Preface

Fundamental safety instructions 1

What is industrial security? 2

Why is industrial security so important? 3

What security measures does Siemens take? 4

Security management 5

General security measures 6

Product-specific security measures 7

References A

01/2015

6FC5397-5EP40-5BA2
Legal information

Warning notice system

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

⚠️ DANGER

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

⚠️ WARNING

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

⚠️ CAUTION

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

NOTICE

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

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

Qualified Personnel

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

Proper use of Siemens products

Note the following:

⚠️ WARNING

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

Trademarks

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

Disclaimer of Liability

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

Documentation

The documentation is divided into the following categories:

- General documentation
- User documentation
- Manufacturer/service documentation

Additional information

You can find information on the following topics under the link (http://www.siemens.com/motioncontrol/docu):

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

If you have any questions about the technical documentation (e.g. suggestions for improvement, corrections), please send us an e-mail (mailto:docu.motioncontrol@siemens.com)

My Documentation Manager (MDM)

At the link to My Documentation Manager (http://www.siemens.com/mdm), you will find information on how to individually compile OEM-specific machine documentation based on the Siemens content:

Training

For information about the range of training courses, refer to:

- SITRAIN (www.siemens.com/sitrain) - training courses from Siemens for products, systems and solutions in automation technology
- Security training, e.g. with SITRAIN: IK-IESEC (Security in Industrial Ethernet networks)

FAQs


SINUMERIK

Information on SINUMERIK can be found on the SINUMERIK homepage (http://www.siemens.com/sinumerik).
SIMOTION

Information on SIMOTION can be found on the SIMOTION homepage (http://www.siemens.com/simotion).

SINAMICS

Information on SINAMICS can be found on the SINAMICS homepage (http://www.siemens.com/sinamics).

Target group

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

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

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

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

Benefits

The "Industrial Security" documentation contains recommendations and information for the planning and design of secure systems or plants. The documentation serves as a reference manual and guideline.

This documentation is strictly of a recommendatory nature and is intended to support customers in safely operating their controls or plants. You, as operator, are responsible for implementing the security recommendations.
Hotline and Internet address

Technical Support

Country-specific telephone numbers for technical support are provided under Product support (www.siemens.com/automation/service&support)
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>...........................................................................................................</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>Fundamental safety instructions</td>
<td>9</td>
</tr>
<tr>
<td>1.1</td>
<td>General safety instructions</td>
<td>9</td>
</tr>
<tr>
<td>1.2</td>
<td>Industrial security</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>What is industrial security?</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>Why is industrial security so important?</td>
<td>13</td>
</tr>
<tr>
<td>3.1</td>
<td>Trends in the IT sector</td>
<td>13</td>
</tr>
<tr>
<td>3.2</td>
<td>Possible corporate security holes</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>What security measures does Siemens take?</td>
<td>17</td>
</tr>
<tr>
<td>5</td>
<td>Security management</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>General security measures</td>
<td>21</td>
</tr>
<tr>
<td>6.1</td>
<td>Overview</td>
<td>21</td>
</tr>
<tr>
<td>6.2</td>
<td>Plant safety</td>
<td>23</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Physical protection of critical production areas</td>
<td>23</td>
</tr>
<tr>
<td>6.3</td>
<td>Network security</td>
<td>24</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Network segmentation</td>
<td>24</td>
</tr>
<tr>
<td>6.3.1.1</td>
<td>Separation between production and office networks</td>
<td>24</td>
</tr>
<tr>
<td>6.3.1.2</td>
<td>Network segmentation with SCALANCE S</td>
<td>25</td>
</tr>
<tr>
<td>6.4</td>
<td>System integrity</td>
<td>27</td>
</tr>
<tr>
<td>6.4.1</td>
<td>System hardening</td>
<td>27</td>
</tr>
<tr>
<td>6.4.1.1</td>
<td>Reduction of attack points</td>
<td>27</td>
</tr>
<tr>
<td>6.4.1.2</td>
<td>Virus scanner</td>
<td>28</td>
</tr>
<tr>
<td>6.4.2</td>
<td>Patch management</td>
<td>28</td>
</tr>
<tr>
<td>7</td>
<td>Product-specific security measures</td>
<td>29</td>
</tr>
<tr>
<td>7.1</td>
<td>SINUMERIK</td>
<td>30</td>
</tr>
<tr>
<td>7.1.1</td>
<td>Firewall and networking</td>
<td>30</td>
</tr>
<tr>
<td>7.1.2</td>
<td>System hardening</td>
<td>33</td>
</tr>
<tr>
<td>7.1.2.1</td>
<td>Deactivating hardware interfaces</td>
<td>33</td>
</tr>
<tr>
<td>7.1.2.2</td>
<td>Notes on virus protection</td>
<td>34</td>
</tr>
<tr>
<td>7.1.2.3</td>
<td>PCU virus scanner</td>
<td>34</td>
</tr>
<tr>
<td>7.1.2.4</td>
<td>Whitelisting</td>
<td>35</td>
</tr>
<tr>
<td>7.1.3</td>
<td>Microsoft security update process</td>
<td>36</td>
</tr>
<tr>
<td>7.1.4</td>
<td>Passwords</td>
<td>37</td>
</tr>
<tr>
<td>7.1.4.1</td>
<td>Definition of access levels</td>
<td>37</td>
</tr>
<tr>
<td>7.1.4.2</td>
<td>PLC web server</td>
<td>38</td>
</tr>
<tr>
<td>7.1.5</td>
<td>Know-how protection</td>
<td>38</td>
</tr>
<tr>
<td>7.1.5.1</td>
<td>SINUMERIK Integrate Lock MyCycle</td>
<td>38</td>
</tr>
<tr>
<td>7.1.5.2</td>
<td>SINUMERIK Integrate Lock MyPLC</td>
<td>39</td>
</tr>
</tbody>
</table>
## Table of contents

7.1.5.3 Encryption of blocks ................................................................. 39
7.1.5.4 SIMATIC Logon ........................................................................ 40
7.2 SIMOTION ....................................................................................... 41
  7.2.1 Overview ................................................................................ 41
  7.2.2 System hardening ...................................................................... 43
  7.2.2.1 Port security ......................................................................... 43
  7.2.2.2 Virus scanners, Windows security patches, SIMOTION P ............ 44
  7.2.3 Secure project storage ............................................................... 45
  7.2.4 Know-how protection .............................................................. 47
  7.2.4.1 Secure access control with SIMATIC Logon ............................... 47
  7.2.4.2 Know-how protection in engineering .................................... 48
  7.2.3 Copy protection for the configuration on the control system ............. 50
  7.2.5 Offline/online comparison ......................................................... 51
  7.2.6 SIMOTION IT Web server .......................................................... 53
7.3 SINAMICS ...................................................................................... 56
  7.3.1 Overview ................................................................................. 56
  7.3.2 Write and know-how protection .............................................. 56
  7.3.3 Communication services and used port numbers ......................... 57
  7.3.4 Web server ............................................................................. 57
  7.3.5 Certificates for the secure data transfer ..................................... 58
  7.3.6 Parameters: Access levels + password ...................................... 59
  7.3.7 Virus protection / memory card ............................................. 59

A References .......................................................................................... 61

Glossary .................................................................................................. 63

Index ...................................................................................................... 65
1.1 General safety instructions

**WARNING**

Risk of death if the safety instructions and remaining risks are not carefully observed

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

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

**WARNING**

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

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

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

Note

Industrial security

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit Hotspot-Text [http://www.siemens.com/industrialsecurity].

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit Hotspot-Text [http://support.automation.siemens.com].

⚠️ WARNING

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

Software manipulation (e.g. by viruses, Trojan horses, malware, worms) can cause unsafe operating states to develop in your installation which can result in death, severe injuries and/or material damage.

- Keep the software up to date.
  
  You will find relevant information and newsletters at this address [http://support.automation.siemens.com].

- Incorporate the automation and drive components into a holistic, state-of-the-art industrial security concept for the installation or machine.
  
  You will find further information at this address [http://www.siemens.com/industrialsecurity].

- Make sure that you include all installed products into the holistic industrial security concept.
What is industrial security?

Definition of industrial security

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

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

Objectives of industrial security

The objectives of industrial security encompass:

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

An optimized and adapted security concept applies for automation technology. The security measures must not hamper or endanger production.
What is industrial security?
Why is industrial security so important?

3.1 Trends in the IT sector

Overview

There are many new trends which affect industrial security:

- Cloud computing in general
  
  The number of network connections across the world is constantly increasing. This enables innovations such as cloud computing and the applications that go hand in hand with it. In conjunction with cloud computing, there has been a massive increase in the number of mobile devices, such as mobile 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.

- Smart Grid
  
  Networking is not only limited to data networks, it also influences our energy infrastructure.

- Worldwide remote access to plants, machines and mobile applications

- The "Internet of things"
  
  Millions of electronic devices are becoming network-capable and are communicating via the Internet, such as onboard computers in cars, which send warranty information to dealers, or water meter sensors that transmit water consumption data to municipal water suppliers via radio.

However, in order for everything from cloud computing to sensors to work without service disruptions, you need reliable network infrastructures that are well protected against attacks from malware and hackers.
3.2 Possible corporate security holes

Possible security holes or weak points

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

- Employees
- Production plants
- Network infrastructure
- Data centers
- PC workstations
- Laptops
- Tablet PCs
- Printers
- Smartphones
- Portable storage media
- Guidelines and regulations

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

The topic of data security and access protection (security) is becoming more and more important in industrial environments. The progressive networking of entire industrial plants, the vertical integration and networking of the individual levels of a company, and new technologies, such as remote maintenance and remote access, are leading to increased requirements for protecting industrial plants.

The threats are diverse and the consequences far-reaching.

Possible threats:

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

- Loss of intellectual property
- Loss of production or reduced product quality
- Company image and economic damage
- Catastrophic environmental influences
- Danger to persons and machines
Why is industrial security so important?

3.2 Possible corporate security holes
What security measures does Siemens take?

Siemens concerns itself with security aspects on three levels:

- **Application security** refers to products and functions which take the needs of industrial security in the field of automation into consideration. This involves particular consideration of the application and task at hand, as well as the persons performing the actions in an automated plant. This allows industrial security to be easily implemented in production processes.

- **Security support** provides support during the analysis, planning, implementation, testing and optimization of industrial security - by means of specialists with special knowledge of networks and the industry. These services lead to the highest possible level of industrial security and operating capacity of the production plant.

- **Security service** provides support to users during all phases of the life cycle, during the planning, implementation and checking of their production plants with regard to industrial security. This includes analysis and security checks of the network structure in the production network and the working out of a holistic security concept.

**Security measures**

For the latest Siemens products, industrial security needs have already been taken into consideration:

- Siemens constantly checks the measures for hardening:
  - Configuring operating systems in such a way that points of attack (e.g. via ports, unneeded services) are minimized.
  - Siemens performs tests with analysis software, such as Nessus, to detect any network and vulnerability weak points.

- The Siemens ProductCERT (Cyber Emergency Readiness Team) is the central department for safety-related incidents in the Siemens product and solution environment. Siemens ProductCERT supports development work with consulting and other services. ProductCERT provides information about current threats and vulnerabilities as well as the appropriate countermeasures.

- Siemens regularly tests leading virus scanners for their compatibility with its products (Page 34).
What security measures does Siemens take?
The security management process as a basis

Protect your system and your company! Security management forms the basis for the successful implementation of industrial security.

The security management process is shown in the following:

1. The first step is to perform a risk analysis. Determine all possible risks and define countermeasures for reducing the risk to an acceptable level. In detail, a risk analysis encompasses the following steps:
   - Identification of threatened objects
   - Analysis of value and potential for damage
   - Threat and weak point analysis
   - Identification of existing security measures
   - Risk evaluation

2. The second step encompasses the specification of guidelines and the introduction of coordinated organizational measures. To this end, the awareness of the importance of industrial security must be borne by all levels of the company. In addition, define guidelines and processes in order to achieve a uniform process and to support compliance with the defined industrial security concept.
3. Introduce coordinated technical measures. You can find a list of general measures that help to protect your plant against threats in Chapter General security measures (Page 21). You can find measures recommended for SINUMERIK, SIMOTION and SINAMICS environments in Chapter Product-specific security measures (Page 29).

4. After the measures are implemented, a security audit must ensure that all of the measures have been implemented and that they have also eliminated or reduced the identified risks.

---

**Note**

**Continuous process**

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

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

Additional specific security measures for SINUMERIK, SIMOTION and SINAMICS products can be found in Chapter Product-specific security measures (Page 29).

Basically, the measures should be coordinated with one another and correspond to the ring-shaped principle of the "Defense in Depth" strategy. The measures are structured according to the "onion" principle and each measure forms an additional protective layer around the core: the production plant.

**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.
General security measures

6.1 Overview

- **System integrity**

  "System integrity" represents the combination of two major measures. PC-based systems and the control level must be protected against attacks. Steps include the following measures:

  - User authentication for machine or plant operators with individual authorization levels
  - Integrated access protection mechanisms in the automation components to prevent unauthorized changes via the engineering system or during maintenance
  - The use of antivirus and whitelisting software to protect PC systems against malware
  - Maintenance and update processes to keep the automation systems up-to-date (e.g. patch management, firmware updates, etc.)
6.2 Plant safety

6.2.1 Physical protection of critical production areas

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.

Company security

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

- Closed off and monitored company premises
- Entry control, keys / card readers and/or security personnel
- Escorting of external personnel by company employees

Physical production security

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

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

Additional information

6.3 Network security

6.3.1 Network segmentation

6.3.1.1 Separation between production and office networks

One important protective measure for your control is the strict separation of the production networks and the other company networks.

Separation by means of a firewall system

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

Separation via a DMZ network

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

Note

The production networks should also be divided into separate automation cells in order to protect critical communication mechanisms.
6.3.1.2  Network segmentation with SCALANCE S

Siemens provides SCALANCE S security modules to meet network protection and network segmentation requirements.

SCALANCE S security modules

SCALANCE S security modules with Security Integrated provide:

- Stateful inspection firewall
  
  In order to implement user-specific control and logging, firewall rules can also be specified that only apply to certain users.

- VPN via IPsec (data encryption and authentication)
  
  This establishes a secure tunnel between authenticated users whose data cannot be intercepted or manipulated. The most important aspect is the protection against external access via the Internet.

- NAT/NATP (address translation)

- Router functionality (PPPoE, DDNS) for broadband Internet access (DSL, cable)

- S623 with additional VPN port (DMZ) enables the secure connection of an additional network for service and remote maintenance purposes. S623 also permits the secure, redundant connection of subordinate networks by means of routers and firewall redundancy.

Principle

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

6.4.1 System hardening

6.4.1.1 Reduction of attack points

Network services and ports

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

A description of the ports used can be found in the Manuals and Function Manuals of the respective products.

User accounts

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

- Reduction of configured/activated user accounts to the actually needed minimum
- Use of secure access data for existing accounts
- Regular checks, especially of the locally configured user accounts
- Regular change of passwords

Passwords

<table>
<thead>
<tr>
<th>NOTICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing default passwords</td>
</tr>
</tbody>
</table>

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

We recommend that default passwords be changed during the commissioning and changed at regularly defined intervals as required.
6.4 System integrity

6.4.1.2 Virus scanner

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

In order to be used on industrial control components, a virus scanner should therefore meet the following requirements:

Virus scanner requirements

- If a local firewall that has been adapted to the production operations is used, it must be possible to install the virus scanner without its own firewall.
- The virus scan clients can be divided into (product- and task-specific) groups and configured separately.
- It must be possible to deactivate the automatic distribution of the virus signatures and other updates.
- It must be possible to carry out the distribution of the virus signatures and updates manually and in groups.
- It must be possible to conduct a file scan and system scan manually and in groups.
- For the virus detection scenario, a message can be configured without a file action such as "Delete", "Clean", etc. being automatically carried out.
- It must be possible to log all of the messages on the virus scan server.
- On a virus scan client, it must be possible to suppress the local message window because it could obscure important messages from the production process.

Note

Installation of software

The installation of software is often a process which represents a serious and complicated change to the respective system. The storage location of the files to be installed must always be free of viruses (e.g. a file server with its own virus scanner or DVD checked for viruses).

6.4.2 Patch management

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

The fully automatic update process ensures that Microsoft security updates are always available on Siemens clients.
This Chapter describes additional product-specific security measures for SINUMERIK, SIMOTION and SINAMICS devices.
7.1 SINUMERIK

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

7.1.1 Firewall and networking

NCU/PCU networking structure

The following graphic shows the networking of the control system (NCU) and the PCU. The networking into the company network is made using X130 to the NCU and Eth 1 to the PCU. A firewall protects these two interfaces against unauthorized access.

The Linux kernel includes packet filter functionality (firewall) that filters the connection to the factory network via this firewall. 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 detected and blocked. This way, the control is protected against brute-force attacks.

NOTICE

X120 security interface

Please note that the X120 interface is exclusively for plant network connections. This is a local network and may not be connected to the Internet!
Product-specific security measures

7.1 SINUMERIK

Figure 7-1 NCU/PCU networking
Deactivating the firewall

The X130 Ethernet interface of the SINUMERIK 840D sl/828D/808D controls is 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 in the following way:

1. Select the "Start-up" operating area.

2. Press the menu forward key.

3. Press the "Network" softkey.

   The "Overview of the Network Settings" window opens.

4. Press the "Company network" softkey.

5. Press the "Change" softkey to edit settings.

6. Add a port, such as **TCP/22**, under "Firewall exceptions" > "Additional ports".

   Alternatively, you can configure the firewall via the "basesys.ini". For further information please refer to the respective manuals.

   More detailed information on the configuration of the firewall can be found in the "NCU (IM7) Operating System" Manual and in the "PCU Base Software (IM10)" Manual.
### 7.1.2 System hardening

#### 7.1.2.1 Deactivating hardware interfaces

## Deactivating Interfaces

<table>
<thead>
<tr>
<th>Measure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deactivate/activate Ethernet interfaces in the BIOS of the PCU</td>
<td>You can activate or deactivate the Ethernet interfaces in the BIOS of the PCU. Detailed information on this topic can be found in the &quot;SINUMERIK 840D sl PCU Base Software (IM8)&quot; Manual, Chapter &quot;BIOS settings&quot;.</td>
</tr>
<tr>
<td>Deactivate/activate USB interfaces</td>
<td>To prevent malicious software entering the control or the plant network via the USB interfaces, you can disable them. Use the service command &quot;sc_usb disable&quot;. Use this function to make your system more secure and protect it from unwanted manipulation and malware. Detailed information can be found in the &quot;SINUMERIK 840D sl PCU Base Software (IM8)&quot; Manual, Chapter &quot;Deactivating USB interfaces&quot;.</td>
</tr>
</tbody>
</table>

## Deactivating ports

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

### Reference

A detailed overview of the logical Ethernet ports used and protocols for SINUMERIK can be found in the “NCU 7x0.3 PN, NCU 7x0.3B PN” Manual.
7.1.2.2 Notes on virus protection

Distribution of virus signatures

Note
Take necessary measures to protect against viruses
Take all the necessary measures for virus protection in the CNC environment. This also includes the proper handling of data carriers, USB flash drives and network connections, precautionary measures when copying data and during software installations, etc.

7.1.2.3 PCU virus scanner

Permitted virus scanners for SINUMERIK
Three virus scanners have been tested for compatibility with our software:

<table>
<thead>
<tr>
<th>Manufacturer</th>
<th>Homepage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trend Micro Inc.</td>
<td>Trend Micro Inc. homepage (<a href="http://www.trendmicro.com">http://www.trendmicro.com</a>)</td>
</tr>
<tr>
<td>Symantec Corporation</td>
<td>Symantec homepage (<a href="http://www.symantec.com/index.jsp">http://www.symantec.com/index.jsp</a>)</td>
</tr>
<tr>
<td>Intel Security (McAfee)</td>
<td>McAffee homepage (<a href="http://www.mcafee.com/us/">http://www.mcafee.com/us/</a>)</td>
</tr>
</tbody>
</table>

You can download the current version of the virus scanners from the manufacturer's homepage or purchase it. During the installation, also note the special information about restrictions.

The simultaneous installation of several virus scanners on a single system has not been tested. We recommend that you do not install several virus scanners on a PCU50 at the same time.

Compatibility tests

Note
Compatibility tests
The functionality of the anti-virus software and virus patterns must be ensured for the system-specific configurations by means of tests. Testing at Siemens can only cover a basic configuration.

Which virus scanners have been tested with which hardware/software combination can be found in the following overview: Compatibility of virus scanner (http://support.automation.siemens.com/WW/view/de/19577116)
**Tips for working with virus scanners**

- The virus scanner allows a real-time virus search each time a file is accessed. This real-time protection of the anti-virus software can have an effect on the performance of the PCU.

- A time-controlled virus test of the entire hard disk can be carried out at preset times (scheduled scan, on-demand scan). This process is generally very time-intensive in terms of calculations and can considerably limit the performance of the simultaneously running HMI software. It is therefore recommended that you carry out this automatic virus test outside of operating hours (e.g. at fixed service times).

- It may happen that part of the required working memory (a few MB) will not be released again during the scan (virus search on the entire hard disk). If the scan is carried out repeatedly for the entire hard disk over a long period of time, without rebooting the system, this can lead to the entire working memory being used up. This can make the SINUMERIK user interface inoperable.

- If the anti-virus software runs a start-up scan, you should expect a considerable decrease in performance during system start-up. If the PCU has insufficient memory space, the system may even become inoperable. It is therefore highly recommended that you set the CPU utilization to low or deactivate the start-up scan.

**Reference**

Current recommendations for the use of virus scanners can be found on the Internet at SINUMERIK virus scanner (http://support.automation.siemens.com/WW/view/en/19577116).

**7.1.2.4 Whitelisting**

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

The basic concept of whitelisting is that all applications are not trusted unless they have been classified as trustworthy following appropriate checks. In other words, a whitelist is a list of trusted applications. This whitelist contains all applications that have been classified as trustworthy - these are allowed to be run on the SINUMERIK PCU.

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

**Reference**

A detailed description can be found on the Internet (http://support.automation.siemens.com/WW/view/de/89027076).
### 7.1.3 Microsoft security update process

#### Use cases of security updates

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

- **Security update before the first use in production**
  
  In a basic HMI system, security updates are integrated until the end of the development. Generally speaking, a few months pass before use in production by the end user (SINUMERIK system test, integration by the OEM, configuration and commissioning by end user). Thus, a new installation of MS security updates is necessary no later than its use in production by the end user.

- **Security update during use in production**
  
  We recommend that you regularly install the latest patches during maintenance intervals. The WSUS system functionality provided by Microsoft is available for this.

---

### Note

#### Availability

The availability of Microsoft security updates is published via Microsoft Security Bulletins. The use of security updates is entirely up to the customer and is their sole responsibility and can be based on the “evaluation of maximum severity” given in the Microsoft Security Bulletin. Microsoft publishes information on security updates and download links on the Internet ([http://www.microsoft.com/technet/security/current.aspx](http://www.microsoft.com/technet/security/current.aspx)).

---

### Reference

Detailed information on the compatibility of Microsoft security updates with a SINUMERIK PCU 50 can be found on the Internet ([http://support.automation.siemens.com/WW/view/de/19756304](http://support.automation.siemens.com/WW/view/de/19756304)).
7.1.4 Passwords

7.1.4.1 Definition of access levels

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

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

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

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

Access rights

Table 7-1 Protection levels concept

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

NOTICE

Changing default passwords

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

The default passwords for the basic commissioning procedure are listed in the documentation. We recommend that default passwords be changed during the commissioning and changed at regularly defined intervals as required.

Reference

You can find additional information on how you can change the passwords of the access levels along with other information on access levels for programs and softkeys and access rights for files in the manual "SINUMERIK Operate (IM9)", in chapter "General settings > Access levels".
7.1.4.2 **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, we recommend that you define a user and an associated password for it.

Further information on the PLC web server can be found in the "SIMATIC S7-300 web server" Function Manual on the Internet (www.siemens.com/automation/service&support).

7.1.5 **Know-how protection**

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

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

7.1.5.1 **SINUMERIK Integrate Lock MyCycle**

Using the "SINUMERIK Integrate Lock MyCycle" (cycle protection) function, cycles can be encrypted and then stored protected in the control. The cycles are encrypted outside the control with the SinuCom Protector program.

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

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

**Reference**

Detailed information on cycle protection can be found in the "CNC Commissioning: NCK, PLC, drive" Commissioning Manual, Chapter "Lock MyCycles - cycle protection".
7.1.5.2 **SINUMERIK Integrate Lock MyPLC**

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

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

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

**Reference**

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

7.1.5.3 **Encryption of blocks**

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

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

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

**Encryption**

You can recognize encrypted or non-encrypted blocks by the following symbols:

- 🔐 Decomilable encrypted block
- 🗝️ Encrypted block that cannot be decompiled

**Note**

**Command execution time**

Usually, the command execution time is increased because encrypted blocks cannot be processed in a fully optimized manner. The final cycle time can only be determined with encrypted blocks.
Note
Prolonged runtimes during POWER ON/CPU memory reset/download

The CPU startup time, the time required for CPU memory reset, and the block download time can be prolonged significantly.

7.1.5.4 SIMATIC Logon

User administration and traceability

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

More detailed information can be found in Chapter Secure access control with SIMATIC Logon (Page 47).
7.2 SIMOTION

7.2.1 Overview

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

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

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

7.2 SIMOTION

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

Reference

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

7.2.2.1 Port security

Deactivating hardware ports

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

**Note**

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

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

**Reference**

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

7.2.2.2 Virus scanners, Windows security patches, SIMOTION P

General information on virus scanners

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

SIMOTION P3x0 virus scanner

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

Note

Because of the resulting performance impairments, the installation and use of a standard virus scanner on a SIMOTION P3x0 during system runtime does not make sense and is not permitted.

Using a virus scanner

As a standard virus scanner cannot be used for SIMOTION P3x0, an alternative procedure is followed. The virus scanner is installed to a separately bootable Windows PE operating system. It is started, for example, from a CD or a USB storage device and then performs a virus scan.

Note

FAQ Service & Support portal

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

Windows security patches

A brief test is performed when a new SIMOTION version is released. During this brief test, a check is performed to establish whether the installation of the security update has affected any basic functions.

See also


7.2.3 Secure project storage

Project data storage in SIMOTION SCOUT

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

File structure

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

Engineering data (ES)

- Standard storage: File structure in project trees
  STEP 7 and SIMOTION SCOUT objects in the project directory. These objects are not secure and can be edited by anyone if there is no know-how protection for programs (in this context programs are synonymous with units, which can contain the programs, function blocks and functions) and libraries or external file encryption is used.

- XML data
  Project data created via an XML export/import. The know-how protection is retained.

Runtime data (data on the CF card (RT))

- ZIP archive of the SIMOTION project (not binary).
  The project archive can be stored on the CF card of the respective SIMOTION controller. The archive can be transferred, e.g. via SIMOTION SCOUT or standard methods (FTP transfer).

- Binaries (zipped, unzipped)
  Binaries contain the compiled, executable project with the configurations and applications.
  Changes cannot be made during runtime without the SIMOTION SCOUT project because the project is stored as binary data on the SIMOTION controller.

The following figure shows an example of possible project data storage with display of the protected data.
Product-specific security measures

7.2 SIMOTION

Figure 7-3 SIMOTION SCOUT project data storage
7.2.4 Know-how protection

7.2.4.1 Secure access control with SIMATIC Logon

User administration and traceability

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

SIMATIC Logon supports the following functions:

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

Change log

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

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

7.2.4.2 Know-how protection in engineering

Know-how protection types

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

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

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

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

Programs and libraries

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

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

- Programs (units in ST, MCC and LAD/FBD that contain programs, function blocks and functions)
- DCC charts
- Libraries
You can select three different security levels for the encryption:

- **Standard**
  Access only with user login and password (backward compatible with versions before V4.2).

- **Medium**
  Improved coding of the password (due to a new procedure, no backward compatibility without knowledge of the password).
  Programs and libraries can be recompiled at any time even without knowledge of the password.

- **High** (only for ST source files in libraries)
  Compilation is only possible after the password has been entered.
  Protected libraries can also be used after an export without knowledge of the password, because in this case the compilation result is also exported.
  - An export without source texts is also possible when exporting libraries
    Highest protection. Complete removal of the source texts in the engineering upon export.
    The export only contains the compilation result (recompilation no longer possible).

The block interfaces are always visible.

**Drive units in SIMOTION SCOUT**

The drive unit know-how protection only applies online and protects intellectual property, in particular, the know-how of machine manufacturers, against unauthorized use or reproduction of their products.

A detailed description can be found in Chapter Write and know-how protection (Page 56).
7.2.4.3 Copy protection for the configuration on the control system.

Copy protection for SIMOTION projects

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

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

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

Figure 7-4 Copy protection of binary SIMOTION SCOUT projects
7.2.5 Offline/online comparison

Project comparison

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

The following comparisons are possible:
- Offline object with offline object from the same project
- Offline object with offline object from a different project
- Offline object with online object

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

The offline/online comparison provides support for service jobs. You can also detect in detail any subsequent manipulations of the project data on the plant in comparison to your secured engineering data.

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

Possible causes can include, for example:
- A program has been changed
- The result of compiling a program is different
- There is a deviation on the global device variables
- The execution system has been changed
- The hardware configuration has been changed
- A library has been changed
- A configuration data item for an axis has been changed

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

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

Figure 7-5  Example of ST detail comparison
7.2.6 SIMOTION IT Web server

Introduction

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

Deactivating/activating the Web server

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

![Image]

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

**Note**

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

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

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

The security status of the Web server is indicated by the security level on the website. There are three possible security levels here: Low, Normal, High.
Security Level Low
The device is supplied with an empty user database. No projects exist yet. The security level is low to allow configuration of the device.

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

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

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

As soon as a project has been loaded to the controller, Security Level Normal is active, with an empty user database as required.

Security Level High
High security with maximum access protection:

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

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

Authentication

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

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

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

Key files

- Delivery state
  In order for you to be able to access the SIMOTION controller via the SIMOTION IT diagnostics standard pages (in their delivery state) via HTTPS, a root certificate and a private key are supplied as a file on the device.

- Create the SSL certificate yourself
  The cert.pl Perl tool can be used to generate the certificates required for customer plants (sites) and combine them into packages for loading.

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

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

Importing the SSL certificate into the browser

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

Reference

A detailed description of the SIMOTION IT Web server and how to use certificates and key files can be found in the "SIMOTION IT Diagnostics and Configuration" Diagnostics Manual.
7.3 SINAMICS

7.3.1 Overview

The following chapter provides an overview of the Industrial Security features available for SINAMICS in order to protect your converters against threats.

- Write and know-how protection
- Communication services and used port numbers
- Web server
- Certificates for the secure data transfer
- Parameters: Access levels + password
- Virus protection / memory card

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

7.3.2 Write and know-how protection

In order to protect your own projects against modifications, unauthorized viewing or copying, SINAMICS S and SINAMICS G have "write protection" and "know-how protection" functions.

<table>
<thead>
<tr>
<th>Protection</th>
<th>Validity</th>
<th>Objective</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write protection</td>
<td>Online</td>
<td>To protect the parameterization from accidental changes by the user.</td>
<td>p-parameters can be read, but cannot be written.</td>
</tr>
<tr>
<td>Know-how protection</td>
<td>Online</td>
<td>To protect intellectual property, especially the know-how of the machine manufacturers, against unauthorized use or reproduction of their products.</td>
<td>p-parameters can neither be read nor written.</td>
</tr>
</tbody>
</table>

Further information

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

- SINAMICS S120 Function Manual, Drive Functions
  Chapter "Write and know-how protection"
- SINAMICS G Operating Instructions
  Chapter "Write and know-how protection"
- SINAMICS S and SINAMICS G List Manuals
  Chapter "Parameters for write protection and know-how protection"
7.3.3 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). As the security measures are limited to Ethernet and PROFINET networks, no PROFIBUS protocols are taken into account.

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

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

7.3.4 Web server

The SINAMICS Web server provides information on a SINAMICS device via its Web pages. 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). With the input of the appropriate address, you can decide yourself whether a normal or secure transmission is used to access the data.

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

Access rights

The normal protection mechanisms of SINAMICS apply for 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 also mostly protected so that only users with the appropriate rights can access or change the data.

Further information

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

- SINAMICS S120 Function Manual, Drive Functions
  Chapter "Web server"
7.3.5 Certificates for the secure data transfer

Protecting the HTTPS access

The Secure Socket Layer protocol (SSL) enables encrypted data transfer between a client and the SINAMICS drive. HTTPS access between the browser and the drive is based on the Secure Socket Layer protocol.

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).

Key files

You need two key files (a public certificate and a private key) for the encryption method used by the Secure Socket Layer protocol.

Certificate handling

Ideally, the certificate handling appears as follows:

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

Further information

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

- SINAMICS S120 Function Manual, Drive Functions
  Chapter "Certificates for the secure data transfer"
7.3.6 Parameters: Access levels + password

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

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

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

Further information

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

- SINAMICS S120 Function Manual, Drive Functions
  Chapter "Parameters"
- SINAMICS G Operating Instructions
  Chapter "Parameters"
- SINAMICS S and SINAMICS G List Manuals
  Chapter "Explanation of the list of parameters"

7.3.7 Virus protection / 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 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.
Product-specific security measures

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

- Industrial security (www.siemens.com/industrialsecurity)

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

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

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.

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

A firewall is a security system that protects a computer network or an individual computer from unauthorized network access and is part of a security concept.
Glossary

**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.

**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).

**Patch**

A patch, also called a bugfix, is an update for software or data for the end user that patches security holes, corrects errors or adds additional functions. With some manufacturers, such as Microsoft, these updates are also called Service Packs when they comprise several patches. The term originates from the time when small software corrections were carried out on punch cards by punching individual holes or patching them up.

**Smart Grid**

The term Smart Grid encompasses the communicative networking and control of power generators, energy stores, electrical loads and operating equipment in power transmission and distribution networks for the supply of electricity. This enables the optimization and monitoring of its individual component parts. The objective is to ensure energy security based on efficient and reliable system operation.

**Switch**

In computer networks, a switch – also called a network switch or switching hub – is a device that links particular network segments.

**VPN (Virtual Private Network)**

VPN is a logical private network tunneled across publicly accessible infrastructure. Only the communication partners within this private network can communicate with one another and exchange information and data.
Index

A
Application security, 17

B
Benefits, 4
Block
  Runtime modification by encryption, 39
Block encryption
  SINUMERIK, 39
Block protection, 39
  SINUMERIK, 39

C
Certificates
  SIMOTION, 55
  SINAMICS, 58
Change
  Password, 27
Changing passwords
  SINUMERIK, 37
Cloud computing, 13
Communication services
  SINAMICS, 57
Company security, 23
Copy protection
  SINUMERIK, 38

D
Deactivating a PROFINET interface
  SINUMERIK, 33
Defense in depth strategy, 21
Disable
  USB interface, 33
Disabling a USB interface
  SINUMERIK, 33
DMZ network, 24
Documentation
  Benefits, 4
  Target group, 4

E
Effects, 15
Encrypting cycles
  SINUMERIK, 38
Exchangeable storage media
  SINAMICS, 59

F
Firewall, 24

H
HTTPS
  SIMOTION Web server, 55

I
Industrial security
  Definition, 11
  Objectives, 11
  Possible effects, 15
Industrial Security
  Threats, 14
  Internet of things, 13

K
Know-how protection
  SINAMICS, 56

L
Lock MyCycle
  SINUMERIK Integrate, 38
Lock MyPLC
  SINUMERIK Integrate, 39
Lock-it
  SINUMERIK Integrate, 38

M
Main entry, 39
<table>
<thead>
<tr>
<th>Page</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Mobile devices</td>
</tr>
<tr>
<td>13</td>
<td>Mobile networks</td>
</tr>
<tr>
<td>21</td>
<td>Network security</td>
</tr>
<tr>
<td>21</td>
<td>Physical production security</td>
</tr>
<tr>
<td>21</td>
<td>Plant security</td>
</tr>
<tr>
<td>21</td>
<td>Protection levels</td>
</tr>
<tr>
<td>23</td>
<td>Physical production security</td>
</tr>
<tr>
<td>21</td>
<td>Network services and ports</td>
</tr>
<tr>
<td>27</td>
<td>Parameters: Access levels</td>
</tr>
<tr>
<td>57</td>
<td>SINAMICS Web server</td>
</tr>
<tr>
<td>57</td>
<td>SINAMICS Communication services</td>
</tr>
<tr>
<td>56</td>
<td>SINAMICS Know-how protection</td>
</tr>
<tr>
<td>57</td>
<td>SINAMICS Used port numbers</td>
</tr>
<tr>
<td>56</td>
<td>SINAMICS Write protection</td>
</tr>
<tr>
<td>58</td>
<td>SINAMICS Secure Socket Layer protocol</td>
</tr>
<tr>
<td>38</td>
<td>SINAMICS Copy protection</td>
</tr>
<tr>
<td>33</td>
<td>SINAMICS Deactivating a PROFINET port</td>
</tr>
<tr>
<td>33</td>
<td>SINAMICS Disabling a USB interface</td>
</tr>
<tr>
<td>38</td>
<td>SINAMICS Encrypting cycles</td>
</tr>
<tr>
<td>37</td>
<td>SINAMICS Protection levels</td>
</tr>
<tr>
<td>37</td>
<td>SINAMICS Security update process</td>
</tr>
<tr>
<td>34</td>
<td>SINAMICS Virus protection</td>
</tr>
<tr>
<td>38</td>
<td>SINAMICS Whitelisting</td>
</tr>
<tr>
<td>38</td>
<td>SINUMERIK Lock MyCycle</td>
</tr>
<tr>
<td>39</td>
<td>SINUMERIK Lock MyPLC</td>
</tr>
<tr>
<td>38</td>
<td>SINUMERIK Lock-it!</td>
</tr>
<tr>
<td>13</td>
<td>Tablet PCs</td>
</tr>
<tr>
<td>4</td>
<td>Target group</td>
</tr>
<tr>
<td>14</td>
<td>Threats</td>
</tr>
</tbody>
</table>

**N**
- Network security, 21
- Network services and ports, 27

**P**
- Parameters: Access levels
  - SINAMICS
- Password
  - Change, 27
- Physical production security, 23
- Plant security, 21
- Protection levels
  - SINUMERIK, 37

**R**
- Remote access, 13
- Requirements
  - Virus scanner, 28
- Risk analysis, 19

**S**
- SCALANCE S, 25
- Secure Socket Layer protocol
  - SINAMICS, 58
- Security audit, 19
- Security holes, 14
- Security module
  - SCALANCE S, 25
- Security service, 17
- Security support, 17
- Security update process
  - SINUMERIK, 36
- SIMATIC Logon, 47
- SIMOTION
  - Copy protection, 50
  - Industrial Security, 41
  - Know-how protection, 48
  - Ports, 43
  - Project comparison, 51
  - Project storage, 45
  - Virus scanners, 44
  - Web server, 53

**T**
- Tablet PCs, 13
- Target group, 4
- Threats, 14
Index

U
Used port numbers
   SINAMICS, 57
User accounts, 27

V
Virus protection
   SINAMICS, 59
   SINUMERIK, 34
Virus scanner
   Requirements, 28
   SINUMERIK, 34

W
Web server
   SIMOTION, 53
   SINAMICS, 57
   SINUMERIK, 38
Whitelisting, (SINUMERIK)
Windows Server Update Service, 28
Wireless technology, 13
Write protection
   SINAMICS, 56
   WSUS, 28