SIEMENS

SINUMERIK/MACHINUM/SINAMICS

Motion Control
Industrial cybersecurity

Configuration Manual

Introduction 1

Fundamental safety instructions 2

What is industrial cybersecurity? 3

Why is industrial cybersecurity so important? 4

Security measures in automation and drive technology 5

Security management 6

General security measures 7

Product-specific security measures 8

References A

03/2025
A5E53888693B AB

Legal information

Warning notice system

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

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

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

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

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

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

Trademarks

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

Disclaimer of Liability

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

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
GERMANY

A5E53888693B AB
Ⓟ 02/2025 Subject to change

Copyright © Siemens 2015 - 2025.
All rights reserved

Table of contents

1 Introduction 7

1.1 About industrial cybersecurity 7

1.2 About this documentation 8

1.3 Feedback on the technical documentation 10

1.4 mySupport documentation 11

1.5 Service and Support 12

1.6 OpenSSL 14

1.7 General Data Protection Regulation 15

2 Fundamental safety instructions 17

2.1 General safety instructions 17

2.2 Warranty and liability for application examples 18

2.3 Cybersecurity information 19

3 What is industrial cybersecurity? 21

4 Why is industrial cybersecurity so important? 23

4.1 Trends with an impact on industrial cybersecurity 23

4.2 Possible corporate security vulnerabilities 24

5 Security measures in automation and drive technology 25

5.1 Security measures 26

5.2 Siemens Industrial Holistic Security Concept 27

5.3 Standards and regulations 28

6 Security management 29

7 General security measures 31

7.1 Defense in depth concept 32

7.2 Plant security 34

7.2.1 Physical protection of critical production areas 34

7.3 Network security 36

7.3.1 Network segmentation 36

7.3.1.1 Separation between production and office networks 36

7.3.1.2 Network segmentation with SCALANCE S 37

7.3.2 PROFINET products and SNMP 41

7.3.3 Cloud Security 41

7.3.4 Smart sensors (IoT) in the network 42

7.4 System integrity 45

7.4.1 System hardening 45

7.4.1.1 Services and ports ... 45
7.4.1.2 User accounts ... 45
7.4.1.3 Operating units used in the industrial context ... 46
7.4.1.4 Store sensitive data securely ... 46
7.4.1.5 Transporting sensitive data securely ... 47
7.4.1.6 Passwords ... 47
7.4.1.7 Virus scanner ... 48
7.4.1.8 Allowlists ... 48
7.4.1.9 Product security notifications ... 49
7.4.2 Patch management ... 49
7.4.2.1 Product software ... 50
7.4.3 Data integrity ... 50
7.4.4 Checking software signatures ... 51
7.4.4.1 Manually checking software signatures under Windows ... 51
7.4.4.2 Automatically checking software signatures under Windows ... 52
7.4.5 Disposal ... 54

8 Product-specific security measures ... 55

8.1 SINUMERIK ... 56
8.1.1 Firewall and networking ... 56
8.1.2 Physical protection of the NCU ... 58
8.1.3 Machine control panels - SINUMERIK (MCP/MPP) ... 58
8.1.4 System hardening ... 59
8.1.4.1 Deactivating hardware interfaces ... 59
8.1.4.2 Communication services and used port numbers ... 60
8.1.4.3 Integrity and authenticity protection ... 60
8.1.5 Virus protection ... 60
8.1.5.1 Positive list ... 61
8.1.5.2 Virus protection / memory card ... 62
8.1.6 Security updates / patch management ... 62
8.1.7 Account management ... 63
8.1.7.1 Definition of access levels ... 63
8.1.7.2 Safety Integrated password ... 65
8.1.7.3 CNC lock function ... 66
8.1.7.4 Deleting the preinstalled SSH key ... 66
8.1.7.5 PLC web server ... 67
8.1.7.6 Access levels for softkeys ... 67
8.1.7.7 BIOS and AMT access protection ... 67
8.1.7.8 Password protection for Create MyConfig (CMC) ... 68
8.1.8 Know-how protection ... 68
8.1.8.1 SINUMERIK Integrate Lock MyCycles ... 68
8.1.8.2 SINUMERIK Integrate Lock MyPLC ... 69
8.1.8.3 OPC UA ... 69
8.1.8.4 User administration in the TIA Portal ... 70
8.1.8.5 SIMATIC Logon ... 71
8.1.9 Data backup ... 71
8.1.10 Disposal ... 72

8.2 MACHINUM (CNC Shopfloor Management software) ... 73
8.2.1 System overview ... 73
8.2.2 Cloud applications (In Cloud) ... 73
8.2.2.1 Manage MyMachines ... 74
8.2.2.2 Manage MyMachines /Remote ... 75

8.2.2.3 Analyze MyPerformance/Mcenter ... 76
8.2.2.4 Manage MyMachines/Mcenter ... 77
8.2.2.5 Access MyData/Collector ... 78
8.2.3 PC/Server/Desktop applications (In Line) ... 80
8.2.3.1 Mcenter ... 80
8.2.3.2 Cloud mode ... 83
8.2.4 ACM-Suite ... 84

8.3 SINAMICS ... 85
8.3.1 Network security ... 85
8.3.2 Know-how protection ... 86
8.3.3 Parameters: Access levels and password ... 87
8.3.4 Using the memory card ... 87
8.3.5 Safety Integrated ... 88
8.3.6 Backing up and restoring data ... 89
8.3.6.1 Backup and restore ... 89
8.3.6.2 Redundant data backup ... 90
8.3.6.3 Redundant_backup_more_info ... 90
8.3.7 Communication services and used port numbers_Further_information ... 91
8.3.8 Communication services and used port numbers ... 91
8.3.9 Integrated web server ... 91
8.3.9.1 Certificates for the secure data transfer ... 92
8.3.10 Information about individual interfaces ... 93
8.3.11 Disposal ... 95
8.3.12 SINAMICS Startdrive and TIA Portal ... 96
8.3.12.1 Malfunctions of the machine as a result of incorrect or changed parameterization ... 96
8.3.12.2 SINAMICS Startdrive ... 96
8.3.12.3 SINAMICS STARTER ... 97
8.3.13 SINAMICS Drive Control Chart (DCC) ... 99
8.3.13.1 Industrial cybersecurity with SINAMICS DCC ... 99
8.3.13.2 Use write and know-how protection ... 102
8.3.14 SINAMICS Smart Access Module ... 102

8.4 SIMOCRANE ... 104

A References ... 105

Glossary ... 109

Index ... 117

1 Introduction

1.1 About industrial cybersecurity

Digitalization and the increasing networking of machines and industrial plants are also increasing the risk of cyberattacks. Appropriate protective measures are therefore mandatory, especially for critical infrastructure facilities. 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.

Visit our website for more information on Industrial cybersecurity (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html).

1.2 About this documentation

Content

The "Industrial Cybersecurity" documentation contains the necessary measures and information for planning and configuring plants and systems. The documentation serves as a reference manual and guideline. This documentation cannot and does not want to suggest that there is 100% security because the current range of threats is much too diverse and complex. This documentation includes all of the necessary measures that should be taken into account for configuring systems in a secure environment. This documentation is intended to support machine manufacturers in safely operating their controls or plants. You, as operator, are responsible for implementing the security measures.

Target group

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

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

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

- Administration of the IT technologies familiar from the office environment
- Configuring the products used:
  - SINUMERIK
  - MACHINUM (Shopfloor Management Software)
  - SIMOTION
  - SINAMICS
  - SIMOCRANE

Structure

The manual is essentially divided into three parts:

- Description of the industrial cybersecurity topic in the industrial context
- General security measures: This chapter describes universal measures you can take in general - regardless of the product used - to make your system secure
- Product-specific security measures: In this chapter - structured according to MC products - special functionalities of the products are explained, which you can use to protect your system.

Restricted product validity

SINUMERIK

The document is generally valid for all SINUMERIK control systems/software products with the following exception:

- For SINUMERIK ONE control systems from CNC software version V6.23, there is a specific "Industrial Cybersecurity" Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109925842), which only describes the general and product-specific security functions of SINUMERIK ONE as of CNC software version V6.23.
- For the SINUMERIK 828D control system from CNC software version V5.24, there is a specific "Industrial Cybersecurity" Configuration Manual, which only describes the general and product-specific security functions of SINUMERIK 828D as of CNC software version V5.24.

SINAMICS

The document is generally valid for all SINAMICS converters with the following exception:

- For SINAMICS converters from firmware version V6.1, there is a specific "SINAMICS Industrial Cybersecurity" Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109955569), which only describes the general and product-specific security functions of SINAMICS converters from firmware version V6.1.

Standard scope

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

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

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

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

Websites of third-party companies

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

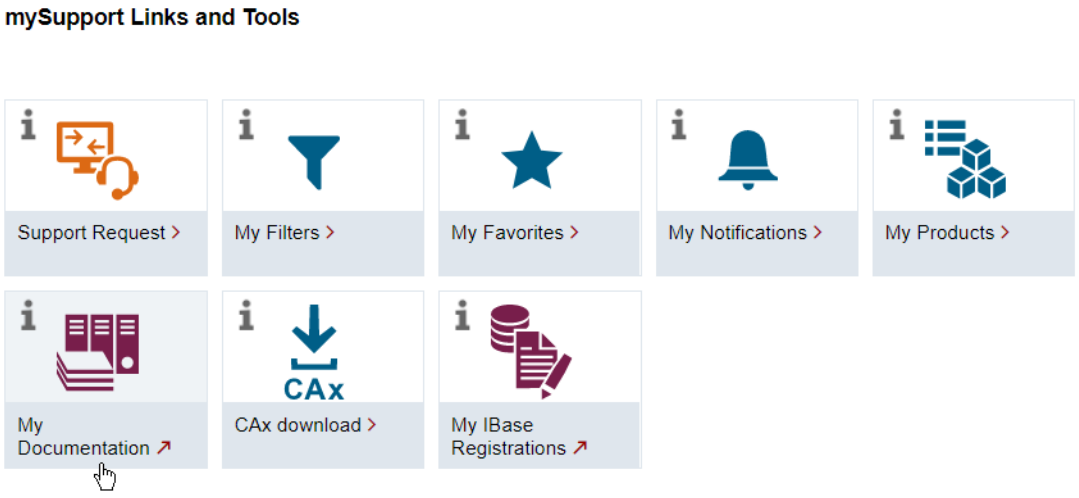
1.3 Feedback on the technical documentation

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.

1.4 mySupport documentation

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

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



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

Note

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

1.5 Service and Support

Product support

You can find more information about products on the internet:

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

The following is provided at this address:

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

Technical support

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

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

Training

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

Siemens support on the go



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

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

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

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

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

1.6 OpenSSL

This product can contain the following software:

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

You can find more information on the internet:

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

1.7 General Data Protection Regulation

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

For this product, this means:

The product does not process or store any personal data, only technical function data (e.g. time stamps). If the user links this data with other data (e.g. shift plans) or if he/she stores person-related data on the same data medium (e.g. hard disk), thus personalizing this data, he/she must ensure compliance with the applicable data protection stipulations.

Fundamental safety instructions

2

2.1 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.

2.2 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.

2.3 Cybersecurity information

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

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

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

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

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

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

Further information is provided on the Internet:

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

What is industrial cybersecurity?

3

Definition of industrial cybersecurity

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

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

Objectives of industrial cybersecurity

The objectives of industrial cybersecurity encompass:

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

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

Why is industrial cybersecurity so important?

4

4.1 Trends with an impact on industrial cybersecurity

Global trends

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

- Cloud computing in general
  The number of network connections across the world is constantly increasing. This increasingly enables technologies such as cloud computing and the associated applications. In conjunction with cloud computing, there has been a massive increase in the number of mobile devices, such as cell phones and tablet PCs.
- Wireless technology
  On the other hand, the increasing use of mobile devices has only become possible thanks to the ubiquitous availability of mobile networks. Wireless LAN is also becoming increasingly available. The development of new WLAN and mobile radio standards continues to advance.
- Worldwide remote access to plants, machines and mobile applications
- The Internet of Things (IoT)
  Millions of electronic devices are now network-capable and are communicating via the Internet.

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

4.2 Possible corporate security vulnerabilities

Possible corporate security vulnerabilities

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

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

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

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

Possible threats:

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

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

Possible effects of a security incident

- Loss of intellectual property
- Loss of production or reduced product quality
- Negative company image and economic damage
- Catastrophic environmental influences
- Danger to people and machines

Security measures in automation and drive technology

5

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

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

5.1 Security measures

Integration of security into the products

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

- The requirements specified in IEC 62443-4-1 for the **product lifecycle management (PLM) process** are implemented. The implementation was certified by TÜV.
- **Code analyses** are used to identify and correct possible errors.
- Siemens implements **measures to secure integrity** in its products and its manufacturing processes.
- Siemens constantly checks the measures relating to **hardening**:
  - Operating systems are configured in such a way that **points of attack** (e.g. via ports, unneeded services) are **minimized**.
  - Siemens **tests its products** to detect weak points at an early stage.
  - Siemens checks its products for security weak points during development and performs appropriate **patch management**.
  - As manufacturer of automation and drive products, Siemens supports secure operation through direct support of system integrators and operating companies **by providing patches, security components and the appropriate services.**

Protection of the development infrastructure and supply chains

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

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

See also

Secure digitalization - holistic approach (https://www.siemens.com/global/en/company/digital-transformation/cybersecurity.html)

5.2 Siemens Industrial Holistic Security Concept

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

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

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

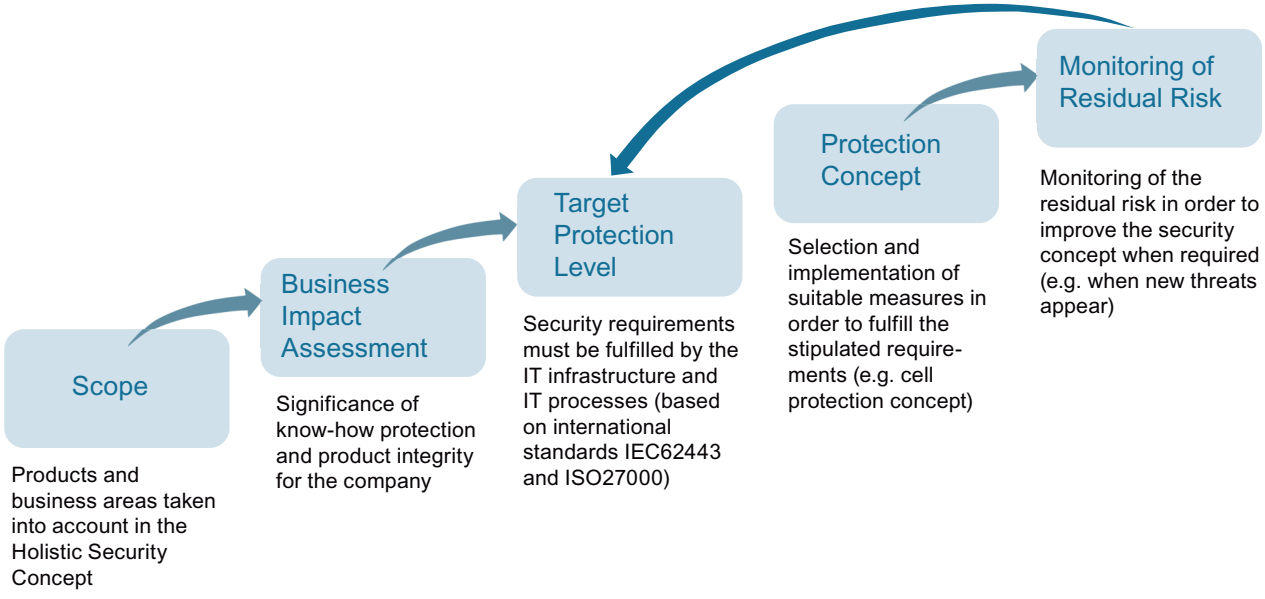


Figure 5-1 SI HSC security management process

5.3 Standards and regulations

Siemens takes the applicable industrial cybersecurity standards and regulations into consideration throughout the entire development process:

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

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

Security management

6

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

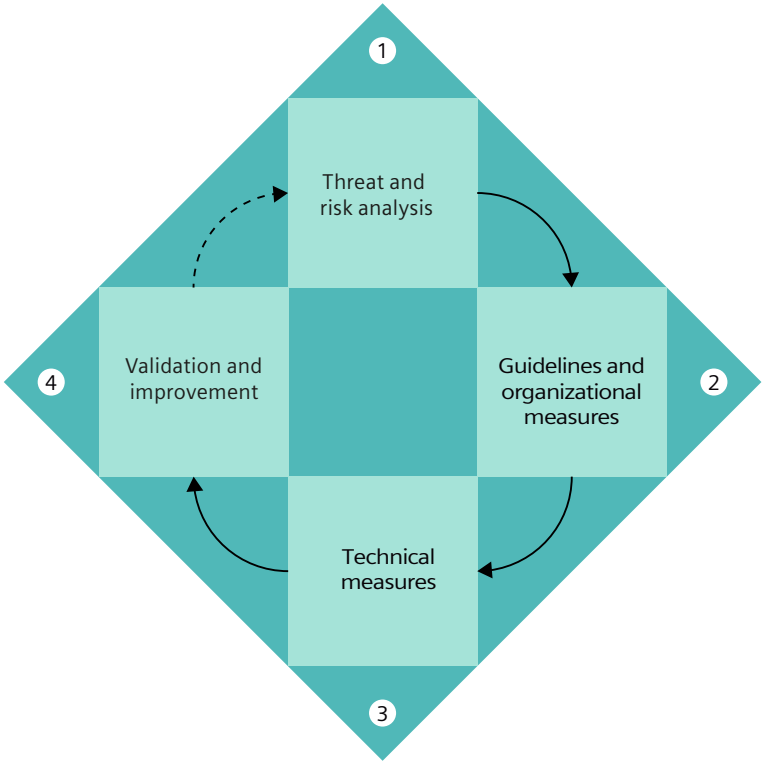


Figure 6-1 Security management process

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.

See also

General security measures (Page 31)

Product-specific security measures (Page 55)

General security measures

7

In this chapter you will learn about the general security measures you must take in order to protect your system from threats.

Additional specific security measures for SINUMERIK, SIMOTION and SINAMICS products can be found in Section Product-specific security measures (Page 55).

7.1 Defense in depth concept

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

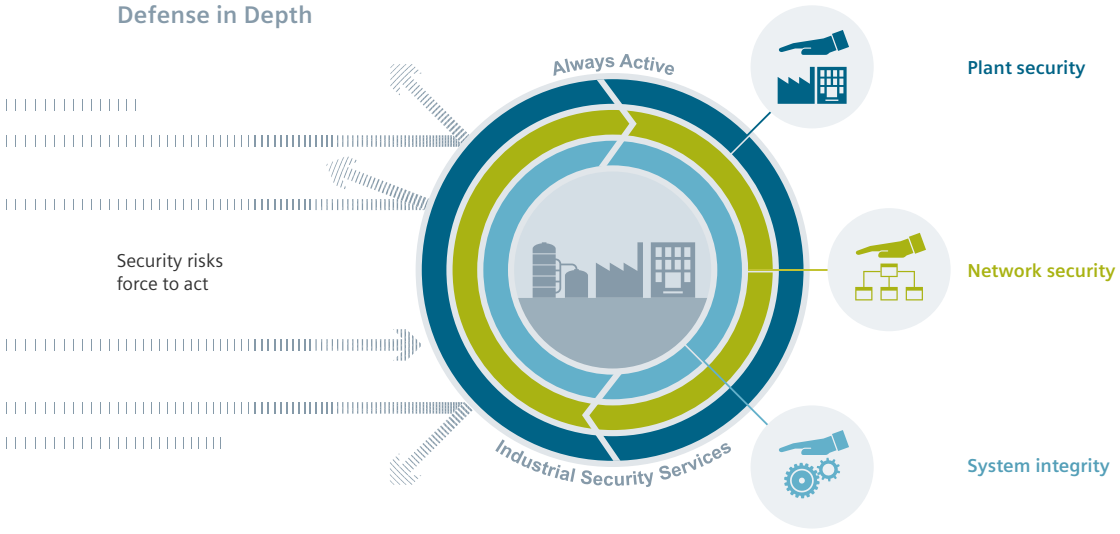


Figure 7-1 Defense in depth strategy

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

Protection levels

A defense in depth model has a three level structure:

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

7.2 Plant security



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.

7.2.1 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
- 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

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

7.3 Network security



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.

7.3.1 Network segmentation

7.3.1.1 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 "Network segmentation with SCALANCE S (Page 37)".

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.

See also

System hardening (Page 45)

7.3.1.2 Network segmentation with SCALANCE S

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

Requirement

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.

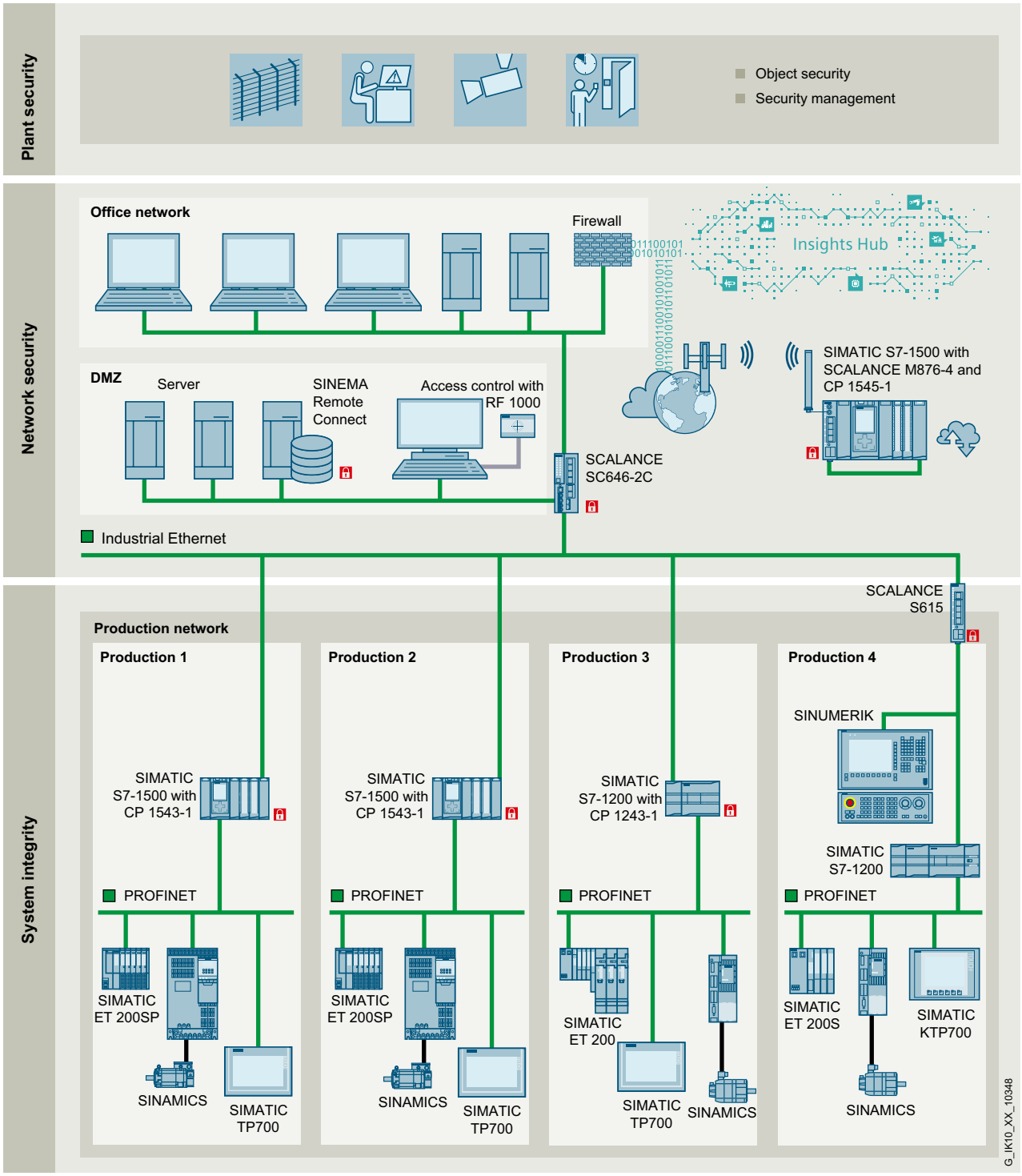


Figure 7-2 SCALANCE S application example

More information

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

Network security with SCALANCE S Industrial Cybersecurity Appliance

See also

SCALANCE S security modules (https://siemens.com/scalance-s)

VPN access

Note

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

7.3.2 PROFINET products and SNMP

Note

Products with PROFINET provide the option of reading out and writing to parameters via **SNMP** (**S**imple **N**etwork **M**anagement **P**rotocol, Port 160/161).

- Do not only identify components based on their SNMP parameters alone, but also use the information provided on the type plate (e.g. MAC address, serial number, etc.).

7.3.3 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.

- Companion Guide for Cloud - CIS Organization (https://www.cisecurity.org/press-release/cis-controls-companion-guide-for-cloud-now-available/)
  - CIS Controls Cloud Companion Guide
- Matrix Cloud Control - CSA Organization (https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/)
  - Cloud Controls Matrix
  - Top Threats

Siemens Cloud solutions

The following addresses provide information about Siemens cloud management solutions:



Figure 7-3 Siemens Cloud solutions

- Overview of Siemens Cloud portfolio (https://www.sw.siemens.com/portfolio/cloud)
- Industrial Cloud Computing (https://www.plm.automation.siemens.com/global/en/our-story/glossary/industrial-cloud-computing/58773)

7.3.4 Smart sensors (IoT) in the network

IoT sensors or smart sensors (e.g. IP cameras) perform analog measurements in the physical world. In addition to the actual measured quantity acquisition, they also combine the complete signal conditioning and signal processing in one enclosure. They process data, exchange data, and even apply their own algorithms to it.

This interaction with the physical world made possible by IoT sensors can result in significant cybersecurity and privacy risks:

⚠ WARNING

Risks when using IoT sensors

- Analog measured values can be easily manipulated (light intensity, temperature, voltage can be falsified).
- The increasing use of IoT sensors can involve the acquisition of enormous amounts of private and sensitive data, which must be handled with confidentiality.
- IoT sensors are also used to protect sensitive areas. In a worst-case scenario, a security attack on such a device could put human lives at risk, cause significant property damage, or result in production downtime or the like.
- IoT network interfaces often enable remote access to physical systems. Manufacturers, vendors and third parties are thus able to remotely access IoT devices for management, monitoring, maintenance and troubleshooting purposes. As a result, the physical systems that are accessible via the IoT may be at much greater risk of security attacks than before.
- Many IoT devices must meet strict requirements regarding performance, reliability, resilience, security, and other objectives. These requirements may conflict with general security requirements and regulations in the company (e.g. regular security patches and updates).
  Whereas non-smart sensors rely exclusively on local networking, Internet networking in smart sensors allows attacks from any location in the world that has Internet access, increasing the machine's exposure and thus the risk of attacks.

Become aware of these risks, consider these risks in your risk analysis, and take appropriate measures to protect your system/plant.

Measures when using IoT sensors



Figure 7-4 Smart sensors

Due to the risks mentioned above, keep the attack surface as small as possible when using IoT sensors and implement the following measures:

- Ensure a secure transmission between sensor and our product (SINUMERIK, Edge, SINAMICS). If possible, use smart sensors with integrated security measures (e.g. integrity protection of communication).
- Ensure self-protection of the sensor (e.g. unique identifiability, redundancy in signal processing (principle of functional safety)).
- Use only smart sensors that are compliant with the law.
- Secure physically vulnerable areas through physical measures (Siemens Industrial Holistic Security Concept (Page 27), Defense in depth concept (Page 32)).

More information

You can obtain more useful information on the topic of "Safe use of IoT sensors" on the Internet from the following sources:

- Only relevant for Germany: Basic IT protection compendium from the Federal Office for Information Security (BSI) (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-it-gs-comp-2019.html?nn=409850)
- Open Web Application Security Project® (OWASP) (https://owasp.org/www-project-internet-of-things/#div-seek_and_understand)
- Internal Report NISTIR 8228 (https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf).

7.4 System integrity



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.

7.4.1 System hardening

7.4.1.1 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.

7.4.1.2 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.

7.4.1.3 Operating units used in the industrial context

Recommendations

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

To minimize risk, take the following security measures:

- The deployed operating unit is set up, administered, regularly checked and patched by the appropriate departments. In terms of the secure configuration of an operating unit, this means:
  - Programs and operating systems are installed on the operating unit only if they are supported and regularly serviced by the manufacturer.
  - Security updates and patches for the installed operating system are regularly installed on the operating unit.
    You can find more information on patch management in Windows operating systems in Chapter "Patch management (Page 49)".
  - A virus scanner is installed on the operating unit and regularly updated. In addition, "Allowlists (Page 48)" and "Network segmentation with SCALANCE S (Page 37)" methods can be used.
  - 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 administrators should have admin rights to the operating unit.
- Only use the deployed operating unit in secured cells. The operating unit must not be used in the office network or via the Internet.
  You can find more information about the separation of the office and automation networks in Chapter "Separation between production and office networks (Page 36)".
- 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.

See also

User accounts (Page 45)

7.4.1.4 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:

- Consequentially mark your documents according to confidentiality levels based on the 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 back up your sensitive data. Protect the backups against unauthorized access, loss and manipulation.

7.4.1.5 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.

7.4.1.6 Passwords

Recommendations

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 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 the 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

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

7.4.1.7 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.

7.4.1.8 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)

See also

Product-specific security measures (Page 55)

7.4.1.9 Product security notifications

Recommendations

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

Therefore, always keep yourself up to date about new and relevant product security announcements for your products: "Industry Online Support (https://support.industry.siemens.com/cs/ww/en/)". Comply with the instructions provided in the product security notifications.

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

7.4.2 Patch management

Windows Server Update Services (WSUS)

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

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

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

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

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

More information

You can find more information about network segmentation in Chapter Network segmentation (Page 36).

7.4.2.1 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.

7.4.3 Data integrity

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.

NOTICE

Corruption of data and the resulting malfunctioning of the system

For automation and drive systems as well as controller components, data such as archives 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 archives, programs, and OA applications can also be saved and archived. The systems currently do not provide the capability of ensuring the integrity of programs, archives, and OA applications.

Therefore take your own measures for ensuring integrity to guarantee the data integrity of your archives, OA applications, or other saved data:

- Apply the Siemens Industrial Holistic Security Concept.
- 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.

7.4.4 Checking software signatures

7.4.4.1 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.

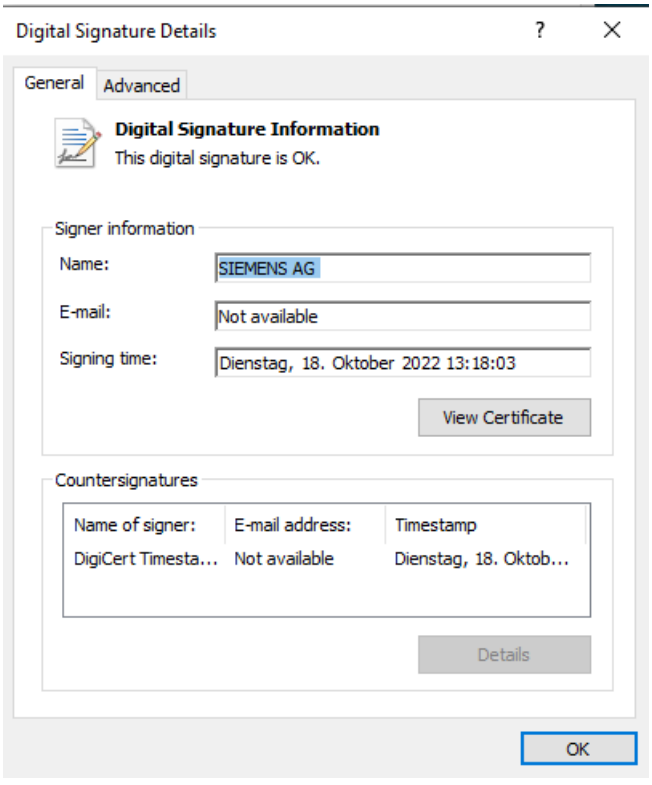


Figure 7-5 Digital signatures properties

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.

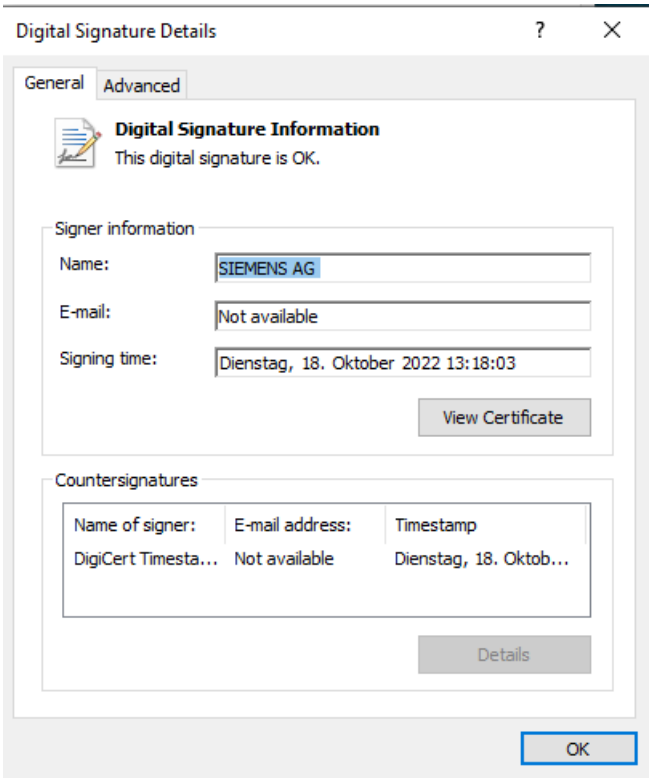


Figure 7-6 Digital signatures details

7.4.4.2 Automatically checking software signatures under Windows

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

Download Microsoft Sigcheck

Note

Preconditions

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

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

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

Checking recursive paths

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

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

Check result

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

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

More information

Additional information about PKI documentation can be found online:

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

7.4.5 Disposal

The products are to be disposed of in accordance with the respectively 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 company.

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 the part programs, archives, etc. by third parties. • Therefore ensure that all storage media are securely deleted **before disposing of the product** : • There are programs that support you in securely deleting/formatting storage media. Alternatively, contact a certified data destruction specialist to take care of this task. – A suitable program to delete data from interchangeable data carriers and flash memories such as SSDs is the Microsoft tool "sdelete", for example. – Another suitable program to delete data is the "Darik's Boot and Nuke" tool.

Also observe the special disposal information of the products in Chapter Product-specific security measures (Page 55).

See also

DBAN Hard Drive Eraser (https://dban.org/)

Microsoft sdelete (https://learn.microsoft.com/en-us/sysinternals/downloads/sdelete)

Product-specific security measures

8

In this chapter, you will find additional product-specific security measures for the products SINUMERIK, MACHINUM (CNC Shopfloor Management software), SIMOTION, SINAMICS, and SIMOCRANE.

Note

Validity for the products

Always note which product families or products this manual applies to (Page 8). For some products, there are separate manuals that describe the security measures and functions on a product-specific basis.

8.1 SINUMERIK

The following chapter provides you with an overview of the security-related measures you must take to protect your classic SINUMERIK control from threats. Detailed descriptions and procedures can be found in the corresponding SINUMERIK documentation.

We have summarized product-specific security-relevant measures and security functions specifically for **SINUMERIK ONE controls from software release V6.23** in separate documentation. This is provided on the Internet at the following address: Industrial Security SINUMERIK ONE Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109925842)

We have summarized product-specific security-relevant measures and security functions specifically for **SINUMERIK 828D control systems from software release V6.24** in separate documentation. You will find it in the Internet.

Detailed descriptions of existing security features are also provided in the SINUMERIK ONE product documentation / online help.

Many products (SINUMERIK, SIMOTION, SINAMICS) contain OpenSSL. The following applies to these products:

- This product contains software (https://www.openssl.org/) that has been developed by the OpenSSL project for use in the OpenSSL toolkit.
- This product contains cryptographic software (mailto:eay@cryptsoft.com) created by Eric Young.
- This product contains software (mailto:eay@cryptsoft.com) developed by Eric Young.

8.1.1 Firewall and networking

NCU/PCU networking structure

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

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

The IPC has the firewall function via the Windows functionality.

NOTICE
Data misuse via an unprotected interface Since the X120 interface of the NCU or the eth2 port of the IPC are not protected by a firewall, there is a risk of misuse of data. The interface only provides the option of establishing a connection to the local plant/system network. • As a consequence, never connect this local network with the Internet/company network.

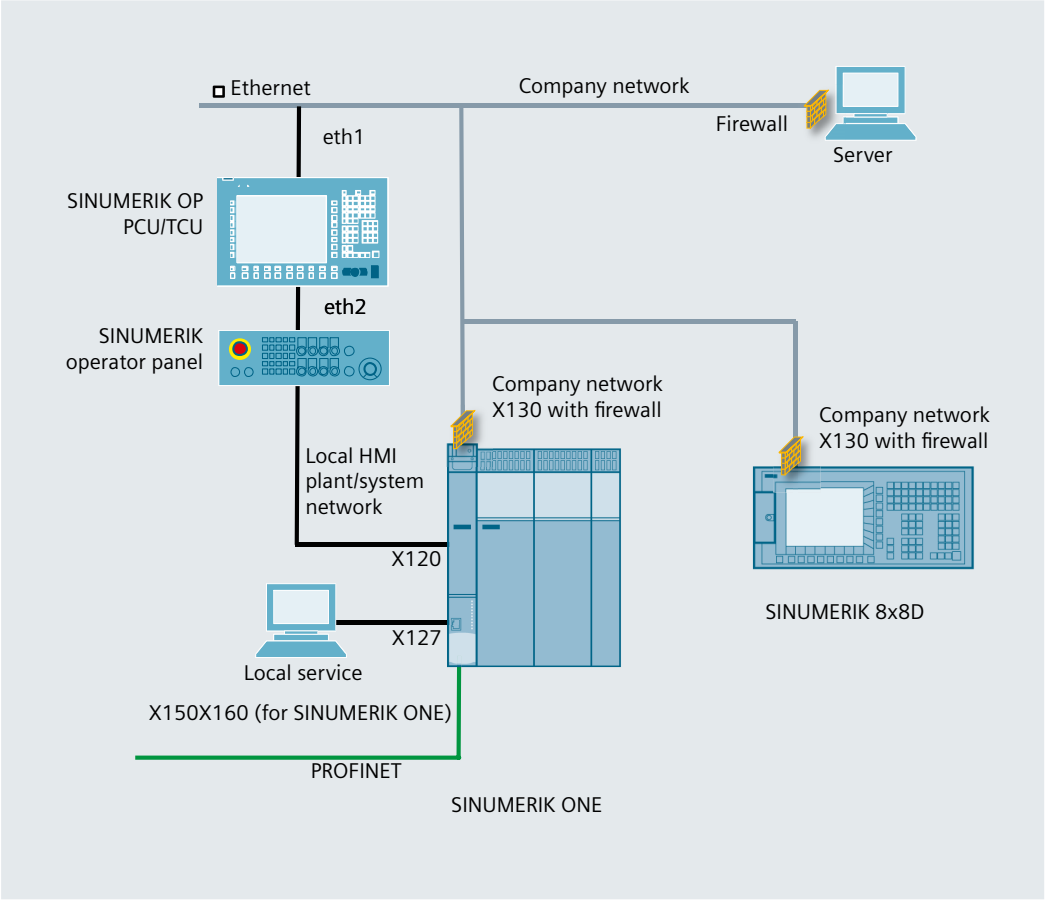


Figure 8-1 Networking of NCU/IPC

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 activate or deactivate the firewall via SINUMERIK Operate. Additional ports can be separately released.

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

Further information

Further information on the configuration of the firewall and default settings can be found in the following manuals:

- SINUMERIK Operate (IM9) (https://support.industry.siemens.com/cs/de/en/view/109769186)
- Diagnostics Manual (808D) (https://support.industry.siemens.com/cs/de/en/view/109763685)

8.1.2 Physical protection of the NCU

NOTICE
Misuse, manipulation and theft Modules, such as the NCU, are open equipment. If not protected, there is the risk of misuse by unauthorized personnel, manipulation or theft of data (e.g. CompactFlash Card). • As a consequence, always install NCUs in housings and locked control cabinets or in electrical rooms. Only appropriately trained and authorized personnel may access these housings, electrical cabinets and electrical rooms. Information on the permitted locks can be found in Chapter Physical protection of critical production areas (Page 34). • **Further information** on the control cabinet installation of the NCU can be found in the SINUMERIK 840D sl NCU 7x0.3 PN Manual (https://support.industry.siemens.com/cs/ww/en/view/109782727) or in the corresponding Equipment Manuals for SINUMERIK ONE: "NCU1750" and "NCU1760".

8.1.3 Machine control panels - SINUMERIK (MCP/MPP)

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

Note

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

Note

Firmware update

For MCP/MPP/PP72-48 firmware updates or module diagnostics (Port 3845) contact Siemens Service&Support (https://support.industry.siemens.com/sc/ww/en/sc/2090).

See also

Passwords (Page 47)

8.1.4 System hardening

8.1.4.1 Deactivating hardware interfaces

Deactivating interfaces

Measure	Description
Deactivate/activate Ethernet interfaces in the BIOS of the PCU	You can activate or deactivate the Ethernet interfaces in the BIOS of the PCU. You can find detailed information on this in PCU-Basesoftware (IM8) Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109748542), Chapter "BIOS settings".
Deactivating/activating USB interfaces	To prevent malware entering the control or the plant network via the USB interfaces, you can disable the USB interfaces of the NCU. Use the service command "sc_usb disable". Enter the relevant command on the Service Desktop in the "Run" dialog box or at the prompt. Use this function to make your system more secure and protect it from unwanted manipulation and malware. **Further information** can be found in the PCU-Basesoftware (IM8) Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109748542), Chapter "How to disconnect the USB interfaces".

Deactivating ports

Measure	Description
Deactivating the PROFINET port for SINUMERIK 840D sl PLC	In STEP 7 HW Config, a PROFINET interface port of a SINUMERIK PLC can be deactivated (X150). It is activated by default. The SINUMERIK PLC cannot be accessed via a deactivated PROFINET interface port. **Further information** can be found in the SIMATIC S7-300 CPU 31xC and CPU 31x Equipment Manual: Technical specifications (https://support.industry.siemens.com/cs/de/en/view/12996906), Chapter "Configuration of the port properties". **No communication function.** Note that no communication functions, such as PG/OP functions, open IE communication or S7 communication (PROFINET IO), are possible via a deactivated port.
Deactivating the PROFINET port for SINUMERIK ONE PLC	The PROFINET port can be deactivated in the TIA Portal under "Device configuration". Select the PLC and then switch to the menu "General > PROFINET interface> Advanced options > Port > Port options". Uncheck the box for "Activate this port for use". **Further information** can be found in the TIA Portal online help.
Deactivating a PROFINET port of SCALANCE X switch (possible as of the X200 series)	For secure operation, only one defined access point should be available to the network for diagnostics/maintenance. All of the other ports to the controls, devices, or switches (Scalance X) should be deactivated. This prevents unauthorized access. **Further information** can be found in the SIMATIC NET Configuration Manual: SCALANCE X-200 Industrial Ethernet switches (https://support.industry.siemens.com/cs/de/en/view/109757352), Chapter "Ports".

8.1.4.2 Communication services and used port numbers

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

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

Further information can be found in the product information for "SINUMERIK port lists" (available soon).

8.1.4.3 Integrity and authenticity protection

Note

System hardening for software solutions

When using SINUMERIK Integrate software and other PC applications, e.g. SINUMERIK Create MyConfig (CMC) or SINUMERIK Access MyMachine /P2P (AMM/P2P), ensure that the PC on which the software is used always fulfills the requirements of industrial cybersecurity.

These include, for example:

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

More information can be found in Chapter System integrity (Page 45).

8.1.5 Virus protection

In the context of the length of the service life of a machine tool, the use of antivirus software does not make sense.

The reasons for this are as follows:

- **Continuous pattern updates necessary**
  The protection of an antivirus program is only as good as the up-to-datedness of its virus patterns. Providing this in day-to-day production of the machine without a direct Internet connection is not possible without further action.
- **Changed patterns and background scans affect the runtime behavior of the controller**
  Scans that run in the background can influence the system load and thus the system behavior of the machine. The longer the pattern list, the more time and resource-consuming the scan, which means the influence increases as the machine ages.

- **Short support times**
  As a rule, updates and patterns for antivirus software are provided by the end of the operating system support, at the latest. However, a machine tool generally has a significantly longer service life than a Windows operating system. Therefore the protection becomes ineffective against new threats over time.
- **Unforeseeable backlash effects on machine functionality**
  In certain circumstances, a pattern update can result in a desired system function being detected by the antivirus software as a suspicious operation and prevented from executing, which can have unforeseeable consequences for the operation of the machine.

Reasons for allowlists

Using allowlists for protecting a Windows-based IPC in the SINUMERIK system makes sense for the following reasons:

- In a normal scenario, allowlists do not require updates in order to continuously protect the machine.
- Over the service life of the machine, allowlists do not lose their protective effect (apart from technical progress).
- Allowlists also protect against malware, which an antivirus program may still not be aware of.

Note

Measures for protecting against viruses in a CNC environment

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

See also

Virus signatures (https://support.automation.siemens.com/WW/view/en/19577116)

8.1.5.1 Positive list

SINUMERIK application example

Application Control freezes the desired system status so that only permitted or desired applications can be executed. Potentially existing vulnerabilities can no longer be exploited.

Only the execution of trusted applications is permitted. Basis: Definition of these applications in a positive list.

Siemens uses McAfee Application Control to improve the protection level of plant computer systems. Application Control is approved for use in various Siemens products such as SIMATIC PCS 7, WinCC, TIA Portal and SINUMERIK. The corresponding software is purchased directly from the manufacturer.

A detailed description of this application can be found on the Internet (https://support.industry.siemens.com/cs/ww/en/sc/4985).

8.1.5.2 Virus protection / memory card

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

⚠ WARNING

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

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

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

8.1.6 Security updates / patch management

For organizational reasons, it is not possible to provide the latest Windows security patch when the **PCU /** the **IPC** is shipped.

Windows 10-based SINUMERIK IPCs are basically delivered with variant LTSB 2016. This version of Windows not only provides extended support, but also gives you the capability of installing patches for specific problems and there are no compulsory updates.

Provide your Windows-based devices with the current security updates in a timely manner. These updates should not take place during machine operation. Therefore, use a local WSUS server (see Chapter Defense in depth concept (Page 32)).

Note

Before installing Microsoft Updates, note the following important points:

- **Prior to the update**, back up the system status for a fallback, if necessary. Ensuring the compatibility of the update with the individual system configuration is the responsibility of the customer.
- Never establish a direct connection to the WSUS server in the Internet! Ensure that the environment is secure and install an intermediate layer (e.g. DMZ network, firewall, SCALANCE S modules, etc.).

Since it is usually difficult to regularly update the Windows operating system of an IPC for a machine that is in use, and no more updates are available after the end of the support period, you should ensure the IPC is protected in accordance with the Defense in Depth concept (Page 32), e.g. by means of a security router and the use of a whitelisting solution.

Possibly identified security weak points of the **NCU** are taken into account or corrected in the current CNC software version.

Note

Availability

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

See also

Patch management (Page 49)

8.1.7 Account management

8.1.7.1 Definition of access levels

Access to functions and machine data

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)

Linux passwords / NCK

Level	User name	UID
1	manufact	102
2	service	103
3	user	104
4	operator3	105
5	operator2	106
6	operator1	107
7	operator	108

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

NOTICE

Data misuse caused by using passwords that are not secure enough

Data can be easily misused when passwords that are not secure enough are created. Passwords that are not secure enough can be easily hacked into.

The default passwords for the basic commissioning procedure are listed in the documentation.

- Therefore, always change the preassigned default passwords during commissioning
- Change the passwords at regularly defined intervals.
- For CNC software <V4.8: During commissioning, change the Linux password in addition to the SINUMERIK Operate passwords. You can find additional information in the Commissioning Manual "NCU operating system".
- A continuous warning appears on the SINUMERIK ONE if the default passwords are not changed.

Further information on assigning secure passwords can be found in Chapter Passwords (Page 47).

Note

Changing passwords between SINUMERIK Operate and Linux

The access levels for SINUMERIK Operate and Linux are merged as of software version 4.8 SP3 (840D sl/828D) and 6.13 (SINUMERIK ONE). Changing a password for SINUMERIK Operate simultaneously changes the relevant password in Linux and vice versa. It is important to note the following behavior:

- When a general NC reset is performed, no passwords are reset to the default passwords.
- Following a software upgrade, the SINUMERIK Operate passwords apply to the NC unchanged.
- Once a password has been changed, it cannot be reset to its original state.
- When recommissioning the system with Restore [-full] (menu item in the Emergency Boot System "Recover system from USB memory stick (reformat CF card)"), the CF card is formatted and restored to a system in the delivery state. The passwords are not included in the SINUMERIK archive. Therefore, always change the default passwords after a Restore [-full] to individual passwords.

8.1.7.2 Safety Integrated password

In SINUMERIK Operate, commissioning data is generally protected via various access levels. You protect the safety-related drive parameterization additionally with the Safety Integrated password. This password is stored in the drive data so that it can be changed only by authorized persons who know the password.

Note

The SINAMICS Safety password must be used for SINUMERIK Safety

The assignment of the Safety Integrated password using the SINUMERIK Operate screen is supported as of V4.8 SP2 HF1. The assignment of the Safety Integrated password is also supported by a screen form of the SINUMERIK ONE Commissioning Tool.

- Always set a Safety password to prevent parameters from being changed using the external configuration software Starter or the commissioning software SINAMICS Startdrive.

Further information can be found in the Safety Integrated plus Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109777982).

Further information

You can find **further information** on how you can change the passwords of the access levels along with other information on access levels for programs and softkeys and access rights for files in the SINUMERIK Operate (IM9) Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109801207), Chapter "General settings > Access levels".

8.1.7.3 CNC lock function

You can use the "CNC lock function" and the encrypted file that was created with SINUMERIK Access MyMachine /P2P (AMM/P2P) application to activate a lock date in the control system. This allows the use of the machine to be limited to the time until the lock date is reached. The NC Start function of the control is locked when the lock date is exceeded.

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

Note

Only for SINUMERIK 828D

Note that the CNC lock function is only available on the SINUMERIK 828D controller.

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

- "SINUMERIK Integrate Access MyMachine /P2P (PC)" Operating Manual (https://support.industry.siemens.com/cs/de/en/view/109770206)
- "PLC" Function Manual, Chapter "P4: PLC for SINUMERIK 828D > CNC lock function"

8.1.7.4 Deleting the preinstalled SSH key

Application

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

Service command

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

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

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

Further information

You can find additional information in the Base Software and Operating Software Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109763236).

8.1.7.5 PLC web server

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

Note

- If you activate the PLC web server in the S7 project, you must define an appropriate user and an associated password for it. Create a secure password. When creating a new password, carefully follow the information provided in Chapter Passwords (Page 47).
- Only use the HTTPS protocol to establish communication confidentiality and integrity.

More information

Further information on the PLC web server can be found in the Function Manual S7-1500, ET 200SP, ET200pro web server (https://support.industry.siemens.com/cs/ww/en/view/59193560).

8.1.7.6 Access levels for softkeys

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

Note

Applicability of modified access levels for softkeys

The setting of specific access levels for softkeys on a PCU only affects the respective PCU softkeys themselves. To implement access rights on the NCU, both the manufacturer and the user must use the appropriate mechanisms and set the rights accordingly.

Further information can be found in the SINUMERIK Operate (IM9) Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109801207), Chapter "Access levels for programs".

8.1.7.7 BIOS and AMT access protection

In order to prevent unauthorized access to the BIOS of the PCU 50 and the SIMATIC IPCs, make sure that you use a very secure BIOS password (see Section Passwords (Page 47))

Further information

Further information on BIOS settings of the PCU 50 can be found in the PCU-Basesoftware (IM8) Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109748542).

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

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

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

Further information on the AMT function of the PCU as well as the procedure for changing the password can be found on the Internet (https://support.industry.siemens.com/cs/de/en/view/52310936).

8.1.7.8 Password protection for Create MyConfig (CMC)

NOTICE
Data misuse due to incorrect assignment of rights Access data, such as the pre-configured passwords for access to the control system, can be stolen and misused. • For that reason, set up organizational measures to ensure that only authorized persons are given access to these files.

8.1.8 Know-how protection

The following functions provide protection of technological know-how and prevent unauthorized access to the SINUMERIK controllers:

8.1.8.1 SINUMERIK Integrate Lock MyCycles

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

8.1.8.2 SINUMERIK Integrate Lock MyPLC

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

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

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

Further information

You can find further information on block protection in the SIMATIC Programming with STEP 7 Programming and Operating Manual (https://support.industry.siemens.com/cs/de/en/view/109751825), Chapter "Block properties".

Note

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

Encryption of blocks

As of STEP 7 Version 5.5 SP3 and the CNC system software 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).

8.1.8.3 OPC UA

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

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! More information on selecting a secure password can be found in Chapter Passwords (Page 47).

8.1.8.4 User administration in the TIA Portal

The TIA Portal gives you the capability of using user administration for projects. In this way, for example, a project can be protected against unintentional or unauthorized modification. A user sets up the project protection to activate user management. This user is created as a project administrator. Once the project protection has been activated, the project can only be opened and edited by authorized users. Note that project protection cannot be revoked.

User administration via the TIA Portal is available for the SINUMERIK 840D sl and SINUMERIK ONE controllers.

UMC - User Management Component

In addition, you can install the "User Management Component UMC" software package, which provides central user administration, on one or more computers.

Further information

Further information on the topic of secure user administration can be found in the TIA Portal online help.

8.1.8.5 SIMATIC Logon

User administration and traceability

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

More detailed information can be found in Chapter AUTOHOTSPOT.

8.1.9 Data backup

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

Time of the data backup

Perform a data backup at the following times:

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

You can find **further information** in the following manuals:

- SINUMERIK 840Dsl Commissioning CNC Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109801198)
- Installation Manual SINUMERIK ONE New installation and upgrade

Note the general information on secure data storage with regard to archives in Section Store sensitive data securely (Page 46).

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

8.1.10 Disposal

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 the part programs, archives, etc. by third parties. • Therefore ensure that all storage media are securely deleted **before disposing of the product** : • There are programs that support you in securely deleting/formatting storage media. Alternatively, contact a certified data destruction specialist to take care of this task.

8.2 MACHINUM (CNC Shopfloor Management software)

The following chapter provides you with an overview of the security-related measures you can take to protect your MACHINUM (CNC Shopfloor Management software) products from threats. Detailed descriptions and procedures can be found in the corresponding documentation of the MACHINUM software (CNC Shopfloor Management software).

8.2.1 System overview

With the 3 levels "In Cloud", "In Line", and "In Machine", MACHINUM (CNC Shopfloor Management software) has created a leading-edge IT architecture. These levels correspond to the 3 platforms "Insights Hub", "Mcenter", and "SINUMERIK", with their numerous tailored functions extending from the field to the cloud.

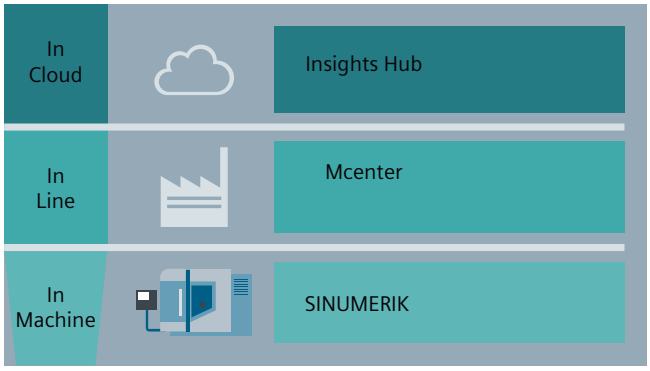


Figure 8-2 MACHINUM (CNC Shopfloor Management software)

8.2.2 Cloud applications (In Cloud)

Insights Hub provides state-of-the-art security during on-site data collection and when transferring and saving to the Cloud.

The security framework is oriented on the principles of industry standards, e.g. IEC 62443, International Organization for Standardization (ISO)/IEC 27001, and the Federal Office for Information Security (BSI) and recommendations from authorities on working with data in Cloud environments.

In accordance with proven communication practices of the industry, all communication between the client and Insights Hub is protected by TLS V1.2 via public end points. Reliable x509 certificates from the Siemens Trust Center are used. These correspond to the requirements of the European Telecommunications Standards Institute (ETSI) and of the Certification Authority Browser Forum (CA/B Forum).

More information on encryption for Insights Hub can be found in the Insights Hub Whitepaper (https://www.plm.automation.siemens.com/global/en/topic/mindsphere-whitepaper/28842).

Saved data is always saved by Siemens on high-performance servers in the computer centers of the infrastructure providers. All of the infrastructure centers meet the highest standards

for data security and are protected against cyber threats. As commercial providers of a Cloud IaaS (Infrastructure as a Service), they provide higher security standards than typical private, local facilities for data storage. The computer centers are operated in accordance with the Best Practices of the industry.

As an additional layer of security, all of the Cloud infrastructure partners must ensure on-site security measures such as electronic photo ID badges, card owner access control, biometrics, digital video monitoring with recording and alarm monitoring.

8.2.2.1 Manage MyMachines

Security standards for SINUMERIK and other supported control systems with Insights Hub connection

The connection between controllers and Insights Hub via TLS 1.2 /HTTPS complies with the highest security standards.

SINUMERIK versions and software versions of other supported control systems that do not comply with these standards are not part of the product. Additional security measures must be taken for these versions.

You are solely responsible for preventing unauthorized access to your plants, systems, machines, and networks. Systems, machines and components should only be connected to the company network or the Internet when necessary. And if so, only if appropriate security measures (e.g. use of firewalls and network segmentation) are in place.

NOTICE
Data misuse due to an unprotected Internet connection An unprotected Internet connection can lead to data misuse, e.g. when transferring asset data. Therefore, before you establish a network connection, make sure that your PC is connected to the Internet only through a secure connection. Pay attention to the security-relevant notes.

Plant and system security for SINUMERIK control systems/other supported control systems

The necessary security measures (e.g. virus scanners, firewalls, operating system patching, etc.) must be implemented and updated on the control systems.

Operational safety of the PC

The necessary security measures (e.g. virus scanners, firewalls, operating system patching, etc.) must be implemented on the PCs used for visualization and configuration of Insights Hub applications at the OEM or at the end user.

8.2.2.2 Manage MyMachines /Remote

Security measures and system hardening

Note

As user of Manage MyMachines /Remote, always ensure that you operate the product with the latest versions of SINUMERIK Integrate client/client of other supported control systems and Manage MyMachines /Remote Service Engineer and Machine Operator Clients. Also follow the guidelines for industrial security contained in Chapters 1.3 and 2.3 of the Manage MyMachines / Remote Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109759394).

The connection of SINUMERIK controllers and other supported controllers to Insights Hub via "TLS 1.2 /HTTPS" meets the highest security standards.

The automatic confirmation of the machine identity, used in conjunction with token provided in Insights Hub for the onboarding of the machine, ensures that the correct machine is accessed during a remote session.

Disposal

To completely remove an installation of Manage MyMachines /Remote, you should ensure that all of the software and certificates have been properly deleted from your Microsoft Windows device or SINUMERIK control system or any other supported control systems, including backup systems. The data will continue to be available in Insights Hub, unless the tenant is closed.

More information on the topic of disposal can be found in the Manage MyMachines /Remote Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109759394).

More information on general concepts for secure remote access to industrial plants can be found in the following documents:

- cRSP IT Security Concept (https://support.industry.siemens.com/cs/ww/en/view/109759394)
- Siemens common Remote Service Platform (cRSP) (https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=A6V11272777)

Secure archiving

When archiving your exported data, keep in mind that you are responsible for ensuring that this data is archived securely.
This includes, for example, the following measures:

- Save exported data to an area with restricted access within the OEM/end user location:
  - e.g. on SharePoints with access restrictions
  - or databases with user administration/authorization
- Protect your encrypted data storage locations, such as SharePoints, against manipulation.

- If necessary, store your confidential or security-relevant data only as encrypted data on your PC/system or in the network. Security-relevant data includes sensitive data such as archives, passwords or executable files (*.exe).
- Regularly back up your security-relevant data and carefully protect it from loss and tampering.

See also

cRSP IT security concept (https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=A6V11272775)

8.2.2.3 Analyze MyPerformance/Mcenter

Secure disposal

If you want to uninstall the Mcenter instance, you can follow the instructions in the Mcenter Installation Manual, chapter "Uninstalling the server setup" (https://support.industry.siemens.com/cs/ww/en/view/109762628), to completely remove Mcenter and its artifacts from the device.

If you want to uninstall a specific application, you can remove the selected application from the Mcenter Application Management functionality to fully remove the application. However, you must bear in mind that the database records and tables generated by the application will still be in the database of the host device after the application has been removed. If you wish, these records and tables can be deleted manually to complete the product disposal.

Secure configuration

To protect the Apache Tomcat® web server from potential security vulnerabilities, you must ensure that the web server is securely installed, configured, and regularly maintained. End users are required to set up the web server strictly according to the instructions in the Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628) and Operating Manual (https://support.industry.siemens.com/cs/ww/en/view/109762630). Failure to follow these guidelines may result in incorrect configuration or security vulnerabilities. In addition, best practices for the security of Apache Tomcat® must be followed to ensure the security of the server and prevent potential threats.

Data integrity and authenticity

To protect the integrity and authenticity of the Manage MyMachine/Mcenter application, you must ensure the following points:

- TLS is enabled for the Apache Tomcat® web server (see Mcenter Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628), chapter "Setting up an encrypted connection for Tomcat").
- TLS is enabled for SQL communication (see Mcenter Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628), chapter "Setting up encrypted communication for SQL Server").
- Encryption of dormant data is activated for SQL Server.

HMI & IPC security

To protect the Analyze MyPerformance application from malicious actions, you must take the following measures to protect your HMI and other IPC end devices:

- **Access control**: Terminals may only be accessed by authorized users. Regular checks are carried out.
- **Authentication**: Terminals should be protected, where possible, by the use of strong, unique passwords for each user, following best practice in terms of complexity (e.g. a mixture of upper and lower case letters, numbers and symbols) and length (at least 8-12 characters). Passwords must be updated regularly and regular checks for authorized persons and authorization rights must be performed. If possible, the timeout for the authenticated session must be activated.
- **Secure environment**: Terminals must be located in restricted areas where physical security controls are implemented.
- **Training and awareness building**: The end user must ensure that appropriate training is provided to staff on the security of such systems.

8.2.2.4 Manage MyMachines/Mcenter

Secure disposal

If you want to uninstall the Mcenter instance, you can follow the instructions in the Mcenter Installation Manual, chapter "Uninstalling the server setup" (https://support.industry.siemens.com/cs/ww/en/view/109762628), to completely remove Mcenter and its artifacts from the device.

If you want to uninstall a specific application, you can remove the selected application from the Mcenter Application Management functionality to fully remove the application. However, you must bear in mind that the database records and tables generated by the application will still be in the database of the host device after the application has been removed. If you wish, these records and tables can be deleted manually to complete the product disposal.

Secure configuration

To protect the Apache Tomcat® web server from potential security vulnerabilities, you must ensure that the web server is securely installed, configured, and regularly maintained. End users are required to set up the web server strictly according to the instructions in the Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628) and Operating Manual (https://support.industry.siemens.com/cs/ww/en/view/109762630). Failure to follow these guidelines may result in incorrect configuration or security vulnerabilities. In addition, best practices for the security of Apache Tomcat® must be followed to ensure the security of the server and prevent potential threats.

Data integrity and authenticity

To protect the integrity and authenticity of the Manage MyMachine/Mcenter application, you must ensure the following points:

- TLS is enabled for the Apache Tomcat® web server (see Mcenter Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628), chapter "Setting up an encrypted connection for Tomcat").
- TLS is enabled for SQL communication (see Mcenter Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628), chapter "Setting up encrypted communication for SQL Server").
- Encryption of dormant data is activated for SQL Server.

8.2.2.5 Access MyData/Collector

Secure disposal

If you want to uninstall the Mcenter instance, you can follow the instructions in the Mcenter Installation Manual, chapter "Uninstalling the server setup" (https://support.industry.siemens.com/cs/ww/en/view/109762628), to completely remove Mcenter and its artifacts from the device.

If you want to uninstall a specific application, you can remove the selected application from the Mcenter Application Management functionality to fully remove the application. However, you must bear in mind that the database records and tables generated by the application will still be in the database of the host device after the application has been removed. If you wish, these records and tables can be deleted manually to complete the product disposal.

Secure configuration

To protect the IIS web server from potential security vulnerabilities, you must ensure that IIS is securely installed, configured, and regularly maintained. End users are required to set up the web server strictly according to the instructions in the Installation Manual (https://support.industry.siemens.com/cs/ww/en/view/109762628) and Operating Manual (https://support.industry.siemens.com/cs/ww/en/view/109762630). Failure to follow these guidelines may result in incorrect configuration or security vulnerabilities. In addition, best security practices for IIS must be followed to ensure the security of the server and prevent potential threats.

Data integrity and authenticity

To protect the integrity and authenticity of the Access MyData application, you must ensure the following points:

- TLS is enabled for the IIS web server (see Mcenter Installation Manual, chapter "Setting up an encrypted connection for IIS (https://support.industry.siemens.com/cs/ww/en/view/109762628)").
- TLS is enabled for SQL communication (see Mcenter Installation Manual, chapter "Setting up encrypted communication for SQL Server" (https://support.industry.siemens.com/cs/ww/en/view/109762628)).
- Encryption of dormant data is activated for SQL Server.

Activating MQTTS (MQTT with TLS)

To improve the security status of the Access MyData application, the use of MQTT via TLS (MQTTS) must be enabled. To configure and use MQTTS in the product, follow the instructions below:

1. **Enable client authentication**: Access your MQTT broker settings and enable the client authentication feature. This will ensure that all clients connecting to the broker are verified, providing an additional layer of security.
2. **Secure MQTT broker data**: It is important to secure your MQTT broker's sensitive data, including TLS certificates and keys. Make sure these files are stored in a secure location with limited access authorizations.
3. **Update configuration**: Change your client and server configuration to use MQTTS instead of standard MQTT. To do this, you must update the port to the standard MQTTS port and specify the storage location of the TLS certificates.
4. **Test the connection**: After configuring MQTTS, test the connection to ensure that the client can establish a secure connection using the certificates and client authentication settings provided.

By following these steps, you will increase the security of your MQTT communication through encrypted transmission and client authentication.

8.2.3 PC/Server/Desktop applications (In Line)

8.2.3.1 Mcenter

Access to Mcenter server resources

Note

Access to Mcenter server resources

Read and write access to the file system and resources of the operating system (in particular the Microsoft Windows Registry) of the Mcenter server is only granted to users with administration rights. Make sure that these administrator IDs have sufficiently strong passwords.

NOTICE

Data manipulation possible

There is a risk that hackers could access the file system of the MCenter server or the various Mcenter clients within the production/machine network (intranet). There, the hacker can manipulate various system components (e.g. the content of databases). As a consequence, the attacker can change tool data, NC programs, machine archives or the system structure itself, for example. This type of attack cannot be prevented by MCenter.

- As the person responsible for the machine network, it is therefore imperative that you take the appropriate industrial security measures for the production/machine network.

Use of open programming interfaces

NOTICE

Data misuse by using open programming interfaces

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

- Therefore, when using open programming interfaces, only use clients that communicate with the Mcenter server at least via "TLS /https" communication paths.

Communication security for Mcenter applications

The system is prepared for the use of the TLS protocol. All modules and services must communicate via encrypted channels that meet current security requirements. Consequently, the system is prepared to use the TLS protocol. The server requires a digital certificate that confirms the identity of the server. You can purchase these items from certification bodies (certification authorities). The certificate must be digitally signed. The clients must trust these certificates. If you use your own generated, self-signed certificate, the master certificates must be provided on the control elements on Linux and Windows computers. And the master certificates must also be provided on TLS proxies when they are used. You are fully responsible for the correct implementation and verification of your system.

If you are using an outdated client (e.g. a Microsoft Windows NT computer) that does not support the required TLS protocols, you should use a hardware proxy to resolve this issue. Such hardware can provide an additional encryption layer for the communication channel. You must also ensure that the hardware proxy is appropriately and properly encrypted. The hardware proxy is not part of the product.

Note

- For a secured communication (HTTPS) between a client and the server, you require a digital certificate that confirms the identity of the server.
- If the database is running on a separate server, encrypted SQL communication requires a certificate on the DB server.

For more information, see the Mcenter Installation Manual, sections "Setting up an encrypted connection" and "Setting up encrypted communication for SQL server".

System hardening

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

To protect your assets or production unit, you must have the appropriate knowledge and the installed system must be hardened. System hardening should be based on the appropriate Microsoft and other hardening guidelines. For example, you can find expert instructions in CIS (Center for Internet Security) manuals or, if accessible, in documents available at the company, or you can choose the source that best suits you.

Installation and maintenance technicians need to continuously improve their industrial cybersecurity knowledge because information security threats are increasing by the day. System security risks are increasing continuously, and as a Siemens customer you need to prepare accordingly.
You can reuse system configurations that have already been hardened. However, these configurations should also be reviewed periodically and new rules must be applied.

System hardening of third-party software: Microsoft™ Internet Information Server, Microsoft™ SQL Server, web browsers

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

System hardening of products adjacent to Mcenter

Mcenter communicates with neighboring software products, such as tool presetters or TeamCenter. They must be hardened according to the latest technology so that there are no negative effects via this communication path.

Finally, you must also have the knowledge and the experience to configure the IIS server. You must always be prepared to respond to the actual hardship requirements. You are responsible for making the correct system security settings in the client environment.

Examples:

- If a remote desktop connection is provided, the highest possible security configuration must be ensured to avoid a possible MITM (man-in-the-middle) attack.
- Protect your system from code injection by using state-of-the-art technology and expertise.
- Store certificates securely so that they cannot be exported by unauthorized entities. In such cases, you must follow the hardening guidelines when setting up.
- Servers must run in a secure, restricted server zone/server room that can only be accessed by authorized personnel.
- Encrypt server memory or the data on it to prevent attacks on the system if the system is physically compromised.
- Back up your system regularly to protect your data.
- The license server is provided or available only locally.

Network file exchange via common drives

Note

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

If you use SMBs to exchange files with Mcenter functionalities, be sure to only use standard authentication mechanisms (user name/password). Also restrict the accesses for each user accordingly. Data storage on shared drives should be kept to a minimum.

Virus scanner

Protect files from malware using appropriate protective measures, such as virus scanners. Use an external virus scanner when uploading files with Mcenter and its applications.

Data backup

For data backup on machine tools, see Section "Data backup (Page 71)".

Create a backup copy of your data in the following cases:

- Before and after upgrading the software
- After setup/commissioning
- When changing the hardware configuration
- After replacing the hardware
- On a regular basis

The backup must contain all elements of Mcenter, such as:

- Database
- IIS configuration

- License server
- Applications

Firewall settings

Make absolutely sure that firewalls are "enabled" and only open ports that are actually used and absolutely necessary for operation. Other ports must not be left open, as they could also provide another attack surface.

If a remote desktop connection is provided, the highest possible security configuration must be ensured to avoid a possible MITM (man-in-the-middle) attack.

Prepare yourself against DoS (Denial of Service) attacks, for example, by setting up appropriate firewall rules, implementing an IPS (Intrusion Prevention System) and/or a WAF (Web Application Firewall).

Phishing for passwords

Hackers could attempt to obtain login data that would allow them to perform actions within Mcenter on behalf of the user. Hackers could, for example, forge Siemens emails and websites and thus gain access to confidential information of Mcenter users. Users are then prompted, for example, to enter access data into a form and then send it to their Mcenter organization.

Note

In case of suspicious emails, you should pay attention to the following:

- Be on your guard when you receive emails from someone you do not know, especially if the emails contain links and attachments. Never open suspicious attachments and do not click on any links in the email.
- Carefully check the sender's complete email address.
- Check the integrity of the links embedded in the email (e.g. by moving the mouse over the link). Telltale signs are misspellings or links containing a confusing company name.
- Use digital signatures in emails.
- If in doubt, never disclose confidential information.

8.2.3.2 Cloud mode

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

Firewall of the machine network

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

Phishing for passwords

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

Note

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

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

Handling of confidential information

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

8.2.4 ACM-Suite

8.3 SINAMICS

The following chapter provides you with an overview of the industrial cybersecurity features available for SINAMICS to protect your converters from threats. The chapter is valid for SINAMICS converters with a firmware version less than V6.1.

We have summarized product-specific security-relevant measures and security functions specifically for SINAMICS converters from firmware release V6.1 in a dedicated Configuration Manual. This is provided on the Internet at the following address: SINAMICS Industrial Cybersecurity Configuration Manual (https://support.industry.siemens.com/cs/ww/en/view/109955569)

Topics, where you should pay particular attention to industrial cybersecurity, are listed in the following chapter:

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

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

Many products (SINUMERIK, SIMOTION, SINAMICS) contain OpenSSL. The following applies to these products:

- This product contains software (https://www.openssl.org/) that has been developed by the OpenSSL project for use in the OpenSSL toolkit.
- This product contains cryptographic software (mailto:eay@cryptsoft.com) created by Eric Young.
- This product contains software (mailto:eay@cryptsoft.com) developed by Eric Young.

8.3.1 Network security

Note

SINAMICS products may only be used in a secure and trusted network. Observe the information on this topic in Chapter "Network segmentation (Page 36)".

8.3.2 Know-how protection

Some SINAMICS converters provide you with a "Know-how protection" function: This function offers you protection of your intellectual property, especially the know-how of machine manufacturers against unauthorized use, modification or reproduction of their products.

Effect

Adjustable parameters which are not recorded in an exception list can neither be read nor written.

Exceptions

- The know-how protection does not affect parameters that are provided with the following attributes:
  - KHP_WRITE_NO_LOCK
    - These parameters are excepted from the know-how protection and can therefore be written to despite the know-how protection.
    - For a list of these parameters, see the List Manual of the respective product.
    - These parameters are not included in the exception list.
  - KHP_ACTIVE_READ
    - These parameters can also be read, but not written, with activated know-how protection.
    - For a list of these parameters, see the List Manual of the respective product.
    - These parameters are not included in the exception list.
- Know-how protection does not prevent the execution of certain functions:
  - In particular, the "Restore factory settings" function is still possible despite know-how protection.
  - For a full list of executable functions, please refer to the following references.

Further information

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

- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  Chapter "Know-how protection"
- SINAMICS G110M operating instructions (https://support.industry.siemens.com/cs/de/en/view/109757594)
  Chapter "Know-how protection"
- SINAMICS G120 Operating Instructions
  Chapter "Know-how protection"
- SINAMICS S and SINAMICS G List Manuals
  Section "Parameters for write protection and know-how protection"
- SINAMICS G130, G150 and S150 Operating Instructions
  Chapter "Know-how protection"

8.3.3 Parameters: Access levels and password

For the G110M, G120, G130, G150, S110, S120 and S150 series devices, the SINAMICS parameters are divided into the access levels 0 to 4. With the aid of the access levels, you can specify which parameters can be modified by which user or input/output device:

- With the aid of parameter p0003, you can specify which access levels you can select with the BOP or IOP.
- Parameters of access level 4 are password-protected and only visible for experts up to SINAMICS RT V4.9.

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

Further information

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

- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  Chapter "Parameters"
- SINAMICS S120 Safety Integrated Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781722)
  Section "Handling the safety password"
- SINAMICS G110M List Manual
  Chapter "Overview of parameters"
- SINAMICS G120 Operating Instructions
  Chapter "Parameters"
- SINAMICS S and SINAMICS G List Manuals
  Section "Explanation of the list of parameters"
- SINAMICS G130, G150 and S150 Operating Instructions
  Chapter "Parameters"

8.3.4 Using the memory card

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

⚠ WARNING

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

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

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

⚠ WARNING

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

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

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

8.3.5 Safety Integrated

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

⚠ DANGER

Unexpected movement of machines caused by inactive safety functions

Inactive or non-adapted safety functions can trigger unexpected machine movements that may result in serious injury or death.

- Observe the information in the appropriate product documentation before commissioning.
- Carry out a safety inspection for functions relevant to safety on the entire system, including all safety-related components.
- Ensure that the safety functions used in your drives and automation tasks are adjusted and activated through appropriate parameterizing.
- Perform a function test.
- Only put your plant into live operation once you have guaranteed that the functions relevant to safety are running correctly.

Note

Important safety notices for Safety Integrated functions

If you want to use Safety Integrated functions, you must observe the safety instructions in the Safety Integrated manuals.

8.3.6 Backing up and restoring data

8.3.6.1 Backup and restore

SINAMICS provides several procedures for backing up and restoring your data. In the documentation ("More information") you will find which procedures can be used with which devices.

Web server/Startdrive

The "Back up and restore" function provides you with the following options:

- Backing up parameters that have already been set
- Assigning a name to the backup file
- Restoring parameters from a valid parameter backup and loading them to the drive
- Restore drive factory settings

Smart Access Module

- Via the backup web page, you can back up parameters to the Smart Access Module and download the backup file to your local hard drive.
- Via the restore web page, you can upload, download, delete or restore the selected file.

SINAMICS V20 parameter loader

Up to 100 parameter sets with parameter settings can be written from the memory card to the converter or saved from the converter to the memory card without connecting the converter to the line supply.

More information

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

- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  Chapter "Web server"
- SINAMICS S120 Commissioning Manual with Startdrive (https://support.industry.siemens.com/cs/ww/de/view/109781583/en)
  Chapter "Saving settings on the memory card of the drive"
- SINAMICS S210 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109771824)
  Chapter "Backup and restore"
- SINAMICS G120 Operating Instructions "SINAMICS G120 Smart Access" (https://support.industry.siemens.com/cs/ww/en/view/109771299)
  Chapter "Backup and restore"

- SINAMICS G130, G150 and S150 Operating Instructions
  Chapter "Web server"
- SINAMICS V20 Operating Instructions (https://support.industry.siemens.com/cs/de/de/view/109768394/en)
  Chapter "Commissioning via the SINAMICS V20 Smart Access" and "Parameter loader"

8.3.6.2 Redundant data backup

Saving settings outside the converter

We recommend that you additionally back up the settings on a storage medium outside the converter. Without a backup, your settings will be lost in the event of a converter failure.

The following storage media are available for your settings:

- Memory card
- PG/PC
- Operator panel

In the documentation ("More information") you will find which procedures can be used with which devices.

SINAMICS S120

In conjunction with the "Firmware update via the web server" and the associated remote access, the "Redundant data backup on a memory card" provides safe access again to the device in the event of an interruption of the connection or the power supply. This redundant data backup cannot be deactivated.

8.3.6.3 Redundant_backup_more_info

More information

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

- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  Chapter "Redundant data backup on a memory card"
- SINAMICS S120 Commissioning Manual with Startdrive (https://support.industry.siemens.com/cs/ww/de/view/109781583/en)
  Chapter "Saving settings on the memory card of the drive"
- SINAMICS S210 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109771824)
  Chapter "Backup and restore"
- SINAMICS G Operating Instructions

- SINAMICS G130, G150 and S150 Operating Instructions
- SINAMICS V20 Operating Instructions (https://support.industry.siemens.com/cs/de/de/view/109768394/en)
  Chapter "Backup and restore"

8.3.7 Communication services and used port numbers_Further_information

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

- SINAMICS S120
  - Starting from firmware Version 5.2
    SINAMICS S120 Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109771803)
  - Older firmware versions
    SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  - Including: Section "Communication services and used port numbers"
- SINAMICS G Function Manual Fieldbuses (https://support.industry.siemens.com/cs/ww/de/view/109757336/en)
  Section "Ethernet and PROFINET protocols that are used"
- SINAMICS G130, G150 and S150 Operating Instructions
  Chapter "Communication services and used port numbers"

8.3.8 Communication services and used port numbers

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

8.3.9 Integrated web server

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

Data transfer

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

Note

Smart Access Module

The web server of the Smart Access Module does not support secure transmission (HTTPS). Alternatively, you can use an encrypted WLAN transmission.

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

For security reasons, secure transmission can be forced by deactivating the HTTP port.

Access rights

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

Further information

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

- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  Section "Web server"
- SINAMICS S210 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109771824)
- SINAMICS V20 Operating Instructions (https://support.industry.siemens.com/cs/de/de/view/109768394/en)
- SINAMICS G120 Smart Access Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109771299)
- SINAMICS G130, G150 and S150 Operating Instructions

8.3.9.1 Certificates for the secure data transfer

Protecting the HTTPS access

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

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

TLS

Transport Layer Security (TLS V1.2 or higher) is a hybrid encryption protocol for secure transfer of data in the Internet.

Key files

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

Certificate handling

The necessary certificate and key is generated on the drive so that you can access the drive via HTTPS in the SINAMICS as delivered. For this reason, the firmware certificate should only be used in secure networks (e.g. PROFINET below a PLC) or for direct point-to-point connections on the service interface X127.

Instead, use a certificate confirmed by an external certification center. The references cited in the following contain a detailed description of the procedure.

Further information

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

- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
  Section "Certificates for the secure data transfer"
- SINAMICS G130, G150 and S150 Operating Instructions

8.3.10 Information about individual interfaces

X127 LAN (Ethernet)

Ethernet interface X127 is intended for commissioning and diagnostics, which means that it must always be accessible. Note the following restrictions for the X127 interface:

- Only local access is possible
- No networking or only local networking in a locked control cabinet permissible

If you require remote access to the control cabinet, then you must apply additional security measures so that misuse through sabotage, data manipulation by unqualified persons and intercepting confidential data are completely ruled out.

X140 serial interface (RS232)

You connect an external HMI device for operator control/parameter assignment via the serial interface X140.

NOTICE
Access to the inverters only for authorized personnel Unauthorized persons may be able to damage or alter production equipment as a result of gaps in a company's physical security. Confidential information can also be lost or altered as a result of this. You can prevent this if you protect the company site and the production areas accordingly. • You can find information on suitable protective measures in Section "Physical protection of critical production areas (Page 34)".

X150 LAN (Ethernet)

The network with which interface X150 is connected must be separated from the rest of the plant network in accordance with the Defense in Depth concept (see Chapter "General security measures (Page 31)"). Access to cables and possibly open connections must be implemented in a protected fashion, as in a control cabinet.

X1400 LAN (Ethernet)

The network with which interface X1400 is connected must be separated from the rest of the plant network in accordance with the Defense in Depth concept (see Chapter "General security measures (Page 31)"). Access to cables and possibly open connections must be implemented in a protected fashion, as in a control cabinet.

Further information

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

- SINAMICS S120
  - SINAMICS S120 Control Units and Additional System Components Equipment Manual (https://support.industry.siemens.com/cs/ww/en/view/109782370)
    Section on the respective interfaces
  - Starting from firmware Version 5.2: SINAMICS S120 Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109771803)
  - Older firmware versions:
    SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
- SINAMICS G and SINAMICS S Operating Instructions
- SINAMICS V90 Operating Instructions

8.3.11 Disposal

NOTICE
Data misuse resulting from unsafe disposal of the product
Unsafe disposal of the product can lead to misuse of the parameter data by third parties. • Therefore, before disposal, restore all the parameters to the factory settings. You can find further information on restoring the factory settings in the Function Manual or Operating Instructions of the respective product.

NOTICE
Data misuse resulting from unsafe disposal of the memory card
Unsafe disposal of the memory card can lead to misuse of the data etc. by third parties. Among other things, the data backups required for operating the converter are located on the memory card. • Therefore, ensure that the data on the memory card is securely deleted before disposing of the product. There are programs that support you in securely deleting/formatting the memory card. • This concerns all products that have a memory card.

Note

Deleting user-defined certificates

Make sure you securely remove all user-defined certificates before disposing of a SINAMICS product. A hacker can use your certificates to gain access to your protected data transmission.

- Products with memory card
  - Delete the files SINAMICS.key and SINAMICS.crt from the directory OEM\SINAMICS\WEB\WEBCONF\CERT on the memory card.
- Products with optional memory card (e.g. SINAMICS S210)
  - Create empty files ("SINAMICS.key" and "SINAMICS.crt") with the corresponding file names.
  - Copy these files to the memory card.
  - Insert the memory card into the converter.
  - Restart the converter.
  - Alternatively, when you no longer need data from the memory card: reformat the memory card.

You can find further information in the Function Manual or Operating Instructions of the respective product.

8.3.12 SINAMICS Startdrive and TIA Portal

8.3.12.1 Malfunctions of the machine as a result of incorrect or changed parameterization

⚠ WARNING

Malfunctions of the machine as a result of incorrect or changed parameterization

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

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

8.3.12.2 SINAMICS Startdrive

Startdrive in the TIA Portal

SINAMICS Startdrive is an option package in the TIA Portal with which SINAMICS drives are commissioned. With regard to industrial cybersecurity, you must consider the corresponding specifications for SINAMICS drives and for the TIA Portal.

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

Commissioning computer

Ensure the security of the commissioning computer. Follow the general security measures (Page 31) for this purpose.

Device know-how protection

- You can protect the parameterization of your drive from unauthorized access via the "know-how protection" function.
- The function is only available online.
- Device know-how protection is supported as of Startdrive V16.

Security functions

- Activation/deactivation of unused functions (web server, ports)
- Write protection for the parameter assignment, p-parameters are readable, but not writeable, protects against unintentional changes to the parameter assignment (only available online).

Protecting backup files in the Windows file system

If you create backup files of charts or projects with Windows tools, also protect these files with Windows tools against unauthorized access using secure passwords. The Startdrive project itself is protected for integrity.

Scripting (Openness)

Scripts (Openness) are used for automating sequences in Startdrive. You must therefore test the scripts before using them on machines.

⚠ WARNING

Risk due to incorrect configurations for automated operating actions

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

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

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

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

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

8.3.12.3 SINAMICS STARTER

Commissioning drives with STARTER

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

Commissioning computer

Ensure the security of the commissioning computer. Follow the general security measures (Page 31) for this purpose.

Protecting backup files in the Windows file system

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

Security functions

- Know-how protection for the parameter assignment, scripts and DCCs and DCC libraries with password and encryption
- Copy protection for the configuration on the drive unit. The project can only be opened together with the original card.
- Detection of parameter manipulation with STARTER via the project comparison, see also "AUTOHOTSPOT"
- Activation/deactivation of unused functions (web server, ports), see also "Integrated web server (Page 91)"
- Write protection for the parameter assignment, p-parameters are readable, but not writeable, protects against unintentional changes to the parameter assignment (only available online).

Know-how protection for drive units

In addition to the know-how protection for DCCs, DCC libraries and scripts, you can also protect the parameter assignment of your drive against unauthorized access via the know-how protection for the drive. The function is only available online. See also "Know-how protection (Page 86)".

Scripting

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

⚠ WARNING

Risk due to incorrect configurations for automated operating actions

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

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

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

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

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

8.3.13 SINAMICS Drive Control Chart (DCC)

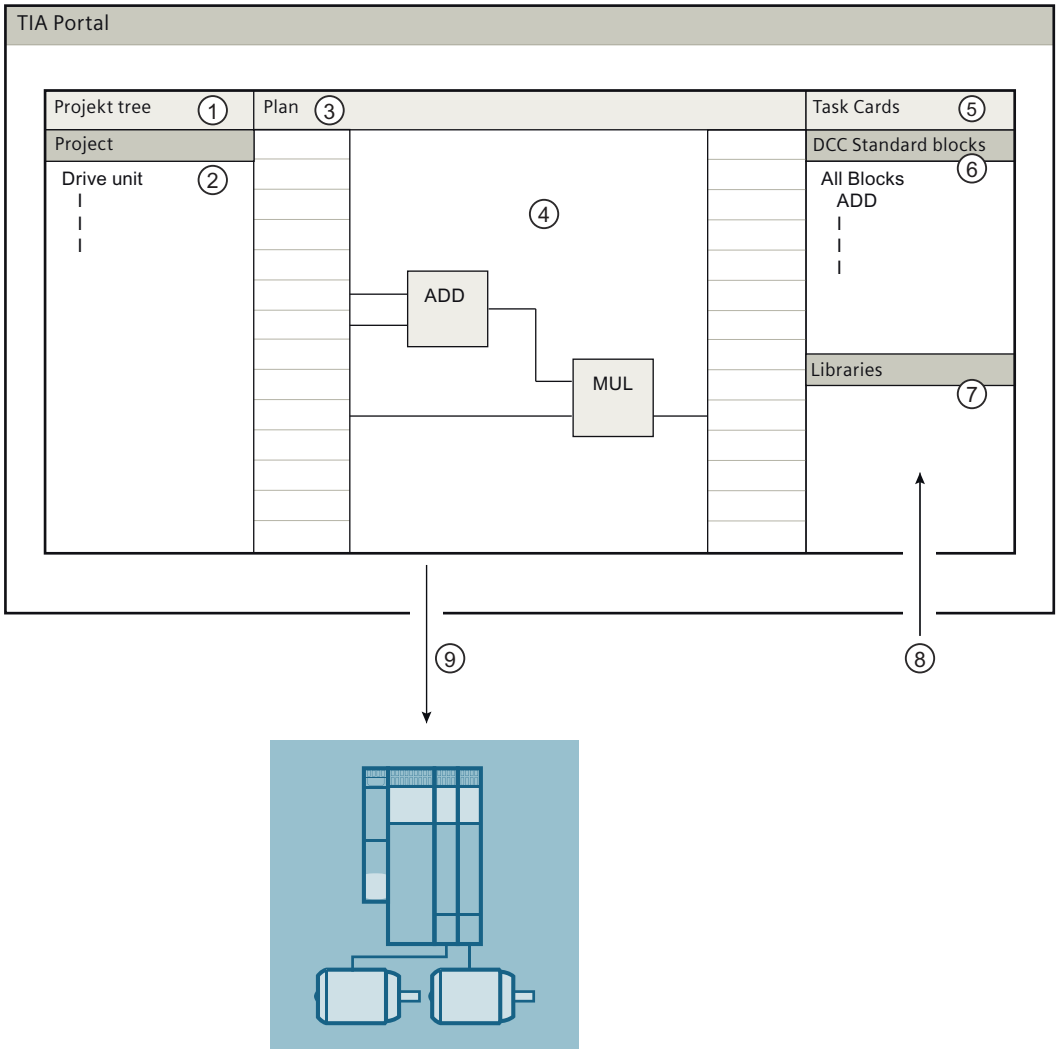
8.3.13.1 Industrial cybersecurity with SINAMICS DCC

Overview

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

With the Drive Control Chart Editor based on CFC, you configure the technology functions with DCC for SINAMICS drives graphically.

- Startdrive
  The following figure shows the data flow of the configuration data when configuring with SINAMICS DCC:



① Loading
② Import of DCB libraries

Figure 8-3 Flow of configuration data: TIA-DCC

- STARTER
  The following figure illustrates the data flow of the configuration data when configuring with SINAMICS DCC and the ways to protect the configured/programmed DCC sources:

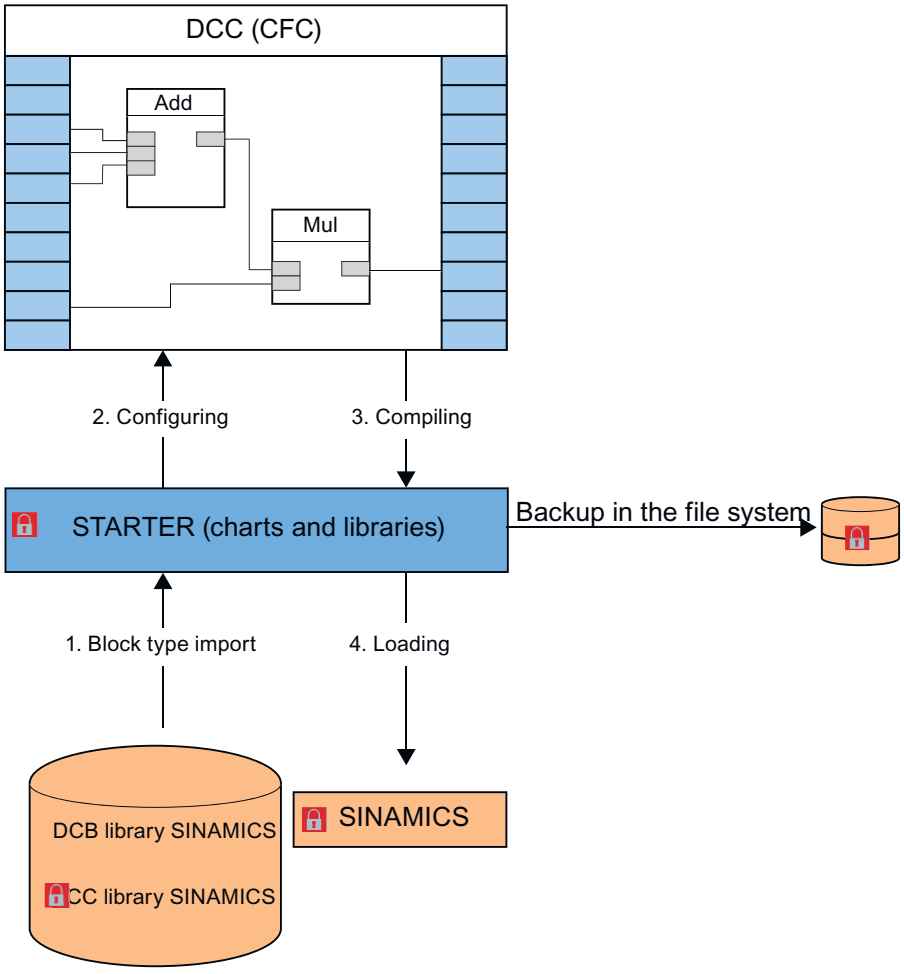


Figure 8-4 Flow of configuration data: Example for DCC Classic V2.1 ... V3.4 (STARTER)

Startdrive: Option package DCC

Note the following special features regarding Startdrive:

- DCC does not provide a backup in the file system.
- The DCB libraries used are loaded implicitly with the project into the target device
- DCC does not offer any chart know-how protection

Commissioning computer

Ensure the security of the commissioning computer. Follow the general security measures (Page 31) for this purpose.

Using know-how protection

DCCs, DCC libraries, programs and backup files are subject to an increased risk of manipulation. Therefore, use the know-how protection, the write protection for drive units and the know-how protection for DCC charts and DCC libraries in STARTER, see also Use write and know-how protection (Page 102).

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

Protecting backup files in the Windows file system

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

Note the information on SINAMICS and on the engineering systems

Also note the industrial cybersecurity information for SINAMICS drives and engineering systems with which SINAMICS drives are commissioned. Particularly the information on network security is important, see also Network security (Page 36).

8.3.13.2 Use write and know-how protection

Prevent unauthorized changes by means of know-how protection

⚠ WARNING

Danger to life through manipulation of DCC charts and DCC libraries

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

- Protect important DCC charts and DCC libraries via "Know-how protection programs" or "Know-how protection drive units" in SCOUT or STARTER. Assign a strong password to prevent manipulation.
- Protect important DCC charts and DCC libraries via "Know-how protection drive units" in Startdrive V16 or higher. Assign a strong password to prevent manipulation.
- Therefore, for "Know-how protection programs" or "Know-how protection drive units", use passwords which include at least eight characters, upper and lower case letters, numbers, and special characters.
- Make sure that only authorized personnel can access the passwords.
- Protect the backup files on your file system using a write protection.

8.3.14 SINAMICS Smart Access Module

The optional Smart Access Module offers you an intelligent solution for commissioning the SINAMICS V20 or G120 converter.

The Smart Access Module is a web server module with integrated WLAN connectivity. It allows web-based access to the converter from a connected device (conventional PC with WLAN adapter, tablet or smartphone). This module is only intended for commissioning and therefore cannot be used with the converter for the long term.

NOTICE

WLAN: Changing a default password

The misuse of passwords can also represent a considerable security risk. As a result of incorrect or changed parameterization, machines can malfunction, which in turn can lead to injuries or death.

- After logging on to the Smart Access Module for the first time, change the module's default password.
- Assign a secure password. Information on this can be found in the Operating Instructions of the respective converter.

NOTICE

Unauthorized access to the converter via the SINAMICS Smart Access Module

Unauthorized access to the converter via the Smart Access Module as a result of cyber attacks could lead to interruptions in the process and thus to property damage or personal injury.

- Before you log in to the web pages, check the status LED on the Smart Access Module. If the status LED is green or flashing, unauthorized access could have occurred: Switch the SINAMICS Smart Access Module off and then on again using the on-off switch to re-establish the WLAN connection.

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

- SINAMICS V20 Converter Operating Instructions (https://support.industry.siemens.com/cs/de/en/view/109773836)
- SINAMICS G120 Smart Access Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109771299)

8.4 SIMOCRANE

Availability, productivity, and safety are the decisive factors in crane applications. Since SIMOCRANE products are based on products from SIMOTION and SINAMICS, observe the product-specific hardening measures in Chapters AUTOHOTSPOT and SINAMICS (Page 85) for hardening.

References

A

General information

Further **general information** on industrial cybersecurity is available on the Internet:

- Industrial cybersecurity (https://www.siemens.com/global/en/products/automation/topic-areas/industrial-cybersecurity.html)
- Cybersecurity topics (https://new.siemens.com/global/en/company/topic-areas/cybersecurity.html)
- Secure Digitalization (https://www.siemens.com/global/en/company/digital-transformation/cybersecurity.html)
- Certifications and standards (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/certification-standards.html)
- Whitepapers and downloads (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/downloads.html)

Secure passwords

More information on assigning secure passwords can be found in the chapter under the following addresses:

- European Network and Information Security Agency (enisa). (https://www.enisa.europa.eu/media/news-items/basic-security-practices-regarding-passwords-and-online-identities)
- National Institute of Standards and Technology (NIST) (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf)
- Federal Office for Information Security (BSI) (https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html)(only relevant for Germany)

Web pages of the products

Further product-specific information about industrial cybersecurity is available at the **individual product websites**:

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

Product-specific manuals

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

- "SINUMERIK 840D sl NCU 7x0.3 PN" Equipment Manual (https://support.industry.siemens.com/cs/ww/en/view/109782727)
- "Commissioning CNC: NC, PLC, Drive" Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109801198)
- "SINUMERIK 840D sl Operating System NCU (IM7)" Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109783230)
- "SINUMERIK 840D sl Base Software and HMI sl" Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109254363)
- SINUMERIK 840Dsl Safety Integrated plus Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109777982)
- "SINUMERIK Operate (IM9)" Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109801207)
- PCU-Basesoftware (IM8) Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109748542)
- "PCU Base Software (IM10)" Commissioning Manual (https://support.industry.siemens.com/cs/de/en/view/109769185)
- SINUMERIK Access MyMachine /P2P (PC) Operating Manual (https://support.industry.siemens.com/cs/ww/en/view/109811131)
- SINUMERIK Access MyMachine /OPC UA Configuration Manual (https://support.industry.siemens.com/cs/us/en/view/109807257)
- Manage MyMachines /Remote Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109759394)
- Diagnostics Manual 808D (https://support.industry.siemens.com/cs/de/en/view/109763685)
- SIMOTION IT Programming and Web Services Programming Manual (https://support.industry.siemens.com/cs/ae/en/view/109801546)
- SIMOTION IT Diagnostics and Configuration Diagnostics Manual (https://support.industry.siemens.com/cs/ww/en/view/109801545)
- SIMOTION IT Virtual Machine and Servlets Programming Manual (https://support.industry.siemens.com/cs/ww/en/view/109801548)
- SIMOTION IT OPC UA Programming Manual (https://support.industry.siemens.com/cs/ww/en/view/109801547)
- BA_G110M (https://support.industry.siemens.com/cs/ww/en/view/109782996)
- Communication with SIMOTION System Manual (https://support.industry.siemens.com/cs/ww/en/view/109801516)
- SINAMICS S120 Drive Functions Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781535)
- SINAMICS S120 Control Units and Additional System Components Equipment Manual (https://support.industry.siemens.com/cs/ww/en/view/109782370)

- SINAMICS S120 Safety Integrated Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781722)
- SINAMICS S120 Communication Function Manual (https://support.industry.siemens.com/cs/ww/en/view/109781721)
- SINAMICS S120/S150 List Manual (https://support.industry.siemens.com/cs/ww/en/view/109781807)
- G110M Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109782996)
- G120 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109771299)
- SINAMICS G Fieldbuses Function Manual (https://support.industry.siemens.com/cs/ww/de/view/109757336/en)
- S210 Operating Instructions (https://support.industry.siemens.com/cs/ww/en/view/109801184)
- V20 Operating Instructions (https://support.industry.siemens.com/cs/de/en/view/109773836)
- Function Manual S7-1500, ET 200SP, ET200pro web server (https://support.industry.siemens.com/cs/ww/en/view/59193560)
- SIMATIC Programming with STEP 7 Programming and Operating Manual (https://support.industry.siemens.com/cs/de/en/view/109751825)
- SIMATIC S7-300 CPU 31xC and CPU 31x Equipment Manual: Technical specifications (https://support.industry.siemens.com/cs/de/en/view/12996906)
- SIMATIC NET Configuration Manual: SCALANCE X-200 Industrial Ethernet switches (https://support.industry.siemens.com/cs/de/en/view/109757352)

See also

Industrial Cybersecurity (https://new.siemens.com/global/en/products/automation/topic-areas/industrial-security/planning.html)

Safety Integrated plus Commissioning Manual (https://support.industry.siemens.com/cs/ww/en/view/109777982)

Glossary

Allowlist

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

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

AMC

Abbreviation for SINUMERIK Integrate Analyze MyCondition

AMD

Abbreviation for SINUMERIK Integrate Access MyData

AMM

Abbreviation for SINUMERIK Integrate Access MyMachine

AMP

Abbreviation for SINUMERIK Integrate Analyze MyPerformance

AMT

Abbreviation for Intel® Active Management Technology

Area of attack

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

Attack

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

Authentication

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

Authorization

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

Availability

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

Blocklist

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

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

Brute force

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

Cloud computing

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

Code injection

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

Confidentiality

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

Cyber security

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

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

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

Denial of service (DoS)

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

DMZ

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

Firewall

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

Hacker

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

Hardening

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

IANA

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

Incident

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

Industrial cybersecurity

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

Information security

Safeguards the confidentiality, integrity and availability of information.

Integrity

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

Internet of Things (IoT)

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

IPsec (Internet Protocol Security)

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

Least Privilege principle

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.

Malware

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

Man-in-the-disk attack

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

Man-in-the-middle attack

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

MMP

Abbreviation for SINUMERIK Integrate Manage MyPrograms

MMT

Abbreviation for SINUMERIK Integrate Manage MyTools

NAT (Network Address Translation)

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

NCU

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

OpenVPN

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

Pairing

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

Patch management

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

Patterns of viruses

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

PCU

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

Phishing

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

Remote access

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

SCADA

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

Security

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

Security hole

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

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

SIEM system

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

Switch

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

Threat

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

Threat and Risk Analysis (TRA)

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

TIA Portal

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

TLS

Transport Layer Security (TLS V1.2 or higher) is a hybrid encryption protocol for secure transfer of data in the Internet.

VPN (Virtual Private Network)

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

WSUS (Windows Server Update Services)

Windows Server Update Services (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-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

Anti-virus program, 48
Application security, 25

B

BIOS password
    PCU 50, 67
Block encryption
    SINUMERIK, 69
Block protection, 69
    SINUMERIK, 69

C

Certificates
    SINAMICS, 92
Changing passwords
    SINUMERIK, 65
Cloud, 41
Cloud Applications, 41
Cloud computing, 23
Cloud Security, 41
Code analysis, 26
Communication
    Communication services, 60
    Used port numbers, 60
Communication services
    SINAMICS, 91
Company security, 34
Confidentiality levels, 47
Copy protection
    SINUMERIK, 68

D

Data
    transporting, 47
Data privacy, 24
Deactivating a PROFINET interface
    SINUMERIK 840D sl, 59
    SINUMERIK ONE, 59
Defense in depth, 32
Defense in depth concept, 32
Disable
    USB interface, 59
Disabling a USB interface
    SINUMERIK, 59
DMZ network, 37

E

Effects, 24
Encrypting cycles
    SINUMERIK, 68
Exchangeable storage media
    SINAMICS, 87, 88
    SINUMERIK, 62
Exchangeable storage medium, 47

F

Firewall, 37
Firmware update
    MCP/MPP, 58

H

Hard disk, 47
HMI password, 65

I

IEC 62443, 28
Industrial Cybersecurity
    Definition, 21
    Objectives, 21
    Possible effects, 24
    Threats, 24
Internet of things, 23
Internet of Things, 23
IoT, 23
ISO 27005, 28

K

Know-how protection
    SINAMICS, 86

L

Linux password, 65
Lock MyCycles
  SINUMERIK Integrate, 68
Lock MyPLC
  SINUMERIK Integrate, 69

M

Main entry, 69
MCP/MPP
  Firmware update, 58
Mobile devices, 23
Mobile networks, 23
Mobile radio standards, 23

N

NCK password, 65
Network security, 33

P

Parameters: Access levels
  SINAMICS, 87
Patch management, 26
Patches, 62
PCU 50 BIOS password, 67
Plant security, 33
PLM, 26
Ports, 45
Positive list, (SINUMERIK)
Product Lifecycle Management process, 26
ProductCERT, 26
Production security, 34
Protection levels, 33
Protection zone, 36

R

Regulations, 28
Remote access, 23

S

SCALANCE S, 37
Security integrity, 26
Security management process, 29
Security Module
  SCALANCE S, 37
Security service, 25
Security support, 25
Security update, 62
  IPC, 62
  PCU, 62
Security vulnerabilities, 24
Services, 45
SI HSC, 27
Siemens Industrial Holistic Security Concept, 27
  Business Impact Assessment, 27
  Monitoring of residual risk, 27
  Scope, 27
  Target Protection Level, 27
SINAMICS
  Certificates, 92
  Communication services, 91
  Exchangeable storage media, 87, 88
  Know-how protection, 86
  Parameters: Access levels, 87
  Software manipulation, 87, 88
  Transport Layer Security, 92
  Used port numbers, 91
  Virus protection, 87, 88
  Web server, 91
  X140, 94
SINUMERIK
  Block encryption, 69
  Block protection, 69
  Changing passwords, 65
  Copy protection, 68
  Deactivating a PROFINET port, 59
  Disabling a USB interface, 59
  Encrypting cycles, 68
  Exchangeable storage media, 62
  Positive list, 61
  Software manipulation, 62
  Virus protection, 61, 62
  Web server, 67
SINUMERIK 808D, 56
SINUMERIK 828D, 56
SINUMERIK 840D sl, 56
SINUMERIK Integrate
  Lock MyCycles, 68
  Lock MyPLC, 69
SINUMERIK MC, 56
SINUMERIK ONE, 56
Smart Access Module
  SINAMICS G120, 102
  SINAMICS V20, 102

Software manipulation
SINAMICS, 87, 88
SINUMERIK, 62
Standards, 28
System integrity, 33

T

Tablet PCs, 23
Threats, 24
TLS, 92
Transport
Data, 47
Transport Layer Security
SINAMICS, 92

U

USB stick, 47
Used port numbers
SINAMICS, 91
User accounts, 45

V

Validity
Documentation, 9
Virus protection
SINAMICS, 87, 88
SINUMERIK, 61, 62
Virus protection program, 48
Virus scanner, 48

W

Web server
SINAMICS, 91
SINUMERIK, 67
Windows Server Update Service, 49
Wireless technology, 23
WSUS, 49

X

X140
SINAMICS, 94