer" or "Security admin end user" role. The softkey is visible to other users; but read-only access only.	If user management is deactivated, this softkey is not visible or the function cannot be used.

More information

A description of all individual steps and setting options for user management in SINUMERIK Operate can be found at Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139) and in the SINUMERIK Operate online help.

9.3.4.7 Backing up/restoring data

In order to save the settings of the user management or to be able to restore them at another time or for another machine, it is possible to save the data of the user management in the security archive.

Data in the security archive

In addition to the security data, the security archive contains the following user management data:

- User (incl. encrypted access data)
- Groups
- Assignment of users to groups
- Assignment of groups to roles
- Settings for user management / rules (password rules, failed login attempts, etc.)

Password security archive

The security archive is encrypted and protected with an individual password. The password can be stored in SINUMERIK Operate. To store or change the password in SINUMERIK Operate, you need one of the following roles:

- If user management is deactivated:
  - End user (3)
  - Service (2)
  - Machine manufacturer (1)
- If user management is activated:
  - Security admin manufacturer
  - Security admin end user

More information

More information about the security archive is provided in Chapter Backup and restore (Page 69) and in the Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139).

9.4 Backup and restore

9.4.1 Options for backing up and restoring data

The following options are available for backing up and restoring your data:

- Portable SINUMERIK service system
- SINUMERIK archives

Backup and restoring from the SINUMERIK service system

The SINUMERIK service system supports you in the following tasks:

- New installation
- Update
- Replacement
- Service tasks

The portable SINUMERIK service system or "Emergency Boot System" (EBS) is created on a USB flash drive. This enables you to start booting the NCU from the service system and to carry out various service tasks, such as data backup or updates, in a service menu.

Backup and restoring from the SINUMERIK archive

To restore the data, use the data from the DSF archive.

The data from the DSF archive map the exact status of the previously stored control.

The following components are contained in a SINUMERIK archive (DSF archive):

- NC
- PLC
- HMI
- Drives
- System settings
- Security (Page 70)

Note

Security component

If the DSF archive from another system contains a security component, the data is confidential and therefore password-protected.

To transfer it, you must set the correct archive password on the controller or, in the case of backup and restore, input the correct archive password on the control system when you want to write the security component to the DSF archive or restore it.

Enter the security password in the dialog before the archive transfer or in the operating area "Setup > Security > Security settings".

A DSF archive can be imported into SINUMERIK Operate via the "Setup" operating area. This allows you to commission the NC, PLC, HMI, system and drive components.

Archive types

After reading in, the machine has exactly the status that was previously defined with the archive type. The import differs principally with the following behavior:

Backup (for users)

- The existing control data are overwritten by the data from the DSF archive and may be added to the machine status.

Setup (for manufacturers)

- The data from the DSF archive map the exact status of the previously stored control.
- The components selected from the DSF archive are generally reset on the control system when the data is imported.

For **more information** on the compatibility of archives from different systems and archive formats, see the "Final steps for commissioning" Commissioning Manual.

9.4.2 Security archive

SINUMERIK ONE has a "Security" archive component to back up and restore confidential data in a DSF file. The data comprise configurations from the security components: User management, PLC security, Security Eventlog and Trusted devices (pairing). A complete list of all archive data can be found in the online help.

To protect this data, it is encrypted before creating an archive. An individual key is generated to do this.

To generate the key, a "Security archive password" must be entered under"Setup > Security > Security settings > HMI security".

NOTICE
Security archive password Keep the security archive password in a secure place, as it is required to restore a security archive. The security archive will not be able to be restored if the password is unknown!

Observe the following password guidelines for the security archive password:

- Minimum password length: 8 characters
- Minimum number of digits: 1
- At least one uppercase letter and one lowercase letter

This password must be entered to restore the security archive.

If the security archive contains the password to protect confidential PLC configuration data, this password must be activated manually after importing the archive and the PLC must then be restarted.

Note

Note that after restoring the security archive, the "Password for protecting confidential PLC configuration data" known from the TIA Portal configuration must still be activated in SINUMERIK Operate under "Setup". To do this, click the "Activate" softkey in the settings under "Security > PLC Security > Password for PLC configuration data".

Note

Access level "End user" and/or role "Security Admin Manufacturer" or "Security Admin End User" is required to change the security archive password.

Note

After activating the password, the PLC or SINUMERIK Operate must be restarted to display the correct status.

9.5 System integrity

9.5.1 Integrity check on the NCU

Secure Boot

SINUMERIK ONE provides a secure boot technique (**Secure Boot**) so that only software with a valid Siemens signature can run on the device.

In spite of this, SINUMERIK provides the option of allowing applications of machine OEMs to run on their systems, which were programmed with a special Siemens programming environment. These applications are the only exception and no other code can be run on a SINUMERIK control system without a valid signature.

If one of the signatures is not valid, then a SigErr error is displayed with the corresponding error number.

9.5.2 PLC security

The PLC provides numerous functions for integrating and protecting confidential data.

An overview of the options can be found here:

- Password to protect confidential PLC configuration data (Page 74)
- Access level password to protect the PLC against unauthorized access (Page 72)
- Password for the protection of the offline safety program (Page 75)
- Know-how protection password (Page 76)
- Copy protection password (Page 76)
- Write protection password (Page 77)

Once the PLC passwords have been assigned, only authorized persons can access the PLC, change data or configurations.

This chapter provides an overview of the PLC passwords and their significance.

9.5.2.1 Password to protect confidential PLC configuration data

Purpose

Proper functioning of certificate-based communication mechanisms for secure communication such as Secure PG/PC and HMI communication, Secure Open User Communication, HTTPS, Secure SMTP over TLS or OPC UA requires that the private keys used by these certificates are protected in the best possible way. As of CNC software V6.21, you can set up a user-defined password to protect these keys and other sensitive data: Password to protect confidential PLC - CPU configuration data.

Generation

The password to protect confidential PLC configuration data is configured in the TIA Portal in PLC properties in area "Protection & Security > Protection of the PLC configuration data"; this allows confidential PLC configuration data to be encrypted on an individual basis for control systems.

If the password is set in the TIA Portal for the PLC, this password must also be stored in the memory area of the internal PLC-CPU of the SINUMERIK. Otherwise the PLC cannot be set to RUN mode, it remains in STOP.

The password is thus saved in the hardware, and is not contained in the project itself (load memory).

You have the following options of setting the password in the NCU:

- Setting the password via the TIA Portal
  More information on this topic is provided in the TIA Portal help under "Protection of confidential configuration data".
- Setting the password via SINUMERIK Operate (recommended)
  This is the only way that the password can subsequently be saved as a security component of a SINUMERIK archive and restored when this component is read in.

  Note

  It is recommended that the password be set via SINUMERIK Operate:
  - If the password is set via SINUMERIK Operate, it is saved in the internal password manager of SINUMERIK Operate.
  - If an archive is created that contains the security component, the password is included in the archive.
  - If the NCU needs to be replaced, the archive can be read in and the password can thus be restored.
  - In case of a memory reset of the PLC, the password for protecting confidential PLC configuration data in the NCU is not deleted. This can only be removed again via SINUMERIK Operate or the TIA Portal.
  - If a password is set in the memory area of the PLC-CPU, but the project in the load memory does not contain any protection for confidential PLC configuration data, then the PLC cannot be set to RUN mode either.

- The settings in the project can be changed via Openness.

Workflow

You can set the password in operating area "Setup" under "Security > PLC Security". The password is saved in the PLC.

Note

To display the correct status, the PLC must be restarted after the change. After entering the password, the "Restore connection" dialog opens, in which you confirm the restart of the PLC.

Conditions to set the password

- To set the password to protect confidential PLC configuration data, the PLC must be in the STOP operating state.
- The access level "Full access incl. fail-safe (no protection)" is set in the TIA Portal.
- To be able to access the settings in the "PLC Security" window, you must have the following access levels/roles:
  - If user management is activated: Role "Security Admin" or access level 3 (end user).
  - If user management is not activated: Access level 3 (user) or higher

More information

More information about setting a password to protect confidential PLC configuration data in SINUMERIK Operate can be found in the Commissioning Manual Work steps for configuring and commissioning and in the online help for SINUMERIK Operate.

9.5.2.2 Access level password

Purpose

The access level password for protecting the PLC against unauthorized access is used to protect the integrity and know-how of the PLC project.

The PLCs have different access levels to restrict access to certain functions, such as hardware configuration, PLC project, safety and access via S7 communication and blocks.

The access level password is configured in the TIA Portal. SINUMERIK Operate uses the access level password to gain access to the PLC.

Generation

The access levels of a PLC are configured in the TIA Portal in PLC properties in the area "Protection & Security > Access level".

More information on this topic is provided in the TIA Portal help under "Parameterizing access levels".

The settings can be changed via Openness.

Workflow

The access level "Full access incl. fail-safe (no protection)" is required for the correct operation of SINUMERIK Operate. From PLC firmware 2.9, the default setting for the access level is "No access (complete protection)". When using this setting, you can assign a password for every access level. This prevents anybody from downloading the PLC project or overwriting it without knowing the passwords. The password is still required to communicate with the PLC via S7 communication.

If a lower level than the "Full access incl. fail-safe (no protection)" access level has been set in the TIA Portal, the password for the "Full access incl. fail-safe (no protection)" access level must be made known in SINUMERIK Operate.

Therefore, save the access level password for "Full access including failsafe (no protection)" in SINUMERIK Operate under "Setup> Security > PLC Security > PLC access level password".

Note that, in accordance with the product safety regulations, the access level password must be entered manually when restoring a PLC archive if the access level password has been set, even though it has been saved.

Note

To display the correct status and use the password that has been entered, the PLC must be restarted after the change.

After entering the password, the "Restore connection" dialog opens, in which you confirm the restart of the PLC.

Effects

If the access level password is set for a PLC, this password is required for the following activities, even if it has been stored in SINUMERIK Operate:

- Access via TIA Portal for diagnostics or upload (from access level "No access")
- Access via TIA Portal for changes (from access level "Read access")
- Importing a PLC archive

More information

More information about access level passwords can be found in the Commissioning Manual Work steps for configuring and commissioning and in the online help for SINUMERIK Operate.

9.5.2.3 Password for the protection of the offline safety program

Purpose

The password for the protection of the offline safety program is used for the integrity and know-how protection of the safety-relevant blocks of the PLC project. It involves a pure engineering password.

The safety program can only be edited after entering the password.

Workflow

You set the password for protecting the offline safety program in TIA Portal in the properties of the PLC under "Safety Administration > Access protection".

If the user management of the TIA Portal is used, this password is no longer required, since the rights to edit Safety are mapped to roles.

More information

For more information on the topic of setting a password to protect the offline safety program, refer to "Access protection for the safety-relevant project data" in the TIA Portal help.

9.5.2.4 Know-how protection password

Purpose

The know-how protection password is used for the protection of PLC blocks.

Workflow

You set the know-how protection password in the TIA Portal in the properties of the FC and FB blocks.

More information

For more information on setting the know-how protection password, refer to the TIA Portal help under "Protecting blocks".

9.5.2.5 Copy protection password

Purpose

The copy protection password prevents a block from being executed on a PLC other than the one configured. Only if the block is located on the device with the specified serial number, it can be executed.

If you set up such copy protection for a block, it is important to also provide this block with know-how protection. Otherwise, anyone can reset the copy protection.

Workflow

You set the copy protection password in TIA Portal in the properties of the block.

More information

For more information on setting the copy protection password, refer to the TIA Portal help under "Protecting blocks".

9.5.2.6 Write protection password

Purpose

A write protection password for blocks of type OB, FB, FC is used to prevent unintentional modification.

Blocks with a write protection can only be opened in read-only mode, but you can still edit the block properties.

Workflow

You set the write protection password in TIA Portal in the properties of the block.

More information

For more information on setting the write protection password, refer to the TIA Portal help under "Protecting blocks".

9.5.3 Trusted devices

9.5.3.1 Overview

If the SINUMERIK system is distributed over the IPC and NCU, it is essential for secure functioning of the device that a connection is established between the IPC and NCU that can be used to transmit confidential information between the IPC and NCU. For user management, too, it is important to know that the components can be trusted. For this reason, a relationship of trust must be established from the beginning between the IPC and NCU. This operation is referred to as "pairing" and is similar to familiar technologies such as Bluetooth.

The purpose of pairing in SINUMERIK ONE

Note

Pairing for IPC systems only

Pairing only has to be performed if an IPC is installed in your SINUMERIK ONE system.

Because of the distributed architecture of IPC and NCU and implementation of the security function of the "user management (Page 59)" on the IPC, the IPC and NCU should establish a relationship of trust before these functions are used.

This relationship of trust is established by an operation known as pairing. During pairing, the devices to be paired are checked by the commissioning engineer and the relationship of trust is established.

This is achieved using certificates. The principle is that an NCU can only ever trust one IPC. This is necessary because the SINUMERIK user management is located on the IPC and the NCU could otherwise not decide which user management is valid.

- The relationship of trust is set up in the IPC by SINUMERIK Operate. The NCU accepts the request for the relationship of trust by transmitting the valid machine manufacturer password. You will find the precise rights required to use the pairing functions in the Commissioning Manual "Final commissioning steps" or in the associated online help.
- Only one IPC can enter into a trust relationship with one or more NCU(s) **(1:N)**.
- The user management function does not work without pairing between the NCU and IPC.

Note

Only one instance of SINUMERIK Operate on the IPC

In a distributed system with IPC and NCU, only one instance of SINUMERIK Operate is permitted on the IPC.

- Deactivate all running instances of SINUMERIK Operate on the NCU before pairing the NCU.

NOTICE
Resetting the NCU to the factory settings Never delete the pairing in the IPC without a connection to the NCU because otherwise the NCU will have to be reset to the factory settings.

Note

Unpairing

A paired NCU can only be released from the pairing by the IPC with which it is paired.

NOTICE
Hostile takeover of data and manipulation of data Because of the distributed architecture of IPC and NCU and implementation of the "User management" functionality on the IPC, there is a risk of hostile takeover of data and manipulation of the system by simply replacing the IPC. • This hostile takeover of data is prevented by the pairing function. • For this reason, establish a relationship of trust between the IPC and NCU by pairing the two devices securely before you use the security functions of the SINUMERIK ONE.

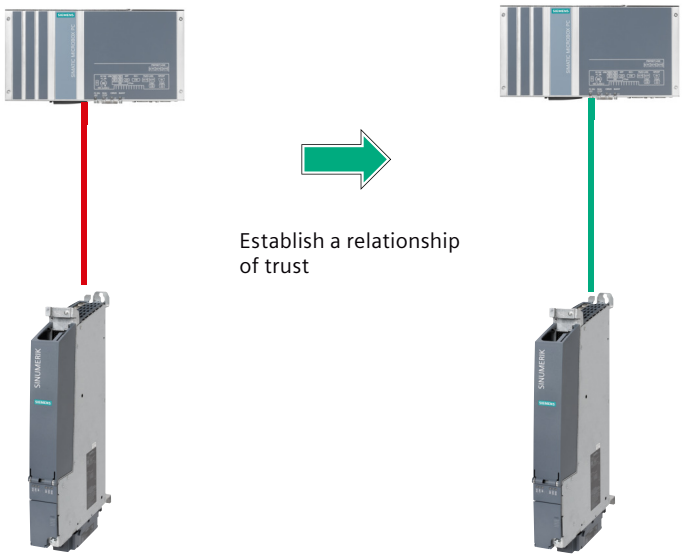


Figure 9-3 Pairing: Establishing a relationship of trust

9.5.3.2 Pairing the NCU and IPC

Requirement

Note

Pairing for IPC systems only

Pairing only has to be performed if an IPC is installed in your SINUMERIK ONE system.

- The NCU to be paired is configured correctly via SINUMERIK Operate.
  OR
- The NCUs to be paired are configured correctly in the "mmc.ini" file.
- The NCU to be paired uses group-based access levels.

Introduction

- If you want to use the security function "User management (Page 59)", you should first pair your IPC with an NCU, i.e. establish a relationship of trust between the two devices.

Procedure

Start pairing by calling the function via Operate under "Security > Trusted devices > Pair NCU".

More information

You will find more information on pairing, important requirements, the exact procedure for all worksteps in SINUMERIK Operate, and possible error cases and how to remedy them in the Commissioning Manual "Final commissioning steps" and the associated online help.

9.5.3.3 Unpairing the NCU and IPC

Overview

If you want to remove the relationship of trust between the IPC and NCU again, you can use the "Unpair NCU" dialog in SINUMERIK Operate.

The possible use cases for unpairing might be:

- Replacement of an NCU if a spare part is required
- Accidental incorrect pairing
- Scrapping of a machine

NOTICE
No secure communication: User management on the NCU is deactivated / old access level passwords are active again As soon as you remove the relationship of trust between the IPC and NCU, secure communication between the two devices is no longer possible. • The user management on the NCU is deactivated as soon as you actively terminate the pairing. The user management on the IPC is still active. • After unpairing, the access level passwords that were valid before activating the user management in the NCU are active again. Therefore **only** unpair the NCU from the IPC if you are sure that you know the old access level passwords. If you no longer know the old access level passwords, you must reset the NCU to the factory default state!

The analogous use case occurs if you have to replace the pairing certificate of the IPC. As soon as you replace the pairing certificate, all active pairings with all NCUs are disconnected. In this scenario, too, the user management is deactivated on the NCU and the old access level passwords are active again.

More information

You will find more information about unpairing, the requirements, and the exact procedure for the worksteps in SINUMERIK Operate in the Commissioning Manual "Final commissioning steps" and the associated online help.

9.6 Know-how protection

9.6.1 SINUMERIK Integrate Lock MyCycles

Using the "SINUMERIK Integrate Lock MyCycles" (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.

The objective of this functionality is know-how protection and integrity protection of the cycle.

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.

This software option is available for the SINUMERIK ONE, 828D, MC, 840D sl and 808D controllers.

More information

Further information on cycle protection can be found in the SINUMERIK Access MyMachine /P2P (PC) Operating Manual (https://support.industry.siemens.com/cs/ww/en/view/109811131).

For the alternative way of cycle encryption via the software application "protector.exe", contact your responsible Siemens sales representative.

9.6.2 Encryption of blocks

Encryption of blocks

As of STEP 7 Version 5.5 SP3 and the CNC system software V4.5 SP2 for 840D sl/ 840D sl or V6.13 for SINUMERIK ONE, 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).

9.7 Secure communication

9.7.1 OPC UA

OPC UA (Unified Architecture) is a standardized, industrial communication protocol for access to control data, e.g. by higher-level control systems.

With the SINUMERIK Integrate Access MyMachine /OPC UA software option, variables of a SINUMERIK ONE can be read and written via this communication protocol. Furthermore, the following functions are supported:

- Transfer of part programs
- Support for file and folder objects
- Event-based provision of SINUMERIK alarms and messages from HMI, NC and PLC
- Methods for selecting part programs of the NC file system and external memory and methods for tool management
- Multiple languages are supported for alarms and warnings.
- The OPC UA server supports customer-specific object models
- The OPC UA Server supports OPC UA Advanced functionalities like pallet handling or tool management with CNCs in your manufacturing system

OPC UA with client/server communication is widely used in automation. In this "one-to-one" communication mechanism, each OPC UA client obtains access to the data of the OPC UA server via point-to-point communication: The OPC UA client sends a request to the OPC UA server and receives a response from it. This enables reliable, secured and encrypted data exchange with reduced bandwidth and without data loss, even if the environment and network quality are not optimal and are subject to interference. Client/server communication is always based on TCP/IP.

Observe the following notes when using the OPC UA communication protocol:

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 SINUMERIK Access MyMachine /OPC UA Configuration Manual (https://support.industry.siemens.com/cs/us/en/view/109807257).

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 Secure passwords (Page 40).

9.7.2 Protocols for network drives

The following communication protocols for integrating network drives are supported:

SMB server protocol

To connect the NCU and the PC system in the network to an external Microsoft Windows server, the server protocol SMB (Server Message Block) is used. Microsoft Windows 10 supports SMB servers with protocol versions SMBv1, SMBv2 and SMBv3. Depending on the configuration, different servers require a different protocol version to enable a connection with the NCU and the PC system.

The SMB protocol versions are compatible with the following software:

CNC software	Supported SMB protocol version
V6.1x (ONE)	V1.0, V2.0, V3.0.2
V6.2x (ONE)	V1.0, V2.0, V3.0.2, V3.1.1

More information on the following topics can be found in the online help of SINUMERIK Operate:

- Permit SMB V1 in auto-negotiation
- Use SMB encryption (only from SMB V3)
- Storing the SMB server in the network of NCU and the PC system in SINUMERIK Operate
- Configuration of the SMB server as softkey in the program manager
- Setting up the SMB server as a Microsoft Windows network drive "NW Windows"

NFS server protocol

To connect the controller and the PC system in the network to an external NFS server, the NFS server protocol (Network File System) is used. Depending on the configuration, different servers require a different protocol version to enable a connection with the NCU and the PC system.

The NFS protocol versions are compatible with the following software:

CNC software	Supported NFS protocol version
V6.1x (ONE)	V2.0, V3.0, V4.0, V4.1, V4.2
V6.2x (ONE)	

More information on the following topics can be found in the online help of SINUMERIK Operate:

- Configuration of the NFS server as softkey in the program manager

Recommendations for secure protocols

Where possible, only use secure communication protocols to integrate network drives. Protocol standard SMB > V3.0 is regarded as a secure communication protocol but NFS and SMB < V3.0 are classed as insecure.

9.7.3 SSH encryption

You can use remote access to access devices from the PC system.

An SSH environment is initially set up when installing PCU-Basesoftware /IPC for Microsoft Windows 10. You can log on with PuTTY.

You can use an SSH key to log on. A script for setting up the infrastructure on devices is provided. However, for security reasons no previously generated keys have been stored.

For **more information** on the procedure for setting up users and using remote access with SSH, refer to the "PCU Base for IPC" Commissioning Manual.

9.8 Logging and monitoring

9.8.1 Security Eventlog

9.8.1.1 Overview of Security Eventlog

Definition

The Security Eventlog records security-relevant events and can deliver these via SysLog (RFC 5424) to a central SysLog server or a Security Information and Event Management (SIEM) so that attacks can be detected at a higher level.

Moreover, events are also kept locally for a certain time and can be viewed in SINUMERIK Operate.
The Security Eventlog is only accessible to authorized persons and can only be deleted by authorized persons. Manual deletion of the memory is required for data protection. On manual deletion of the memory, a new entry in the log indicating this is created.

Note

Personal data are processed and stored in the Security Eventlog.

If the SINUMERIK system is distributed across IPCs and NCUs and several NCUs are linked to one IPC, each NCU forwards the Security Eventlog to the paired IPC. The IPC sends these Security Eventlogs to the external SysLog server.

Purpose of the Security Eventlog

The Security Eventlog is used to record and provide security events of the SINUMERIK system.

The Security Eventlog supports the system and security administrators with monitoring all processes within a factory.

A Security Eventlog is used to detect attacks on a system or infrastructure early on in order to be able to take countermeasures. Attacks often take months in which an attacker progresses bit by bit. Discovering attacks of this type is the aim of a SIEM system that receives patterns from the security events of all components of the plant and can use these to detect threats.

If there is no central system, the events relevant to security are also displayed in SINUMERIK Operate under "Eventlog".

9.8.1.2 Features of Security Eventlog

The Security Eventlog logs the events relevant to security according to IEC 62443-4-2. Recurring events are grouped together to form an entry with a frequency counter to prevent a manipulation from being protected by a denial of service attack.

The Security Eventlog is permanently active from when the system starts and cannot be deactivated.

Approx. 1000 events are stored in the Security Eventlog. After this, the events are overwritten by new events.

The last 200 entries in the Security Eventlog are displayed in SINUMERIK Operate in the operating area "Diagnosis" under "Eventlog".

The Security Eventlog configured in SINUMERIK Operate only provides events of the NCU and events generated in the context of Operate.
To access Microsoft Windows operating system events when a IPC is used, there are common commercially available solutions. The Microsoft Windows operating system messages are not recorded by the SINUMERIK Eventlog.

The Security Admin can delete the local event memory. Manual deletion of the memory is required for data protection. On manual deletion of the memory, a new entry in the log indicating this is created.

SIEM is a combination of Security Information Management (SIM) and Security Event Management (SEM).

Both a central SysLog server and a Security Incident and Event Monitoring (SIEM) System enable a holistic view of the IT security and provide the following advantages:

- Fast and reliable detection of threats
- Fast and appropriate response to events relevant to security
- Compliance with legal requirements and compliance regulations
- Subsequent proof of security events
- Tamper-proof and audit-proof storage of all events relevant for security

More information

- You will find more information on the structure of the Security Eventlog in the List Manual "Security Eventlog Lists".

9.8.1.3 Transmission of events relevant to security

The stored events relevant to security are transmitted to a central SysLog server or a Security Incident and Event Monitoring (SIEM) System according to the SysLog standard RFC 5424.

To ensure data security during transmissions, the data are encrypted (TCP/IP with TLS).
To achieve this, the server certificate or a root certificate to which the server certificate can be traced must be imported in Operate. Importing a client certificate for authorization on the server is optional. The Security Eventlog supports server-based and client-based authorization.

Note

The end user is responsible for selecting and setting up a SysLog server or a SIEM system.

Note

You set up the connection to the central SysLog server or to the Security Incident and Event Monitoring (SIEM) System in SINUMERIK Operate.

You will find **more information** about the topic of "Setting up Syslog server" in the Commissioning Manual Work steps for configuring and commissioning and in the online help for SINUMERIK Operate.

9.8.1.4 Content of the EventLog

Each event contains a time stamp together with the event information itself and the origin IP/ domain name for identification.

For each event, the following information is recorded:

- Date and time
- Event source
- ID of the event type
- Event information

Events relevant to security are logged from the following sources:

- Linux system
- HMI and HMI applications
- OEM applications
- Security process
- Siemens OA applications, e.g. OPC UA

9.9 Network security and firewall

9.9.1 Overview

Concerning network security, it is assumed that the protective measures from section "Network security (Page 34)" are implemented.

Under the following link you will find an application example for network segmentation using a SCALANCE SC622-2C and a SINUMERIK ONE: Network security through SCALANCE SC622-2C for the SINUMERIK environment (https://support.industry.siemens.com/cs/ww/en/view/109481158)

9.9.2 Firewall settings

NCU/PCU networking structure

The following graphic shows the networking of the control (NCU) and the IPC. X130 at the NCU and eth 1 at the IPC 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 IPC has the firewall function via the Windows functionality.

NOTICE
Data misuse via an unprotected interface Since the X120 interface of the NCU or the eth2 port of the IPC are not protected by a firewall, there is a risk of misuse of data. 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.

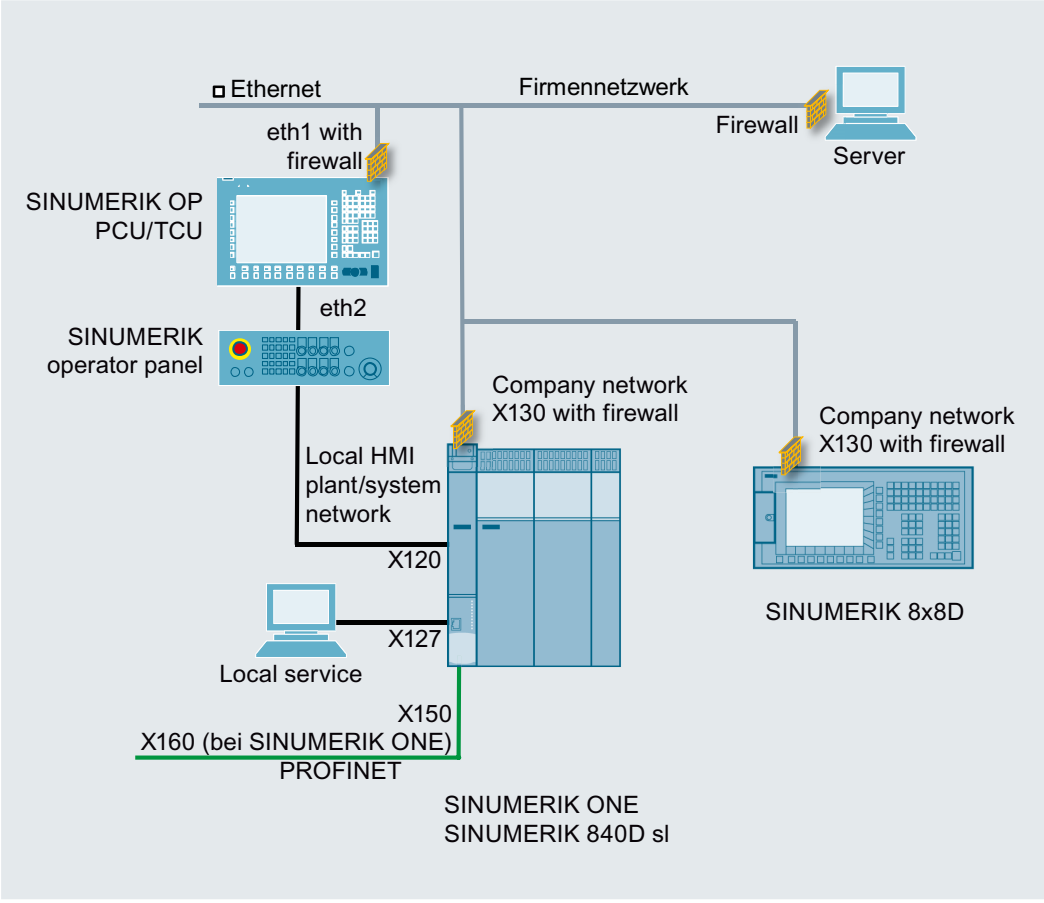


Figure 9-4 Networking of NCU/IPC

Firewall settings

Ethernet interface X130 of the NCU and the eth1 interface of the IPC are protected by a firewall for security reasons. If individual programs require access to a communication port for communication purposes, you can define firewall exceptions for specific ports via SINUMERIK Operate.

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

Generally, unused ports must be closed in the firewall and an up-to-date virus scanner or software with a positive list/allowlist must be installed on the PCU.

9.10 Reduction of the attack surface

9.10.1 Least functionality of hardware ports and their drivers

Hardware ports and their drivers should - if possible - be closed or physically protected. The following table provides recommendations on which settings are recommended for operation and why these recommendations are useful.

Recommendations for hardware ports

Ports and drivers	Status when delivered	**Best practice for operation**	Reason
X120	Open	Open	The X120 interface is the internal machine network of the control system, to which the HMI should be connected.
X126	Closed	Depends on the operation	In the TIA Portal, the PROFIBUS interface can be activated/deactivated if this is not required for operation.
X127	Open	Depends on the operation	The interface should be closed again after commissioning to reduce the attack surface as much as possible. The interface can be opened again temporarily for maintenance purposes.
X130	Open	Depends on the operation	X130 is the external network for connection to the production network. In rare cases when there is no connection to other networks, this port can be deactivated.
X150	Open	Depends on the operation	X150 is the main network to control machine I/Os. As a consequence, this port must normally be open. This interface can be deactivated if PROFIBUS is used instead of PROFINET.
X160	Open	Depends on the operation	Interface X160 is mainly used for machine communication. This port can be deactivated in the TIA Portal if it is not required.

Note

You should generally take additional actions to protect hardware ports against manipulation and unauthorized access. This can include all the recommendations and actions listed in the following chapters:

- Defense in depth concept (Page 26)
- Physical protection of critical production areas (Page 32)

9.10.2 Least functionality of protocols and ports as well as their associated drivers and services

Recommendations

Unnecessary network protocols and ports, as well as their drivers and services, should always be disabled to ensure maximum security and minimize the attack surface.

SINUMERIK ONE offers the option of deactivating unused ports using BIOS or the operating system. You can find a comprehensive list of all ports and protocols used with SINUMERIK ONE in the documentation SINUMERIK port lists (https://support.industry.siemens.com/cs/ww/en/view/109812283).

SINUMERIK supports the ports and protocols listed in this product information. For each port, its protocol, service, description, and affected interfaces are listed. It also indicates whether the port is open or closed by default, and whether this port is necessary for operation or service, or whether it is a Windows service.

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

Note

Always load the appropriate version of the documentation

The port lists may differ according to the CNC software version. Therefore, make sure that you always download the latest version matching your CNC version from the Internet. Instructions on how to ensure this can be found at the end of the chapter.

9.10.3 Finding the latest documentation in SiePortal

To ensure that you always find the latest version of the respective documentation in SiePortal, proceed as follows:

Procedure

1. Follow the direct link to the SiePortal article or search for the desired documentation in SiePortal.
2. Click on the "Edition" drop-down menu to display a list of all available editions of the document.

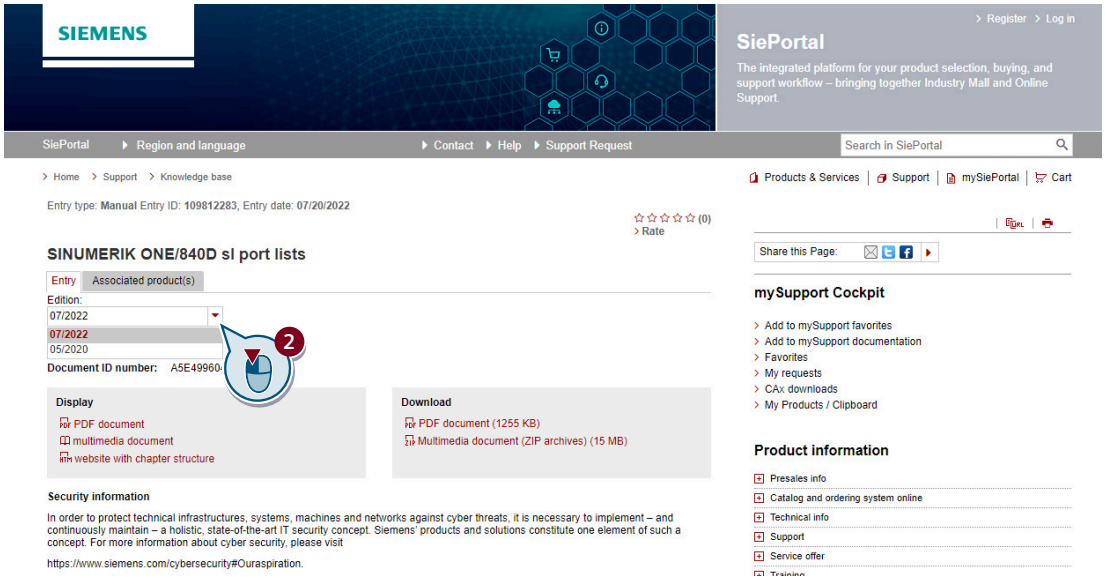


Figure 9-5 Selection of edition in SiePortal

3. **Always** choose the most recent edition of the document to ensure you have access to the latest and most up-to-date information. The link provided may not always refer to the most current edition.

9.11 Plant security

9.11.1 Physical protection against manipulation of the NCU

Authenticity label on the NCU

An authenticity label is attached to all installed NCUs of the SINUMERIK ONE for protection against hardware manipulation.

You will find the authenticity label glued between the side panel and the front of the NCU. It is printed with a hologram structure for security reasons.

Figure 9-6 Authenticity label NCU

If the authenticity label is intact, it guarantees you that no one has tampered with the component before or after delivery.

⚠ CAUTION

Authenticity label is broken

- The manufacturer's warranty for the product expires with immediate effect if the authenticity label is damaged.
- A damaged authenticity label may indicate that the component has been manipulated and it is recommended that no further use be made of affected components. Contact your Siemens customer service immediately.

Recommendations for secure operation and secure disposal

10

Options for secure configuration of the product are described in Chapter Security functions of the product (Page 55). The secure configuration of the product is part of a **overall technical security design**, which a system integrator provides to the operating company.

To protect the product in operation, the technical security design must be supplemented by the appropriate procedure for secure operation and secure disposal. The operating company is responsible for these procedures. The system integrator provides the operating company with a **Manual for secure operation**.

Recommendations for secure operation and securely disposing of the product are provided in this section. The system integrator can use this data for the manual for secure operation.

10.1 Recommendations for secure operation of the product

To ensure secure operation, the assumptions listed in Chapter Intended operational environment (Page 51) should be complied with.

Further, the following recommendations apply:

- Activate the SINUMERIK user management (Page 59)
- If you do not work with the SINUMERIK user management, change the default SINUMERIK passwords to secure passwords. Appropriately safeguard passwords (need-to-know principle), as many security measures depend on the correct user level.
- Allowlist software is recommended for SINUMERIK systems that are equipped with an IPC for visualization. In conjunction with SINUMERIK, Siemens offers McAffee.
- At the network interface of the company, open as few ports as possible; this especially applies to port 102, which should not be opened.
- Perform backups regularly. (Page 69)
- Make sure that the NCU is only accessible to authorized personnel.
- Protect your network according to the cell protection concept (Page 34).
- SINUMERIK Operate on the IPC should run under a normal user account. Do not use an administration account.
- Create a BIOS password during setup. The BIOS password prevents unauthorized users from accessing the BIOS or making changes to the settings in the BIOS.

10.2 Security by default

Definition of and statement on implementation

The "Security by default" concept means that the default configuration settings of a product are automatically the most secure settings.

Due to series commissioning, the "Security by default" concept is not currently available with SINUMERIK ONE.

10.3 Recommendations for secure product disposal

10.3.1 General recommendations for disposal

The products should be disposed of in accordance with valid national regulations. The products described in this manual are extensively recyclable on account of the low-toxic composition of the materials used. To recycle and dispose of your old equipment in an environmentally friendly way, please contact an appropriate disposal service.

NOTICE
Misuse of data resulting from insecure methods of deleting data Incomplete or insecure deletion of data from memory cards or hard drives can lead to misuse of the data of part programs, archives, etc. by third parties. • Therefore ensure that all storage media are securely deleted **before disposing of the product** : • There are programs that support you in securely deleting/formatting storage media. Alternatively, contact a certified disposal service provider who can professionally handle this task.

Securely deleting data

- **Non-encrypted data**:
  If non-encrypted data is used (this is not recommended), digitally rewritable data storage media must be completely overwritten with a data stream of random values (e.g. PRNG stream).
  Various manufacturers, e.g. Microsoft also offer (free-of-charge) tools that support you when securely deleting data.
- **Encrypted data**:
  To be able to quickly and securely delete data, we recommend that sensitive data is always stored encrypted.
  When deleting/disposing of data, it is then sufficient if the cryptographic key, used to decrypt the data, is overwritten with random values so that data to be protected cannot be accessed.

More information

Additional information on securely deleting data is provided in the following sources:

- German Federal Office for Information Security (BSI) Completely deleting data on hard disks and smart phones (https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Daten-sichern-verschluesseln-und-loeschen/Daten-endgueltig-loeschen/daten-endgueltig-loeschen_node.html)(only available in German)
- BSI IT Compendium of protection fundamentals - CON.6.A12 Minimum requirements for techniques to destroy and delete (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf?__blob=publicationFile&v=4)

- NIST Special Publication 800-88 Guidelines for Media Sanitization (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf)
- On the VDMA homepage, in the area Industrial Cybersecurity (https://www.vdma.org/industrial-security), articles and news on the subject of industrial cybersecurity are published on a regular basis.
- Secure destruction of data storage media is officially regulated in Standard DIN 66399. The Standard discusses the following topics:
  - Part 1 of the Standard: Determination of the protection requirements and assignment of protection classes (1, 2 or 3).
  - Part 2 of the Standard: Definition of the permissible material parts as a function of the data media type (semiconductor memory, here: flash memory) corresponding to the security level to be implemented (Table 6) . For magnetic data storage media, see Table 5.

10.3.2 Securely disposing of data storage media

Data storage media contained

The subsequently listed data storage media used in SINUMERIK ONE can potentially include customer data and, depending on the protection requirement, must be securely deleted or physically destroyed when disposing of the media.

- Internal PLC SD card
- External SD card
- 2 SSD memory
- NVRAM

Note

Physically destroying SD cards

SD cards are flash memories with defect management and if at all possible these should be physically destroyed.

For the remaining data storage media, we recommend that you proceed as described in Chapter General recommendations for disposal (Page 98).

Security-critical system states 11

11.1 Overview

Security-critical system states represent an increased risk of a security attack, and should therefore be avoided as far as possible when developing the product. Nevertheless, it is not possible to suppress all safety-critical system states, as these may be required for various scenarios. We would therefore like to make you aware of the following known critical system states of the SINUMERIK ONE so that you can take them into account accordingly.

- Eboot service system on an USB memory (Page 102)
- Operating system with access to the SD card (Page 103)
- Access to the Linux file system with CMC with USB stick (Page 104)

11.2 Eboot service system on an USB memory

Description of the security-critical system state

If service is required, create a portable "Emergency Boot System" (EBS) or eBoot service system on a USB memory. This enables you to start running up the NCU from the service system and to carry out various service tasks in a service menu, such as data backup or updates.

Reaching the security-critical system state

How you insert the USB memory into the NCU and operate the service system is explained in the SINUMERIK ONE Installation Manual "Creating the SINUMERIK Service System" (https://support.industry.siemens.com/cs/ww/en/view/109817152).

After running up the NCU and unzipping the service system, the system can be fully used without any additional authentication.

Reason for the security-critical system state

The eBoot service system is required to support you when carrying out the following tasks:

- New installation
- Update
- Replacement
- Service tasks

A detailed description of these tasks is provided in the SINUMERIK ONE Installation Manual "New installation and update" (https://support.industry.siemens.com/cs/ww/en/view/109817147).

Protective measures

Prevent access to the USB slots of the NCU and IPC.

11.3 Operating system with access to the SD card

Description of the security-critical system state

The SD card can be removed from the control system. The SD card contains a large percentage of the runtime software as well as all of the configuration data. The SD card is organized in a LINUX file system, and can be manipulated using a LINUX-PC.

The control system cannot be used if the SD card is not inserted in the control system.

Reaching the security-critical system state

- Withdraw the SD card and insert in a LINUX-PC card reader.
- Manipulate the card and reinsert it into the control system.

Risk due to the security-critical system state

Access to data, which in the context of the control system, are protected against unauthorized access. Risk of losing know-how and manipulation of the integrity of the configuration.

Reason for the security critical system state

For the case that a component has to be replaced because defective hardware, a main requirement is that the data and licenses can be transferred as quickly and simply as possible to new control system hardware. This is the reason that the data must be available on the SD card and the licenses are linked to the card.

Protective measures

Take precautions to ensure that the SD card is only accessible to authorized persons.

11.4 Access to the Linux file system with CMC with USB stick

Description of the security-critical system state

Engineering software Create MyConfig (CMC) supports machine manufacturers when creating and running projects for automated production and commissioning of machines with SINUMERIK ONE control systems. Updates of these control systems are also configured by the OEM and then performed automatically at the end user's installation.

The service on the control system, which executes the package, runs with access level "Machine manufacturer". This is the reason that it is possible to create a script and to access the LINUX file system without authorization.

Reaching the security-critical system state

The rights required for execution are automatically assigned to the package. The assignment of these rights gives the user comprehensive access to the LINUX file system corresponding to the rights of the machine manufacturer. However, to do this, a USB stick with the CMC package must be inserted in the NCU, and this must be restarted.

Risk due to the security-critical system state

Access to data, which in the context of the control system, are protected against unauthorized access. Risk of losing know-how and manipulation of the integrity of the configuration.

Reason for the security critical system state

It must be possible to execute installation packages in machine production and machine service.

Protective measures

Prevent access to the USB slots of the NCU and IPC and to the USB stick.

Procedure for managing security updates 12

12.1 Vulnerability management

How do I check my installed CNC software release?

1. In SINUMERIK Operate, select the "Diagnostics" operating area.
2. Press softkey "Version".
   Window "Version data" opens.
   The data of the components available are displayed.
3. The presently installed software release is displayed under "CNC software". You can obtain more detailed data on the displayed components using softkey "Details".

More information

More information on checking the installed CNC software release is available in the Operating Manual SINUMERIK ONE Universal (https://support.industry.siemens.com/cs/ww/en/view/109801320) or through the SINUMERIK ONE online help.

12.2 Sourcing software updates

Information about software updates

You have two ways of checking whether a new software update is available for the SINUMERIK ONE control system:

- Through the "Product Support" in the Industry Online Support International (https://support.industry.siemens.com/cs/ww/en/). You can find the following at this address:
  - Up-to-date product information (product announcements)
  - FAQs (frequently asked questions)
  - Manuals
  - Downloads
  - Newsletters with the latest information about your products
  - Global forum for information and best practice sharing between users and specialists
  - Local contact persons via our Contacts at Siemens database (→ "Contact")
  - Information about field services, repairs, spare parts and much more (→ "Services")
- Or there, subscribe to the free-of-charge Newsletter for SINUMERIK ONE control systems. The newsletter provides information about regular software updates for your product.

Siemens ProductCERT

Siemens ProductCERT (https://siemens.com/cert) (Cyber Emergency Readiness Team) is the central department for security-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development departments in the form of consulting and other services. ProductCERT provides information about current threats and vulnerabilities as well as the appropriate countermeasures.

Sourcing software updates

You can directly source a new software update through your SIEMENS sales person.

You can scan our Contact person database (https://support.industry.siemens.com/cs/ww/en/) if you are not sure who your contact person is.

See also

Installation and update (https://support.industry.siemens.com/cs/ww/en/view/109801347)

12.3 Installing software updates

Detailed instructions on how you install a software update on a SINUMERIK ONE control system is provided in the Installation Manual SINUMERIK ONE – new installation and updating (https://support.industry.siemens.com/cs/de/en/view/109801347).

12.4 Windows update for IPC systems

Windows Server Update Services (WSUS)

NOTICE
Data manipulation through security vulnerabilities in the operating system Microsoft does not provide any automatic security updates, service packs or hotfixes for operating systems older than Windows 10. This can leave the operating system with dangerous security vulnerabilities. • If you are using an operating system older than Windows 10, take additional measures to protect the operating system. • If possible, always upgrade the operating system of your operating unit to the current version.

The **WSUS** (Windows Server Update Services) system functionality provided by Microsoft is available for Windows operating systems.

WSUS supports administrators by rolling out Microsoft updates in large local networks. WSUS automatically downloads update packages and offers them to the Windows clients for installation. The automated update process ensures that the latest system and security updates are installed on the Windows clients.

Before installing system and security updates, please note the following points:

- Perform a system backup.
- Administrators must ensure that system and security updates do not impair the operability of production plants.
- Do not establish a direct Internet connection to the WSUS server! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

More information

You can find more information about network segmentation in Chapter Network segmentation (Page 34).

Tips for security checks

13

You can additionally check the security of your SINUMERIK ONE system using the following routines and checks:

Security checks

- Check the firewall settings
- Check the default passwords
  Check whether you have changed the default passwords after commissioning.
- Deactivate unused ports
  Check whether you have deactivated all unused ports
- Check the communication settings of OPC UA
  In the server settings, check if the highest encryption level is activated and that "Anonymous access" is not allowed.
- Check the communication settings of OPC UA (Page 110)
  In the server settings, check if the highest encryption level is activated and that "Anonymous access" is not allowed.
- Check that SINUMERIK Operate does not have admin rights under the Windows account.
- Make sure that the USB ports of the NCU are only accessible to authorized personnel.
- Make sure that the SD card and SD port of the NCU are only accessible for authorized personnel.

13.1 Checking software signatures

13.1.1 Manually checking software signatures under Windows

Executable files and scripts can be digitally signed to confirm and guarantee that the code has not been changed or corrupted since signing. This method uses cryptographic hashes to verify authenticity and integrity.

To manually verify the authenticity and integrity of the installed Windows software, proceed as described below.

Procedure

1. First open the Windows File Explorer. Navigate to the storage location of your program.
2. Right-click the setup file and select "Properties".
3. Navigate to the "Digital Signatures" tab.

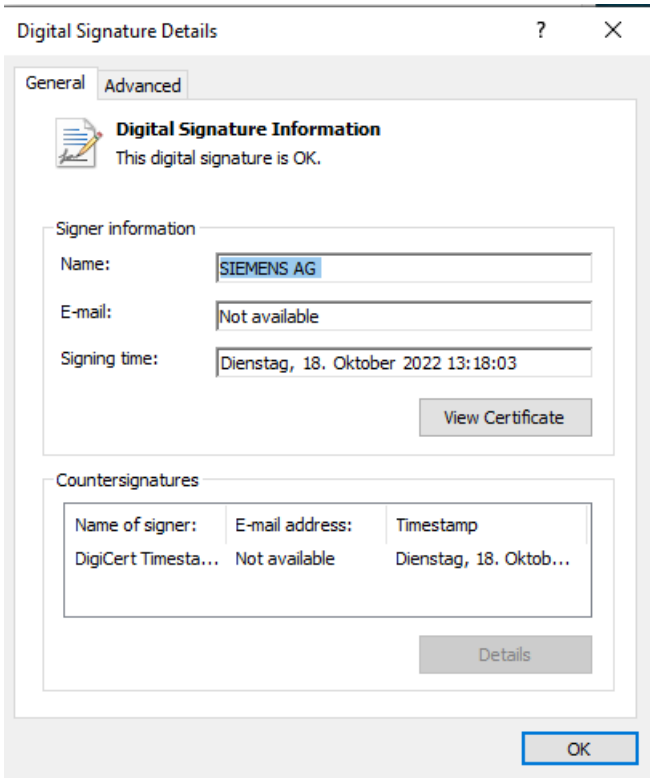


Figure 13-1 Digital signatures properties

4. If you do not see this tab, then the file was not signed or the signature was removed - the verification failed
5. If you see entries in the signature list, it means that your file is digitally signed. You can double-click on any of these entries to view more details about the signing authority. You can also verify whether the file is signed by the original distributor of the software or not.

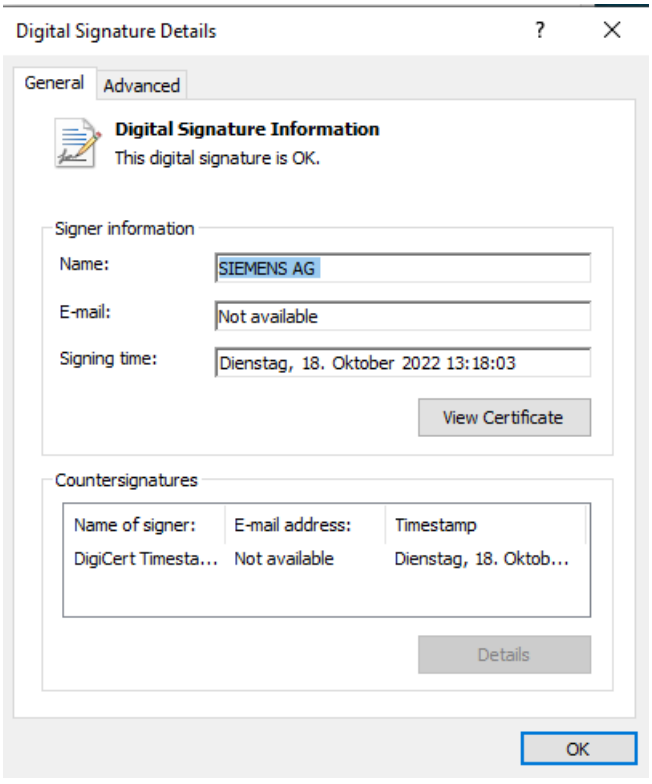


Figure 13-2 Digital signatures details

13.1.2 Automatically checking software signatures under Windows

You can also use suitable checking programs to check the authenticity and integrity of the installed Windows software. The automated check using the "Microsoft Sigcheck" software is subsequently described as example.

Download Microsoft Sigcheck

Note

Preconditions

To be able to use Microsoft Sigcheck, as a minimum Windows Vista or higher must be installed.

1. Download Microsoft Sigcheck from the following page: Microsoft Sigcheck (https://docs.microsoft.com/en-us/sysinternals/downloads/sigcheck).
2. Unzip the .zip file to your local hard disk.

Microsoft Sigcheck is a program that can be run from the command line. You can review the list of all possible parameters through the download page.

Checking recursive paths

Using the software described, you can also check recursive folder paths to ensure that they have the correct digital signature. Option "-s" recursively checks the complete folder path.
The check for all files of the installed "Access MyMachine /P2P" software is shown below:

```
>sigcheck.exe -s "c:\Programs\Siemens\Automation\Access MyMachine
P2P (PC) 4.9"
```

Check result

The software communicates the check result using parameter "Verified".

- If the file was signed with a code signature certificate derived from a root certification authority, which is trusted on the current computer, and the file has not been modified since it was signed, then the software issues "Signed" as result.
- If the file was not signed, then the software issues "Unsigned".
- If it was signed, but there are problems with the signature, then these problems are defined. The problems can include the following:
  - The validity period of the signature certificate has expired when the signature is checked.
  - The root certification authority is not trusted (which can be the case for a self-signed certificate).
  - The file was changed since signing.

More information

Additional information about PKI documentation can be found online:

- Certification Practice Statement (https://en.wikipedia.org/wiki/Certification_Practice_Statement)
- Certificate policy (https://en.wikipedia.org/wiki/Certificate_policy)
- Digital ID information (http://www.siemens.com/industrial-security/pki)

References

A

This documentation makes reference to the following standards and external documentation:

- IEC 62443-3-3, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels (IEC:2013(E))

Glossary

Allowlist

An allowlist or blocklist is a positive or negative list that can be used to protect systems in the IT environment. Allowlists and blocklists, which apply opposing strategies, are used in a wide range of domains.

Allowlists follow the principle that anything not explicitly included on the list is prohibited. The allowlist therefore includes only the requested, trusted entries. This means that the entries in the list represent exceptions to the general block rule.

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.

Blocklist

An allowlist or blocklist is a positive or negative list that can be used to protect systems in the IT environment. Allowlists and blocklists apply opposing strategies and are used in the widest range of domains.

With a blocklist, everything is permitted that is not in the list. The blocklist is a negative list, which lists the targets, programs and addresses that are not trusted or are not permissible. With the negative list, it is possible to specifically prohibit individual applications or communication targets.

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.

Code injection

Code injection is the exploitation of a computer error caused by processing invalid data. Injection is used by an attacker to inject code into a vulnerable computer program and cause it to execute.

Confidentiality

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

Cyber security

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It also includes the security of information technologies and electronic information. The term is broad and applies to everything from computer security to disaster recovery, i.e. the restoration after an incident, to the training of end users.

Defense in depth

Creation of multiple security mechanisms, especially in a layer structure, with the intention of slowing down or completely preventing attacks.

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 Cybersecurity

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.

Internet of Things (IoT)

General term for technologies of a global infrastructure of information organizations which allow physical and virtual objects to be linked together and allows them to work together via information and communication techniques.

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.

Man-in-the-disk attack

The concept of a "man-in-the-disk" attack is similar to that of a "man-in-the-middle" attack as it includes intercepting and editing data, which is exchanged between an external memory and an application.

Man-in-the-middle attack

In cryptography and cyber security, a man-in-the-middle attack is a cyber attack where the attacker secretly interjects in the communication between two parties and possibly changes the associated data. The two parties involved think that they are directly communicating with one another as the attacker interjected himself between the two parties.

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.

Pairing

Process used in computer networks to establish an initial connection between computers to enable communication between them or to establish a trust relationship for a secure connection.

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.

Patterns of viruses

Designation for the database of virus scanners, which contains the schematic and code-specific structure of all known viruses. This is usually a file that is used and processed by the virus scanners. The schemata contained in the file are used when checking for viruses and with them the files to be checked are compared.

PCU

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

Phishing

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.

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 (TRA)

The 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.

TIA Portal

The TIA Portal is an automation framework for the SIMATIC S7-1200, S7-300, S7-400 and S7-1500 CPU families from Siemens.
"TIA" stands for Totally Integrated Automation. In the TIA Portal, all of the necessary software tools are combined under one user interface.

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 (WSUS in short) 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

R

S

T

U

V

W