SIEMENS

SINUMERIK

SINUMERIK ONE
Industrial cybersecurity

Configuration Manual

Valid for the SINUMERIK ONE control system
CNC software version 6.25 SP2

04/2026
A5E51912408B AG

Introduction 1
Security instructions 2
Fundamentals 3
Security measures in automation and drive technology 4
Security management 5
General security measures and concepts 6
System overview 7
Operational environment of the SINUMERIK control system 8
Defense in depth concept SINUMERIK ONE 9
Protection goals and hardening measures 10
Security functions of the product 11
Recommendations for secure operation and secure disposal 12
Security-critical system states 13
Security updates 14
Tips for security checks 15

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 persons are those who, because of their training and experience, are familiar with the installation, assembly, commissioning, operation, decommissioning and disassembly of the product and can recognize risks and avoid possible hazards.

Proper use of Siemens products

Note the following:

⚠ **WARNING**
Siemens products may only be used for the application described in the catalog and the associated usage information. 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 AG
Ⓟ 04/2026 Subject to change

Copyright © Siemens 2024 - 2026.
All rights reserved

Table of contents

1 Introduction 9

1.1 About SINUMERIK 9

1.2 About this documentation 10
1.2.1 Purpose of the documentation 10
1.2.1.1 Target group 10
1.2.1.2 Data for the technical security design and the secure system configuration 10
1.2.2 Standard scope 11

1.3 Documentation on the internet 13
1.3.1 Documentation overview SINUMERIK ONE 13
1.3.2 Documentation overview SINUMERIK operator components 13

1.4 Feedback on the technical documentation 14

1.5 mySupport documentation 15

1.6 Service and Support 16

1.7 Use of third-party software 18

1.8 Compliance with the General Data Protection Regulation 19

1.9 Find EU Declaration of Conformity - Manufacturers for product 20

2 Security instructions 21

2.1 Fundamental safety instructions 21
2.1.1 General safety instructions 21
2.1.2 Warranty and liability for application examples 21
2.1.3 Cybersecurity information 21

3 Fundamentals 23

3.1 Data security in the industrial environment 23

3.2 Industrial cybersecurity 24

3.3 Safety Integrated and Industrial Cybersecurity 25

4 Security measures in automation and drive technology 27

4.1 Security measures 27

4.2 Identifying and notifying security vulnerabilities 29

4.3 Standards and regulations 30

5 Security management 31

6 General security measures and concepts 33

6.1 Categories of access and authorization to access products 33

6.2 Defense in depth concept 35

6.3 Plant security 37

6.3.1 Overview ... 37
6.3.2 Physical protection of critical production areas ... 37
6.4 Network security ... 39
6.4.1 Overview ... 39
6.4.2 Network segmentation ... 39
6.4.2.1 Separation between production and office networks ... 39
6.4.2.2 Network segmentation with SCALANCE S ... 40
6.4.3 Cloud Security ... 44
6.5 System integrity ... 46
6.5.1 Overview ... 46
6.5.2 Measures to harden the IT infrastructure ... 46
6.5.2.1 Services and ports ... 46
6.5.2.2 User accounts ... 47
6.5.2.3 Operating units used in the industrial context ... 47
6.5.2.4 Store sensitive data securely ... 48
6.5.2.5 Transporting sensitive data securely ... 48
6.5.2.6 Secure passwords ... 48
6.5.2.7 Virus scanner ... 49
6.5.2.8 Allowlists ... 50
6.5.3 Patch management ... 50
6.5.3.1 Windows patch management ... 50
6.5.3.2 Program updates in the TIA Portal ... 51
6.5.3.3 Product software ... 51
6.5.4 Data integrity ... 52
7 System overview ... 53
7.1 System overview ... 53
7.2 Essential functions ... 56
7.3 Communication interfaces ... 57
7.4 Data flows and data memory ... 59
8 Operational environment of the SINUMERIK control system ... 61
8.1 Measures to protect the operational application environment ... 61
8.2 Security assumptions for the intended operational environment ... 65
9 Defense in depth concept SINUMERIK ONE ... 67
9.1 Plant security ... 67
9.2 Network security ... 68
9.2.1 Protection status of SINUMERIK networks ... 69
9.2.1.1 HMI network (X120) ... 69
9.2.1.2 Service network (X127) ... 70
9.2.1.3 Factory network (X130) ... 70
9.2.1.4 Machine-internal field network (X150) ... 71
9.2.1.5 Factory network PLC (X160) ... 72
10 Protection goals and hardening measures ... 73
10.1 Overview of protection objectives ... 73
10.2 SINUMERIK ONE system hardening measures ... 74

10.3 Ports and protocols 79
10.4 Security tools 80
11 Security functions of the product 81
11.1 Overview 81
11.2 Operation of the security functions 83
11.3 Role and access requirements for security functions 84
11.4 Time and date setting 85
11.5 User management and access control 86
11.5.1 Types of supported access management systems 86
11.5.2 Classic access management: Group-based access levels 86
11.5.3 Features and benefits of user management 87
11.5.4 SINUMERIK user management 89
11.5.4.1 Overview and definition 89
11.5.4.2 Functions of the SINUMERIK user management 90
11.5.4.3 Architecture of the user management 91
11.5.4.4 Groups and role concept 96
11.5.4.5 Role of the security admin 97
11.5.4.6 Activating and configurating user management 100
11.5.4.7 Policies 103
11.5.4.8 Role and access requirements for security functions of user management 106
11.5.4.9 Backing up/restoring data 107
11.5.5 Drive security 108
11.6 Backup and restore 109
11.6.1 Options for backing up and restoring data 109
11.6.2 Security archive 111
11.6.3 Restoring security data 113
11.6.4 IPC backup and restoration 114
11.7 System integrity 115
11.7.1 Certificate store 115
11.7.2 PLC security 118
11.7.2.1 Password to protect confidential PLC configuration data 118
11.7.2.2 Password for PLC access level 122
11.7.2.3 Password for the protection of the offline safety program 124
11.7.2.4 Know-how protection password 124
11.7.2.5 Copy protection password 124
11.7.2.6 Write protection password 125
11.7.3 Trusted devices 125
11.7.3.1 Overview 125
11.7.3.2 Requirement when pairing 127
11.7.3.3 Pairing the NCU and IPC 127
11.7.3.4 Unpairing the NCU and IPC 128
11.7.3.5 Renewing pairing certificates 129
11.7.4 Safety Integrated log file 130
11.7.4.1 Overview 130
11.7.4.2 Using the Safety Integrated log file 130
11.7.5 Secure Boot operation/Secure Boot 132
11.7.6 Defense against malicious code 133

11.7.6.1 Overview ... 133
11.7.6.2 Antivirus and anti-malware protection of the NCU ... 133
11.7.6.3 Antivirus and anti-malware protection of the IPC ... 133

11.8 Know-how protection ... 137
11.8.1 SINUMERIK ONE password policies ... 137
11.8.2 Secure account management ... 139
11.8.3 SINUMERIK Integrate Lock MyCycles ... 141
11.8.4 Encryption of blocks ... 142

11.9 Protecting data at rest ... 143
11.9.1 Encrypting an SD card ... 143
11.9.2 Restoring the SD card encryption ... 144
11.9.3 IPC Bitlocker hard disk encryption ... 146
11.9.4 Protecting part programs ... 148

11.10 Secure communication ... 149
11.10.1 Overview ... 149
11.10.2 Overview ... 150
11.10.3 OPC UA ... 150
11.10.4 HMI security ... 151
11.10.4.1 SMB and NFS server protocol settings ... 151
11.10.4.2 SSH network protocol ... 152
11.10.5 Secure web server communications via HTTPS ... 154
11.10.6 Network security and firewall ... 155
11.10.6.1 Overview ... 155
11.10.6.2 Firewall settings ... 155

11.11 Security Eventlog ... 158
11.11.1 Overview of Security Eventlog ... 158
11.11.2 Requirement for Security Eventlog ... 159
11.11.3 Features of Security Eventlog ... 159
11.11.4 Transmission of events relevant to security ... 161
11.11.5 Content of the EventLog ... 161

11.12 Reduction of the attack surface ... 162
11.12.1 Least functionality of hardware ports and their drivers ... 162
11.12.2 Least functionality of protocols and ports as well as their associated drivers and services ... 163
11.12.3 Finding the latest documentation in SiePortal ... 163

11.13 Protection against manipulation ... 165
11.13.1 Physical protection against manipulation of the NCU ... 165

12 Recommendations for secure operation and secure disposal ... 167

12.1 Recommendations for secure operation of the product ... 168

12.2 Recommendations for security-related maintenance tasks ... 169

12.3 Recommendations for secure product disposal ... 170
12.3.1 General recommendations for disposal ... 170
12.3.2 Securely disposing of the NCU ... 170
12.3.3 Securely deleting the IPC ... 172

13 Security-critical system states ... 173

13.1 Overview ... 173

13.2 Eboot service system on an USB memory ... 174

13.3 Eboot service system on an USB memory 175
13.4 Operating system with access to the SD card 176
13.5 Access to the Linux file system with CMC with USB stick 177
14 Security updates 179
14.1 Sourcing software updates 179
14.2 Checking the software version 180
14.3 Installing software updates 181
14.4 Windows update for IPC systems 182
15 Tips for security checks 183
15.1 Verification of security functions 183
15.2 Verification of security functions 184
15.3 Checking software signatures 185
15.3.1 Manually checking software signatures under Windows 185
15.3.2 Automatically checking software signatures under Windows 187
Glossary 189
Index 203

1 Introduction

1.1 About SINUMERIK

From simple, standardized CNC machines to premium modular machine designs – 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 manufacturing.

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 81). 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 53).

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 65). 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 65). 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 81). 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 167): Defining the security documentation for secure operation and secure disposal, which the system integrator hands over to customers.
- Chapter Security updates (Page 179): Defining the procedure for managing security updates
- Chapter Tips for security checks (Page 183): 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 documents 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. However, there is no obligation to supply such functions with a new control or when servicing.

For reasons of clarity, this documentation cannot include 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.

Web pages 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 does not check the information on these websites and is not responsible for the content and information provided therein. The user bears the full risk when visiting these websites.

Digital signature

The PDF format of this documentation is digitally signed. The digital signature ensures:

- **Authenticity**: Confirmation that the document was created by Siemens
- **Integrity**: Confirmation that content was not changed after signing

Checking the digital signature

- Always open the PDF document in a PDF viewer (e.g. Adobe Acrobat Reader), and not in an Internet browser. Browsers either do not display digital signatures at all, or in part only.
- The following instructions are for the procedure in Adobe Acrobat Reader. However, the steps in other PDF viewers are comparable.

1. Open the PDF document. The signature status is displayed at the top of the signature window:
   - Green checkmark: Signature is valid
   - Yellow warning sign: Signature is valid, but pay attention to notes
   - Red X: Signature is invalid or corrupted
2. Click on the "Signature window" button.
3. Expand the signature to view detailed information about the electronic signature.
4. You can display further details about the signature via the context menu under "Check signature > Signature properties".

Solutions for invalid/corrupted signatures

- Download the original PDF again from the official Siemens website.
- Check whether the download was fully completed.
- Update the PDF viewer.
- Update the certificates.
- Check the system time.

If these approaches do not solve the problem, contact Siemens Support via SiePortal. It is possible that the PDF has been manipulated by a third party.

1.3 Documentation on the internet

1.3.1 Documentation overview SINUMERIK ONE

You can find extensive documentation on SINUMERIK ONE version 6.13 or later under Documentation overview SINUMERIK ONE (https://support.industry.siemens.com/cs/document/109768483).

The documentation is available for viewing or download in PDF and HTML5 format.



1.3.2 Documentation overview SINUMERIK operator components

Comprehensive documentation about the SINUMERIK operator components is provided in the Documentation overview SINUMERIK operator components (ttps://support.industry.siemens.com/cs/document/109783841).

The documentation is available for viewing or download in PDF and HTML5 format.

The documentation is divided into the following categories:

- Operator panels
- Handheld units
- Machine control panels
- Further operator components

An overview of the most important documents, entries and links on the topic of "SINUMERIK" is provided at SINUMERIK Overview - Topic Page (https://support.industry.siemens.com/cs/document/109766201).

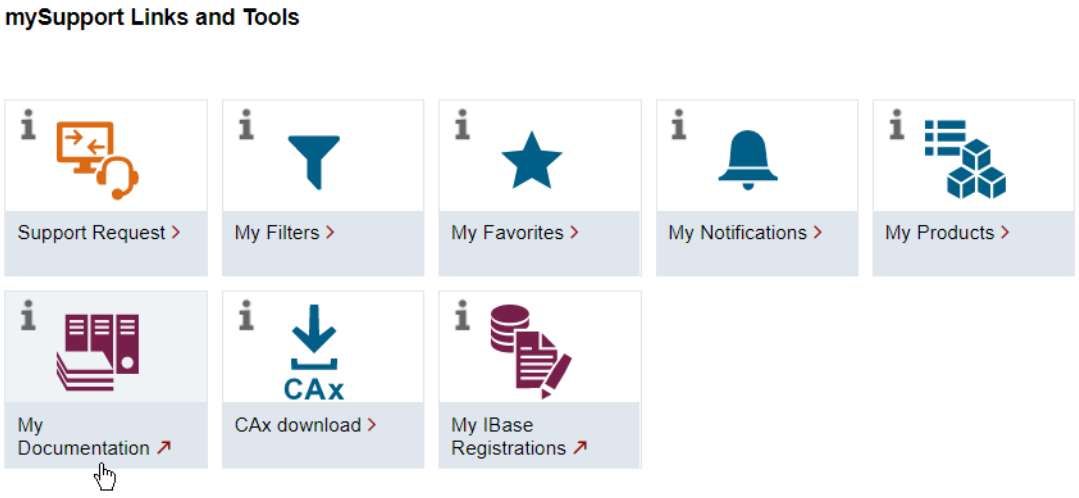
1.4 Feedback on the technical documentation

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

1.5 mySupport documentation

With the "mySupport documentation" web-based system you can compile individual documentation based on Siemens content, and adapt it for your 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) SiePortal 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 (→ "Support Request")
- Information about on-site services, repairs, spare parts, and much more (→ "Field Service Request")

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) under "Extended Services".

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

Training

You can find information on SITRAIN here 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 "Siemens 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 in the event of faults
- Expanding a system or planning a new system

You will also have access to the Technical Forum and articles prepared for you by our experts:

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

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

1.7 Use of third-party software

This product, this solution, or this service ("product") contains third-party software components. These are either open source software licensed under a license recognized by the Open Source Initiative (www.opensource.org) or a license defined by Siemens as comparable ("OSS") and/or commercial software or freeware. With regard to the OSS components, the relevant OSS licensing terms take precedence over all other conditions applicable to this product.

The licensing terms and copyright information of the third-party software components used by the product can be accessed digitally as part of the scope of supply of the product.

1.8 Compliance with the General Data Protection Regulation

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: Only if user management is activated
- 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 identifying authorized operating personnel. (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 – pseudonymized, as identifying operating personnel cannot otherwise be achieved.

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

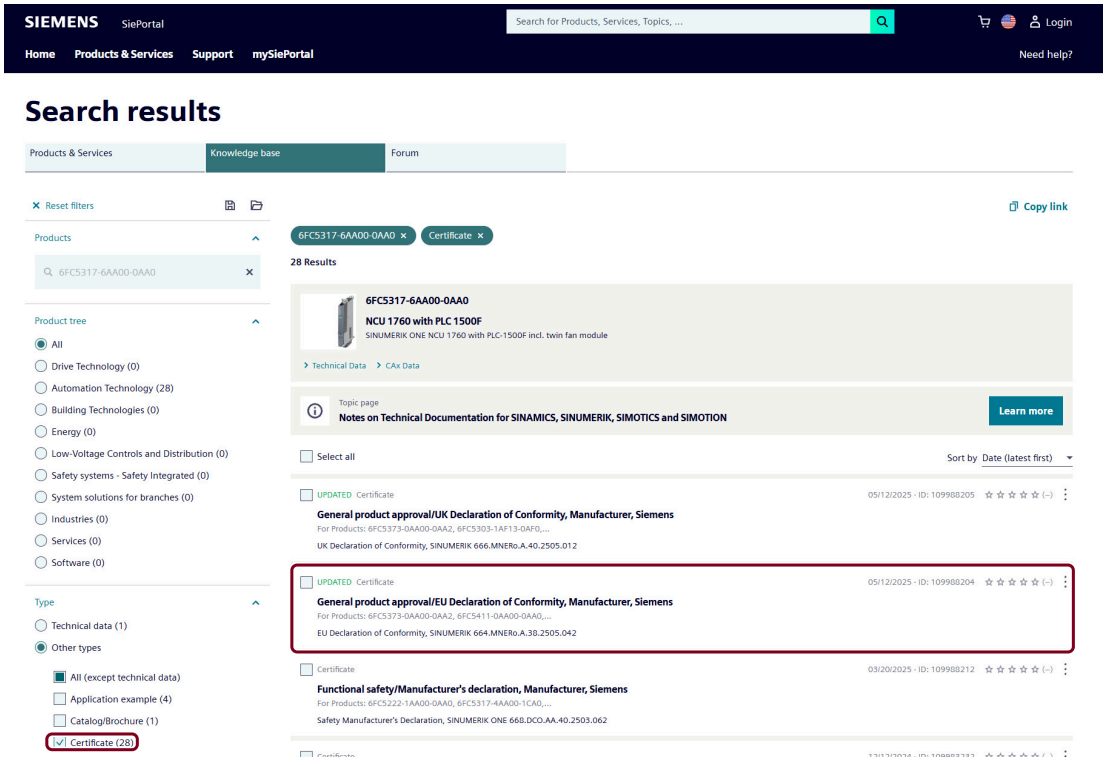
The above data is secured against loss of integrity and confidentiality by Industry State-of-the-Art Product Security mechanisms.

1.9 Find EU Declaration of Conformity - Manufacturers for product

To ensure that you find the correct EU Declaration of Conformity from the manufacturer, proceed as follows:

Procedure

1. Search for the article number of your product in the Siemens SiePortal.
2. Filter the knowledge base by entry type "Certificate" to display only the valid certificates for the respective product.



3. Select General product approval/EU Declaration of Conformity, manufacturer.

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 customer-specific solutions, but merely serve to provide assistance with 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://www.siemens.com/cert.

Further information is provided on the Internet:

Configuration Manual Industrial Cybersecurity (https://support.industry.siemens.com/cs/ww/en/view/109975311)

⚠ 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 with suitable protection measures, e.g. virus scanners.
- Carefully check all cybersecurity-related settings once commissioning has been completed.

Fundamentals

3

3.1 Data security in the industrial environment

Overview

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:

- Espionage of data
- Manipulation of data or software
- Sabotage of production plants
- Plant downtime, for example due to malware

Possible corporate security vulnerabilities

Examples of security vulnerabilities at a company:

- Employees
- Subcontractors
- Production plants and their components
- Network infrastructure
- Cellular and landline end devices
- The use of mobile data storage media (e.g. USB flash drives)

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

Possible effects of a security incident

Examples of possible consequences 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

3.2 Industrial cybersecurity

Overview

Industrial cybersecurity brings together all the measures used to protect against:

- Loss of availability; e.g. due to destruction of data or Denial-of-Service (DoS)
- Loss of confidentiality; e.g. due to unauthorized access to data and networks
- Loss of integrity of data and applications due to changes or manipulation following unauthorized access

Protection objectives

Industrial cybersecurity pursues the following objectives:

- Guaranteed trouble-free operation and availability of production plants and processes
- Prevention of hazards to people and production due to cyber attacks
- Protection of industrial automation systems and components from unauthorized access, manipulation and loss of data
- Protection of industrial communication from espionage and manipulation
- Protection of confidential data from unauthorized accesses

When you implement security measures, make sure that the measures do not impair or endanger the operability of automation systems and components.

Networking and wireless technology

The developments below underscore the relevance of security functions and measures:

- Cloud computing, vertical integration and Internet of Things (IoT):
  Networking is becoming increasingly prevalent within and outside production plants, for example in applications for cloud computing, vertical integration and Internet of Things.
- Wireless technologies:
  The use of wireless technologies in production plants is more and more widespread, for example through the introduction of new WLAN and mobile communication standards.
- Worldwide remote access to plants and machines

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

3.3 Safety Integrated and Industrial Cybersecurity

Safety Integrated

Safety Integrated ensures the reliable functioning of safety-related components and functions whose job it is to make certain a plant is put into, or remains in, a safe state if a fault should occur.

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

Safety Integrated ensures the safety of persons and goods located in the immediate vicinity of a component.

Industrial cybersecurity

Security functions and measures 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.

Security measures in automation and drive technology

4

4.1 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:

- Siemens implements the "Secure product development lifecycle requirements" specified in IEC 62443-4-1. The implementation was certified by TÜV.
- Siemens uses code analyses to identify possible bugs and flaws. Code analyses run automatically.
- Siemens implements measures to safeguard 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 of unneeded services, are minimized.
  - Siemens tests its products to detect weak points at an early stage.
  - Siemens offers a focused hotfix/patch management service.

Protection of the development infrastructure and supply chain

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

- Siemens ProductCERT (Cyber Emergency Readiness Team) is the central department for security-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development work with consulting and other services. Siemens ProductCERT makes information available on the Internet about current threats and vulnerabilities as well as the appropriate countermeasures:
  Siemens ProductCERT (https://www.siemens.com/cert)
- Industrial cybersecurity is a dynamic and complex subject that requires continuous monitoring, the adaptation of existing security measures and the introduction of new security measures. Information on how Siemens protects its products against cyber attacks can be found on the Internet.
  Securing Digitalization (https://securing-digitalization.dc.siemens.com)

Provision of patches, security components, and appropriate services

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:

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

4.2 Identifying and notifying security vulnerabilities

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

Siemens ProductCERT

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

SINUMERIK documentation is provided on the following
Internet page Siemens Aktiengesellschaft: Siemens ProductCERT
and Siemens CERT (https://www.siemens.com/global/en/products/services/cert.html?s=SINUMERIK&_originalHost=new.siemens.com#SecurityPublications)

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

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

- Contact persons for matters related to vulnerabilities
- Options for automated notifications regarding vulnerabilities
- Notifications are also possible in CSAF format
- Option to subscribe to RSS feeds and newsletters
- List of all current vulnerabilities and detailed information such as:
  - Description
  - Classification according to Common Vulnerability Scoring System (CVSS)
  - Measures
  - Availability
  - Etc.

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

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

4.3 Standards and regulations

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 62443-4-1: Security for industrial automation and control systems: Secure product development lifecycle requirements

More information

More information on certifications and standards in the industrial cybersecurity field can be found on the Internet:

Certifications and standards (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html)

Security management

5

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

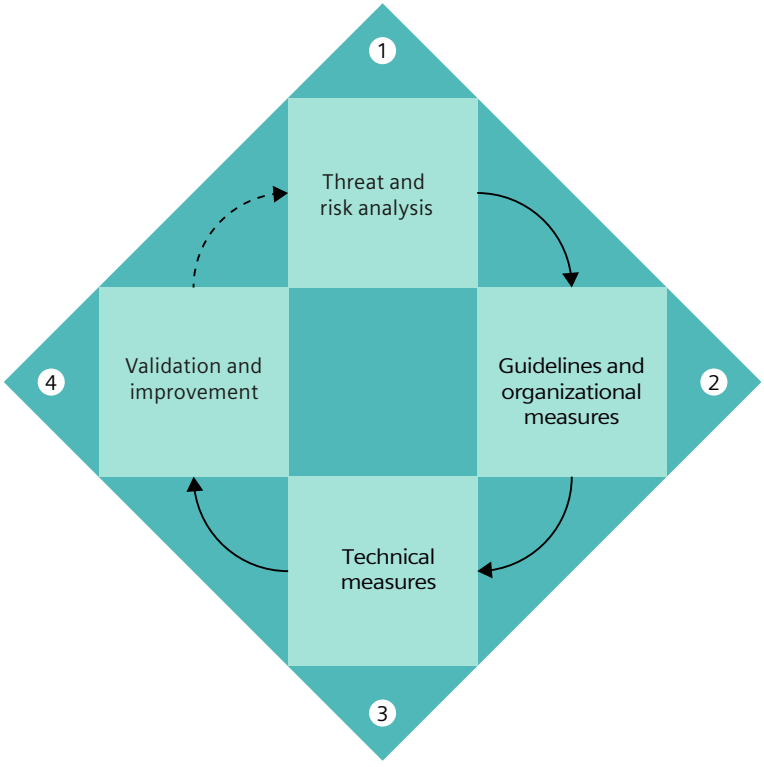


Figure 5-1 Security management process

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.

General security measures and concepts

6

6.1 Categories of access and authorization to access products

To prevent cyber attacks, operating companies must ensure adequate security measures in the operational use of products.

The concept of security context is used to systematically assess cybersecurity requirements. This concept is based on standardization activities within the scope of the EU Cyber Resilience Act and Standard EN IEC 62443-4-1.

The security context describes the operational application environment based on 3 categories: "Persons", "Physical access" and "Communications access".

Settings "Public", "Restricted" or "Controlled" defined the extent to which products should be protected.

The categories define the cybersecurity requirements in a product-specific and context-related manner, and the various deployment scenarios and user groups are appropriately taken into account.

Note

Product-specific cybersecurity requirements

You can find product-specific cybersecurity requirements relating to the operational application environment based on the following categories for the complete SINUMERIK system in this manual (Page 61), as well as for other SINUMERIK products in Chapter "Industrial Cybersecurity".

Category 1: Persons

The level of security knowledge and skill sets of the intended product user.

Persons	Features
"Unqualified" person (ordinary person)	• Has no product knowledge • Has no security-specific skills or knowledge • Has received no instructions regarding the user documentation
Instructed person	• Was trained and instructed on the product and its security features by a qualified person. • Understands how the product is installed, operated and maintained
Qualified person	• Has in-depth knowledge about industrial cybersecurity • Has had special training and extensive experience with the product and the system and their security features • Has in-depth knowledge as to how the product is installed, operated and maintained • Is in a position to assess potential security vulnerabilities

Category 2: Physical access

Physical access – The level of physical access restrictions for the product.

Physical access	Features
Public	Products that are physically and easily accessible for anybody, without any access restrictions
Restricted	Products that are not free or easily accessible for everybody. Access is protected using limited physical security measures.
Controlled	Products that are only accessible to authorized persons. Access is protected using rugged physical security measures.

Category 3: Communications access

The level of restricting communications access to the product.

Communications access	Features
Public	• Products can be easily accessed via communications or network • Products/networks have no access restriction
Restricted	• Partially controlled communication or network access • Access restricted to certain groups or entities (generally defined using roles)
Controlled	• Only authorized communication or network access • Rugged security measures, e.g. authentication and secure access controls

6.2 Defense in depth concept

Overview

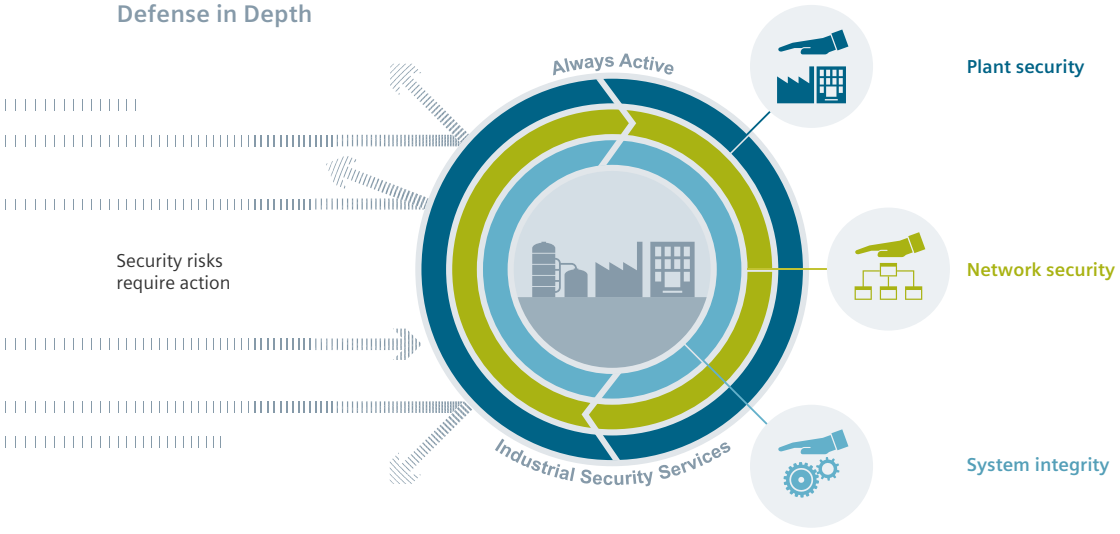
Defense in depth is the name of a general concept for deeply layered defense against cyber attacks and risks following the recommendations of IEC 62443.

Description

Digitalization and the increasing networking of machines and industrial plants are also increasing the risk of cyber attacks. 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.

Defense in depth addresses the following levels:

- **Plant security**
  Plant security uses various methods to secure the physical access of persons to critical components. This begins with the classical building entrance and extends to the safeguarding of sensitive areas using code cards.
- **Network security**
  Network security includes all measures taken to plan, implement and monitor security in networks. This includes the control of all interfaces, for example between the production and office networks, and remote maintenance access.
- **System integrity**
  PC-based systems and the control and field level must be protected against cyber attacks. Steps include the following measures:
  - Integrated access protection to prevent unauthorized configuration changes using engineering tools or during maintenance.
  - Protection of communication against unauthorized manipulation to ensure high plant availability.
  - Use of antivirus software and allowlists to protect PC systems against malware.
  - Maintenance and update processes to keep the automation and drive systems up to date.



Further information

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://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

We recommend that our customers make their employees aware of security risks (e.g. phishing attacks) through regular measures (e.g. training).

6.3 Plant security

6.3.1 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.

6.3.2 Physical protection of critical production areas

Physical protection of critical production areas comprises 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 controls with locks, coded passes, security personnel
- Escorting of external personnel by company employees
- Access authorizations are documented, monitored and regularly checked
- Security processes in the company are taught and followed by all employees

Production security

- Separate access control for critical production areas
- Installation of critical components in lockable control cabinets/electrical rooms
  Control cabinets/electrical rooms must be secured with locks and must have monitoring and alarm signaling options. Do not use simple locks such as universal, triangular/square or double-bit locks.
- Protection of power and data cables
  The flow of power and data between components of your control must be protected against manipulation involving cutting cables, for example.

- 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 for using mobile data storage media, e.g. USB flash drives and memory cards
- Guidelines for using operating units, e.g. PGs/PCs or mobile end devices

More information

Information on the intended operating environment is provided in Chapter AUTOHOTSPOT.

Detailed requirements relating to physical access protection are provided in the following sources:

- NIST Security and Privacy Controls for Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)
- BSI basic protection blocks (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html)
  - INF.1 General buildings
  - ORP.1 organization
  - OPP.2 personnel
  - ORP.3 Awareness and training on information security

See also

Security management (https://new.siemens.com/global/en/products/buildings/security/security-management.html)

6.4 Network security

6.4.1 Overview



Network security includes all measures taken to plan, implement and monitor security in networks. This includes controlling and checking all interfaces, for example between the production and office networks, and remote access for maintenance work.

Information about the architecture design for secure production and office networks is provided in the following Siemens White Paper: Industrial Network Security Architecture. (https://www.siemens.com/us/en/company/topic-areas/cybersecurity/industrial-security/downloads.html)

6.4.2 Network segmentation

6.4.2.1 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

In the cell protection concept, a production network is segmented into individual protection cells, between which all components securely communicate with each other. The protection cells are part of a defined protection area that is separated from other protection areas and other company networks, for example by firewall systems.

This restricts threats and security incidents to individual protection cells. This reduces the vulnerability of the entire production plant and 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 162)".

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

Protecting critical communication mechanisms

Production networks within a protection area must be split up into separate protection cells to protect critical communication mechanisms.

6.4.2.2 Network segmentation with SCALANCE S

To comply with security requirements for network protection and network segmentation, Siemens offers SCALANCE S Industrial Cybersecurity Appliances.

Precondition

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

Description

SCALANCE S Industrial Cybersecurity Appliances set themselves apart as a result of the following features:

- 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.
- Protecting different network topologies
  Components such as the SCALANCE S615 have 5 Ethernet ports that can be used to protect different network topologies by firewall or VPN (IPsec and OpenVPN).

Principle

The following application example demonstrates cell segmentation using several SCALANCE S modules. Data traffic to and from the devices within the production network can be filtered and controlled using a SCALANCE S firewall. Traffic between the protection zones can be encrypted and authenticated if necessary.

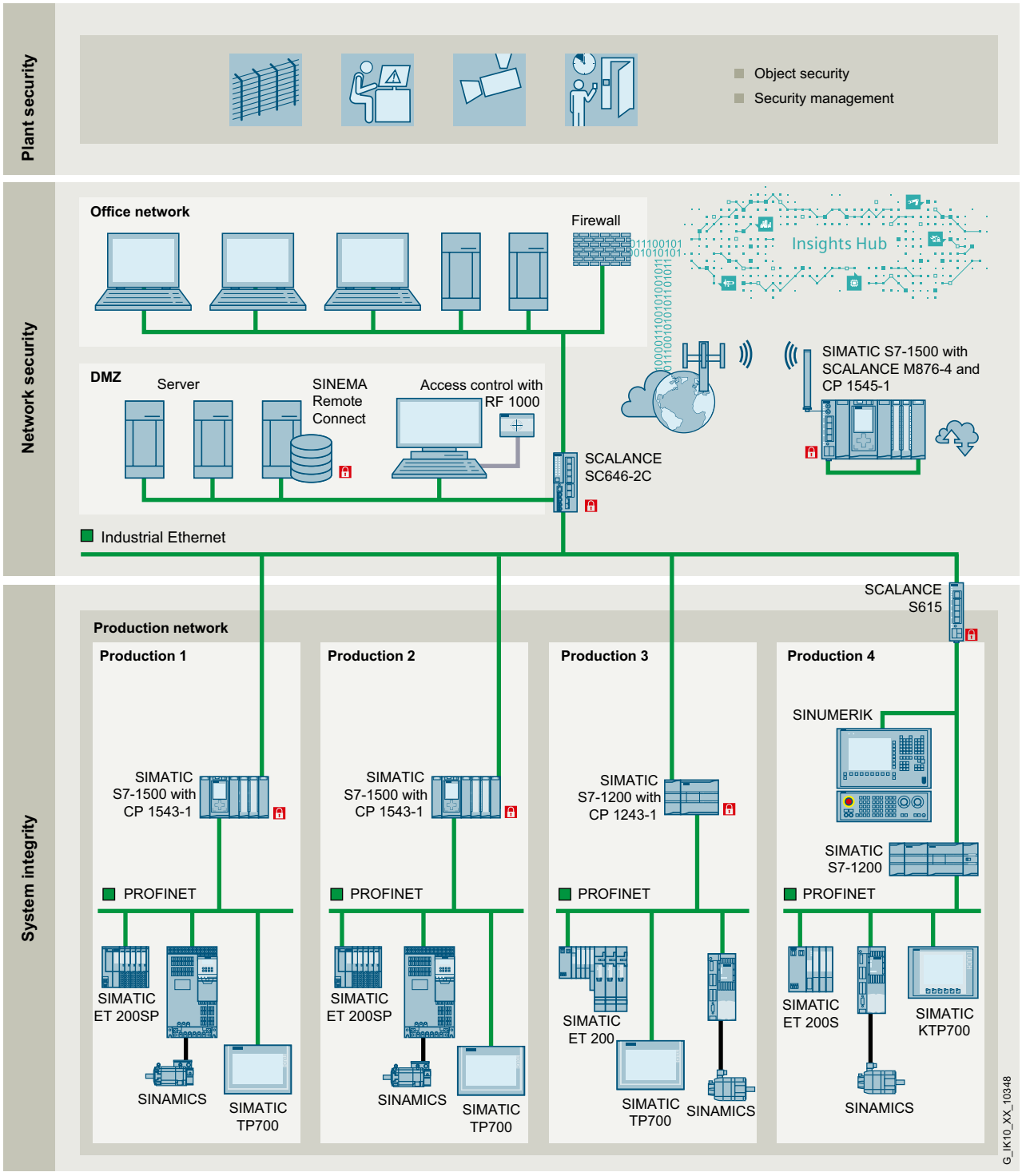


Figure 6-1 SCALANCE S application example

More information

More information on SCALANCE S Industrial Cybersecurity Appliances is available on the Internet:

Network security with SCALANCE S Industrial Cybersecurity Appliance (https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security/scalance-s.html)

Detailed requirements relating to network security and network segmentation are provided in the following sources:

- NIST Security and Privacy Controls for Information Systems and Organizations (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf)
- BSI basic protection blocks (https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html)
  - Network architecture and design

6.4.3 Cloud Security

The number of cloud applications is constantly increasing. That makes security measures in the cloud environment more important.

Initial orientation

The following addresses are designed to give you a general idea of how you can secure your system in the cloud environment. Inform yourself about the applicable requirements and tried and tested solutions and best practices.

- Center for Internet Security (CIS) (https://www.cisecurity.org)
  - CIS Controls Cloud Companion Guide
- Cloud Security Alliance (CSA) (https://cloudsecurityalliance.org)
  - Cloud Controls Matrix
  - Top Threats

Siemens Cloud solutions

The following addresses provide information about Siemens cloud management solutions:



Figure 6-2 Siemens Cloud solutions

- Industrial Cloud Computing (https://www.plm.automation.siemens.com/global/en/our-story/glossary/industrial-cloud-computing/58773)
- Insights Hub (https://plm.sw.siemens.com/en-US/insights-hub/)

6.5 System integrity

6.5.1 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.

6.5.2 Measures to harden the IT infrastructure

6.5.2.1 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 used ports can be found in the Equipment Manuals/Function Manuals of the respective products.

See also

Reduction of the attack surface (Page 162)

6.5.2.2 User accounts

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

- Use secure access data for user accounts. In particular, this includes assigning secure passwords.
- Reduce the number of user accounts to the necessary minimum. Deactivate or delete user accounts that are no longer being used.
- Only assign the necessary authorizations to user accounts.

6.5.2.3 Operating units used in the industrial context

Recommendations

Operating units, e.g. PGs/PCs, tablet PCs and smartphones, used in the industrial environment 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 50)".
  - A virus scanner is installed on the operating unit and regularly updated. In addition, the following measures can be applied: "Allowlists (Page 50)" and methods of the "Network segmentation with SCALANCE S (Page 40)".
  - A firewall with appropriate settings is activated on the operating unit.
  - To protect sensitive data against unauthorized access, storage media (e.g. hard disks, SSD, eMMC) are encrypted.
  - To prevent unintended changes to the configuration, only system administrators should have administrator rights to the operating unit.
- Use the operating unit deployed in defined protection areas only. The operating unit must not be used in the office network or via the Internet.
  Information about separating production and office networks is provided in Chapter "Network security (Page 39)".
- Secure PG/PCs against data theft using a lock or do not leave them unmonitored.
- Make sure that the screen of the operating unit is automatically locked if there is no activity.
- Deactivate interfaces that are not required, such as USB ports.

6.5.2.4 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.
- Store sensitive data on an operating unit or on network drives in encrypted form only.
- Protect your encrypted storage locations against unauthorized access and manipulations.
- Regularly create backup copies of sensitive data. Protect the backup copies against unauthorized access, loss and manipulation.

6.5.2.5 Transporting sensitive data securely

Take the following security measures when transporting sensitive data:

- Only send sensitive data when absolutely necessary. Only use encrypted and signed emails or storage media with encryption. The storage media, such as USB flash drives and external hard disks, used to send the data must be checked regularly for viruses.
- Only transport sensitive data on a storage medium with encryption. The storage media, such as USB flash drives and external hard disks, used to transport the data must be checked regularly for viruses.

6.5.2.6 Secure passwords

NOTICE
Damage to components due to data misuse Data can be easily misused by using passwords that are not secure enough. Attackers can use compromised access data to log into systems and manipulate the behavior of the control system. This can result in damage to components. • Develop guidelines for password renewal. Base the guidelines on the specifications of the national institutions for security and information technology. • Develop guidelines on handling access data. Make sure that the guidelines are implemented consistently in the deployed engineering tools. • Always keep access data secret and make sure only an authorized group of people is given access to the data.

Observe the following guidelines when assigning new passwords:

- Do not assign passwords that can be easily guessed, e.g. words, simple key combinations on the keyboard.
- Passwords must always contain a combination of upper- and lower-case letters as well as numbers and special characters. PINs must comprise an arbitrary sequence of digits.

- Assign passwords with the required minimum length.
- When assigning a password, always ensure you are adhering to the applicable company specifications, e.g. special password policy of the respective company.

Password management programs can be used to generate, save and manage passwords and PINs according to configurable rules.

More information

Additional rules for the assignment of secure passwords can be found at Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, abbreviated as 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).

6.5.2.7 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.

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.

6.5.2.8 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)

6.5.3 Patch management

6.5.3.1 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 older operating systems. This can leave the operating system with dangerous security vulnerabilities. • If you are using an operating system for which no more updates are provided, 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 39).

6.5.3.2 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.

Before installing program updates, please note the following points:

- Do not establish a direct Internet connection to the TIA Portal Update 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 39)".

6.5.3.3 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.

6.5.4 Data integrity

Description

NOTICE
Damage to data and the resulting malfunctioning of the system For automation and drive systems as well as controller components, data such as backups and programs can be imported from external sources. This data influences the behavior of these systems and should therefore be protected against unauthorized changes. Data such as backups, programs, and Technology Extensions can also be saved and archived. The systems currently do not provide the capability of ensuring the integrity of programs, backups, and Technology Extensions. Therefore take your own measures for ensuring integrity to guarantee the data integrity of your backups, Technology Extensions, or other saved data: • Apply the Siemens Industrial Holistic Security Concept: Siemens Industrial Holistic Security Concept (https://securing-digitalization.dc.siemens.com/). • Use digital signatures to protect data. • Ensure there is sufficient access protection: – Restrict access rights such as to data archives/Sharepoints accordingly. – Do not send any unencrypted/unsigned emails.

Data integrity is understood to mean the correctness (integrity) of data and the correct functioning of systems. Ensuring the integrity of the data is thus an essential goal of information security. Integrity protection should not be confused with protecting the confidentiality.

System overview

7

7.1 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:

- SIMATIC IPC for SINUMERIK
- SINUMERIK ONE / Machine Push Button Panel
- SIMATIC Thin Client ITC xx00-V3 (from firmware V3.2.3)
- SINUMERIK handheld units
- Distributed PLC I/O
  - SIMATIC, e.g. ET200SP and ET200MP
  - 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 operating mechanism motors:
  - Feed motors: 1FT, 1FK
  - Main spindle motors: 1PH, 1FE, 2SP1
  - Motors with direct operating mechanism: 1FN3, 1FW6

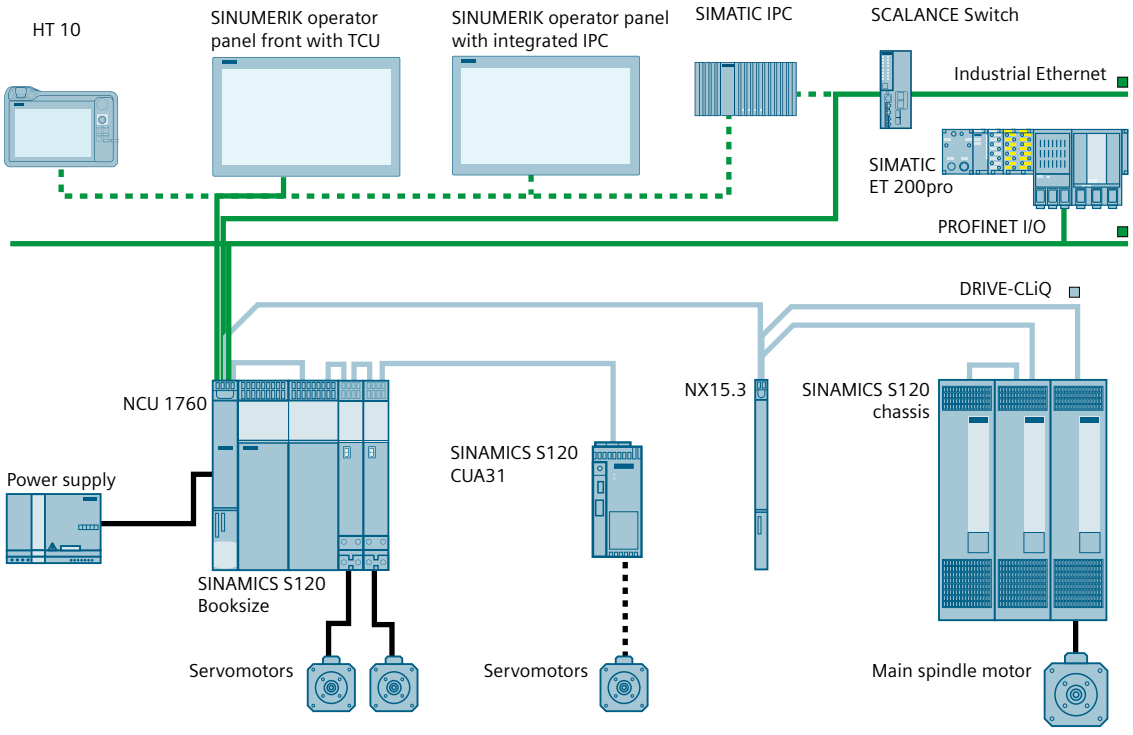


Figure 7-1 Typical topology of the SINUMERIK ONE complete system

7.2 Essential functions

The SINUMERIK system is primarily used to control a machine tool or associated robots.

This results in the following essential functions for the system in the order described:

- Ensuring machine safety
- Machining the workpiece without compromising quality
- Controlling auxiliary units
- Operating the machine via the human-machine interface
- Providing production/quality data via OPC UA

7.3 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 graphic provides an overview of the interfaces of SINUMERIK ONE and their function:

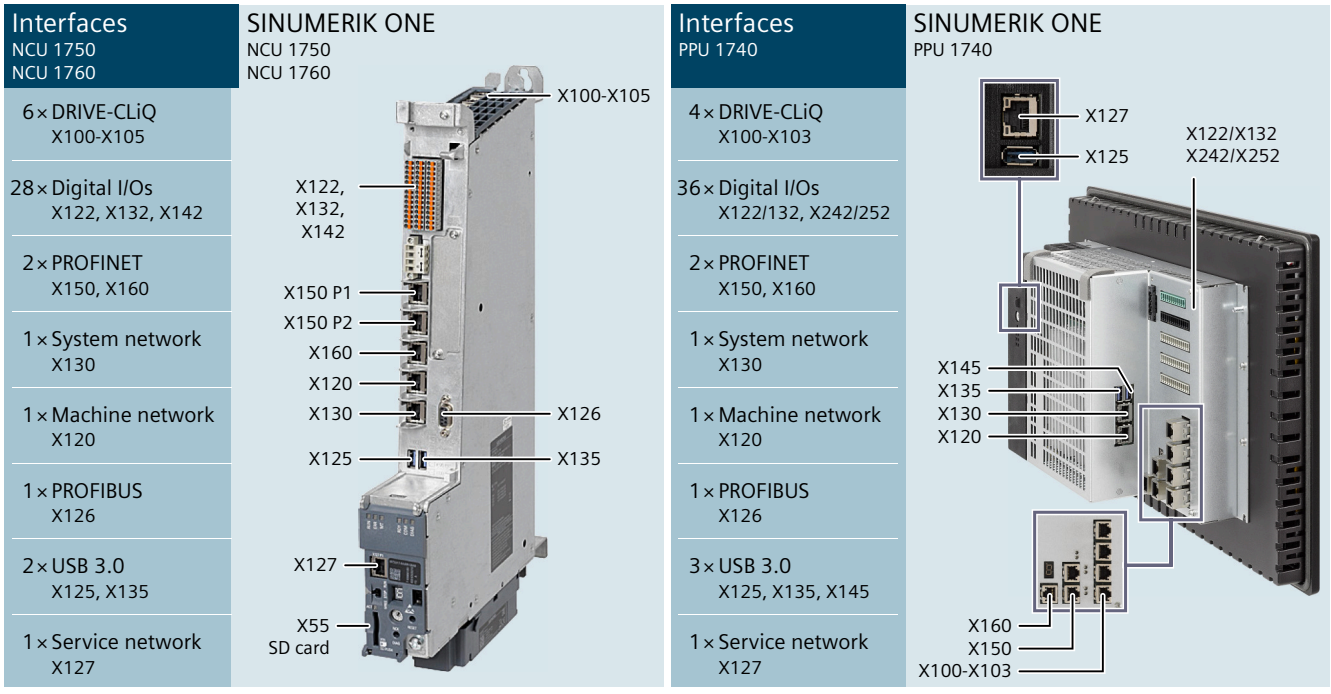


Figure 7-2 Overview of SINUMERIK ONE interfaces

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:

- Machine-internal field network (interface X126, X150)
  The field network should be a machine-internal network, on which the PROFINET/PROFIBUS is used to connect sensors and actuators, including drives to the controller. 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 purely internal network.
- HMI network (interface X120): The HMI 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.
- Factory network (interface X130): Connection to the factory network should be established via X130 on the NCU and eth1 on the IPC. A firewall protects these two interfaces against unauthorized access.
- The factory network PLC (interface X160) and production network: The factory network PLC is the network in 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.

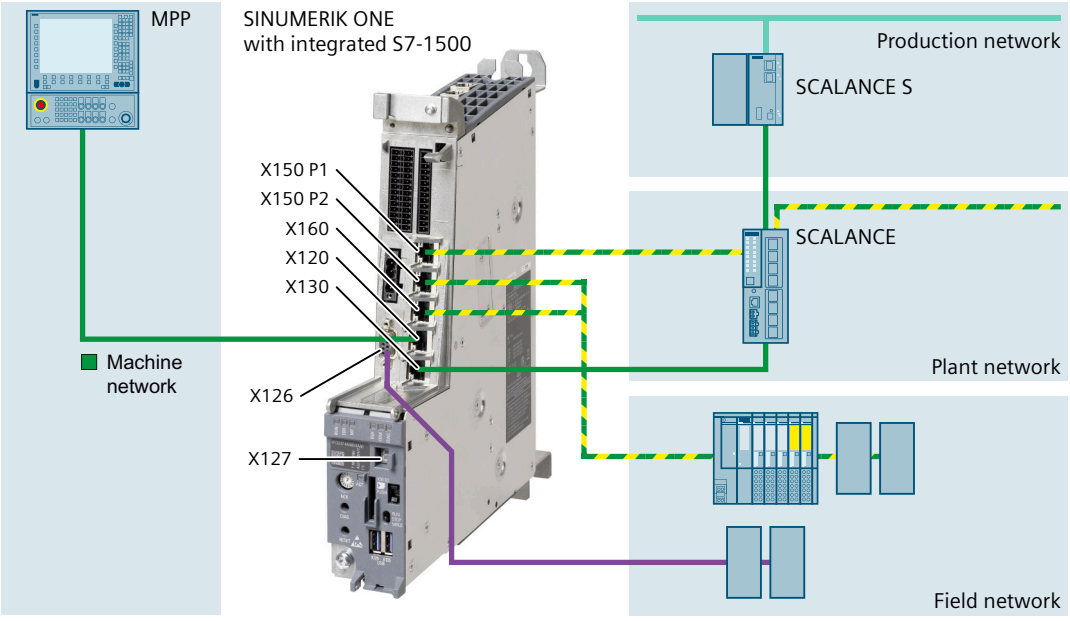


Figure 7-3 SINUMERIK ONE communication concept

7.4 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.

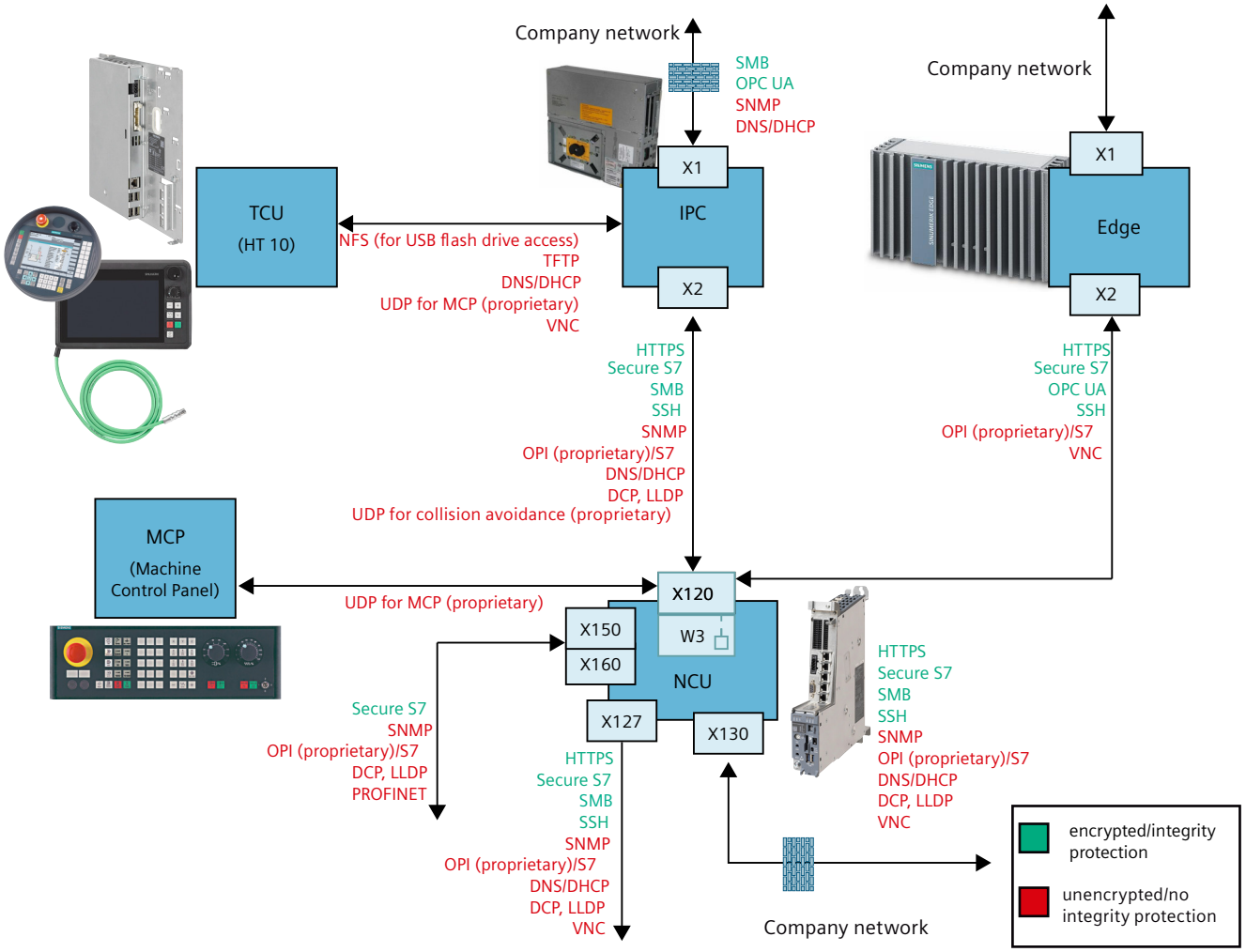


Figure 7-4 SINUMERIK ONE data flows and data memory

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.

Operational environment of the SINUMERIK control system

8

8.1 Measures to protect the operational application environment

Intended purpose and intended operating 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. They may only be operated in **defined protection areas** that are protected in accordance with the **Defense in Depth concept**.

Generally, in the healthcare sector, the machine is installed in a piece of medical equipment that is normally located in areas with restricted access.

Classification according to the security context for the product

An appropriate operational application environment is required to protect the product against cyber threats. You achieve this by taking into account the subsequent classification in categories according to the security context.

You can find a description of the categories in Chapter AUTOHOTSPOT.

Category	Usage phase/physical access/ access	Classification	Required measures
Persons	Mounting	**Instructed person**	• Product training courses • Documented instruction procedure • Implementation of safety and EMC measures in accordance with the specifications described in this manual and recognized engineering practices.
	Connecting	**Instructed person**	
	Configuring, programming	**Qualified person**	• Regular training courses for the product, system and cybersecurity • Documented instruction procedure • Clear responsibilities and accountabilities • Monitoring and checking qualifications of personnel
	Testing, commissioning, maintaining	**Qualified person**	
	Operating	**Qualified person**	

Category	Usage phase/physical access/ access	Classification	Required measures
Physical access	Device with SIMATIC memory card, mode switch, interfaces, wiring	**Controlled**	• Operation of a control system, an IPC if available and other devices that are not used to interact with a user are operated **exclusively indoors and inside a control cabinet or closed enclosure.** • Always install NCUs in housings and locked control cabinets or in electrical rooms that can be locked. Observe monitoring and alarming options and ensure physical separation from areas that are accessible to the public. Escorting external personnel • 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. • Components within the SINUMERIK system that are intended for display or operation, such as **thin client units and machine control panels:** – Externally accessible from the front – Rear side in a locked enclosure • Interfaces such as USB or network sockets and **connecting cables** must be installed in such a way that they are protected against access or manipulation by unauthorized personnel. • **More information** on the control cabinet installation of the NCU is provided in the corresponding Equipment Manuals for SINUMERIK.

Category	Usage phase/physical access/ access	Classification	Required measures
Communications access	Industrial Ethernet, PROFINET	**Controlled**	• Cable protection by routing bus cables in protected cable ducts/shafts • Covering unused ports using port blockers • User management/authentication • Network segmentation using firewalls • Deactivating communications services and ports that are not required
	Engineering access	**Controlled**	• User management/authentication • Strong authentication and encryption • VPN connections for remote access operations
	CPU display	**Restricted**	• Display password
	OPC UA	**Controlled**	• User management/authentication • Deactivation of OPC UA if not required

General requirements

You may only use the products in compliance with the following requirements:

- All regulations and directives that are applicable at the place of final use, especially with regard to electrical safety, functional safety and electromagnetic compatibility.
- All instructions, notes, technical data, safety information and cybersecurity information contained in this document and other supporting documentation.

Before using the products, you must perform a risk evaluation of the entire application and implement appropriate system design measures to ensure the safety of persons and property, fulfillment of cybersecurity requirements, and electromagnetic compatibility. Open-type products (IP20) are intended for installation in operator panels or cabinets which provide the necessary protection. Any use other than that expressly permitted is prohibited, and can result in unforeseen dangers.

Requirements relating to network protection

- The operating environment must ensure that **access to internal networks**, such as the machine network (X120), the service network (X127), and the automation network (X150, X160), is **protected against access by unauthorized personnel** by means of appropriate measures.
- This access protection includes **not** physically or logically **connecting internal networks to any external machine networks** and protecting **physical access to network cables or connectors**. In addition, **no IP-based wireless technologies** may be used in the machine-internal networks.
- The **connection to external networks**, especially if it includes direct or indirect access to larger networks, must be adequately protected with a **security firewall** (e.g. SCALANCE SC62x). Only authorized and integrity-protected protocols, such as OPC UA, may be used for communications via this firewall.

See also

Categories of access and authorization to access products (Page 33)
Defense in depth concept (Page 35)

8.2 Security assumptions for the intended operational environment

A SINUMERIK 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 control system is directly connected with the Internet or a part of an office network.

Table 8-1 Security assumptions for the intended operational environment

Assumption ID	Assumption	Responsible
AS-01	Physically accessing a SINUMERIK system (controller, IPC, TCU, MCP, HT2, HT10) is strictly limited to authorized persons only.	Machine builder and end user
AS-02	The internal networks of a SINUMERIK control system (X120, X127, X150) are not available outside a 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	All ports of network interface X130 are closed, in particular port 102. If necessary, the ports for OPC UA and VNC can be opened.	Machine builder and end user

NOTICE

Operation not possible

The requirements for the intended operating environment were assumed as preconditions in the risk analysis underlying this system.

If the operating environment does not correspond to the requirements relating to the intended operating requirements, then it is not permissible that the SINUMERIK system is operated there. Otherwise, the integrity and confidentiality of customer data as well as the integrity and availability of the plant are exposed to higher security risks.

Defense in depth concept SINUMERIK ONE

9

9.1 Plant security

Protective measures

Machines and solutions operated with SINUMERIK systems must be protected in terms of their availability, confidentiality, and integrity.

- This requires appropriate measures to ensure that **only authorized personnel** can access the machine. Otherwise, there is a risk that the availability of the machine could be easily compromised, e.g. by cutting cables or other mechanical damage.
- In addition, for maintenance and troubleshooting reasons, it must always be possible to reset the machines to their initial state or modify them in other ways (e.g. if the security admin password is lost) based on physical access. For this reason as well, access to the machine must also be restricted to authorized personnel by means of appropriate measures.

Addressed threats and protection objectives

- Integrity, confidentiality, and availability of the machine through man-in-the-middle attacks on internal networks
- Availability of the machine through damage or removal of operationally relevant components
- Confidentiality through access to unsecured storage media (hard drives, SD cards, USB flash drives)
- Protection of the machine from damage through operation by unauthorized persons
- Integrity of the machine through the replacement of operationally relevant components, addition of further elements
- The integrity of the safety configuration cannot be guaranteed despite increased system integrity measures in the event of physical access by an attacker.

9.2 Network security

Overview

A SINUMERIK system is not designed for direct operation on the Internet.

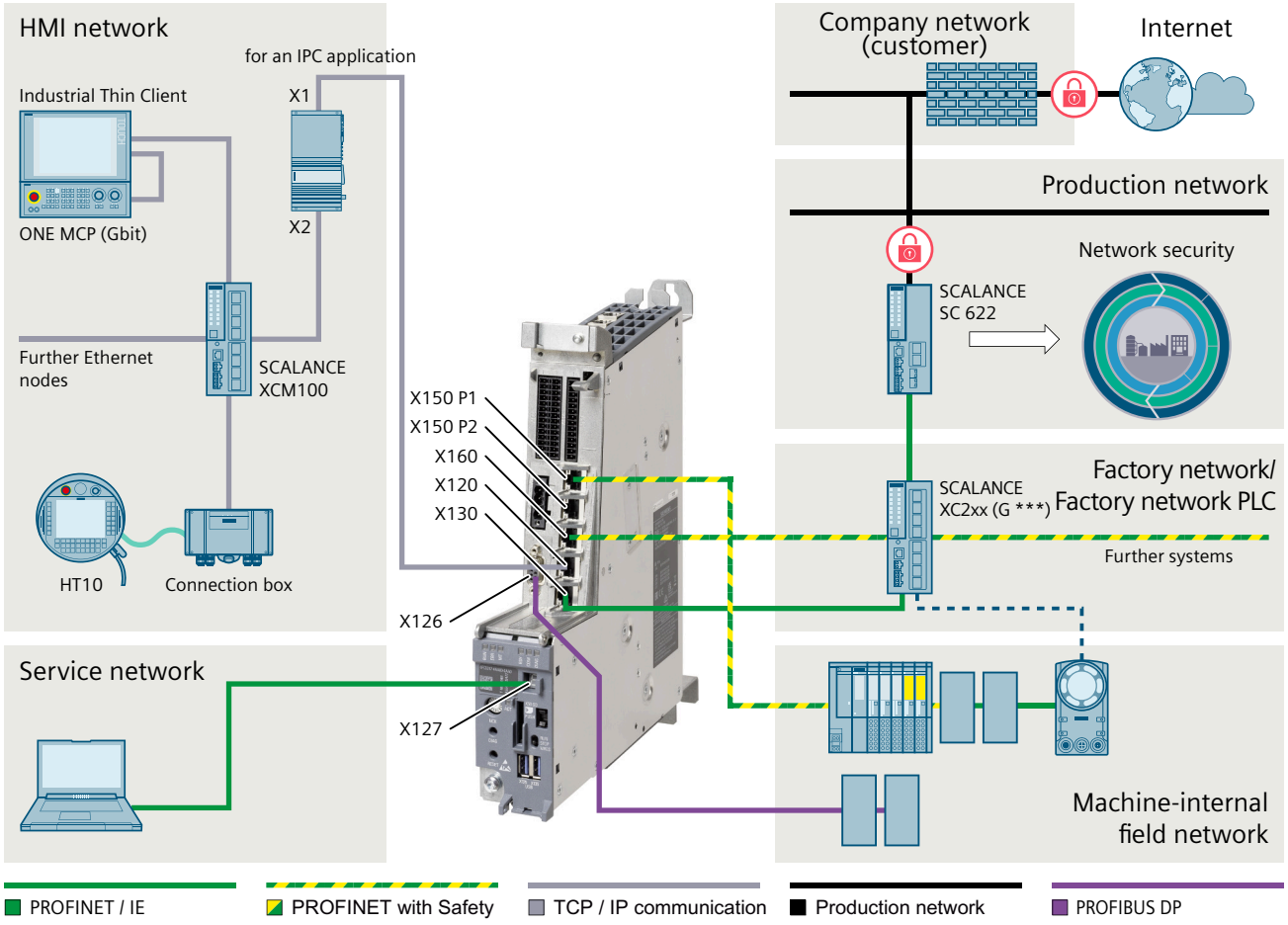


Figure 9-1 Network segmentation SINUMERIK ONE

The HMI network and the field network in particular are considered internal networks in the risk analysis. This means that the connecting cables and physical interfaces must be protected against access by unauthorized personnel using suitable measures (e.g. access protection).
External communication access to these networks must be prevented. If this is not possible, suitable measures must be taken to ensure that these networks can only be accessed via authorized and integrity-protected communication connections.

Access to the service interface must also only be granted to authorized personnel for maintenance purposes. If IP-based wireless networks are used in these networks, they must be adequately secured.
The external interface of the system forms the factory network interface (X130 or X1 for IPC-based systems). Despite the firewall present at this interface, this interface should be shielded with a security router (e.g. SCALANCE SC600) so that only authorized services can

communicate with the machine.
Only communication protocols that offer suitable authorization and integrity protection, or known-know protection if necessary, may be used at this interface.

In addition to specific requirements relating to network security, also observe the general requirements relating to network security and network segmentation (Page 39).

Network concept for direct manufacturing

Familiarize yourself in advance with a secure network concept for factory automation and the security measures for a secure reference architecture, and set up your customer network securely in accordance with the specified measures.

You will find **more information** on this topic on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109802750).

9.2.1 Protection status of SINUMERIK networks

9.2.1.1 HMI network (X120)

Protective measures

The HMI network is a machine-internal network used to connect operating devices (IPCs/thin client units, machine control panels, etc.) and also, if applicable, Edge devices.

For reasons of better interoperability and error prevention, the controller in this network is not protected by a firewall. Furthermore, communication protocols without cryptographic protection are used to maintain confidentiality/integrity and, where necessary, without the need for authorization.

Accordingly, the **physical and logical shielding of the network** is an integral part of the defense in depth concept of SINUMERIK ONE.

Addressed threats and protection objectives

- Unauthorized manipulation of settings/configurations (including functional safety)
- Man-in-the-middle attacks (confidentiality and manipulation)
- DoS attacks
- Monitoring of the operator action/inputs via VNC
- Unauthorized operation of the machine during a regular login

9.2.1.2 Service network (X127)

Protective measures

The service network is intended exclusively for commissioning and maintenance of the machine. However, you can still access the controller via this interface if, for example, a system error occurs or one or more components (e.g. display) fail.

The service network should not be used to connect participants to the system, but exclusively for connecting service PCs. A point-to-point connection between the service PC and the controller is assumed here.

For reasons of better interoperability and error prevention, the controller in this network is not protected by a firewall. Furthermore, communication protocols without cryptographic protection are used to maintain confidentiality/integrity and, where necessary, without the need for authorization.

Accordingly, the **physical and logical shielding of the network** is an integral part of the defense in depth concept of SINUMERIK ONE.

Addressed threats and protection objectives

- Unauthorized manipulation of settings/configurations (including functional safety)
- Man-in-the-middle attacks (confidentiality and manipulation)
- DoS attacks
- Monitoring of the operator action/inputs via VNC
- Unauthorized operation of the machine during a regular login

9.2.1.3 Factory network (X130)

Protective measures

The factory network interface is intended for connecting the machine to the operator's network. This is used for interaction between the machine and higher-level services.

This interface has an activated firewall on both the NCU and the IPC, which is closed in the delivery state and is intended to protect the devices.

Nevertheless, the use of a security firewall (e.g. SCALANCE SC622/626) at the transition from the machine to the protected area of the customer's company network/production network is recommended, as these have extended security functions for more fine-grained access control and better detection mechanisms.

At least when using remote maintenance or networking the X160 outside the protected area, a security firewall must be used at the machine transition/transition of the protected area.

Note

Only secure communication protocols permissible

Since this is the most exposed interface of the system, only secure communication protocols may be used here. The following protocols are envisaged:

- Communication protocol for data communication and file transfer:
  - OPC UA
- Connection of network drives:
  - SMB V3
  - NFS
- Time synchronization:
  - NTP

Enabling ports on X130 is only intended for OPC UA. If additional ports are enabled, a new risk analysis and corresponding cybersecurity concept are required to address the resulting risks.

Note

Remote maintenance

Use a suitable remote maintenance concept (e.g. SCLANACE Remote Connect) for remote maintenance to protect the connection.

- Due to its extensive possibilities for influencing the system, it is recommended that you do not enable the **port for SSH connections on the factory network**, even if the protocol supports both integrity protection and authorization.
- The use of Secure S7 must not be used with participants outside the protected area, as it uses the same port (102) as unprotected S7 communication.

Addressed threats and protection objectives

- Unauthorized manipulation of settings/configurations (including functional safety)
- Man-in-the-middle attacks (confidentiality and manipulation)
- DoS attacks
- Monitoring of the operator action/inputs via VNC
- Unauthorized operation of the machine during a regular login

9.2.1.4 Machine-internal field network (X150)

Protective measures

The machine-internal field network is a network where real-time data is exchanged between the integrated SINUMERIK PLC and devices such as sensors and actuators using the PROFINET protocol.

In addition, the architecture of the PROFINET protocol also allows the use of normal Ethernet/IP-based data exchange.

PROFINET offers some protection against manipulation in Real Time (RT)/Isochronous Real Time (IRT) mode. However, this is not cryptographic integrity protection. There is also no confidentiality protection on this network.

Accordingly, the **physical and logical shielding of the network** is an integral part of the defense in depth concept of SINUMERIK ONE.

Addressed threats and protection objectives

- Unauthorized manipulation of settings/configurations (including functional safety) by using the S7 protocol/acyclic PROFINET protocol
- Man-in-the-middle attacks (confidentiality and manipulation)
- DoS attacks

9.2.1.5 Factory network PLC (X160)

Protective measures

The factory network PLC is the network in the production environment that is typically used to connect various machines in a common production process.

Although this network exits the machine, it is not intended for direct networking with the factory network. Here too, exclusive use in a protected area is assumed.

However, if communication from this interface to participants outside the protected area is necessary, only the following secure communication protocols may be accessible or ports for these protocols may be enabled on the cell protection firewall:

- OPC UA
- Secure Open User communication

The use of Secure S7 must not be used with participants outside the protected area, as it uses the same port (102) as unprotected S7 communication.

For networking the X160 outside the protected area, a security firewall must be used at the machine transition/transition of the protected area.

Addressed threats

- Unauthorized manipulation of settings/configurations (including functional safety) by using the S7 protocol/acyclic PROFINET protocol
- Man-in-the-middle attacks (confidentiality and manipulation)
- DoS attacks

Protection goals and hardening measures

10

10.1 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

10.2 SINUMERIK ONE system hardening measures

The following checklist provides an overview of all hardening measures for the SINUMERIK ONE system. When commissioning, ensure that you carefully work through this checklist to guarantee that you configure the most secure settings for the SINUMERIK system. Details and additional descriptions on the individual setting options are provided in the subchapters of this documentation or in the documentation that is specified.

Checklist of hardening measures

Topic field	Hardening measure	Where can I find the setting?	Where do I find more information?	Fulfilled Yes / no
Time settings	NCU time and IPC are synchronized and have the correct value.	SINUMERIK Operate in operating area "Setup > HMI > Date time".	Chapter Time and date setting (Page 85)	
	Central time synchronization via NTP is configured.			
User management	User management is activated.	SINUMERIK Operate menu "Security > User management > Configuration"	Chapter SINUMERIK user management (Page 89)	
	Individual users are created and taken into account corresponding to the Least Privilege principle.	SINUMERIK Operate menu "Security > User management > User"		
	The password policies are configured in accordance with company policies.	SINUMERIK Operate menu "Security > User management > Policies"		
	The login guidelines are activated and configured.	SINUMERIK Operate menu "Security > User management > Policies"		
Security Eventlog	The Security Eventlog server connection is configured.	SINUMERIK Operate menu "Security > Security Eventlog > Settings"	Chapter Security Eventlog (Page 158)	

Topic field	Hardening measure	Where can I find the setting?	Where do I find more information?	Fulfilled Yes / no
PLC security	Password for PLC access level is configured.	SINUMERIK Operate menu "Security > PLC security"	Chapter PLC security (Page 118)	
	Password to protect confidential PLC configuration data is configured.	SINUMERIK Operate menu "Security > PLC security" OR In the TIA Portal in PLC properties in area "Protection & Security > Protection of PLC configuration data".	Chapter PLC security (Page 118) or in the TIA Portal online help	
	Interfaces (HTTP) that are not required are deactivated.	In the TIA Portal in PLC properties in area "Web server > General", the check box "Permit access only with HTTPS"	In the TIA Portal online help	
	Users on the web server are configured.	In the TIA Portal in PLC properties in area "Web server > User management"		
	Secure PG/PC and HMI communication is permitted.	In the TIA Portal menu "PLC security settings > Operating mode for PG/PC and HMI communication > Allow only secure PG/PC and HMI communication"		
	The password to protect the offline safety program of the safety-relevant PLC blocks is configured.	In the TIA Portal, in the properties of the PLC, menu "Safety Administration > Access protection"		
	SNMP is deactivated or is set to write-protected access.	In the TIA Portal in PLC properties in area "Extended configuration > SNMP"	In the TIA Portal online help	
Pairing IPC/ NCU(s)	All NCUs are paired with the IPC.	SINUMERIK Operate menu "Security > Trusted devices"	Chapter Trusted devices (Page 125)	

Topic field	Hardening measure		Where can I find the setting?	Where do I find more information?	Fulfilled Yes / no
HMI security	VNC settings	VNC password for the company interface has been assigned.	SINUMERIK Operate menu "MENU SELECT > Diagnostics > Remote diag. > Password"	In the SINUMERIK Operate online help	
		Agreement for VNC was configured corresponding to the requirements.	SINUMERIK Operate menu "MENU SELECT > Diagnostics > Remote diag. > Request remote diag."		
	SSH settings	Auto-logoff function of the SSH server is configured.	SINUMERIK Operate menu "HMI Security > Auto-logoff server connection in case of inactivity"	Chapter HMI security (Page 151)	
		Legacy access is deactivated	SINUMERIK Operate menu "Security > HMI Security > Allow legacy access for Operate"		
	The Security archives / Security restore password is set.		SINUMERIK Operate menu "Security > HMI Security > Security archives / Security restore password"		
Data at Rest	SD card encryption is activated.		SD card encryption is activated, SINUMERIK Operate menu "Security > HMI-Security > SD card encryption"		
Firewall	Only ports/services that are required are enabled.		SINUMERIK Operate menu "Setup > Company network > Firewall exceptions"	Product information "SINUMERIK ONE Port Lists" (https://support.industry.siemens.com/cs/ww/en/view/109974022)	
	S7 communications and HTTP is deactivated.			In the SINUMERIK Operate online help	
	DCP and LLDP are deactivated.		SINUMERIK Operate menu "Setup > Company network > Active protocols"	In the SINUMERIK Operate online help	

Topic field	Hardening measure	Where can I find the setting?	Where do I find more information?	Fulfilled Yes / no
OPC UA	The network connections that are not required are deactivated.	SINUMERIK Operate menu "Setup > Company network > OPC UA > Settings"	Configuration Manual SINUMERIK ONE "OPC UA" (https://support.industry.siemens.com/cs/ww/en/view/109974027)	
	Encryption methods that are insecure are deactivated.			
	OPC UA users are set up and taken into account with the Least Privilege principle.	SINUMERIK Operate menu "Security > User management > User"		
	OPC UA object model is limited to include just the information that is required using the customer-specific object model (CSOM).	With Siemens OPC UA Modeling Editor (SiOME) (https://support.industry.siemens.com/cs/ww/en/view/109755133)		
	Anonymous access in OPC UA is deactivated.	SINUMERIK Operate menu "Setup > Network > OPC UA > Authentication"		
	Only the most secure guidelines are activated and "permit obsolete guidelines" is only configured if absolutely necessary.			
	Setting "Automatically accept certificates" is deactivated.	SINUMERIK Operate menu "Setup > Network > OPC UA > Authentication"		
IPC	Standard user is created and has no administration rights	Microsoft Windows Control Panel	Commissioning Manual SINUMERIK ONE "PCU Base software /IPC" (https://support.industry.siemens.com/cs/ww/en/view/109973978)	
PCU Base software installation	USB interface is switched off.	Service desktop in dialog "Run" or in the command prompt: sc_usb disable [-minutes] [all] [HOST...]		
	The BitLocker drive encryption is activated.	"Control Panel > BitLocker driver encryption" or via script		
	SMB server is configured and the most secure version of the protocol that is supported is selected.	Via the "basesys.ini" configuration file and SINUMERIK Operate		
	Automatic network share for USB interchangeable data storage devices is deactivated.	Via the "basesys.ini" configuration file		
	Firewall settings (file and printer sharing, SNMP communications, remote access, incoming and outgoing ICMP ping requests) have been checked.	Via the control panel		
SINUMERIK Operate settings	The EXIT softkey has been configured to shut down Microsoft Windows when it is actuated.	Via the "slamconfig.ini" configuration file		

Topic field	Hardening measure	Where can I find the setting?	Where do I find more information?	Fulfilled Yes / no
Own Windows installation	The recommended security settings for IPCs in an industrial environment are configured.		Recommended security settings for IPCs in an industrial environment (https://support.industry.siemens.com/cs/ww/en/view/109475014)	
Network configuration	A decision has been made regarding the necessity of configuring the network routing (PG/PC at interface X127).	In the Service Center Network menu "Network > Network settings > IP routing"	Commissioning Manual SINUMERIK ONE "PCU Base software /IPC" (https://support.industry.siemens.com/cs/ww/en/view/109973978)	
VNC server settings	A secure password is set if you wish to remotely access the PC system in the company network.	Via command prompt: sc_vncpwd set		
Physical access control	The NCU with its USB ports and access to the SD card is securely installed in a lockable cabinet.		Chapter Protection against manipulation (Page 165)	
	NCK commissioning switch (rotary switch) is set to "Position 0" and not to "Position 9".	Via NCK commissioning switch directly at the NCU.	Depending on the NCU variant: e.g.: SINUMERIK ONE "NCU 1760" Equipment Manual (https://support.industry.siemens.com/cs/ww/en/view/109825490)	

10.3 Ports and protocols

Configuring Manual SINUMERIK Port Lists

The Configuration Manual SINUMERIK Port Lists (https://support.industry.siemens.com/cs/ww/en/view/109974022) provides an overview of the ports and protocols that SINUMERIK supports. The protocol, service, description and affected interfaces are listed for each port. It also indicates whether the port is open or closed by default, and whether this port is required for operation or service, or whether it is a Windows service.

A comprehensive and transparent list of all ports and protocols is important for the following reasons:

- **Implementing the principle of "Least Functionality"**
  Using the port list, you can precisely see which services are listening on which ports. If a service is not required for the specific application or environment, (e.g. a remote access service if remote access is not required), then it can be specifically deactivated.
  The port list allows ports that are open as default to be identified. This is an important note to indicate where additional protective measures might be required (e.g. host-based firewalls, network segmentation), even if the service is considered "secure".
- **Rugged firewall configuration and network segmentation**
  Without a precise port list, firewalls would either have to be configured too openly (which represents a security risk) or too restrictively (which results in malfunctions). Using the list, you can create precise firewall rules that only permit the necessary data traffic at the ports required and block everything else.
  Segmentation is decisive in complex industrial networks. The port list enables you to understand the communication relationships between different system components and to optimally define segmentation points, allowing only the strictly necessary communication across segment boundaries.
  Protection against lateral movement: Only opening necessary ports makes it difficult for attackers to move from one compromised system to another within the network (lateral movement).
- **Risk evaluation and weakness management**
  Every open port, especially if it is linked to a specific service and protocol, represents a potential weakness. The list helps to evaluate potential risks and to prioritize these. If you know which services run on which ports, you can perform specific weakness scans and better interpret the results.
  Knowing the services also helps when it comes to patch management. If a service is known, then it is easier to search for relevant security updates and load these.
- **Troubleshooting**
  For network problems or communication errors, using the port list, you can quickly check whether the required ports are open and whether the correct service is listening on these ports. The list also helps to identify incorrect configurations where a service inadvertently runs on an incorrect port or a port that is required is blocked.

10.4 Security tools

The following security tools are used in the SINUMERIK ONE environment. These support you in the administration, monitoring, incident handling or assessment of the product's security status.

- "User Management Component (UMC)" (https://support.industry.siemens.com/cs/ww/en/view/109780337)
  UMC allows a central user management to be set up. This means that you can define and manage users and user groups across software and devices.
- SIEM system
  SIEM stands for Security Information and Event Management. It is a software solution designed to capture, analyze and correlate security data from various sources in order to identify potential threats and security incidents. You set up the connection to the SIEM system in SINUMERIK Operate.
  Examples of SIEM systems include:
  - SPLUNK (https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html)
  - IBM® QRadar (https://www.ibm.com/products/qradar)
- SINEC Security Guard
  SINEC Security Guard is a central security management system that was specifically developed to address the requirements of industrial networks (Operational Technology – OT). It helps companies protect their production plants and critical infrastructures from cyber threats. In the context of a SINUMERIK 828D, it is used for incident handling.
  - SINEC Security Guard - 1000 Asset Package (https://www.siemens.com/en-us/products/sinec/security-guard-1000/)
  - SINEC Security Guard - 5000 Asset Package (https://www.siemens.com/en-us/products/sinec/security-guard-5000/)

See also

Security Eventlog (Page 158)

Security functions of the product

11

11.1 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 89)
- Backup & restore
  - SINUMERIK archive (Page 109)
  - Security archive (Page 111)
  - IPC backup (Page 114)
- System integrity:
  - Certificate store (Page 115)
  - PLC security (Page 118)
  - Trusted devices/pairing IPC and NCU (Page 125)
  - Safety Integrated log file (Page 130)
  - Secure Boot (Page 132)
- Know-how protection
  - Cycle encryption (Page 141)
  - Block encryption (Page 142)
- Protecting data at rest
  - Antivirus and anti-malware protection of the IPC (Page 133)
  - Encryption of the SD card (Page 143)
  - IPC bitlocker hard disk encryption (Page 146)
- Secure communications
  - OPC UA (Page 150)
  - Network protocol settings (SMB, SSH) (Page 151)
  - Secure web server communications via (HTTPS) (Page 154)
  - Network security & firewall (Page 155)
- Security Eventlog (Page 158)

- Reduction of the attack surface
  - Deactivating ports and protocols (Page 163)
- Protection against manipulation
  - Physical protection of the NCU (Page 165)

See also

Antivirus and anti-malware protection of the NCU (Page 133)

11.2 Operation of the security functions

You have two possible operations for most of the security functions described in this manual:

Operation on the real machine

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 (end user).

Operation on the virtual machine

Alternatively, you have the option of calling many of the described security functions virtually via SINUMERIK Operate in SINUMERIK ONE Create MyVirtual Machine. More information is provided in System Manual "SINUMERIK ONE /828D Create MyVirtual Machine" (https://support.industry.siemens.com/cs/ww/en/view/109974033).

NOTICE
Data misuse, virtual and real machines Information obtained from a virtual machine by spying can be used to launch successful, highly effective attacks on real machines. In order to have the highest possible protection against cyber attacks on the virtual machine as well, we recommend that you activate the best-practice Microsoft Windows security measures, e.g.: • Multi-factor authentication • Microsoft Windows Security is activated and up to date (Page 133). • BitLocker hard disk encryption is activated (Page 146).

More information

Additional descriptions of the security functions, the requirements and the precise sequence of all worksteps in SINUMERIK Operate are provided in the Commissioning Manual "Final commissioning steps" (https://support.industry.siemens.com/cs/ww/en/view/109817139) and the associated online help.

11.3 Role and access requirements for security functions

To use certain SINUMERIK ONE security functions, you need different roles and/or access levels in SINUMERIK Operate. These requirements depend on whether you are working with or without active user management (Page 89). 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 89)	You have the "Security Admin" role.	You have access level 1 (machine OEM).
Certificate store (Page 115)	You have the role "Security Admin" or access level 3 (end user).	You have at least access level 3 (end user).
Security Eventlog (Page 158)	You have the role "Security Admin" or access level 2 (service).	You have at least access level 3 (end user).
PLC security (Page 118)	You have the role "Security Admin" or access level 2 (service).	You have at least access level 3 (end user).
HMI security (Page 151)	You have the role "Security Admin" or access level 2 (service).	You have at least access level 3 (end user).
Trusted devices (Page 125)	You have the role "Security Admin" or access level 2 (service).	You have at least access level 3 (end user).

11.4 Time and date setting

The correct time and date setting of the system is an important requirement for the functioning of several security functions.

Manually setting the time: SINUMERIK Operate NCU or IPC

You can manually set the date and time in SINUMERIK Operate in operating area "Setup > HMI > Date Time". A detailed description of the formats for the time display, the precise procedure as well as the requirements are provided in Commissioning Manual SINUMERIK ONE "Final commissioning steps" in Chapter "Basic settings" (https://support.industry.siemens.com/cs/ww/en/view/109817139) or in the SINUMERIK ONE online help Operate Universal/Turning/Milling/Grinding.

Synchronizing the time via the time server

You can connect a time server to the operating software to ensure that the correct time information is always automatically available to the control system. Also make the settings via operating area "Setup > HMI > Date Time".

Additional information about how you use the time server and how you configure time data using file "basesys.ini" is provided in the Commissioning Manual SINUMERIK ONE "Final commissioning steps", in Chapter "Additional time settings" (https://support.industry.siemens.com/cs/ww/en/view/109817139).

11.5 User management and access control

11.5.1 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 86). This form is enabled by default when the system is shipped.
- The SINUMERIK user management (Page 89). 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 user management via the operating area "Setup" > "Security". User management is an optional security function.

⚠ CAUTION

Data misuse and manipulation

The classic form of access management using group-based access levels does not provide adequate protection against data misuse and manipulation of the system, as the default passwords are known and several persons can log in to the system using the same password.

SINUMERIK user management allows personalized authorization of each individual user together with a personalized role and rights assignment.

- We therefore recommend activating user management instead of the classic form of access level management to log in to SINUMERIK Operate. This guarantees better protection against third-party access attempts and ensures the confidentiality of the content in the particular system.

11.5.2 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).

11.5.3 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/her own access credentials, this type of authorization is far more secure than authorization via access levels. Alternatively, starting from software version Vx.25, you can also log in to the system based on your ID. The ID-based login and the classic login method both function in parallel. As a user is linked with their own individual ID, this type of login is personalized and secure.
- **Configuring users, groups and roles**
  - The classic access levels of SINUMERIK (Manufacturer, Service, End 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 end 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, End 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
- Based on the support of a **central user management**, a central UMC server can be created, which controls the authorization of users that are already saved. This means that many users no longer have to be manually created.
- 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)

11.5.4 SINUMERIK user management

11.5.4.1 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. User management is an alternative to authorization based on access level passwords, which was used in older SINUMERIK systems. 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 every user (e.g. based on 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)

See also

Application example, central user management (https://support.industry.siemens.com/cs/ww/en/view/109780337)

11.5.4.2 Functions of the SINUMERIK user management

Main functions at a glance

- **Local user management** (Page 91)
  For local user management, the Security Admin creates the users individually directly in the respective system.
- **Central user management** (Page 91)
  For central user management, the various systems and applications are connected to a central user management system (via an UMC server) where the users are managed centrally. The advantages compared with local user management are:
  - Central control and overview of the users
  - Improved security, e.g. by quickly locking out users
  - Efficiency and time saving due to centralized user provisioning
  - Better integration with other systems
    You can find more information on the topic of central user management and downloads on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109780337).
- **Types of authorization**:
  - **Classic** with user name and password input

– **ID-based login** (Page 103)
For an ID-based login, you can authenticate yourself by reading in a personalized RFID tag on the RFID reader. The SINUMERIK user management recognizes the ID of the previously registered user and logs him or her on to the system.
You can use the "**Standard Euchner Electronic Key System (EKS)** with TCP/IP interface" (EKS-A-IEX-G01-ST02/03) with the SINUMERIK system as standard. For more information on setting up the Euchner EKS, see the Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139) manual.
Additional readers can be set up via the SINUMERIK OA applications. For more information on setting up additional readers, see the Programming Manual "SINUMERIK Integrate Create MyHMI /3GL (Qt Api)" (https://support.industry.siemens.com/cs/ww/en/view/109974182) Programming Manual.

NOTICE
Data misuse / "Security Admin", "Manufacturer" and "Service" roles Note that ID-based login poses a risk of data misuse, as RFID cards or tags can be stolen or copied. • Since the "Security Admin", "Manufacturer", and "Service" roles generally have greater system responsibility than other roles, for these roles/users we recommend the following: – Either you do not set up ID-based login for these roles/users. Then roles "Security Admin", "Manufacturer", and "Service" roles should log in to the system with a user name and password since this authentication method offers a higher degree of security. – Or you utilize a chip technology such as MIFARE DESFire™, which does not permit a token being simply duplicated.

11.5.4.3 Architecture of the user management

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

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 "**Single Sign-On (SSO) 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 impact users logged in to SINUMERIK Operate and vice versa.

Architecture of the local user management NCU system

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

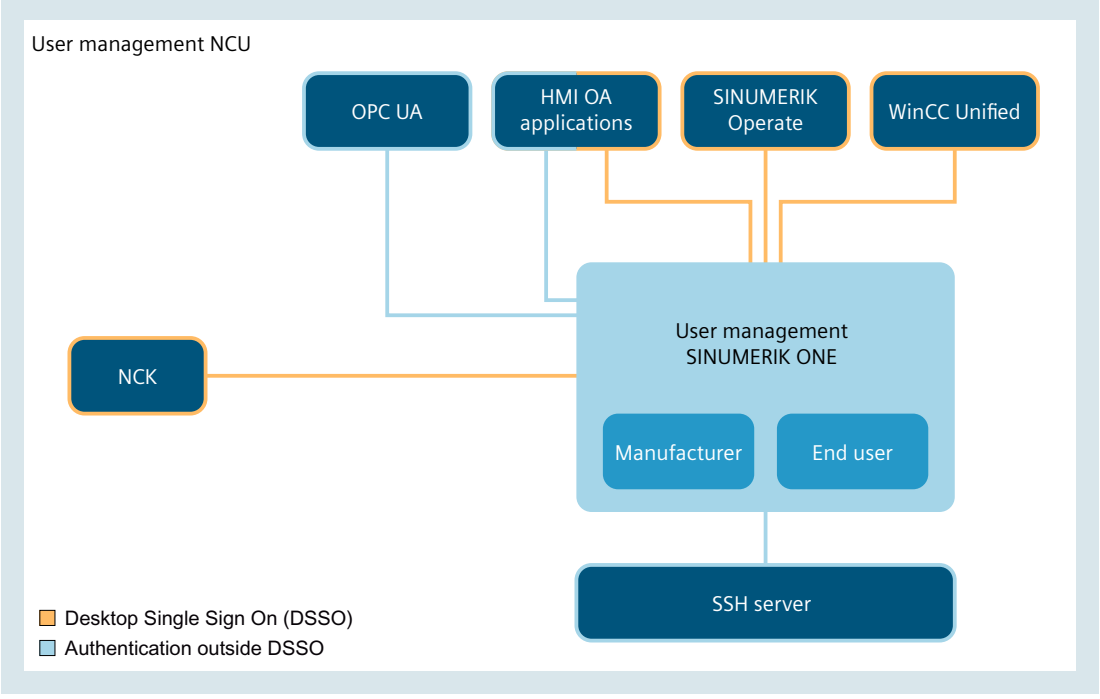


Figure 11-1 Local user management on an NCU system

Architecture of the local user management in the distributed system - NCU & IPC system

If an NCU and an IPC are installed, the **local 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.

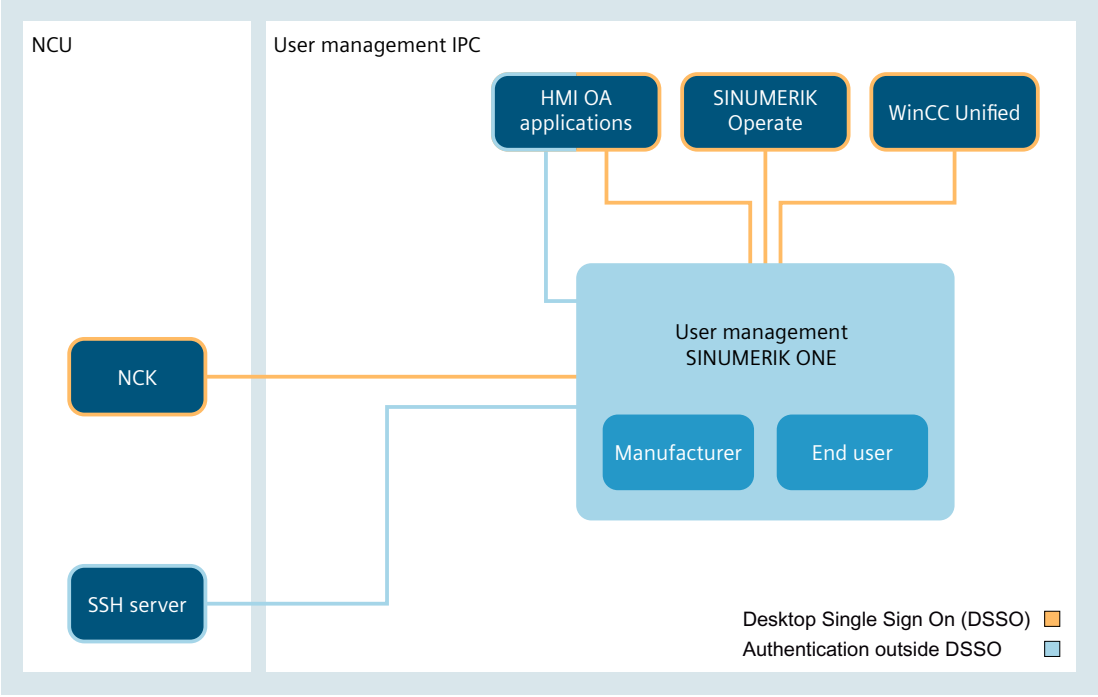


Figure 11-2 Local user management on an IPC system

Architecture of the central user management NCU system

For a **central user management**, the user management on the NCU accesses a central UMC server on which users are centrally managed. The UMC server itself can be configured so that it is synchronized with an "Active Directory".

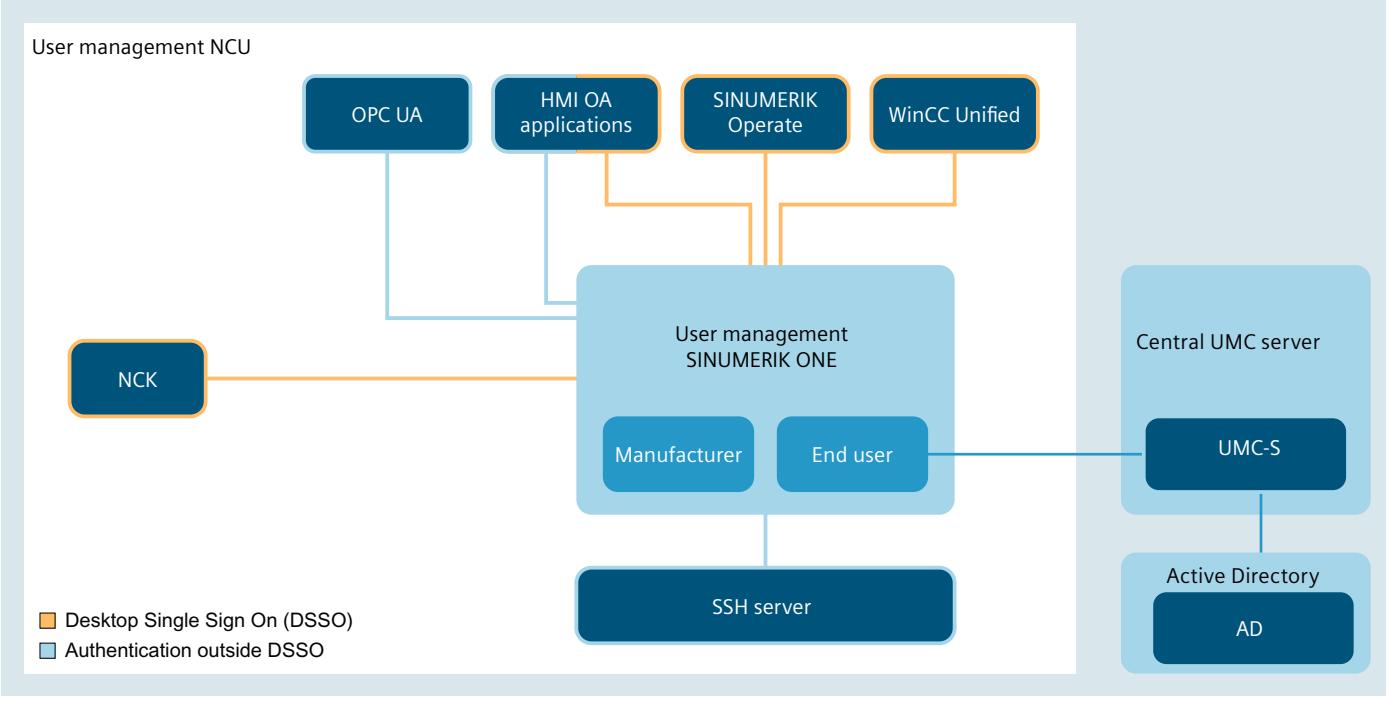


Figure 11-3 Central user management on an NCU system

Architecture of the central user management in the distributed system - NCU & IPC system

For a **central user management**, the user management on the IPC accesses a central UMC server on which users are centrally managed. The UMC server itself can be configured so that it is synchronized with an "Active Directory".

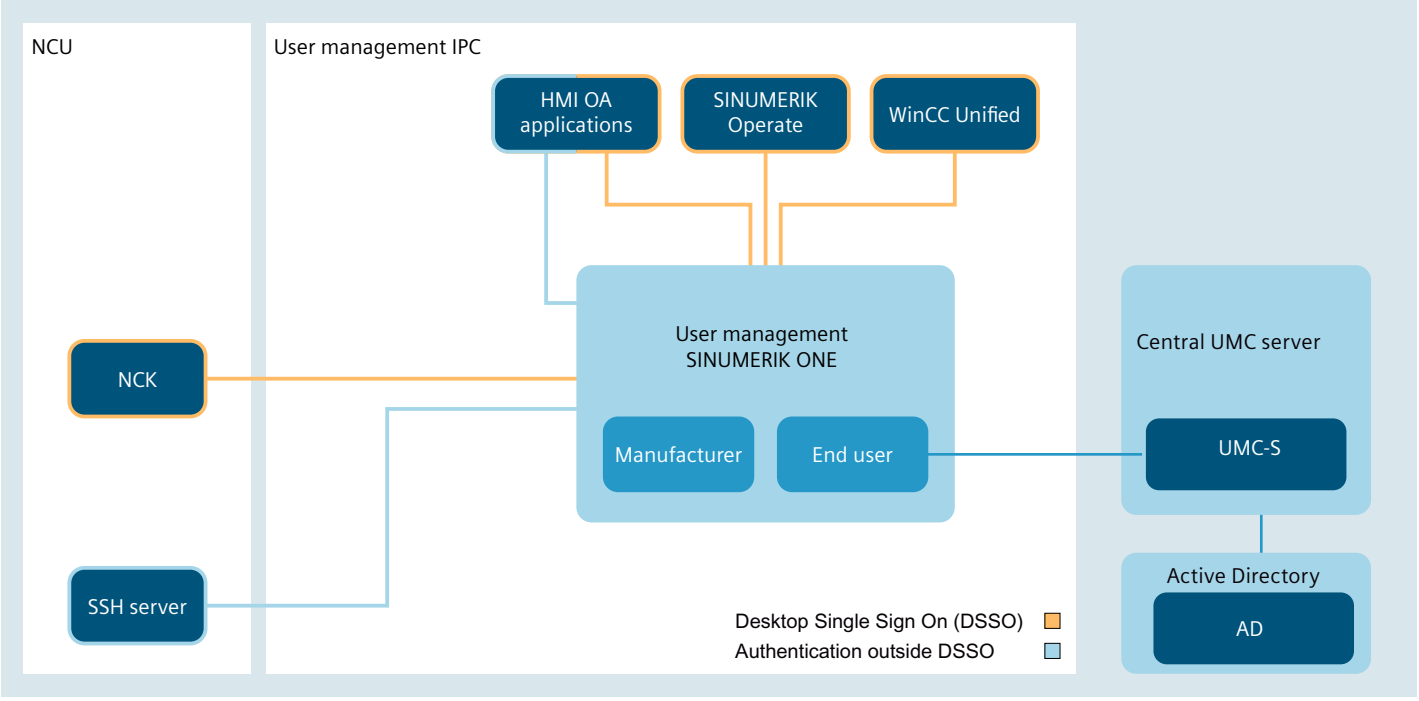


Figure 11-4 Central user management on an IPC system

Domains

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

- Manufacturer
- End user

Each domain can separately define and assign its own administrators, groups, users, and permissions. As a consequence, from Version V6.24, both domains can be independently

activated. 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 with 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.

In addition, you can connect the local manufacturer domain or end user domain with a central user management. This has the advantage that already configured users can be taken from an active directory.

More information

More information on the topic of central user management and downloads is available on the Internet (https://support.industry.siemens.com/cs/ww/en/view/109780337).

11.5.4.4 Groups and role concept

SINUMERIK user management makes a distinction between 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 end 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 is assigned multiple machine roles receives the highest AccessLevel contained in these roles. A higher AccessLevel always also includes the lower access levels.
  A machine role can also include the security administration role and transfer this role to the included user. The "Security admin manufacturer" role can only be held by users from the "Manufacturer" domain; the "Security admin end user" role can only be held by users that belong to the "end user" domain. This means that no user can have both Security Admin roles.
- If the manufacturer domain is linked with a central user management, then machine roles (including the security admin manufacturer) are automatically assigned to existing user groups on the UMC server.
- If the user domain is linked with a central user management, then only the security admin end user role is automatically assigned.

User groups

- A user group is a group for the organizational grouping of users.
- There are local and central user groups.
- 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.

11.5.4.5 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.

As a consequence, the manufacturer has the right to create the manufacturer domain and also the end user domain – and to also delete these domains.

Note

"Security Admin" role or "Manufacturer" role

We recommend that you clearly distinguish between the roles of "Security Admin" and "Manufacturer" and assign these roles to two different persons.

- The Security Admin plays a central role in a company's industrial cybersecurity. This role's tasks include: Implementation and management of security solutions, monitoring and analysis of the system for security threats/violations, security policies and procedures, administration of user management, training of employees.
- The Manufacturer role, on the other hand, has extensive knowledge of computerized numerical control (CNC). This role's tasks include: Programming and setting up the machine, commissioning and maintenance, fault diagnosis and rectification, optimization and adaptation, as well as training and support.

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. In addition, the Security admin manufacturer can connect or disconnect the manufacturer domain to/from a central user management.
- The Security admin end user can only administer the end user domain. In addition, the Security admin end user can connect or disconnect the end user domain to/from a central user management.
- 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 with confidence.

Note

Central security administrator

If the domain is linked with a central user management, via the central user management you are defined as "Security Admin" user and via the central user group who have the appropriate rights that allow you to configure user management in your own local domain.

Note

Changes to own user/user group/machine role as Security Admin

If you, as a Security Admin, change settings for your own user / user group / machine role, you must log out and log in again to make the changes effective.

NOTICE
Forgotten the Security Admin password? • If there is no longer a Security Admin of the **end user domain** who still knows their password, an Admin of the manufacturer domain must manually deactivate user management. When user management is deactivated, all configured data is irrevocably deleted and the old access level passwords that were valid before user management was activated are valid again. The manufacturer can then set up and activate user management again. • If there is no longer a Security Admin of the **manufacturer domain** who still remembers their password, an Admin of the manufacturer domain must reset the SD card to the factory settings, as without passwords for the Security admin manufacturer role, it is no longer possible to manually deactivate user management. Logging in with the Security admin manufacturer role is also no longer possible. To reset the NCU from a USB service stick, in the SINUMERIK ONE service system, select menu item "Clear all + reinstall system SW from USB stick and create system restore point". You must then recommission the CNC software. • Therefore, always keep all passwords - especially the passwords for the Security Admins - in a safe place! We recommend the use of a password manager. • We recommend that you always create more than one Security Admin for both domains, in case you forget a password.

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:

- Configuration
  - Activate user management and set up manufacturer domains
  - Create end user domains
  - Delete end user domains
  - Connect manufacturer domains with a central user management.
  - Disconnect manufacturer domains from a central user management
  - Delete manufacturer domains and 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
  - Defining ID login guidelines
  - Define login guidelines
- 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.

11.5.4.6 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 manuals and online help linked below.

Sensible order of configuring

1. If you are working with a distributed system comprising NCU and IPC, then first pair the two devices (Page 125).
2. 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.

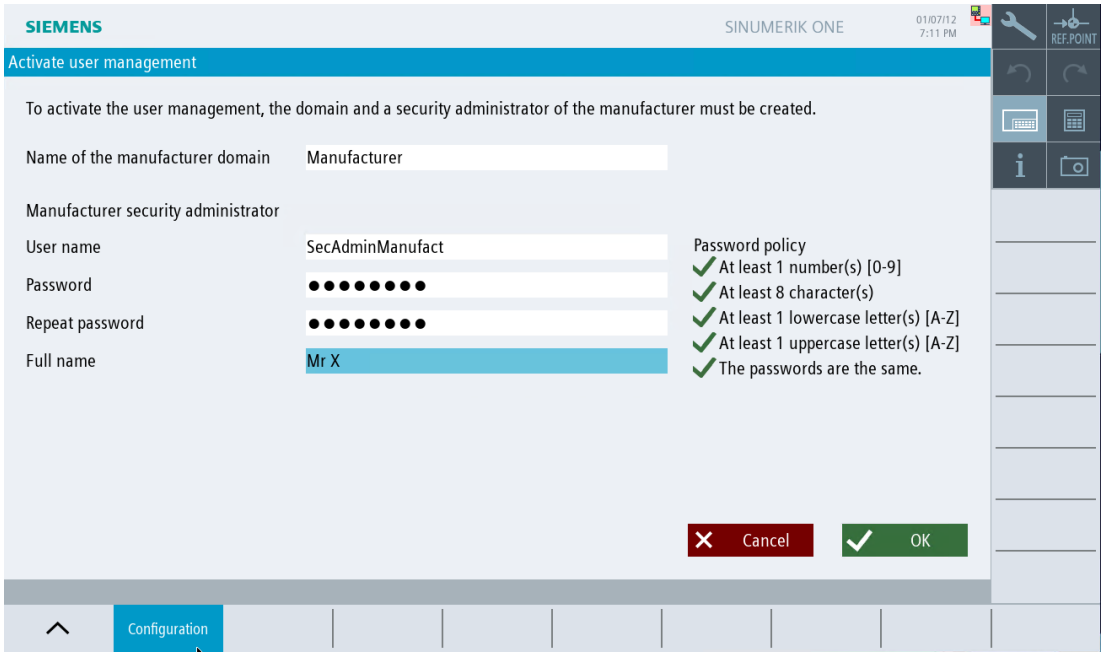


Figure 11-5 Activating user management

3. Define the name for the manufacturer domain.
4. Specify the user name and password for the Security admin manufacturer.
5. Optionally, specify a name for the Security admin manufacturer.
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

   Note

   Optional: Connect the manufacturer domain with a central user management

   Optionally, you can connect the manufacturer domain with a central user management, and you can take central user groups with already preconfigured users from the UMC server.
8. Optionally, activate the domain for the end user.

9. Define a name for the end user domain.
10. Specify the user name and password for the Security admin end user.
11. Optionally, specify a name for the Security admin end user.
12. Configure user management for the end user domain. This includes the following individual steps:
    - Configuration of user groups and assignment of user groups to the machine roles
    - Creation of users
    - Assignment of the users to the user groups

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 with confidence.

Note

Optional: Connect the end user domain with a central user management

Optionally, you can connect the end user domain with a central user management, and you can take central user groups with already preconfigured users from the UMC server.

See also

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

Programming Manual "SINUMERIK Integrate Create MyHMI /3GL (Qt Api)" (https://support.industry.siemens.com/cs/ww/en/view/109974182)

11.5.4.7 Policies

As a Security Admin, you can set the password settings, the ID login policy, the login policy, and the system use notification via the "Policies" dialog.

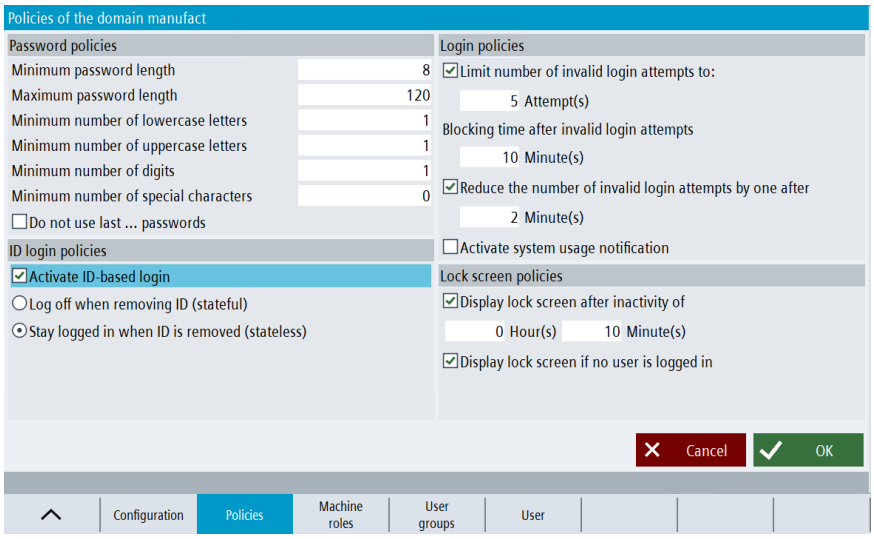


Figure 11-6 Policies

The following settings are possible:

Password policies

You can define which UTF8 characters should be used as basis for defining passwords (Page 137).

ID login guidelines

As of software release V6.25, it is also possible to log in to the SINUMERIK Operate system using the ID-based login.
You can activate/deactivate the ID-based login for the current domains. You can also decide on the login type:

- **Stateful**: With this option, you only remain logged in if the ID carrier is continuously placed on the reader. When you remove the ID carrier, you are automatically logged out.
- **Stateless**: With this option, you are logged in as soon as the reader identifies the ID carrier. After this you can remove the ID carrier. You can then manually log out using the logout dialog.

Work sequence

- Completely set up the reader as described in the Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139) Commissioning Manual.
- Activate the ID-based login in the Policies dialog.
- Assign one or several local user(s) an individual ID via the dialog "User > Create/change". You can also automatically read out this ID.

- If your domain is connected to a central user management, you must also assign the individual ID directly via UMC-S. To do this, enter the individual ID in the menu "User > Details > Account Policy > Autentication alias" in the UMC-S configuration settings.
- Log in at the reader using your individual key.

NOTICE
Data misuse/"Security Admin", "Manufacturer", and "Service" roles Note that ID-based login poses a risk of data misuse, as RFID cards or tags can be stolen or copied. • Since the "Security Admin", "Manufacturer", and "Service" roles generally have greater system responsibility than other roles, we recommend that you **do not** set up ID-based login for these roles/users. • The roles "Security Admin", "Manufacturer", and "Service" roles should **always** log in to the system with a user name and password since this authentication method offers greater security.

Note

Identical ID assigned more than once?

If the Security Admin has inadvertently assigned the same ID to multiple users in the same or different domains, then the following rules and/or sequence apply when logging in:

- The first user that is found with this ID is recognized / authorized.
- A search is first made in the user domain and then in the manufacturer domain.

Login guidelines

You can configure the following in the login guidelines:

- Limit the number of invalid login attempts
- How long a user is blocked after a number of incorrect login attempts
- After which time the failed attempts are reset by one

System use notification

Option to incorporate a system use notification in the login screen form. The system use notification is saved as language file in folder "/user/sinumerik/hmi/lng" for each language.

Carefully ensure that the settings you carry out make your system as secure as possible!

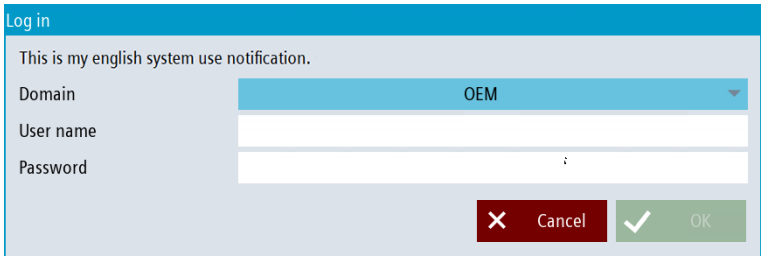


Figure 11-7 System use notification

More information

A description of all individual steps and setting options for user management in SINUMERIK Operate are provided in the following documentation:

- Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139)
- as well as in the SINUMERIK Operate online help.

Lock screen

The lock screen protects your HMI user interface against unauthorized access if the user is inactive or has logged out. The lock screen is automatically activated after a configurable period of inactivity (keyboard or mouse). You can always automatically display the lock screen even if no user is logged in. Alternatively, you can manually activate the lock screen from the logout menu.

NOTICE
Unattended open system / unintentional logouts An incorrectly configured lock screen can result in unsupervised, open systems or undesirable logouts. • As a consequence, carefully consider a period of inactivity after which the automatic activation of the lock screen makes sense in your particular environment.

Advantages of the lock screen from a security perspective

The lock screen is a fundamental measure to increase system security by minimizing risks that occur as a result of unsupervised, logged in user accounts.

- **Preventing unauthorized access**
  An authorized user logs on at the machine, leaves his workplace and forgets to log out. The lock screen ensures that the session is exited after a predefined time of inactivity. This prevents unauthorized persons who gain physical access to the machine from using the previous user's open session to access the system or carry out actions.

Note

General recommendation: Log out or manually lock the screen

Automatic lock-screen activation only ensures that the lock screen is activated if you forget to log out or lock the screen manually.

- We therefore recommend that you always log out of the system or manually activate the lock screen as soon as you leave your workplace at the controller.

- **Reducing the risk of session hijacking**
  In network environments, for open but inactive sessions, attackers can attempt to take over the active session (session hijacking) to pose as legitimate user. The time window for attacks such as these is significantly reduced by terminating inactive sessions.
- **Protecting the confidentiality and integrity of data**
  Sensitive configuration data, process parameters and trade secrets can be displayed on screens or can be accessed via the user interface. The lock screen protects this information from inquisitive glances or unauthorized changes if the workplace is left.
- **Forced authentication**
  When a user returns he must authenticate himself again. This ensures that the person operating the system is really an authorized user, and not simply somebody that has just sat down at the workplace.

11.5.4.8 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 level 1 (machine OEM).
Machine roles	You have role "Security admin manufacturer" or "Security admin end user" (changes not possible). 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.
User groups	You have the "Security admin manufacturer" or "Security admin end user" role. The softkey is not visible to other users.	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 not visible to other users.	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 not visible to other users.	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 are provided in the following documentation:

- Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139)
- as well as in the SINUMERIK Operate online help.

11.5.4.9 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
- User administration / guidelines settings (password guidelines, login guidelines, 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 109) and in the following documentation:

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

11.5.5 Drive security

11.6 Backup and restore

11.6.1 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
- SD card image
- IPC image via Microsoft Windows Service Center

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 running up the NCU/PU 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 111)

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 end user)

- 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.

SD card image

You can also create a complete image of your SD card.

More information about the precise sequence when creating an SD card image is provided in the Installation Manual "Installation and upgrade".

IPC image via Microsoft Windows Service Center

If you are working in a distributed system comprising one IPC, then you have the option of creating or restoring images of data carriers in the Microsoft Windows Service Center. You have the following options:

- Create a data carrier image of the SSD
- Restore a data carrier image of the SSD

- Create a data carrier image of a partition
- Restore a data carrier image of a partition

More information on backing up and restoring data is provided in Commissioning Manual "PCU Base software /IPC".

See also

IPC Bitlocker hard disk encryption (Page 146)

11.6.2 Security archive

The control system 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.

In a distributed system consisting of IPC and NCU, the security data are stored on the IPC. For an autonomous NCU without IPC, the security data are saved on the NCU.

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

You require role "Security Admin" or "Manufacturer" to create and restore the security archive.

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

The "Security archives / security restore password" is also required for restoring SD card encryption if a part has to be replaced.

NOTICE
Security archives / Security restore password Keep the password in a secure place as it is required for restoring the security archive. If the password is not known, it is not possible to restore the security archive and restore the SD card encryption or the security memory! • If you have not assigned the password, SD card encryption (Page 143) cannot be activated. • If you delete or lose the password, the SD card encryption cannot be restored when the hardware is replaced (Page 144). • If you delete or lose the password then the security data cannot be restored when the hardware is replaced (Page 113).

NOTICE

Archive restoration when decoupled not possible

If a backup archive (including security and NCK components) is created on an IPC-NCU subsystem, which has active user management and is coupled, then such an archive can only be restored when the IPC-NCU system is coupled.

Restoring the archive is not possible if the IPC-NCU is decoupled.

In the case that a part must be replaced, the assigned system must first be coupled and then an attempt must be made to restore the archive.

NOTICE

Data misuse by departing employees

As soon as employees who know the Security archives / Security restore password leave the company, there is an increased risk of data misuse. This Security archives / Security restore password is essential for restoring the security archive and encrypting the SD card.

- Therefore, change the Security archives / Security restore password immediately as soon as employees have left the company.
- Deactivate the encryption of the SD card.
- Re-encrypt the SD card with the new Security archives / Security restore password.

This is how you ensure that no confidential and personal information can leave the company and be misused by a third-party.

Observe the following password policies for the security archives / security restore 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".

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

Note

Access level "End user" or the "Security Admin manufacturer" or "Security Admin end user" role is required to change the security archive password/security restore password.

NOTICE
Losing user management data of older Operate versions If you have installed an Operate Version < x.25 and have saved the user management data in a security archive, this data is not saved when restoring a security archive in SINUMERIK Operate x.25 and must be newly configured/created.

11.6.3 Restoring security data

Definition

The security data of the SINUMERIK are encrypted with an individually generated key and can only be decrypted with the device on which the individual key is stored.

In the case that parts must be replaced, it is possible that the hardware on which the key for the security data is saved is replaced.

You require this function in the following use cases:

- **Key to restore security data**:
  - New NCU/PU: Hardware, on which the key is saved, was replaced
  - Old SD card (unencrypted) in the new NCU/PU
  - The key is corrupt/incorrect.
- **Deleting an encrypted memory**:
  - You have forgotten or lost the Security archives / Security restore password.

Preconditions

Note

Security archives / Security restore password

The Security archives / Security restore password (Page 111) is a requirement for restoring the security memory.

- The security memory was not able to be correctly decrypted and after running up SINUMERIK Operate displays Alarm 150434.
- You are logged in with the legacy passwords "Manufacturer" or "End user".
  OR
- With active user management: You have role "Security Admin" or "End user".

Restoring security data

In the "Setup" operating area, select the restoration of the security data via softkeys "Security > HMI security".

The security data are restored after entering the password for security archives / security restore password and a restart. The saved security settings are again available and you can authenticate yourself via the user management.

More information

More information on using function "Restoring the key for the security memory" is provided in the SINUMERIK online help as well as in the following documentation:

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

See also

Restoring the SD card encryption (Page 144)

11.6.4 IPC backup and restoration

Backup options

- From SINUMERIK software version 6.24, Paragon from the Windows Service Center supports you when creating and restoring an encrypted or unencrypted backup.
- You can also create a backup for a hard disk already encrypted with BitLocker.
- Using the Paragon software, you can also create regular backups automatically.

NOTICE
Reduced performance as a result of backups Creating backups can negatively impact the performance of your system. Take this into consideration, especially for automatically created backups. • If possible, create your backups in a non-production period.

Restore

- You can also reimport an image of an encrypted hard disk via Paragon.
- After loading the Paragon image, you must manually reactivate the BitLocker function.

More information

More information about creating and restoring IPC backups can be found in the following documentation:

- Commissioning Manual SINUMERIK ONE PCU Base Software/IPC (https://support.industry.siemens.com/cs/ww/en/view/109925791)

11.7 System integrity

11.7.1 Certificate store

Introduction

All X509 certificates used are securely saved in the certificate store. The certificates are used to certify a trusted security function, for example, secure pairing between an NCU and an IPC. A tabular overview of all the imported certificates can be seen in the overview page of the certificate store.

All certificates stored in the certificate store are part of the security component of the backup archive. This means that these data have been secured and can be read in again.

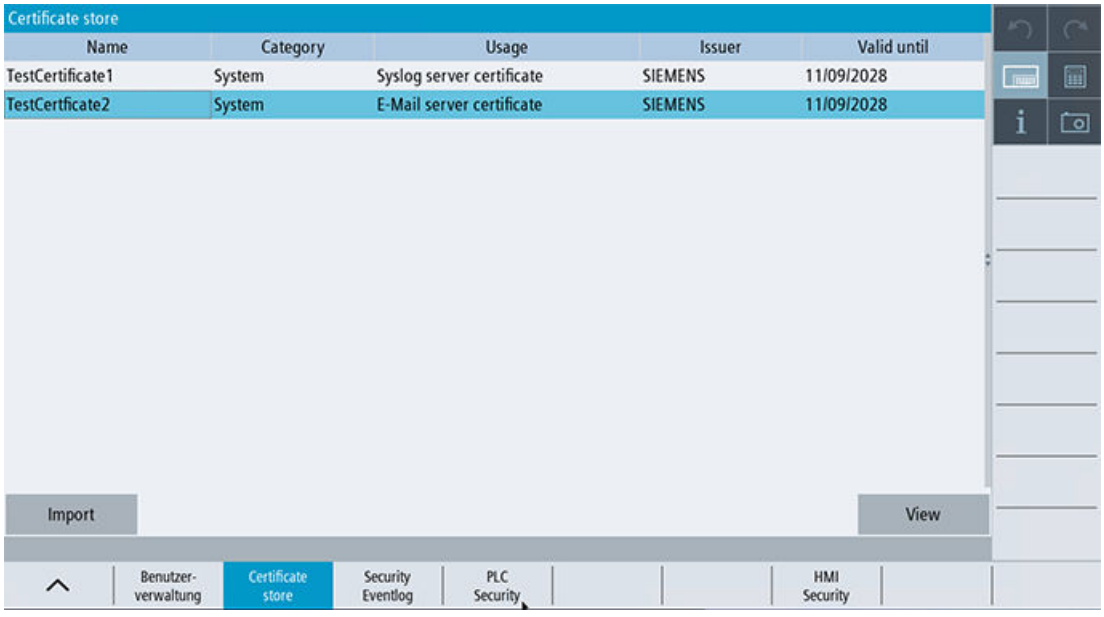


Figure 11-8 Certificate store overview

The certificates are structured based on the following meta data.

- **Name**: certificate name that can be freely assigned
- **Category**: Certificate category: system, device or OA

  Note

  The category is automatically selected based on the selected usage.

- **Usage**: Selectable certificate usage
- **Issuer**: Certificate issuer
- **Valid until**: Certificate expiration date

Purpose of the certificate store

- The certificate store in the SINUMERIK system serves as a **central location** where certificates are safely administered. It allows certificates to be handled in a unified and standard fashion, independent of the NCU and IPC.

NOTICE
Forgery and misuse of certificates There is a risk of misuse and forgery if certificates are not securely stored and administered. A forged certificate can be used to simulate a relationship of trust that does not actually exist. • Always ensure that used certificates are always securely stored in the certificate store. • Only authorized personnel may store and administer certificates in the certificate store. You require the "Security Admin" role with activated user management or role "End user" without activated user management to save and administer certificates for SINUMERIK. • For security reasons, certificates must be regularly extended and must have a short validity.

Note

Renewing certificates / checking the validity

The validity date in the certificate store is assigned a red background as soon as the certificate validity has expired.

- Delete the invalid certificate from your certificate store and import a valid certificate!

Supported security functions

The following SINUMERIK security functions access the certificate store:

- Security Eventlog (Page 158)
- Secure web server communications via HTTPS (Page 154)

Content and structure

A digital certificate contains all the necessary data that confirms certain object properties and whose authenticity and integrity can be verified based on cryptographic methods.

SINUMERIK supports public key certificates according to the X.509 standard.

Using function "View certificate", you can view detailed information about the selected certificate.

Supported certificate types

pkcs12

- pkcs12 certificate file, including the private key (only if the file is encrypted)

  Note

  pkcs12 is supplied with an encrypted bundle comprising certificate and private key.

pem/crt/cer(ASCII)

- pem certificate including the private key (with encryption of the private key)
- pem certificate including the private key (without encryption of the private key)
- pem certificate file (without encryption)
- pem file with private key (with and without encryption)

cer(binary)

- cer certificate file (without encryption)
- cer file with private key (without encryption)

der

- der certificate file (without encryption)
- der file with private key (without encryption)

Note

Encryption password

Only ASCII characters are supported for the certificate password/password for the private key.

Note

- Only X509 V3 certificates are supported.
- The cer and der formats do not support a bundled certificate and do not support a private key in a single file.
- The validation of the sequence/hierarchy in a certificate chain is supported during import.
- Importing just a private key is not supported. This is only supported in the import workflow if the use of a key is required.

More information

More information on using the certificate store is provided in the SINUMERIK online help as well as the following documentation:

- Commissioning Manual SINUMERIK ONE "Final commissioning" (https://support.industry.siemens.com/cs/ww/en/view/109817139)

See also

Overview (Page 125)

Commissioning Manual SINUMERIK 828D "SINUMERIK Operate" (https://support.industry.siemens.com/cs/ww/en/view/109823589)

11.7.2 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 118)
- PLC access level password for protecting the PLC against unauthorized access (Page 122)
- Password for the protection of the offline safety program (Page 124)
- Know-how protection password (Page 124)
- Copy protection password (Page 124)
- Write protection password (Page 125)

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.

11.7.2.1 Password to protect confidential PLC configuration data

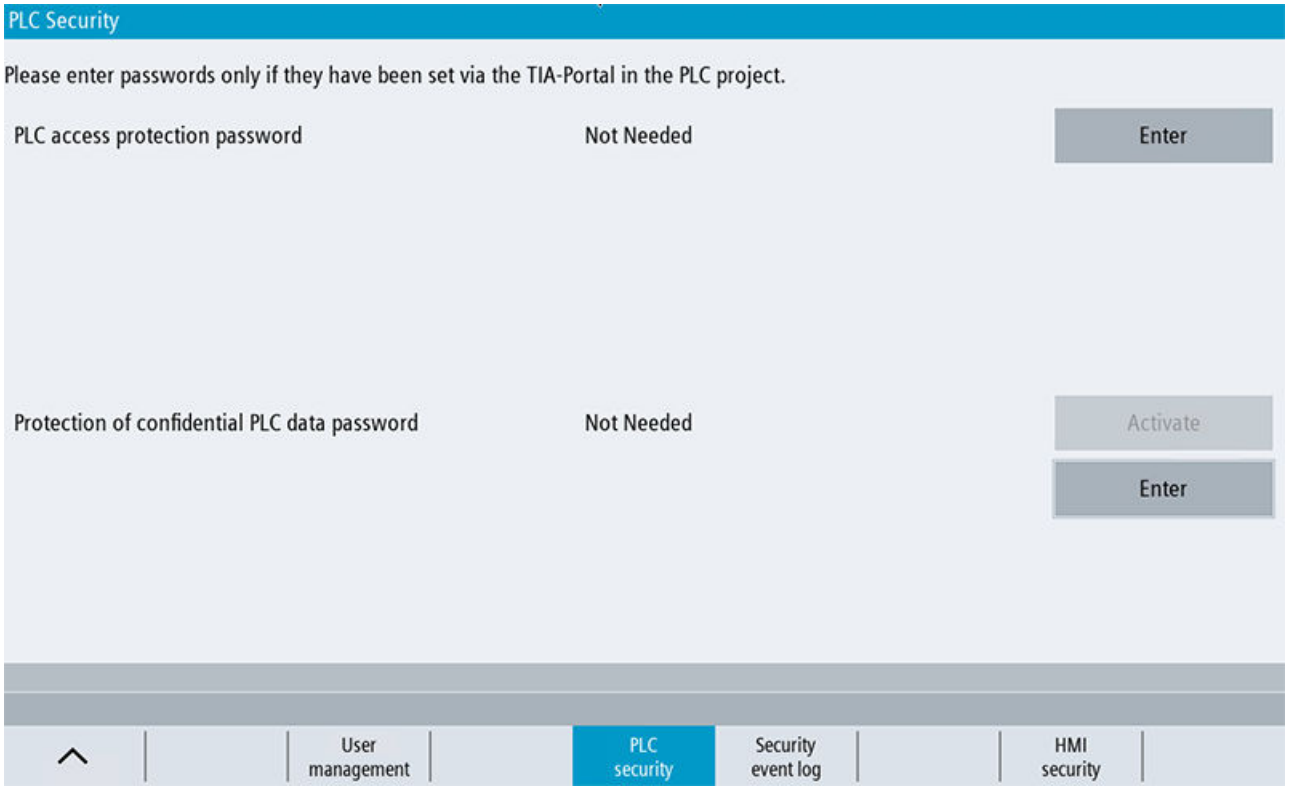
Purpose

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.

The following diagram shows the settings for PLC security passwords in SINUMERIK Operate in the "PLC Security" menu.



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
  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

Configuring sequence and password assignment

- The following sequence is recommended for PLC configuration in the TIA Portal:
  - Download the project to the PLC.
  - Set password to protect confidential PLC configuration data in the TIA Portal.
  - Store PLC passwords (password to protect confidential PLC configuration data and password for the PLC access level) in SINUMERIK Operate.
- When configuring the PLC via the PLC setup archive, you can store the PLC passwords (password to protect confidential PLC configuration data and password for the PLC access level) in SINUMERIK Operate.

Note

Password assignment for PLC configuration in the TIA Portal

It is recommended that you **first** load the project into the PLC and then set the two PLC passwords (one password to protect confidential PLC configuration data and one password for the PLC access level). If the password for protecting confidential PLC configuration data in the TIA Portal does not match the password stored in the PLC, the controller goes into error status.

To be able to load the PLC project into the controller again, you must reset the PLC and the PLC passwords to the factory settings.

If you import a new PLC archive, you do not need to reset the PLC to the factory settings beforehand.

For more information on resetting a controller to the factory settings, see the TIA Portal help under "Resetting an S7-1500 CPU to factory settings".

Note

Special features when setting the password to protect confidential PLC configuration data

- If the password is set via SINUMERIK Operate, it is saved in the internal password manager of SINUMERIK Operate.
- If an archive containing the PLC and security component is created, the password is included in the archive.
- If the NCU needs to be replaced, the archive (PLC and security component) can be read in and the password recovered.
- In case of a memory reset of the PLC, the password for protecting confidential PLC configuration data is deleted.
- 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 the "Setup" operating area, menu "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 PLC access level "Full access incl. fail-safe (no protection)" or "Full access (no protection)" is set (Page 122).
- 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 (end 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.

11.7.2.2 Password for PLC access level

Purpose

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

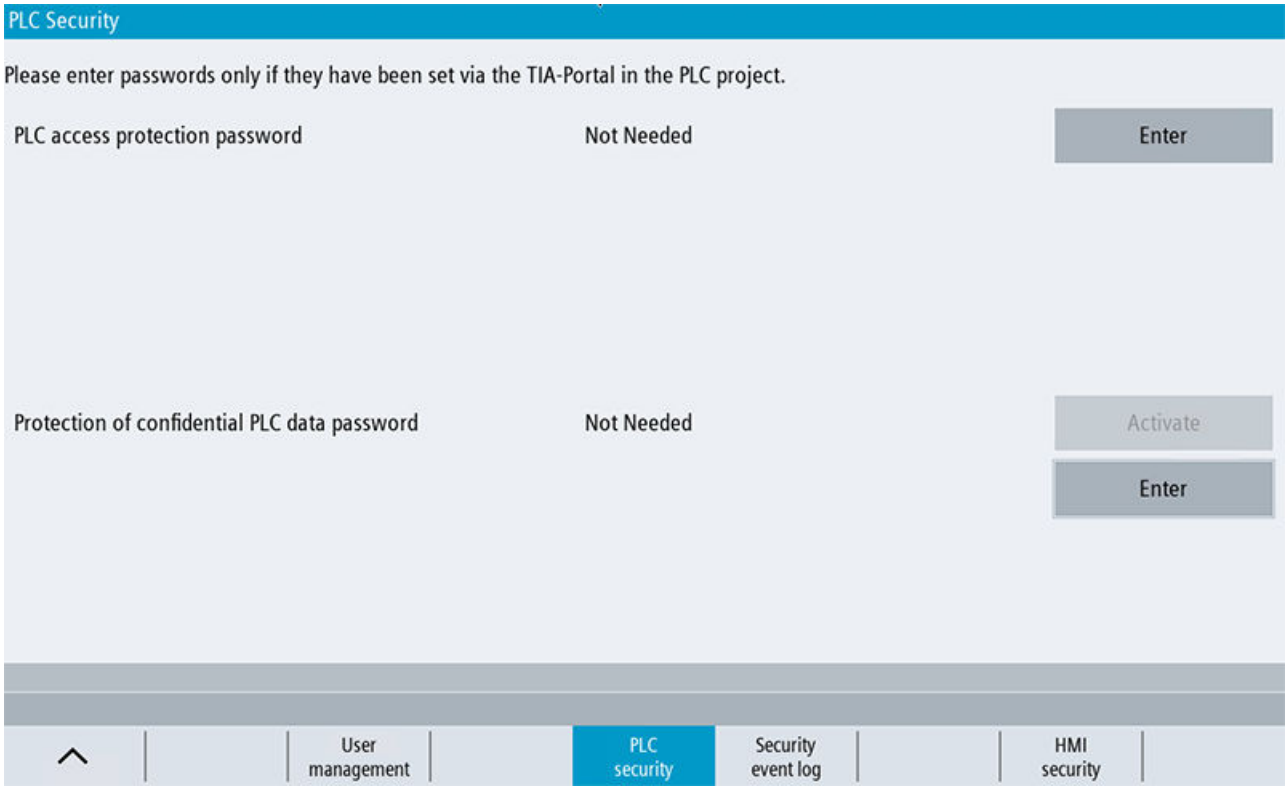
The PLCs have different access levels to restrict access to certain functions, such as hardware configuration, PLC project, safety and access via S7 communication and blocks.

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

Generation

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

The following diagram shows the settings for PLC security passwords in SINUMERIK Operate in the "PLC Security" menu.



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

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

Therefore, save the PLC access level password for "Full access including fail-safe (no protection)" in the SINUMERIK Operate menu "Setup > Security > PLC Security > Password for PLC access level protection".

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

From V6.25 and higher, in the following cases, the password for the PLC access level password must be entered:

- The safety component in the archive has changed.
- The access level is not the machine OEM.
- The archive was created with a version less than V6.25.

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 password for PLC access level 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 passwords for PLC access level can be found in the Commissioning Manual on work steps for configuring and commissioning and in the online help for SINUMERIK Operate.

11.7.2.3 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.

11.7.2.4 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".

11.7.2.5 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".

11.7.2.6 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".

11.7.3 Trusted devices

11.7.3.1 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 89)" 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 SINUMERIK ONE "Final commissioning steps" (https://support.industry.siemens.com/cs/ww/en/view/109817139) 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 NCUs, only one instance of SINUMERIK Operate is permitted on the IPC.

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

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. • 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.

11.7.3.2 Requirement when pairing

For the "Pairing" security function to correctly function, it is imperative that the correct date and time have been set in the system (Page 85).

NOTICE
Date synchronization If the date displays of the IPC and NCU are not synchronized before pairing, you cannot complete the pairing process because the generated certificates may be invalid. • To be on the safe side, synchronize the date settings of both devices before pairing.

11.7.3.3 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.
- The installed Operate version on the PU and the installed Operate version on the PC/IPC should be identical.

Introduction

- If you want to use the security function "User management (Page 89)", you should first pair your IPC with an NCU. This establishes a relationship of trust between the two devices.

Procedure

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

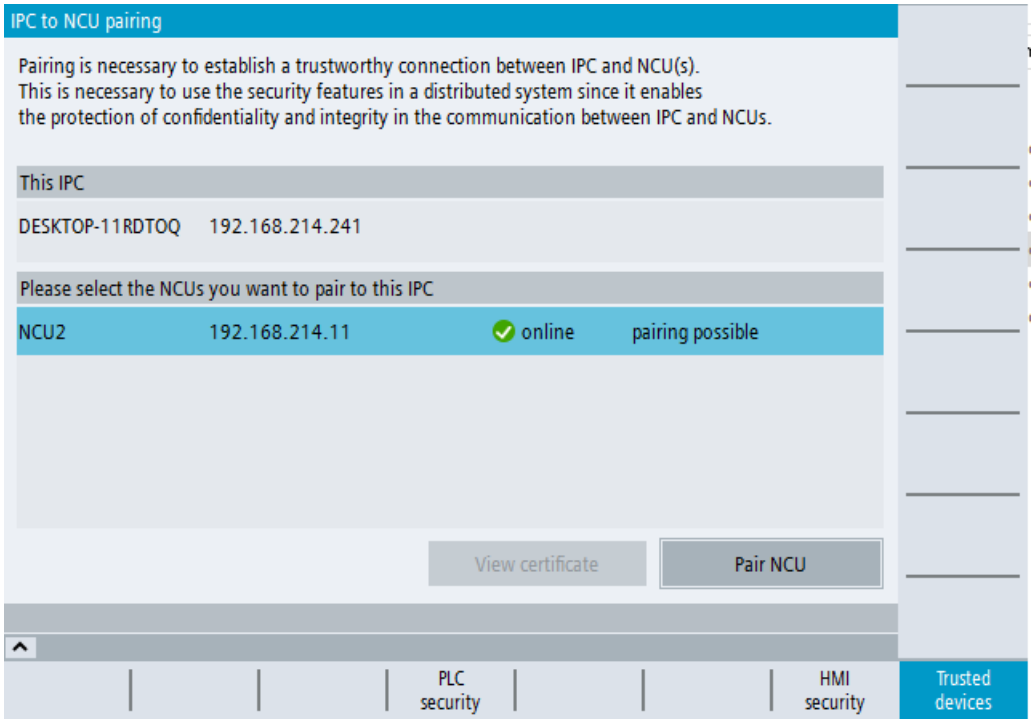


Figure 11-9 Pairing communication and status display

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.

11.7.3.4 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.

Possible use cases for unpairing could include:

- 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 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!

More information

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

11.7.3.5 Renewing pairing certificates

IPC and NCU/PU pairing certificates are only valid for a limited time.

- Pairing certificates are valid for one year. A limited certificate validity time results in a higher level of security.
- Pairing certificates are **automatically** renewed as soon as the particular certificate is to become invalid in the next 3 months or the validity of the certificate expires.

The certificate renewal process is also logged in the Security Eventlog (Page 158).

Note

Automatically renewing pairing certificates has no influence on the pairing status of the paired devices!

Applications

- The final validity of the pairing certificate has expired and the system was not restarted in the last 3 months.
- The validity of the pairing certificate expires in the next 3 months.
- The pairing certificates were corrupted.
- Replacement scenario: Replacement of the IPC.
- Replacement scenario: Replacement of the NCU.

11.7.4 Safety Integrated log file

11.7.4.1 Overview

The Safety Integrated log file reliably documents all changes made to the safety configuration of a machine after it has been delivered. As a consequence, as operator or machine OEM, you receive verifiable proof of the integrity and security of the safety functions. Manipulation or inadvertent changes become transparent, which significantly increases the security and the obligation to provide verification in machine operation.

When the system is delivered each system is assigned its own log file. This serves as the starting point for seamlessly documenting all security-relevant changes from the time of transfer. This makes it possible to track at any time whether and what changes were made by service personnel to the safety configuration after delivery.

The date of the log file must correspond to the delivery date of the system.

Note

When the system is supplied, check the date of the Safety Integrated log file.

All changes to the safety configuration are automatically acquired in SINUMERIK Operate in a log file in the XML format and saved to the SD card.

The validity of the system safety configuration is checked at fixed time intervals. You can freely configure these time intervals.

11.7.4.2 Using the Safety Integrated log file

Sequence and monitoring of the logging function

The logging function automatically becomes active when SINUMERIK Operate starts. When activating, all checksums and signatures are saved in the log file as reference. An original key applied by Siemens at the factory is used for signatures.

Log file SafetyChangeLog.xml and reference file safetylogreference.xml are on the SD card in the directory oem/sinumerik/hmi/data/safety/SafetyChangeLog. File SafetyChangeLog.xml is used as fingerprint for the current safety settings and forms the basis to make comparisons relating to changes in the system. For a change, the information from the reference file is used to update the log file and document the change.

If the system cannot update the log file (e.g. because the SD card is full or defective), an alarm is output indicating that a check is required. For errors or problems, a log entry is created that makes reference to the problem.

Note

The logging function functions both with as well as without SD card encryption.

Content of the log file

The log file contains entries for the following components:

- Global checksums of the SINUMERIK system
- F-PLC signatures (including symbolic names and time stamp):
  - F-Collective
  - F-software
  - F-hardware
  - F-communications
- Checksums of SINAMICS drives (with axis/drive ID and time stamp):
  - dbSI2 (2nd Gen)
  - dbSI3 (3rd Gen)
- SafeUserData (SUD): Signature and change date
- Software versions
- New entries for changes to the safety configuration or security-relevant hardware (SINAMICS, F-modules, SINUMERIK ONE)

Each entry contains the particular component, a time stamp and a signature. Each drive has its own entry and its own signature.

Protecting the log file from being manually deleted and overwritten

The file is cryptographically protected to check the integrity and identify any manipulation.

If the log file is deleted without authorization or is identified as corrupted due to an incorrect HASH checksum, it will be fully restored from the backup file.

Archiving the log file

The maximum log file size can be configured using sldbsidatalog.ini.

The permissible file size lies between 512 kB and 5 MB; the default value is 1 MB, which approximately corresponds to 400 log entries.

The system automatically archives the log file once this limit has been reached. The system creates an archive file with prefix "arc_" and a time stamp in the file name and starts a new log file.

By archiving, all log data are kept for a long period of time even when numerous changes have been made.

Exporting the log file

You can export the log file to an external storage location – for example, on a drive incorporated in SINUMERIK Operate.

More information on exporting the Safety Integrated log file can be found in the Commissioning Manual "Final commissioning steps".

11.7.5 Secure Boot operation/Secure Boot

Secure Boot on the NCU

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=<07> error is displayed in the 7 segment display.

More information on the 7-segment display is provided in the SINUMERIK ONE equipment manuals.

Secure Boot on the IPC

In the BIOS firmware, the PC system also has function "**Secure Boot**". This allows the Microsoft Windows operating system to only boot with a secure configuration. Function Secure Boot only allows Microsoft Windows to boot if certain applications such as the bootloader have not been modified or manipulated due to external causes.

Requirements:

- You have one of the following compatible IPC types with integrated TPM module 2.0:
  - IPC227G
  - IPC BX-39A
  - IPC PX-39A
- PCU base software /IPC as well as Microsoft Windows are installed on your PC system.
- A supervisor password was previously defined in BIOS. The password is required so that function "Secure Boot" cannot be deactivated again by unauthorized parties.

NOTICE
Data corruption as a result of malware when booting When delivered, Secure Boot is **deactivated in the IPC as default**. Malware, such as viruses or rootkits, can be loaded during the booting process. This can result in data misuse and data corruption. • To prevent this and to ensure the integrity of the complete system, **always activate function "Secure Boot" in BIOS**.

Activating Secure Boot in BIOS and defining the supervisor password

More information about activating "Secure Boot" in BIOS and defining the supervisor password is provided in Commissioning Manual SINUMERIK ONE "PCU base software /IPC" (https://support.industry.siemens.com/cs/ww/en/view/109973978).

11.7.6 Defense against malicious code

11.7.6.1 Overview

"Malicious code" refers to malicious software or program code designed to cause damage to computer systems, networks or data. Malicious code can occur in various forms:

- **Viruses**: Programs that infiltrate other software to spread and infect systems.
- **Worms**: Malware that automatically propagates through networks.
- **Trojan horses**: Software that masquerades as a useful application but actually performs malicious functions.
- **Spyware**: Programs that secretly capture information about a user and forward this information on to third parties.
- **Ransomware**: Malware that blocks access to data or systems until ransom money is paid.
- **Adware**: Software that displays unwanted advertisements and may monitor user behavior.

Malicious code is frequently developed to obtain unauthorized access to systems, steal data, disturb the functionality of systems or fraudulently obtain financial gain. Protection against malicious code requires that suitable security measures are applied, including antivirus software, regular system updates (Page 179), firewalls and training users on how to securely handle IT systems.

11.7.6.2 Antivirus and anti-malware protection of the NCU

Hardened Linux and signed code

SINUMERIK ONE NCU uses a hardened Linux as operating system. This system has been specifically designed to guarantee a high degree of security. A central component of these security measures is that the NCU can only execute signed code. This approach ensures that only authorized software whose authenticity and integrity have been verified runs on the system, significantly reducing the risk posed by malware.

As a result of this rugged security structure and the seamless integrity check of the software being executed, a separate malicious code solution is not required for the NCU.

11.7.6.3 Antivirus and anti-malware protection of the IPC

Overview

On the SINUMERIK IPC under Microsoft Windows, SINUMERIK ONE supports the following endpoint protection solutions:

- Antivirus software **Microsoft Windows Security**
- **Allowlists**

Microsoft Windows Security

The application **Microsoft Windows Security** (Windows Defender Security Center) is a security feature integrated into Microsoft Windows to protect your data. Microsoft Windows Security is installed as default on the IPC system, and is supported by SINUMERIK Operate.

NOTICE

Virus/malware/phishing attacks as a result of obsolete virus signatures

Your system can become a target for cyber attacks if Microsoft Windows Security is not kept up to date by regularly installing updates.

- Using automatic updates, always ensure that your system is supplied with the newest virus signatures.
  - **Microsoft Windows security** updates are distributed via Windows updates: Updating Windows security signatures - Microsoft support (https://support.microsoft.com/en-us/windows/update-windows-security-signatures-726d462d-b2a8-5bb2-8a9e-5d5871b06e05)
  - They can be controlled using WSUS: Providing Windows Defender definition updates using WSUS (https://learn.microsoft.com/en-us/troubleshoot/mem/configmgr/update-management/deploy-definition-updates-using-wsus)

NOTICE

Reduced performance due to manual virus scans

Note that manual virus scans cannot be performed on a SINUMERIK control system with integrated IPC during production. System resources can be significantly loaded when a scan such as this starts; this can have a negative impact on the machine performance, or in the worst case scenario, can result in a production stop.

- To guarantee smooth and seamless production, virus scans should only be performed during scheduled maintenance windows or in non-productive periods. Ensure that all security-relevant updates and scans are made in a secure and predictable manner in order to avoid unscheduled production downtimes.

Recommended configuration Microsoft Windows security

To maintain the performance of your IPC system, we also recommend applying the following Microsoft Windows Security configurations by using **Microsoft Windows PowerShell** commands. Microsoft Windows PowerShell must be run with administrator privileges.

- **Reducing CPU utilization levels**: The CPU utilization of Microsoft Windows Security is limited as default to an average of 50 %. CPU utilization can be reduced even further by defining a low CPU priority. This means that other processes can be prioritized:
  - `PS> Set-MpPreference -EnableLowCpuPriority $true`
- **Avoiding nuisance alarms**: Nuisance alarms can be avoided by excluding the HMI path from scans:
  - `PS> Add-MpPreference -ExclusionPath 'C:\Program Files (x86)\Siemens\'`
  - `PS> Add-MpPreference -AttackSurfaceReductionOnlyExclusions 'C:\Program Files (x86)\Siemens\'`
  - `PS> Add-MpPreference -ExclusionPath 'C:\Program Files\Siemens\'`
  - `PS> Add-MpPreference -AttackSurfaceReductionOnlyExclusions 'C:\Program Files\Siemens\'`

Allowlists

Antivirus software must always be kept up to date with the latest virus signatures. As these regular updates are only supported as long as the operating system is still supported by the manufacturer, antivirus software often has a shorter service life than the SINUMERIK machine in the field. We therefore recommend the use of allowlists over the use of antivirus software.

In addition, the use of antivirus software/scans can lead to performance losses, which is not the case when using allowlists.

Compatibility tests

There are regular compatibility tests with the following allowlist software:

- McAfee Application Control

Smart App Control (SAC)

The Microsoft Windows security function "Smart App Control (SAC)" prevents the execution of programs that either do not have a valid digital signature or are classified as untrusted by Microsoft's cloud-based security analysis.

- SIMATIC IPCs with Microsoft Windows 11 and **PCU-Basesoftware V16** are shipped with a standard installation in which the Windows feature Smart App Control (formerly Microsoft Defender Application Control) is **activated**. **If SIMATIC IPCs are used with a SINUMERIK ONE controller, we recommend disabling Smart App Control (SAC).** The precise steps for disabling it in Microsoft Windows can be found in the linked reference documentation.
- As of **PCU-Basesoftware /IPC V16.0 SP1**, Smart App Control is **disabled** by default during the installation of PCU-Base. If you want Smart App Control to remain enabled, adjust the setting in the setup.ini file before starting the installation. The precise steps for enabling it via the setup.ini file can be found in the linked reference documentation.

Note

Reasons for deactivating

- There may be a delay in the initial run up when the function is activated.
- Disturbance-free machine operation cannot be guaranteed (Siemens software and customer software).
- To use SAC efficiently, a permanent Internet connection must be available for the cloud service functionality. This is not available on all SINUMERIK ONE machines.
- SAC is closely linked to capturing diagnostic data. These data are necessary for SAC to function correctly and make decisions about the security of applications. This transfer of data in an industrial environment is to be classified as critical.

NOTICE

Security risks when the SAC function is activated

The following security risks apply if you decide **not** to deactivate SAC:

- **Blocking company-critical software**:
  Industrial applications (e.g. control software, machine interfaces, customer-developed tools) are frequently not digitally signed or do not have a recognized reputation. SAC automatically blocks applications such as these without any possibility of being released by an administrator. This can result in production downtimes or operational disturbances
- **SAC does not permit exception rules (e.g. allowlists)**
  SAC does not permit blocked applications from being released. Once an application is blocked, it remains permanently blocked unless it is signed with a Microsoft-trusted certificate.
- **SAC only functions if optional diagnostic data are sent to Microsoft**
  In sensitive industrial environments, this can represent a data protection risk.

NOTICE

After deactivation, manual activation is no longer possible

Once it has been deactivated, SAC **cannot** be reactivated. A complete Windows reinstallation is required for re-activation.

- As a consequence, clearly understand the security risks first and then make a well-founded decision.

More information

More information about Microsoft Windows Security and commissioning IPCs using PCU Base is provided in the Commissioning Manual SINUMERIK ONE PCU Base Software/IPC (https://support.industry.siemens.com/cs/ww/en/view/109925791).

11.8 Know-how protection

11.8.1 SINUMERIK ONE password policies

The following overview provides a summary of possible passwords for SINUMERIK ONE and their criteria.

TIA Portal PLC passwords

You can adapt the PLC password policies in the TIA Portal under "Security Settings (in Project Navigation) > Settings > Password policies". The following setting options apply:

Password criterion	Minimum/maximum values	Permitted characters
Length	8-32	-
Numbers	0-32	-
Special characters	0-32	°!“§$%&/()=?{[]}\+*~,;.:-_

These PLC password policies refer to the following passwords (where some passwords are allowed to be longer):

- User passwords (project protection): Maximum password length, 120 characters
- Access level passwords (PAL): Maximum password length, 120 characters
- Password configuration data (PMS): Maximum password length, 120 characters
- OPC UA server user: Maximum password length, 120 characters
- Web server user: Maximum password length, 32 characters

PLC know-how protection passwords

PLC know-how protection passwords have the following defined password criteria:

Password criterion	Minimum values
Length	8–120
Numbers	1
Uppercase letters	1
Lowercase letters	1
Special characters	1

SINUMERIK Operate – User management passwords

You can change password criteria for SINUMERIK user management under "Security > User management > Guidelines".

Password criterion	Minimum/ maximum values	Default value	Permitted characters
Length	8–120	-	-
Lowercase letters	0–120	1	-
Uppercase letters	0–120	1	-
Numbers	0–120	1	-
Special characters	0–120	0	("/`!@#$%^&*()_+-=[]{};':|,.<>\\/?~")

SINUMERIK Operate – Security archive passwords

Security archive passwords have the following defined password criteria:

Password criterion	Minimum values
Length	8-100
Numbers	1
Uppercase letters	1
Lowercase letters	1

SINUMERIK Operate – Access level passwords

SINUMERIK Operate access level passwords have the following defined password criteria:

Password criterion	Minimum values
Length	8-32
Numbers	1
Uppercase letters	1
Lowercase letters	1

VNC passwords

VNC passwords have the following defined password criteria:

Password criterion	Minimum values
Length	1-8 (as a result of the VNC protocol)

NOTICE
Data misuse If the VNC connection is hacked, then there is a risk of data manipulation and/or data misuse. The VNC connection is not protected using the most optimal cybersecurity measures, which means that access to VNC communications must be restricted by applying additional organizational measures. This includes, for example, firewall settings, access logging, encryption, etc.

Passwords on the virtual machine

NOTICE
Misuse of passwords There is an increased risk of password misuse on the virtual machine. • Assign different passwords for the security functions on the virtual machine than on the real machine.

11.8.2 Secure account management

Rules for accounts and passwords

Companies define rules for handling user accounts and passwords as part of a risk evaluation process and these rules are regularly evaluated.

An overview of all passwords and their criteria is provided in Chapter AUTOHOTSPOT.

Numerous settings relating to password criteria for SINUMERIK user management can be defined in dialog "Guidelines":

- Rules when entering incorrect passwords
- Rules for automatic logging off
- Rules for renewing passwords
- Configuring ID-based login

Overview of access and authentication types

System	Access	Management via	Responsible user management	Authentication type
SINUMERIK Operate	SINUMERIK Operate	SINUMERIK Operate	SINUMERIK Operate	ID-based, user name + password
NCK (Numerical Control Kernel)	PLC	TIA Portal	PLC	User name + password
	PLC engineering			
	PLC web server			
	PLC OPC UA			
SSH file system	SSH	SINUMERIK Operate	SINUMERIK Operate	User name + password
	OPC UA SINUMERIK	SINUMERIK Operate	Own user management or SINUMERIK Operate	User name and password, certificate-based
	VNC SINUMERIK	SINUMERIK Operate	-	8-character password, optional confirmation

Accessing NCK file systems and machine data via OPC UA, HMI applications or the PLC depends on the user currently logged on at the machine as there is no session capability. NC Extend and the Linux file system can be accessed independent of the logged on user.

Microsoft Windows user management and SINUMERIK user management

Microsoft Windows user management and SINUMERIK user management are separate systems.

Reasons for the separation are as follows:

- Presently, function accounts are used in SINUMERIK Operate as it would be too complex to switch over to Windows users.
- It is difficult to set up ID-based login with Windows accounts
- There are different security requirements between machine and Windows.

If you wish to use the Microsoft Windows user management for SINUMERIK user management, then you can connect the SINUMERIK control system to an active directory (https://support.industry.siemens.com/cs/ww/en/view/109780337) via UMC-S.

UMC-S is a basic solution for small up to medium-sized companies without a link to an active directory. Allows shopfloor accesses to be directly managed. Supports ID-based login.
For large companies an active directory can be linked, which simplifies central administration and adaptation of authentication technologies.

VNC access

The VNC password is limited to 8 characters as this corresponds to the VNC standard, and any change could result in incompatibilities.

VNC is only used to provide access protection and is not a full-fledged user management system (no separate sessions or remote desktop functions)

NOTICE
Data misuse Under certain preconditions, VNC access can be insecure and can result in data misuse. • It is urgently recommended that VNC access is not directly enabled via the X130 firewall. • If remote maintenance is required, a higher level firewall with two-factor authentication should be used as the VNC itself does not support two-factor authentication. • The S7 port at the X130 should also remain closed if it is not used via a protected zone of a higher level firewall.

SINUMERIK OPC UA

OPC UA has its own user management, as SINUMERIK Operate user management does not support certificate-based authentication. This allows function accounts and user accounts to be separated.
Standardization is possible by linking OPC UA to the SINUMERIK User Management.

SSH access rights

SSH access rights are currently linked to the SINUMERIK role and cannot be separated from the SINUMERIK Operate login. This means that anyone who can log in via SINUMERIK Operate can also access the system via SSH.

See also

SINUMERIK ONE password policies (Page 137)

11.8.3 SINUMERIK Integrate Lock MyCycles

Using the "SINUMERIK Integrate Lock MyCycles" (cycle protection) function, cycles can be encrypted and then stored protected in the control. Cycles are encrypted outside the control system using the SINUMERIK 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.

11.8.4 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).

Know-how protection with the TIA Portal

With the help of know-how protection, you can also protect blocks in the TIA Portal against unauthorized access with a password. More information can be found in the TIA Portal online help under "Programming the PLC > Protecting blocks > Protection of blocks".

11.9 Protecting data at rest

11.9.1 Encrypting an SD card

Definition

Encrypting SD cards is a security measure where data saved on the card (security data, Linux authorization data configuration data) are encrypted to improve integrity protection and knowledge protection. If you have encrypted the SD card, then the data can only be read with the device which was used for encryption.

Purpose of encrypting SD cards

SD card encryption is primarily intended to protect your data if the SD card was removed from its intended control system and is externally accessible (e.g. when stolen or when connected to an external PC). Encryption offers the following specific advantages:

- **Integrity and access protection for external access**: Encryption prevents the content of the SD card from being manipulated or read out by unauthorized third parties if the card is connected outside the associated control system to an external PC or to another device. Only the control system that was used to encrypt the data, can decrypt and use this data.

  Note

  This encryption is not intended to prevent accessing the data if the SD card is inserted in your control system and is accessed via its interfaces (e.g. SSH).

- **Knowledge protection for theft:** If the physical SD card is stolen, all of the data on it are individually encrypted and therefore unusable by any attacker.

Encrypted folder

SINUMERIK SD card encryption involves a partial encryption, where the complete SD card is not encrypted but only the relevant folders.

The content of the following folders, including all subfolders, are encrypted:

- /oem
- /user

Preconditions

Note

Function "SD card encryption" is not available for distributed systems.

Note

The Security archives / Security restore password was already set

The Security archives / Security restore password (Page 111) is a precondition for encrypting the SD card. It is required in order to restore access to the encrypted SD card.

Note

Setting not part of the security archive

Note that the SD card encryption setting is not saved in the security archive, and can only be manually activated/deactivated.

- With active user management: You have the role "Security Admin" or at least "Service".
  OR
- Without active user management: You have at least access level 3 (end user).

Procedure

Start SD card encryption by calling the function via SINUMERIK Operate under "Security > HMI security > SD card encryption".

Restoring access to an encrypted SD card

If you wish to access the data of the encrypted SD card from an NCU/PU other than the NCU/PU that was used to encrypt the data, then you can do this using a special function provided in SINUMERIK Operate (Page 144).

More information

More information on using function "SD card encryption" is provided in the SINUMERIK online help as well as the following documentation:

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

11.9.2 Restoring the SD card encryption

Definition

In practice, the hardware on which the key for the SD card encryption is stored may be replaced.

If an encrypted SD card is run up with a new NCU, then SINUMERIK Operate runs up and cannot read out the data of the encrypted SD card or the data of the encrypted security memory.

To avoid having to completely reconfigure the data, you can use the Security archive / Security restore password to restore the SD card encryption.

You require this function in the following use cases:

- **Restoring the SD card encryption**:
  - New NCU: Hardware, on which the key is saved, was replaced
  - The key is corrupt/incorrect.
- **Deleting encrypted memory (folder /oem and /user)**:
  - You have forgotten or lost the Security archives / Security restore password.

Requirements and procedure

Note

Function not available for distributed systems with IPC

This function is restricted to NCU-only systems.

Note

Security archives / Security restore password

The Security archives / Security restore password (Page 111) is a requirement for restoring the key for decrypting the SD card.

⚠ CAUTION

Functional restrictions when restoring the SD card encryption

- It is not possible to use an external VNC viewer via the company network as the settings are reset to default settings.
- The default firewall settings apply again.
- SSH access is only possible using standard passwords.

- The SD card was not able to be correctly decrypted and after running up SINUMERIK Operate displays Alarm 150438.
- You are logged in with the standard Legacy password "Manufacturer" or "End user".

Restoring the SD card encryption

In the "Setup" operating area, select restoration of SD card decryption using softkeys "Security > HMI security".

After entering the Security archives / Security restore password and a restart, the SD card encryption and the security memory are restored. The encrypted /oem and /user folders are again readable and encrypted; the saved security settings are again available and you can authenticate yourself using user management.

Deleting an encrypted folder

- The SD card was not able to be correctly decrypted and after running up SINUMERIK Operate displays Alarm 150438.
- You are logged in with the legacy passwords of role "Manufacturer" or role "End user".

If you forgot or lost the Security archives / Security restore password, as last resort you can delete the encrypted /oem and /user folders.

In the "Setup" operating area, select memory deletion using softkeys "Security > HMI security".

NOTICE
Data loss When deleting the memory, the following data are permanently deleted or reset to the factory settings: • **For encrypted SD card**: – Complete folder /oem and /user. This security memory is part of this folder. – Login data for user management

After the restart, the encrypted data on the SD card are deleted and folders /oem and /user are empty. You can now login with role "End user", read in a security archive that has been generated and subsequently newly encrypt the SD card.

More information

More information on using function "Restoration of SD card decryption" is provided in the SINUMERIK online help as well as in the following documentation:

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

See also

Restoring security data (Page 113)

11.9.3 IPC Bitlocker hard disk encryption

Definition

BitLocker is a security function that provides encryption for all data carriers of the PC system. At the same time, risks as a result of data theft or data disclosure due to lost, stolen or inappropriately decommissioned devices are avoided. The data carriers can only be used with the assigned PC system. When using the data carrier in another PC system, without the appropriate certification, all data remain encrypted and cannot be used.

You can set up the BitLocker function for automatic management via script or you can manually manage this via Microsoft Windows Explorer.

SINUMERIK Operate functions if your hard disk is encrypted with BitLocker

Purpose of the Bitlocker hard disk encryption

The BitLocker hard disk encryption offers a whole raft of advantages, which improve the protection of your data and security:

- **Full drive encryption**
  BitLocker encrypts the complete drive, including the operating system, programs and user data. As a consequence, all of the information saved on the drive are secure.
- **Hardware-based encryption**
  BitLocker uses the **Trusted Platform Module (TPM)** or a USB key to secure the decryption process. This prevents unauthorized users from accessing the data.
- **Protection against theft and loss**
  Even if a laptop or a hard disk is stolen, the data stored on it are secure and cannot be decrypted without having the right key.

Note

To increase the security of your data, we recommend that you always encrypt the hard disk of your IPC. This especially applies if you have saved your part programs on the hard disk of your IPC.

NOTICE
Encrypted data no longer accessible For data carrier decryption, in the case of service or an emergency, an active BitLocker always requires a restore password. If the BitLocker restore password is lost, then access to encrypted data can be denied. Always save the password outside the system to prevent data loss or data misuse.

Requirement

- You have an IPC with Trusted Platform Module (TPM), e.g. BX-39A. Older models, such as the IPC 427E, do not support BitLocker hard disk encryption.
- PCU base software /IPC from version 15 SP3, including Paragon Hard Disk Manager software™ 17 Suite
- Administration rights for the PC system

Backup & restore

Observe additional notes for data backup and restore with encrypted hard disk provided in Chapter IPC backup and restoration (Page 114).

More information

More information on activating BitLocker hard disk encryption via Microsoft Windows or for service purposes using script is provided in the following manuals:

- Commissioning Manual SINUMERIK ONE "PCU Base/IPC" (https://support.industry.siemens.com/cs/ww/en/view/109925791)

11.9.4 Protecting part programs

To ensure the security and integrity of a CNC machine, it is also important to protect saved SINUMERIK part programs from misuse.

NOTICE
Data misuse If you do not protect your saved SINUMERIK part programs, an attacker can access the saved part programs, sabotage the machine or steal sensitive information. Therefore, protect your saved part programs, independent of the data storage location.

Possible storage locations for part programs

You can store SINUMERIK part programs at the following locations on the control system:

- NCK memory
- "NC Extend" folder on the SD card
- "NC Extend" folder on the IPC
- On a network drive

Protective measures

Depending on the storage location, we recommend the following protective measures to protect your data in the best possible way:

- **NCK memory:** Currently, part programs are not protected in this memory. We therefore recommend that you save your part programs either in the "NC Extend" folder or on a network drive.
- **"NC Extend" folder on the SD card**: Encrypt your SD card (Page 143).
- **"NC Extend" folder on the IPC**: Encrypt your hard disk using the BitLocker hard disk encryption (Page 146).
- **On a network drive**: Apply general protective measures to protect network drives. Comply with the regulations recommended by your company.

Cycle protection

If you wish to protect your cycle files, then you can encrypt the cycle files (Page 141).

11.10 Secure communication

11.10.1 Overview

Application of secure communication protocols

The following secure communication protocols are provided in the SINUMERIK ONE system for the following use cases:

- External communication to the company network:
  - **OPC UA**
  - **SMB V3**
- Internal communication:
  - **OPC UA**: Standardized, industrial communication protocol for access to control data
  - **HTTPS**: Communication with the PLC's internal web server via Secure Sockets Layer (SSL)
  - **Secure Open User Communication** (Secure S7): Message-oriented data exchange to remote CPU or software controllers
  - **SMB V3**: Connection of network drives:
  - **SSH**: Access to the file system of the NCU

Data streams

You will find a graphical illustration of all data streams (protocols) between the system components system in the Data flows and data memory (Page 59) section.

Secure communication protocols in the network context

You will find a description of the secure communication protocols in the network context in Protection status of SINUMERIK networks (Page 69) section.

11.10.2 Overview

Application of secure communication protocols

The following secure communication protocols are provided in the SINUMERIK 828D system for the following use cases:

- External communication to the company network:
  - **OPC UA**
  - **SMB V3**
- Internal communication:
  - **OPC UA**: Standardized, industrial communication protocol for access to control data
  - **HTTPS**: Communication with the PLC's internal web server via Secure Sockets Layer (SSL)
  - **Secure Open User Communication** (Secure S7): Message-oriented data exchange to remote CPU or software controllers
  - **SMB V3**: Connection of network drives:
  - **SSH**: Access to the file system of the PU/PPU

Data streams

You will find a graphical illustration of all data streams (protocols) between the system components system in the AUTOHOTSPOT section.

11.10.3 OPC UA

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

With the SINUMERIK Integrate Access MyMachine /OPC UA software option, variables of a SINUMERIK can be read and written using 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 functions (only applicable for SINUMERIK ONE), such as 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 48).

11.10.4 HMI security

11.10.4.1 SMB and NFS server protocol settings

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 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.

11.10.4.2 SSH network protocol

You can make the following settings to improve the security level of the SSH server on the NCU/PU:

Deactivate legacy access for SINUMERIK Operate via a standard key

Via SSH, SINUMERIK also provides the option of accessing the NCU/PU file system. SINUMERIK Operate on the IPC also uses SSH to access the NCU/PU. For basic commissioning/maintenance, the NCU/PU allows SINUMERIK Operate to be accessed based on a fixed standard key.

The SSH key is automatically individualized by pairing an NCU/PU with the IPC (Page 125). This step is not necessary for NCU/PU-based systems.

Beyond this, the change involves protection against brute force attacks (wait time after incorrect login, 30 seconds).

However, the SSH standard key can still be used. **As a consequence, it is recommended to manually deactivate the standard key** to prevent access based on the standard key.

⚠ CAUTION

Data misuse by compromising the SSH standard key

The legacy access for SSH connections via a standard key represents a security risk. If this standard key is compromised (e.g. by an external IPC), then an attacker can access system data.

- Therefore, de-activate the legacy access for SSH connections via the standard key in SINUMERIK Operate under Security > HMI security.

Note

By deactivating the SSH standard key, you exclude all non-paired devices from an SSH connection!

However, you have the following options if you still wish to establish an SSH connection to non-paired external devices:

- **SSH connection to a non-paired IPC**: using software "WinSCP" ™, "PuTTY" ™ or via SINUMERIK Access MyMachine/ P2P
  - With user management activated: User name and password
  - Without activated user management: Access level and password
- **SSH connection to SINUMERIK Edge, SINUMERIK commissioning tool or HMI base application on an external device**
  - Import a private SSH key or activate the legacy access in SINUMERIK Operate.

Auto-logoff function

SINUMERIK provides the option of configuring an auto-logoff function for the SSH connection:

Note

The auto-logoff function of the SSH server is not available for distributed systems.

Note

Activating the auto-logoff function

To improve the security level, on the NCU/PU/PPU, you should activate the "Auto-logoff function" after a time that can be individually configured. In this way you ensure that remote access via SSH is not inadvertently maintained for an excessively long time, therefore providing an unnecessary attack surface.

You can activate/deactivate the SSH server auto-logoff function at the NCU/PU/PPU via SINUMERIK Operate "Security > HMI security".

More information

More information on the topic of SSH, the precise operating description or a description of how you can import a private SSH key is provided in the SINUMERIK online help or in the SINUMERIK ONE "Final commissioning steps" (https://support.industry.siemens.com/cs/ww/en/view/109817139) commissioning manuals and SINUMERIK 828D "SINUMERIK Operate" (https://support.industry.siemens.com/cs/ww/en/view/109823589).

See also

Commissioning Manual 828D "PCU Base for IPC" (https://support.industry.siemens.com/cs/ww/en/view/109823590)

Commissioning Manual SINUMERIK ONE "PCU Base for IPC" (https://support.industry.siemens.com/cs/ww/en/view/109925791)

Authorizations with SSH access

Depending on your SINUMERIK role, you have certain authorizations with SSH access in certain folders. The following table shows an overview of the authorizations depending on the assigned SINUMERIK role. The SINUMERIK roles in the table refer to both classic access level management and SINUMERIK user management.

SINUMERIK role	Authorized action in the folder							
	/card/user		/card/oem		/var/log		card/install/cmc	
	Read	Write	Read	Write	Read	Write	Read	Write
Manufacturer	x	x	x	x	x	-	x	x
Service	x	x	x	- [1]	x	-	x [2]	-
End user	x	x	x	-	x	-	x	-

[1] If the file has different rights than the folder, then it is possible that files might have changed, but none deleted or added.

[2] Only for CMC and saved in TRA

11.10.5 Secure web server communications via HTTPS

For example, if you wish to work with the SINUMERIK PLC web server, a secure connection (via HTTPS) between the web browser of SINUMERIK Operate and the web server is decisive to protect configuration data and to guarantee system integrity.

Basic procedure

- The following settings for the NCU-PLC web server were first made in the TIA Portal:
  - HTTPS was activated
  - It was defined via which Ethernet interface the PLC web server should be accessible
  - The web server certificate was exported and transferred to the SINUMERIK control system.
- Import the web server certificate via "Security > Certificate memory > Import". In the additional import dialog menu "Use", select "Web server certificate".

More information

- Principle of operation of the certificate memory from the security perspective (Page 115)
- SINAMICS Industrial Cybersecurity Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109999221), Chapter "Establishing a protected HTTPS connection to the web server"
- Detailed information on how you import a certificate into the certificate store is provided in the SINUMERIK Operate online help.
- The web server is configured using a dedicated softkey in the SINUMERIK Operate menu "Commissioning > HMI > Operating area menu"

11.10.6 Network security and firewall

11.10.6.1 Overview

Concerning network security, it is assumed that the protective measures from section "Network security (Page 39)" 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)

11.10.6.2 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.

Firewall of the NCU

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.

Firewall of the IPC

The Microsoft Windows Firewall settings on your PC system are appropriately configured by PCU-Basesoftware/IPC for the use of SINUMERIK software and systems. For security reasons,

the Microsoft Windows Firewall is activated in the company network and expanded by additional rules. The Microsoft Windows Firewall is deactivated in the system network.

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.

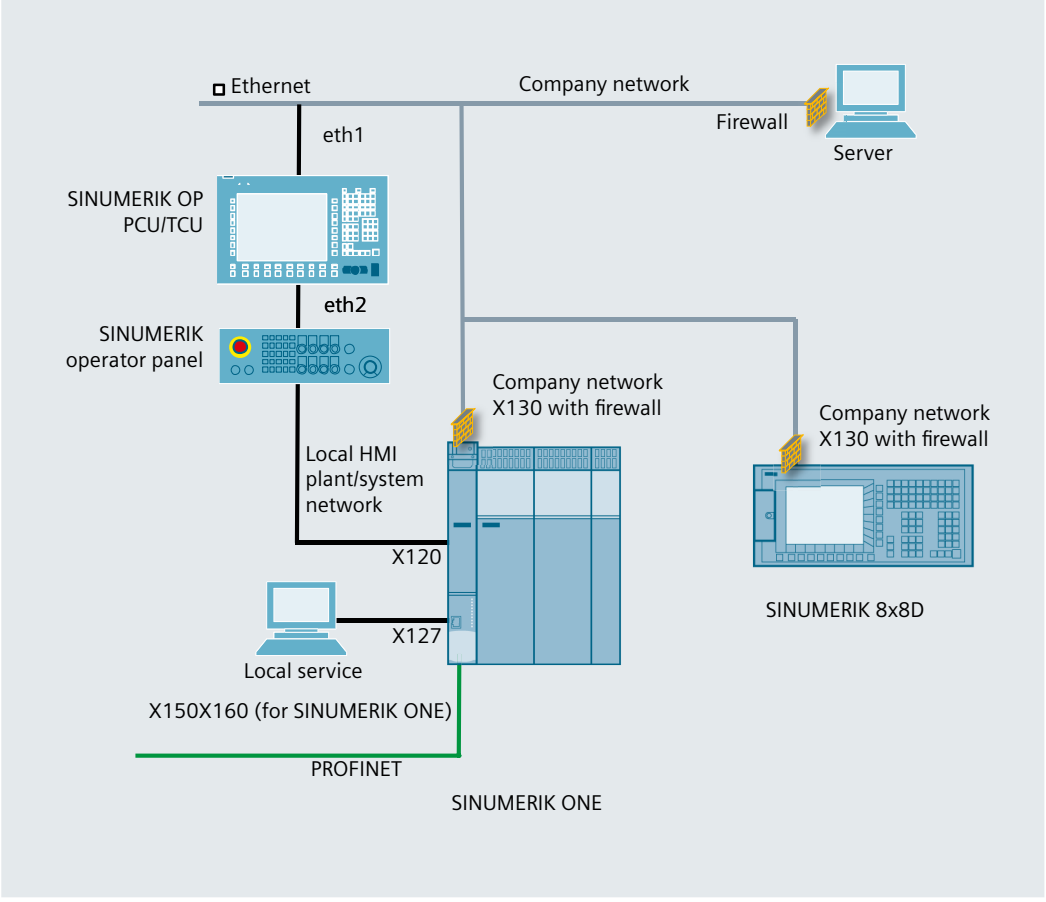


Figure 11-10 Networking of NCU/IPC

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.

More information

More information about the recommended firewall settings for IPC is provided in the following manuals:

- Commissioning Manual SINUMERIK ONE "PCU Base for IPC" (https://support.industry.siemens.com/cs/ww/en/view/109925791)

See also

Commissioning Manual SINUMERIK 828D "SINUMERIK Operate" (https://support.industry.siemens.com/cs/ww/en/view/109823589)

11.11 Security Eventlog

11.11.1 Overview of Security Eventlog

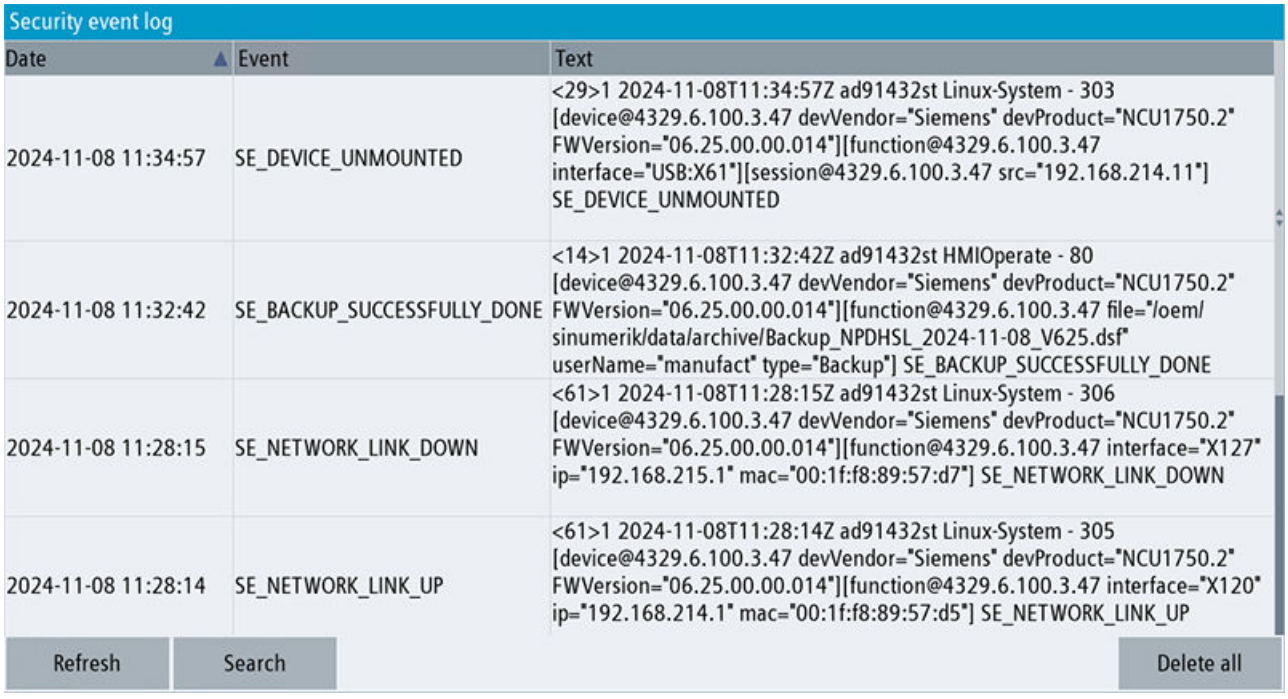
The Security Eventlog is used to record and provide security events of the SINUMERIK system and supports system and security administrators when monitoring all events that take place in a factory.

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.

The SINUMERIK 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.

Further, events are also kept locally for a certain time until the NCU or IPC is restarted and can be viewed in SINUMERIK Operate.
The Security Eventlog is only accessible to authorized persons and can only be deleted by authorized persons.

An example from a Security Eventlog is shown in the following diagram:



You can sort security-relevant events either in ascending or descending order according to date and time. As standard, the latest event is displayed right at the top.

You have the option of configuring a buffer memory limit value for events. An alarm is triggered if this limit value is reached.

Note

Personal data are processed and stored in the Security Eventlog.

If a SINUMERIK system is distributed via IPC and NCU, then the IPC and NCU must be paired so that the Security Eventlog functions.

If several NCUs are paired with an IPC, then each NCU transfers the Security Eventlog to the paired IPC. The IPC sends these Security Eventlogs to the external SysLog server.

If the pairing between the NCU and the IPC is lost, then the Security Eventlogs of the NCU are not sent to the Syslog server.

If the IPC is restarted or run down, all security-relevant events from the IPC are deleted.

After the restart, all security relevant events are deleted.

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

Note

If a Syslog server or Security Information and Event Management (SIEM) is neither configured nor available, then older security events are overwritten in SINUMERIK Operate. The security events are not persisted.

11.11.2 Requirement for Security Eventlog

For the "Security Eventlog" security function to correctly function, it is imperative that the correct date and time have been set in the system (Page 85).

NOTICE
Incorrect sequence of security events If the date and time are incorrectly set in the SINUMERIK system, then the security events cannot be recorded in the correct sequence in time. • This is the reason that before using the Security Eventlog for the first time, carefully check whether the date and time settings of your system correspond to the correct actual time, and if required change the time settings using the recommendations referenced below.

If a SINUMERIK system is distributed via IPC and NCU, then the IPC and NCU must be paired so that the Security Eventlog functions.

11.11.3 Features of Security Eventlog

The Security Eventlog logs the events relevant to security according to IEC 62443-4-2.

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

Approx. 500 events are stored in the Security Eventlog. After this, the events are overwritten by new events.

The last 500 entries in the Security Eventlog are displayed in SINUMERIK Operate in 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.

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

Both a central SysLog server and a Security Information and Event Monitoring (SIEM) System enable a holistic view of the IT security to be obtained 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

The system automatically checks the syslog server connection every 10 minutes if the connection is disconnected. When the server becomes available, the connection is automatically re-established.

Data are transferred encrypted as standard in order to guarantee data security to the syslog server.

Encryption and decryption are performed using certificates for TLS (Transport Layer Security). For encrypted communications with the Syslog server, only High Security Cipher Suites are supported.

Note

Using UDP

Data are transferred unencrypted if you use UDP (User Datagram Protocol). Anybody can record data traffic in the network and check data content.

A server certificate is required when setting up the connection to the Syslog server. The client certificate is optional. You must import both certificates from the certificate store.

More information

- You will find more information on the structure of the Security Eventlog in the List Manual "Security Eventlog Lists".
- More information about cipher suites for TLS encryption is provided in the SINUMERIK Operate online help.

11.11.4 Transmission of events relevant to security

The stored events relevant to security are transmitted to a central SysLog server or a Security Information 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) or unencrypted (UDP). For the encrypted transfer, the server certificate or a root certificate, to which the server certificate is traced, must be imported into Operate.

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 Information 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.

11.11.5 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
- Security process

The security host, also known as the security process, is a security-related system component that is responsible for configuring and managing security policies, as well as for authentication and secure pairing between the IPC and the NCU. The security process is a source for the security events in the Eventlog.

11.12 Reduction of the attack surface

11.12.1 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:

- AUTOHOTSPOT
- Physical protection of critical production areas (Page 37)

11.12.2 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.

11.12.3 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.

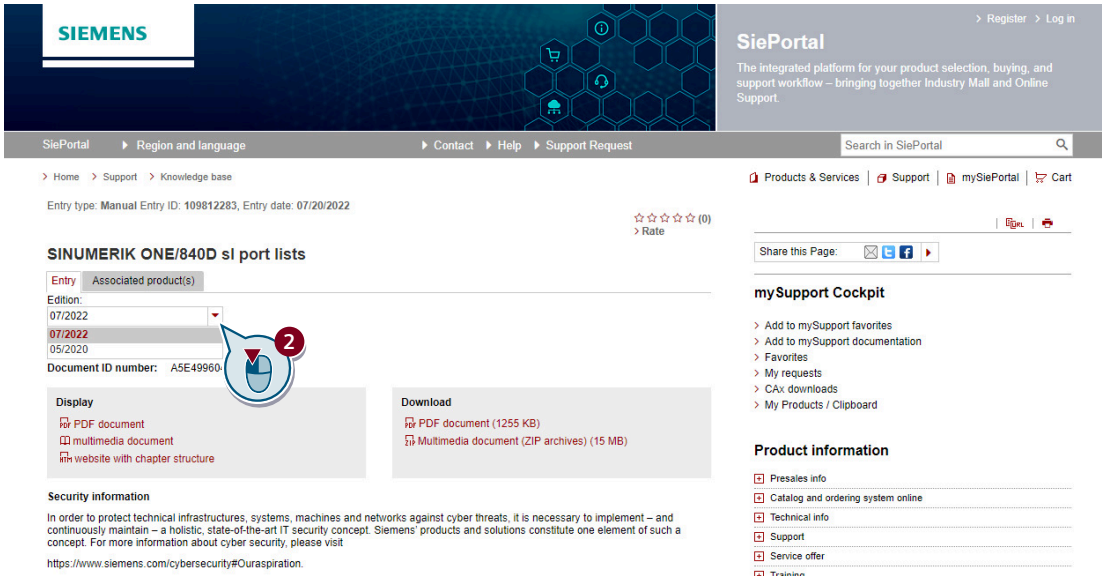


Figure 11-11 Selection of edition in SiePortal

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.

11.13 Protection against manipulation

NOTICE
Misuse, manipulation and theft Modules, such as NCUs/PUs, 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/PUs in housings and locked control cabinets or in electrical rooms. Only appropriately trained and authorized personnel may access these housings, electrical cabinets and electrical rooms. Information on the permitted locks can be found in Chapter Physical protection of critical production areas (Page 37). • **More information** on installing an NCU/PU in a control cabinet is provided in the corresponding Equipment Manuals for SINUMERIK ONE.

11.13.1 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 11-12 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

12

Options for secure configuration of the product are described in Chapter Security functions of the product (Page 81). 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.

12.1 Recommendations for secure operation of the product

To ensure secure operation, the assumptions listed in Chapter General security measures and concepts (Page 33) should be complied with. Carefully work through the Checklist of all hardening measures (Page 74) and make the required settings.

Further, the following recommendations apply:

- Activate the SINUMERIK user management (Page 89)
- 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.
- If you work in a distributed system comprising an IPC and NCU, check whether you have established a relationship of trust through pairing.
- 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.
- 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.
- Perform backups regularly. (Page 109)
- Ensure that the NCU/PU is only accessible to authorized personnel.
- Protect your network according to the cell protection concept (Page 39).
- SINUMERIK Operate on the IPC should run under a normal user account. Do not use an administration account.
- Check the software signature
  Checking software signatures (Page 185) Check whether the delivered software actually originates from Siemens or whether it has been modified prior to delivery.
- Check whether you have set the security archive/restore password.
- Check whether you have set the password for PLC access level as well as the password for PLC configuration data.
- 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.

12.2 Recommendations for security-related maintenance tasks

Maintenance tasks

You can perform the following maintenance tasks in regular cycles to guarantee a high degree of security for your system:

- Regularly check that the authenticity label on the NCU (Page 165) is not damaged.
- Regularly check whether important system certificates have expired (Page 115), and if this is the case, then renew them.
- Regularly check that your password policies (Page 137) fully comply with current standards and/or company policies.
- Change your VNC password at regular intervals.
- Regularly create backups (Page 109):
  - Archives
  - IPC image
  - SD card image
- Regularly check that the installed software is up to date and install updates (Page 179).
- Regularly check your firewall settings (Page 155).
- Regularly check your date and time settings (Page 85).
- Regularly check the connection status of your Security Eventlog server (Page 158).
- Regularly check the Windows version of your IPC and install the latest updates (Page 182).
- Regularly check - especially after replacing hardware - the activity status of the BitLocker hard disk encryption (Page 146) and after replacing the NCU, the status of the SD card encryption (Page 143).

See also

Checking software signatures (Page 185)

12.3 Recommendations for secure product disposal

12.3.1 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.

12.3.2 Securely disposing of the NCU

From version V6.24, SINUMERIK ONE in conjunction with the appropriate SINUMERIK service system allows the memory of the SINUMERIK ONE to be securely and reliably deleted when it is decommissioned.

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 used are securely and reliably deleted **before disposing of the NCU**: Follow the handling recommendations referenced below for reliably and securely deleting data.

NOTICE
Misuse of data resulting from withdrawing the SD card unnoticed during a deletion operation While being deleted, unauthorized persons can withdraw the SD card if the deletion operation is executed via a remote connection. Data can be misused in this way. • Therefore always securely and reliably delete the NCU and the SD card directly at the machine and never via a remote connection. It is not permissible that the machine is unsupervised during the complete deletion operation.

Data storage media included

The subsequently listed data storage media installed in SINUMERIK ONE can potentially include customer data and must be securely and reliably deleted before disposal.

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

Initializing the PLC

NOTICE
Observe the run sequence Before you securely delete the memory of the NCU and the SD card using the service system, you must first delete the **PLC user program** when the control system runs up. This deletes the internal PLC memory and the retentive data is initialized. **More information** on the precise PLC initialization sequence is provided in the appropriate chapter in the Installation Manual "New installation and upgrade" (https://support.industry.siemens.com/cs/ww/en/view/109925794).

Securely and reliably deleting the memory of the NCU and SD card

You can automatically and securely delete the memory of the NCU and the SD card using the "SINUMERIK service system" under menu item " Change network settings > Secure Disposal".

More information about the "SINUMERIK service system" as well as a precise description of the handling steps to securely delete the NCU and SD card are provided in the Installation Manual "New installation and upgrade" (https://support.industry.siemens.com/cs/ww/en/view/109925794).

Note

- As a consequence, only delete the memories if you are certain that you wish to dispose of the NCU.
- You must reinstall the SD card if you inadvertently deleted the NCU memory. **More information** can be found in the Installation Manual "New installation and upgrade" (https://support.industry.siemens.com/cs/ww/en/view/109925794).

Note

Physically destroying SD cards

SD cards are flash memories with defect management and if at all possible these can also be physically destroyed after they have been securely deleted.

More information

More general 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.

12.3.3 Securely deleting the IPC

Paragon™ and other external applications support reliably and securely deleting data from your Microsoft Windows IPC. Paragon™ is provided when installing PCU Base for IPC.

Software "Paragon Disk Wiper" ™ is one way of securely deleting data on the hard disk(s) of your IPC. It offers various deletion methods, including:

- Overwriting data: Data is overwritten a multiple number times with random information.
- Physical destruction: You can physically destroy the hard disk if absolute security is mandatory.
- Encryption and subsequent deletion of the key: Encrypt the hard disk and then delete the encryption key.
- Secure formatting: Use the integrated "Wipe Data" function to securely format your hard disk.

Note

Regarding this topic, always comply with the security recommendations provided by your company.

More information

More information is provided in the following documentation:

- Paragon™ online help
- Commissioning Manual SINUMERIK ONE PCU Base Software/IPC (https://support.industry.siemens.com/cs/ww/en/view/109925791)
- Commissioning Manual SINUMERIK 828D PCU Base Software/IPC (https://support.industry.siemens.com/cs/ww/en/view/109823590)

Security-critical system states

13

13.1 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 174)
- Operating system with access to the SD card (Page 176)
- Access to the Linux file system with CMC with USB stick (Page 177)

13.2 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.

13.3 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 PU 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 PU and operate the service system is explained in the Internet (https://support.industry.siemens.com/cs/ww/en/view/109822107).

After the PU has run up and the service system unzipped, 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 828D Commissioning Manual "CNC commissioning" (https://support.industry.siemens.com/cs/ww/en/view/109823588).

Protective measures

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

13.4 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.

13.5 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.

Security updates

14

14.1 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.

14.2 Checking the software version

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.

14.3 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).

14.4 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 older operating systems. This can leave the operating system with dangerous security vulnerabilities. • If you are using an operating system for which no more updates are provided, 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 39).

15 Tips for security checks

15.1 Verification of security functions

Checklist with test cases

After successful security commissioning, you can check whether the activated security mechanisms are working as desired.

You will find a checklist with test cases in the following documentation: Commissioning Manual Final steps for commissioning (https://support.industry.siemens.com/cs/ww/en/view/109817139).

15.2 Verification of security functions

Checklist with test cases

After successful security commissioning, you can check whether the activated security mechanisms are working as desired.

You will find a checklist with test cases in the following documentation: Commissioning Manual SINUMERIK 828D "SINUMERIK Operate" (https://support.industry.siemens.com/cs/ww/en/view/109823589).

15.3 Checking software signatures

15.3.1 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. In addition to these digital signatures, cryptographic hashes are used 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.

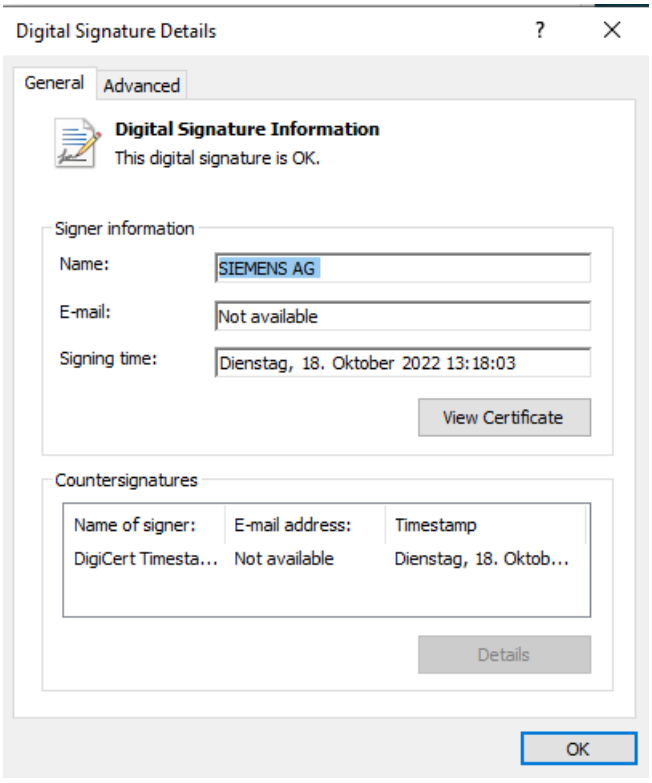


Figure 15-1 Digital signatures properties

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.

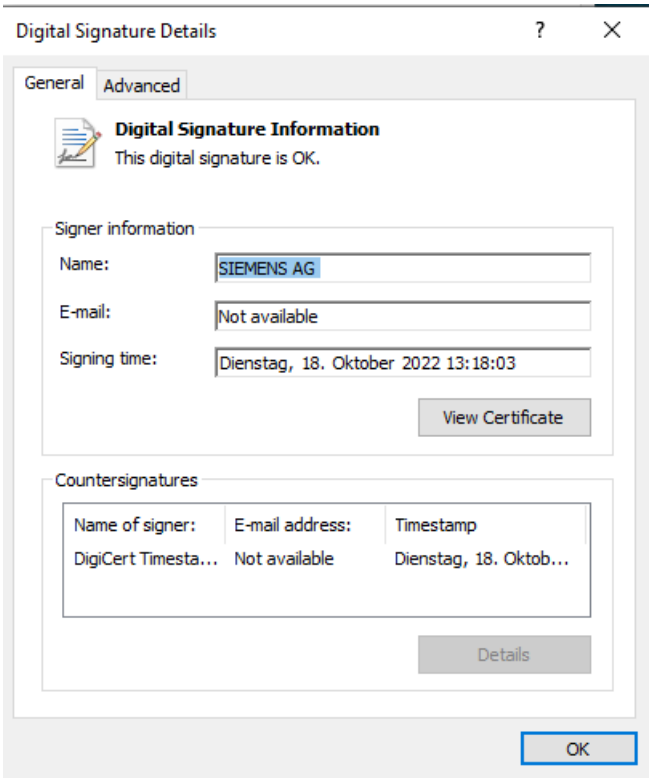


Figure 15-2 Digital signatures details

Check result

NOTICE
Software code manipulated or damaged If the signature check shows that the checked software is **not digitally signed**, this indicates that the software code has been manipulated or damaged. • In this case, contact your Siemens support immediately.

See also

How do you check the digital footprint of an installation file (.exe) after download from the SiePortal? (https://support.industry.siemens.com/cs/ww/en/view/109995833)

How do I determine the SHA-256 or SHA-512 checksum of a file? (https://support.industry.siemens.com/cs/de/de/view/109483101/en)

15.3.2 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".

NOTICE
Software code manipulated or damaged If the signature check shows that the checked software is **not digitally signed**, this indicates that the software code has been manipulated or damaged. • In this case, contact your Siemens support immediately.

- 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://assets.new.siemens.com/siemens/assets/api/uuid:a23d3578-6a5c-4256-9168-8bf2ce5ec172/PPKI-Infra-CPS.pdf)
- Certificate policy (https://assets.new.siemens.com/siemens/assets/api/uuid:f48da8a8-e51b-4628-b1da-00a6e3fb6651/PPKI-Infra-CP.pdf)
- Digital ID information (http://www.siemens.com/industrial-security/pki)

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

Designates the totality of all potential entry points and vulnerabilities that an attacker can utilize to penetrate a system, network or an application. This also includes digital components, such as open ports and insecure software as well as physical components, such as unprotected devices and social elements, such as employees who can be victims of phishing attacks. The larger the attack surface, the more options the attacker has to compromise the system. It is therefore important to minimize the attack surface using suitable security measures.

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

Process where the identity of a person or a system is checked. Generally, this is realized by checking logon information such as user name and password, biometric data (e.g. fingerprint or face ID) and additional identification methods. The objective of the authentication is to ensure that only authorized persons or systems are granted access to resources or information.

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.

Cipher Suites

Defined combinations of encryption algorithms that are used to establish secure network connections. You define which algorithms are used for encryption, authentication and key transfer. Cipher Suites are frequently used in protocols, such as TLS (Transport Layer Security) and SSL (Secure Sockets Layer), where they guarantee data transfer security on the Internet.

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.

Data at rest

In the IT environment, data at rest are data that are resident on a computer data memory in any digital form. Compare with "Data in motion".

Data in motion

Data during transfer, as well as data in motion and data in transit, are data that are being transferred between source and destination, typically in a computer network. Compare with "Data at rest".

Defense in Depth

"Defense in Depth" is a multi-level defense system according to IEC 62443 "Industrial communication networks - IT security for networks and systems". Cybersecurity measures are applied at all levels (physical, technical and administrative) and stages (plant security, network security and system integrity). The measures start with the security fence around the company grounds and continues down to the network protocol level and its layers.

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.

Deterministic output

A deterministic output signifies that for the same input, a system or algorithm always returns the same output. This is an essential feature of deterministic algorithms, whose essential characteristics include predictability and consistency. An example of this is the Euclidean algorithm for calculating the greatest common divisor (GCD), which always yields the same result for the same input values. In automation technology, a deterministic output signifies that the deterministic behavior is decisive for the predictability and the reliability of automated processes. An example of this is an industrial robot, which when mounting components, always executes the same movements assuming it receives the same commands. This predictability is especially important in security-critical applications where deviations can result in dangerous situations.

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.

File authenticity

The authenticity of files refers to the genuineness and trustworthiness of a file. A file is considered authentic if it actually originates from the specified source and was neither manipulated nor falsified. Authenticity is frequently guaranteed using digital signatures or certificates, which confirm that the file originated from a trusted issuer and was not changed since it was first created.

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

Process to configure and secure systems, networks and applications so that they are as resilient as possible to attacks and security threats.

Measures:

- Remove services and applications that are not required
- Closing security vulnerabilities
- Applying security updates and patches
- Implementing firewalls and intrusion detection systems
- Setting up stronger access and authentication types

IANA

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

Incident handling

Describes the organized process with which an organization responds to a cybersecurity incident or a security breach and how it manages this.

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 of files

The integrity of files verifies that a file is unchanged and complete since it was originally created or was last modified by an authorized body. The file is free of any unauthorized changes, corruption and losses. The integrity of files is a central security aspect, especially in domains such as data security, information security and data transfer.

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.

Intrusion Detection System (IDS)

An IDS monitors networks and systems for suspicious activities or security violations. An IDS analyzes data traffic and system activities for anomalies and known attack patterns. If a potential threat is identified, IDS notifies the administrators so that these measures can be applied.

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.

Least Functionality principal

The "Least Functionality" principle means that systems and applications should provide only the strictly necessary functions and services required to perform their tasks. This reduces the attack surface and minimizes potential security risks.

Least Privilege principle

The "Least Privilege" principle is an information security concept, where users are only assigned the access rights and authorizations that they absolutely require to perform their tasks. This minimizes the risk of security breaches, as less damage would be inflicted via the accounts of less privileged users if they were to be compromised.

Example: Users with low privileges can only read data but they cannot change it. The Least Privilege principle means that a certain user account only has the access rights that are actually required to execute the tasks of the specific role - not more, not less.

Legacy code

Code in modern software, that was not written in compliance with today's security guidelines for software development and therefore represents a security risk.

Legacy code cannot be removed or replaced as nobody understands the code any longer and it was either poorly documented or not documented at all.

Logging

Logging security events involves acquiring and saving security-relevant events and activities within an IT system. The logs contain detailed information about security-relevant system configurations.

The main objectives of security event logging include:

1. Monitoring and identifying
   Identifying unusual or suspicious activities that could indicate security incidents.
2. Analysis and investigation
   Providing data for forensic analysis when security incidents occur.

3. Compliance
   Satisfying legal and regulatory requirements.
4. Reporting
   Generating reports about security-relevant events and trends for management and other stakeholders.

Security event logging is an essential component of a comprehensive security management system.

Malicious code

Designates malicious software or program code designed to cause damage to computer systems, networks or data.

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.

Need-to-Know principle

An individual (person or system component) should only have access to the information, resources or systems that they absolutely need to fulfill their assigned tasks and responsibilities.

Non-repudiation

If the principle of non-repudiation is satisfied in a system, transactions, notifications or actions can be uniquely assigned to a person or system. Non-repudiation is frequently achieved using cryptographic methods such as digital signatures, which establish a unique, unambiguous link between an action and its originator.

Example: Digital signatures for emails and documents uniquely identify the sender of a message and its original state.

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.

Personal data

Personal data is any information relating to an identified or identifiable natural person.
A person is considered to be identifiable if they can be identified directly or indirectly, specifically through the assignment of an identifier, such as a name, an identification number, location data, online identifier or to one or more specific attributes. These identifiers allow conclusions to be drawn about a person's physical, physiological, genetic, psychological, economic, cultural or social identity.

Examples of personal data include:

- Name
- Address
- Date of birth
- Telephone number
- Email address
- IP address
- Account data

Personal data is particularly important in the context of data protection and the General Data Protection Regulation (GDPR), which governs the protection and processing of personal data.

Phishing

A phishing attack is a cyberattack in which attackers use fraudulent emails, text messages, phone calls or websites to trick people into revealing sensitive information, such as passwords, credit card numbers, or other personal data.

Typical attributes of a phishing attack are:

- Falsified sender addresses: At first glance it appears that the messages are coming from a trusted source.
- Urgency: The messages create a sense of urgency or fear in order to prompt the victims to react quickly.
- Links to fake websites: Frequently, these websites look authentic but they are designed to steal personal data.

Privacy by design

The objective of privacy by design is to integrate data protection and the private sphere right from the start in the process of developing products, services and systems.

The concept is based on seven fundamental principles:

1. Proactive instead of reactive measures
   Data protection problems are prevented before they occur.
2. Data protection as default setting
   Personal data are automatically protected without users having to take action.
3. Data protection integrated in the design
   Data protection is an integral component of the overall system.
4. Full functionality
   Data protection measures do not restrict system functionality.
5. End-to-end security
   Data protection measures cover the complete lifecycle of data.
6. Transparency
   All those involved are informed about data protection measures.
7. Respect for the private sphere of the user
   The focus is on the requirements and expectations of the user.

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.

RSS feed

An RSS feed (Really Simple Syndication Feed) allows website operators to publish content in a standardized format. RSS feeds are frequently used on message pages, blogs and podcasts to continually provide users with new content. An RSS feed comprises an XML file, which contains structured information, such as title, description and date of publication of new content.

To subscribe to an RSS feed:

1. Selecting the RSS reader: You require an RSS reader. There are many free and paid options, such as Feedly, Inoreader or The Old Reader.
2. Finding the RSS feed URL: Visit the web site from where you wish to subscribe to the RSS feed. Search for the RSS icon (generally an orange icon) or a link that refers to the RSS feed.
3. Copying the RSS feed URL: Right click on the RSS icon or the link and select "Copy link address" or a similar option.
4. Inserting a URL in the RSS reader: Open your RSS reader and insert the copied URL into the corresponding field (e.g. under "Add new feed" or similar) to subscribe to the feed.
5. Read feed: You can now read the latest content of the subscribed website directly in your RSS reader.

SCADA

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

Secure by default

"Secure by default" (also called "Security-by-default") signifies that software or systems are designed and configured so that in their default settings they provide the highest possible level of security. Therefore, to achieve a high security level it is not necessary that user parameters are adapted. Existing security functions are automatically activated.

Examples: Two-factor authentication when logging on or automatically blocking phishing mails in email programs

Security

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

Security advisory

A security advisory is a notification that provides detailed information about identified vulnerabilities in the software or hardware. Generally, these advisories are published by manufacturers or security organizations to inform users about potential risks and to provide instructions on how to resolve vulnerabilities or minimize the risk.

Security guidelines

Security guidelines are formal rules and techniques, which define how the security of information, systems and networks within an organization should be guaranteed. These guidelines are for employees and IT teams to ensure that all security measures are consistently and effectively implemented. They encompass domains such as access controls, password management, data security, emergency restoration, network security and reaction to security incidents.

Security Information and Event Management (SIEM)

SIEM combines functions for real-time monitoring, identification and response to security incidents. SIEM systems capture and analyze protocol data from various sources within a network, e.g. from firewalls, servers, applications and end devices. These data are correlated in order to identify suspicious activities and anomalies.

Session hijacking

In network environments, for open but inactive sessions, attackers can attempt to take over the active session or pose as legitimate user.

SIEM system (Security Information and Event Management)

Software solution designed to capture, analyze and correlate security data from various sources in order to identify potential threats and security incidents.

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.

Two-factor authentication

Two-factor authentication (2FA), frequently called multifactor authentication (MFA), is a security technique where users must provide two different types of authentication to confirm their identity and obtain access to a system, an application or a service.

VPN (Virtual Private Network)

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

Vulnerability

A vulnerability is a location in a system, an organization or a process that is prone to disturbances, attacks or failures. In IT and OT security, the term often refers to security vulnerabilities in the software that attackers can utilize to obtain unauthorized access to systems or inflict damage.

Vulnerability examples include:

- Software bugs: Error in the code that causes security gaps.
- Unpatched systems: Systems that do not have the latest security updates.
- Human error: Carelessness or a lack of security awareness on the part of employees.

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.

Zero Trust

With a zero trust concept, initially, every user and/or device is expressly not trusted. This behavior is independent of whether the user or the device is located inside or outside the company network. Instead, all access queries are checked and authenticated before access to resources is granted. Zero Trust involves continually checking the identity and the security status of users and devices as well as implementing strict access controls and monitoring mechanisms.

Zero-day vulnerability

A zero-day vulnerability is an error in an application or operating system that has not yet been identified. A security vulnerability for which there is no protection or patch as the software manufacturer does not know that it exists - he has "zero days" to prepare for an effective response.

Index

A

Access Control, 106
Access types, 140
Account management, 140
Accounts, 139
Active directory link, 140
Adware, 133
Allowlists, 135
    Malicious code, 133
Anti-virus program, 49
Archive restoration
    Decoupling, 112
    Pairing, 112
Authentication Outside principle, 92
Authentication type, 140
Authentication types, 140

B

Basesys.ini
    Time data, 85
BIOS password, 132
Block encryption
    SINUMERIK, 142
Brute force attacks, 153

C

Central security administrator, 98
central user management, 94
    NCU system, 94
    NCU&IPC system, 95
Certificate store, 115
Change
    Password, 48
Cloud, 44
Cloud Applications, 44
Cloud Security, 44
Company security, 37
Confidentiality levels, 48
Create MyVirtual Machine, 83
Cycle protection, 148

D

Data
    transporting, 48
Daylight saving time, 85
Decommissioning, 171
Deleting data storage media, 171
Disposal, 171
DMZ network, 40
Domain
    User domain, 95
Domains
    Manufacturer domain, 95

E

Employee
    left the company, 112
    terminated, 112
Essential system functions, 56
Exchangeable storage medium, 48

F

Firewall, 40

H

Hard disk, 48
Hardened Linux, 133

I

ID assigned more than once, 104
ID-based login, 91
Import
    Web server certificate, 154
Initializing the PLC, 171
IPC pairing certificate
    automatically renew, 129
ISO-on-TCP, 149, 150

L

Least Privilege, 106

Legacy access
Deactivate, 152
local user management, 92
NCU & IPC system, 93
NCU system, 92
Lock MyCycles
SINUMERIK Integrate, 141

M

Machine roles, 96
Main entry, 116, 142
Malicious code
Allowlists, 133
Virus scanner, 133
Malicious code mechanisms, 133
Microsoft Windows Security, 134
Microsoft Windows user management, 140
Multi-factor authentication, 83

N

NCK (Numerical Control Kernel), 140
NCU pairing certificate
automatically renew, 129
Need-to-Know, 106
Non-repudiation, 130

O

OPC UA SINUMERIK access, 140
Operation
real machine, 83
virtual machine, 83

P

Pairing certificate
automatically renew, 129
Part programs, 148
Password
Change, 48
Characters, 48
Complexity, 48
Inputs, 48
Length, 48
Safe, 48
Password quality, 48
Passwords, 139
PLC access, 140
PLC engineering access, 140
PLC OPC UA access, 140
PLC user program
securely deleting, 171
PLC web server access, 140
Ports, 46
Preventing unauthorized access, 106
Production security, 37
Proper and intended use
Requirements, 63
Protection zone, 39

R

Ransomware, 133

S

SAC, 135
Safety Integrated log file, 130
Same ID, 104
SCALANCE S, 40
Secure Boot
BIOS, 132
IPC, 132
NCU, 132
Secure Open User communication, 72
Secure Open User Communication, 149, 150
Secure S7, 72, 149, 150
Securely deleting, 171
Security Admin
central, 98
End user, 88
Manufacturer, 88
Security Admin password
Forgotten, 99
Security Eventlog
Events, 161
Properties, 161
Transmission to server, 161
Security management process, 31
Security Module
SCALANCE S, 40
Services, 46
Session hijacking, 106
Set date, 85
Set the NTP server, 85
Set the time server, 85
Set time, 85
signed code, 133
Single Sign-On (DSSO) principle, 92

SINUMERIK
    Block encryption, 142
SINUMERIK Integrate
    Lock MyCycles, 141
SINUMERIK OPC UA, 141
SINUMERIK Operate access, 140
SINUMERIK service system, 171
SINUMERIK user management, 140
Smart App Control, 135
Spyware, 133
SSH, 152
    Auto-logoff function, 153
SSH access, 140
SSH access rights, 141
SSH standard key
    Deactivate, 152
Standard time, 85

T

Time data
    basesys.ini, 85
Transport
    Data, 48
Trojan horses, 133
Types of authorization, 90

U

USB stick, 48
User accounts, 47
User groups, 97
User management
    Advantages, 88
    Differences to authorization with access levels, 87
    Purpose, 88
Users, 97

V

Virtual machine, 83
Virus protection program, 49
Virus scanner, 49
    Malicious code, 133
Viruses, 133
VNC access, 140
VNC SINUMERIK access, 140

W

Web server certificate
    import, 154
Web server communications, 154
Web server connection, 154
Windows Server Update Service, 51, 182
Worms, 133
WSUS, 51, 182

X

X.509 standard, 116