Cyber security checklist

Protect your CNC machine tool from cyber attacks!

- This document describes ways to protect CNC machine tools from cyberattacks
- This document is primarily aimed at operators of CNC machine tools.
- The functions and features listed can be used for the specification of new machines.
- Some of the functions and features listed can also be implemented subsequently and thus increase the cybersecurity of existing machines.

SIEMENS

Cybersecurity check list

Overview

Aim of this document

Increasing digitalization and networking makes CNC machine tools more vulnerable to manipulation and cyberattacks. This means that criminal attempts to damage operating companies and their infrastructures are increasing disproportionately.

Cyberattacks are used to steal sensitive and confidential data, such as CNC programs in the aerospace or defense industries. Cyberattacks are also used to sabotage manufacturing facilities, for example those of competitors, or to extort ransoms.

For small companies with unprotected infrastructure, cyber attacks can quickly threaten their existence.

Authorities at regional and international levels have defined stricter rules and established guidelines for implementing cybersecurity guidelines and measures. Non-compliance may lead to punishment of the respective decision-makers.

Operators of CNC machine tools should therefore take measures to secure their production infrastructure. This reduces the risk of successful attacks and the resulting downtime and financial damage.

Properties and measures that contribute to increasing the cybersecurity of CNC machine tools are shown below

- The specific threat situation is made clear.
- A basic solution approach is shown.
- Suitable solutions from the Siemens product range are presented.
- Possible scenarios for implementing the solutions are shown.
- More information about the solutions will be provided.

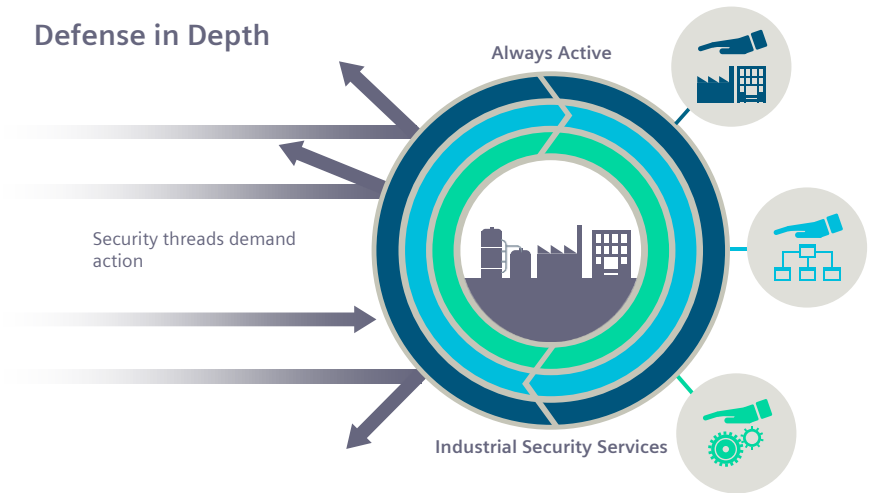
Basis of this document

The Siemens Defense in Depth approach

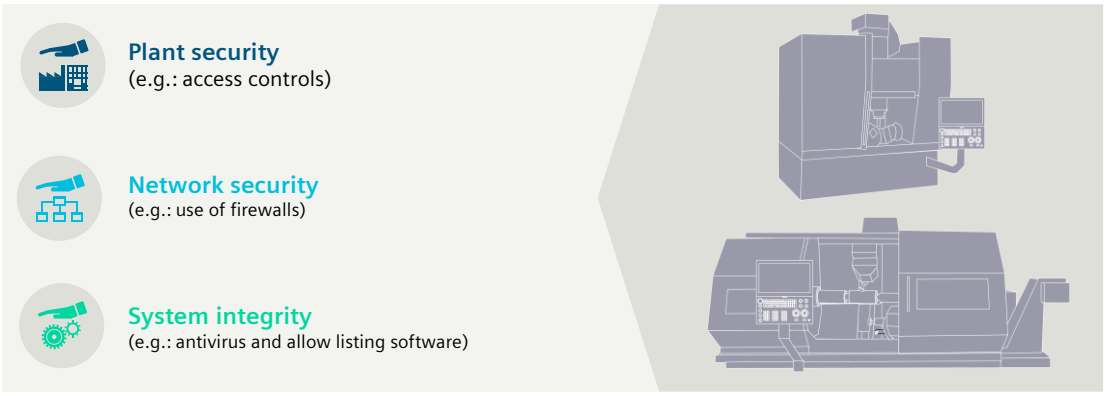
To comprehensively protect industrial plants from cyber-attacks from inside and outside, action must be taken at all levels simultaneously
– from the operational level to the field level, from access control to copy protection.

For this purpose, Siemens offers “Defense in Depth”, a depth-based defense as a comprehensive protection concept.

This concept is the perfect basis for the recommendations of ISA99 / IEC 62443, the leading standard for security in industrial automation.



For further information : Industrial Cybersecurity



Dieses Dokument zeigt, mit welchen Eigenschaften und Maßnahmen CNC-Werkzeugmaschinen in das dargestellte Defense-in-Depth-Konzept integriert werden können.

☑ CNC with security by design

Threatening situation

CNC controls are highly complex systems with multiple access options for operating personnel, IT systems or automation solutions. These access options are potential points of attack for cyber attacks of all kinds.

Solution approach

CNC system with development process from a cybersecurity perspective

Siemens solution

SINUMERIK

CNC system software with consistent development from a cybersecurity perspective

Certified reference process for product lifecycle management (TÜV Süd, IEC 62433-4-1 since 2018)

Digital birth certificate (device certificate)

System software with protection against manipulation through secure boot and software signatures

Implementation

System feature of SINUMERIK from a certain release level:

- Provision in new machines tools by the manufacturer
- Retrofit of existing machine tools by Siemens Customer Service

SINUMERIK ONE, SINUMERIK 828D

☑ Protection of machine operation from unauthorized access

Threatening situation

In contrast to the office environment, the use and operation of machines is usually permitted with fairly extensive access rights.

The hurdle for manipulation of production or theft of high-quality or sensitive production data by personnel working on the machine is therefore very low.

Solution approach

Implementation of user management with person- and activity-specific access rights

Unique identification of each user (e.g.: via a combination of username and password)

Siemens solution

SINUMERIK

Local user management integrated into the CNC user interface with person- and activity-specific access rights as well as definable password guidelines

Additional option for connecting to a central user administration (e.g.: Active Directory)

Implementation

System feature of SINUMERIK from a certain release level:

- Activation in new machine tools by the manufacture
- Activation when retrofitting existing machines by Siemens Customer Service
- Adaptation by the operating companies

SINUMERIK ONE, SINUMERIK 828D

☑ Trust relationship between CNC hardware components

Threatening situation

CNC systems are often equipped with PC-based control units for additional software applications.

If user management only affects individual components, there is a risk of access protection being circumvented.

Solution approach

Trusted relationship between CNC and PC components of the CNC equipment package

Siemens solution

SINUMERIK
Certificate-based CNC-PC coupling
Trust relationship between CNC and PC components based on certificates to ensure consistency of user management across all components

Implementation

System feature of SINUMERIK from a certain release level:

- Activation in new machine tools by the manufacture
- Activation when retrofitting existing machines by Siemens Customer Service

SINUMERIK ONE, SINUMERIK 828D

☑ Network security through segmentation

Threatening situation

Office networks and production networks are often directly connected to each other. Cyber-attacks, which typically target office networks, can therefore also directly affect production.

Solution approach

Strict separation of production networks both from each other and from the other office networks through network segmentation with its own automation firewall

Siemens solution

Consulting and solution concept for manufacturing

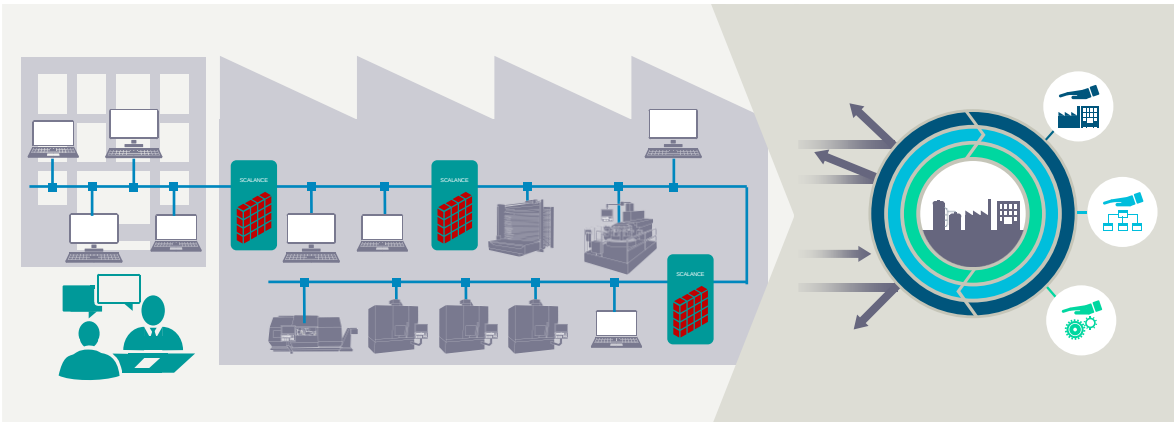
Wide product range for network segmentation

Comprehensive consulting / concept creation for network segmentation of industrial networks

Implementation

Cross-system solution concept for the manufacturing environment:

- Implementation by Siemens Customer Service
- Implementation possible by experienced specialist staff in the operating companies



[Network concept for discrete manufacturing]

[Cybersecurity Consulting for Operational Technology (OT)]

☑ Network security through cell protection and firewall

Threatening situation

Today, electrical equipment for machine tools consists of a large number of networked hardware components. The high number of interfaces of these components are potential points for cyberattacks.

Solution approach

Segmentation of the machine tool for secure communication between components within a protected cell

Firewall in this protection cell for secure communication of the machine tool with the production network

Siemens solution

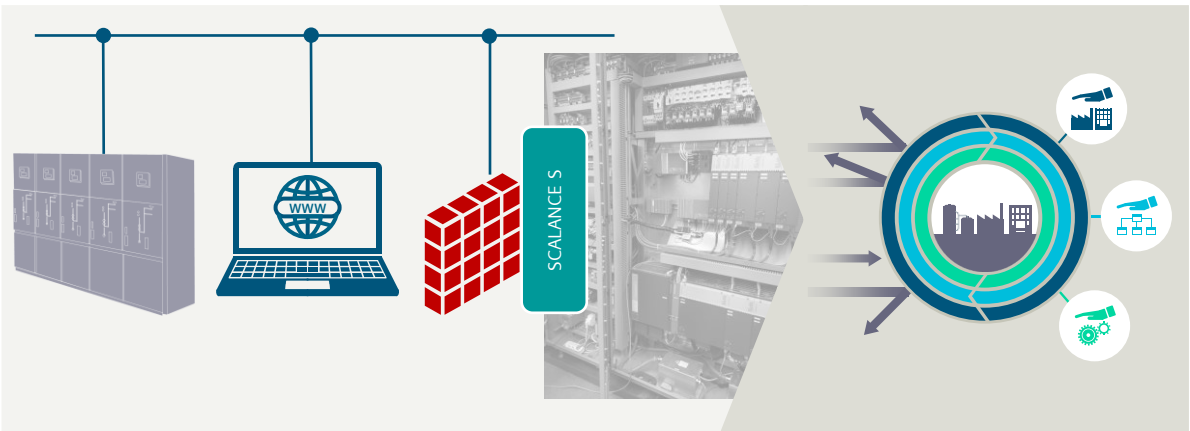
SCALANCE S
Industrial Security Appliance

Firewall and VPN appliances SCALANCE S to protect industrial networks and automation systems by segmenting the network via established secure communication channels

Implementation

Cross-system solution within the machine tool:

- Implementation in new machine tools by the manufacturer
- Retrofitting in existing machines by Siemens Customer Service



SCALANCE for the SINUMERIK Environment

☑ Secure protocols for connecting network drives

Threatening situation

The Windows network protocol SMB V1, which was previously often used in CNC controls to share network drives, has numerous vulnerabilities and is therefore considered insecure.

Solution approach

Consistent use of secure communication protocols standards from
SMB V3 (MS Windows) or NFS V4 (Linux)

Siemens solution

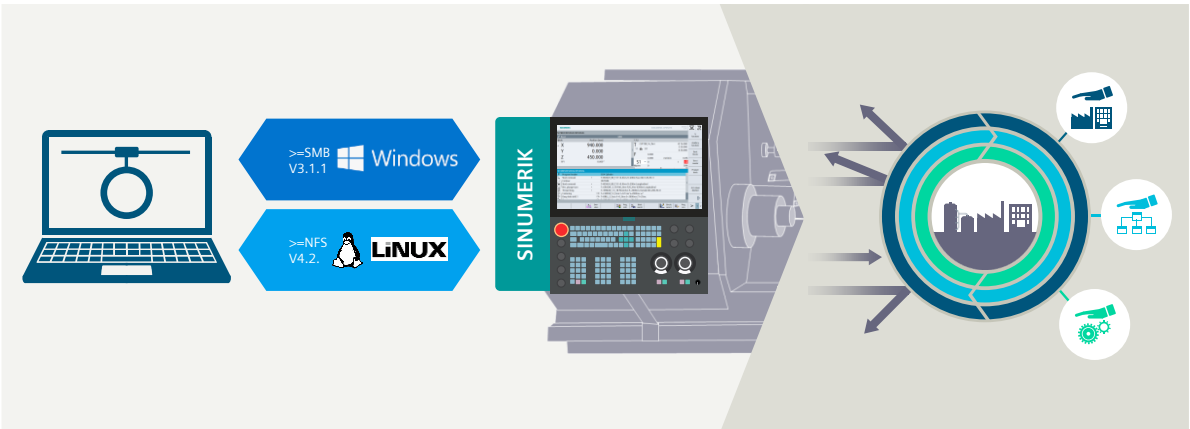
SINUMERIK

Constantly updated to support the latest and most secure communication protocols

Implementation

System feature of SINUMERIK from a certain release level:

- Activation in new machine tools by the manufacture
- Activation when retrofitting existing machines by Siemens Customer Service



SINUMERIK ONE, SINUMERIK 828D

☑ Secure protocols for connecting network drives (retrofitting)

Threatening situation

The Windows network protocol SMB V1, which was previously often used in CNC controls to share network drives, has numerous vulnerabilities and is therefore considered insecure.

Solution approach

Consistent use of secure communication protocols from standards SMB V3 (MS Windows)

Siemens solution

Siemens Machine Protocol Gateway

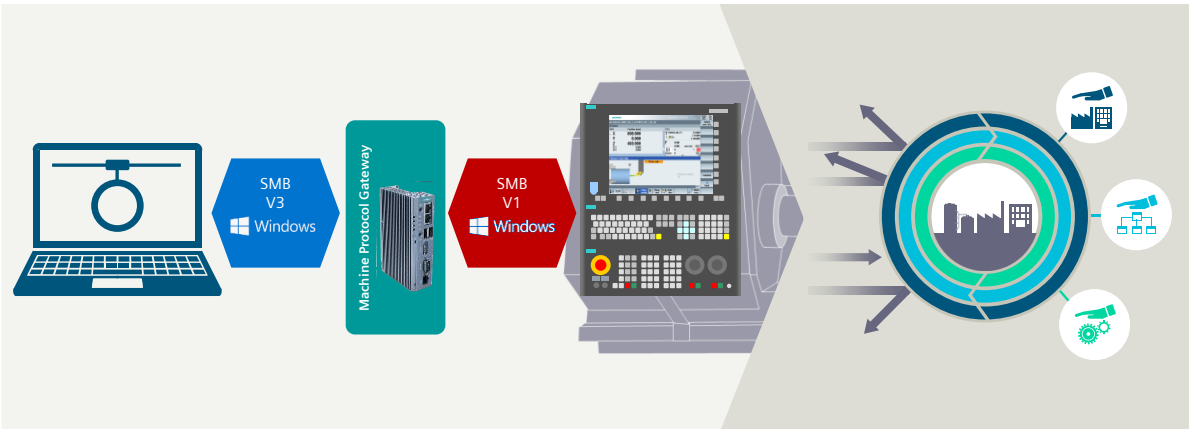
Hardware-based retrofit solution for older CNC controls

Seamless translation of the Windows network protocol SMB V1 to SMB V3

Implementation

System-independent solution for retrofitting existing machines:

- Implementation by Siemens Customer Service
- Implementation possible by experienced specialist staff in the operating companies



Machine Protocol Gateway

☑ Updating industrial PCs for CNCs with Windows user interface

Threatening situation

Machine tools are often operated for a very long time. This creates weak points in the integrated operating components based on Windows as a result of end-of-life, end-of-support or end-of-sale.

Solution approach

Timely replacement of existing MMC and PCU modules with current SIMATIC IPC modules

Siemens solution

Retrofit by Siemens Customer Service

Replacing the hardware components in the machine's control cabinet

Porting of existing CNC applications to current CNC system software versions

Activation of functions for the highest possible cybersecurity

Implementation

Solution for retrofitting existing machines:

- Retrofit by Siemens Customer Service
- Retrofitting offers from various machine manufacturers on request

Retrofit for Machine Tools

☑ Integration of additional Windows security applications

Threatening situation

Machine tools are often operated longer than the availability of updates to the Windows operating system on the integrated industrial PCs. This means the risk of cyber-attacks increases significantly.

Solution approach

Integration of additional Windows security applications to protect against viruses, worms and trojans

Siemens solution

Allow-Listing (Whitelisting) by Siemens Customer Service

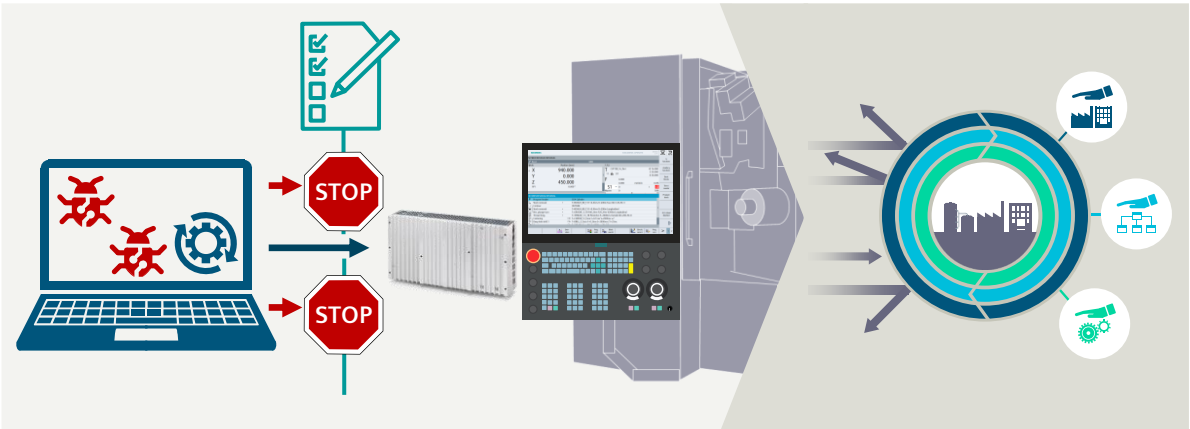
Consistent limitation to only start trustworthy software applications
(allow listing based on Trellix™)

Service for individual configuration

Implementation

Basic solution for existing and new machines:

- Implementation in existing machines by Siemens Customer Service
- Implementation in new machines by the manufacturer upon request



Cyber-security Services

☑ Secure communication when accessing CNC process data

Threatening situation

During the digitalization of manufacturing processes, there is an increasing need to access CNC process data. Examples of this are BDE or MES control systems. However, proprietary insecure communication protocols represent a target for cyberattacks on machines.

Solution approach

Consistent use of modern and standardized communication protocols for secure and encrypted data exchange between CNC and external software applications

Siemens solution

SINUMERIK Integrate Access MyMachine /OPC UA

Standardized industrial communication protocol OPC UA (Unified Architecture) for SINUMERIK

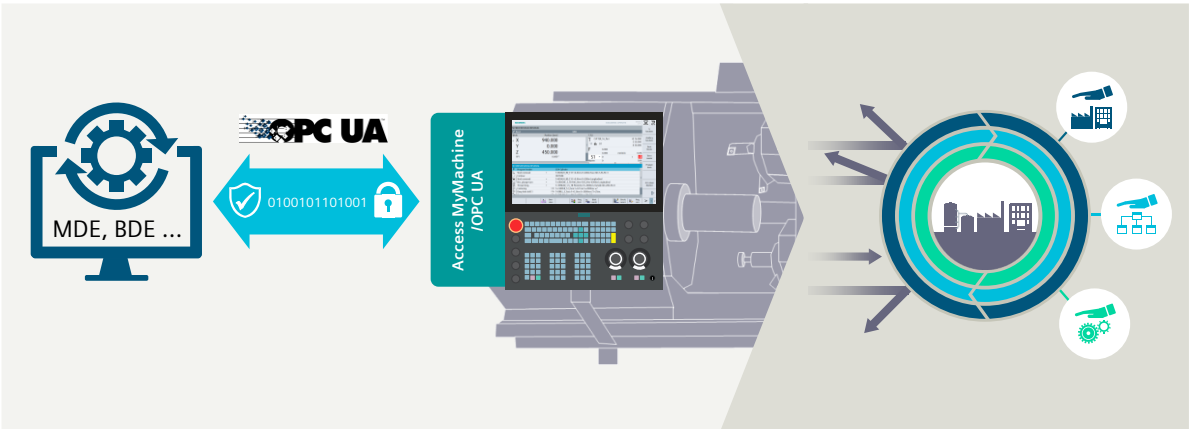
Client/server communication with reliable, secured and encrypted data exchange

A wide range of possible applications, from exchanging variables, alarms and files to selecting production orders

Implementation

System feature of SINUMERIK from a certain release level:

- Activation in new machine tools by the manufacture
- Activation in existing machine tools by the Siemens Customer Service
- Activation possible by experienced specialist staff in the operating companies



Access MyMachine /OPC UA

☑ Secure remote access to machines (based on VPN)

Threatening situation

Malware can enter the machine via unmonitored remote maintenance access and disrupt the production process. Unmonitored remote maintenance access can also be used to steal high-quality or valuable CNC data (CNC programs).

Solution approach

Remote access to machines exclusively via secure VPN access isolated from the rest of the company network while at the same time providing clear and secure access management and network segmentation that separates machines from different manufacturers

Siemens solution

SINEMA Remote Connect und SCALANCE industrial router

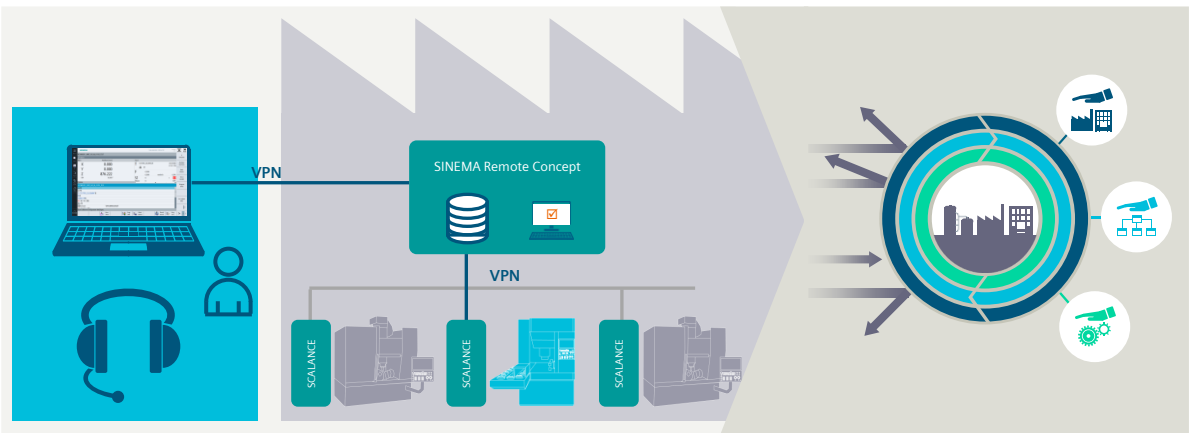
Remote maintenance access exclusively via isolated, encrypted VPN connections (OpenVPN and IPsec)

Multifactor authentication of remote access with username/password or PKI smart card, support for the current TLS version

Implementation

Cross-system solution concept for the manufacturing environment:

- Integration of SCALANCE by the machine tool manufacturer
- Integration of SCALANCE by Siemens Customer Support
- Implementation of SINEMA Remote Connect on the IT infrastructure of the machine manufacturer or the operating company



SINEMA Remote Connect: Management platform for remote networks

☑ Secure remote access to machines (based on cloud)

Threatening situation

Malware can enter the machine via unmonitored remote maintenance access and disrupt the production process. Unmonitored remote maintenance access can also be used to steal high-quality or valuable CNC data (CNC programs).

Solution approach

Remote access to machines via secure cloud connection with clear and secure access management

Siemens solution

Manage MyMachines /Remote

Remote maintenance access exclusively via encrypted cloud architecture

Multifactor authentication of remote access with username/password

Access via different devices (PC, smartphone, tablet, etc.)

Implementation

Cross-system solution concept for the manufacturing environment:

- Implementation by machine tool manufacturer
- Implementation by Siemens Customer Service in the operating companies

Manage MyMachines /Remote

☑ Integrity check of CNC software applications

Threatening situation

Systems are particularly vulnerable to all kinds of manipulation during the boot phase, for example by malware. Manipulation of the CNC system inevitably leads to disruptions in the machine tool manufacturing process.

Solution approach

CNC system with hardened system environment for secure system startup

Siemens solution

SINUMERIK Secure Boot

Secure boot behavior to ensure that software applications only run with a valid Siemens signature

Flexible integrating software applications from the machine manufacturers into the secure boot behavior

Implementation

System feature of SINUMERIK from a certain release level:

- Activation in new machine tools by the manufacture
- Activation when retrofitting existing machines by Siemens Customer Service

SINUMERIK ONE, SINUMERIK 828D

☑ Integrity check of the PLC controller

Threatening situation

In new CNC systems, functions for the safe execution of machine functions are implemented via software logic in the in the integrated programmable logic controller (PLC). The PLC is therefore a potential target for sabotage.

Solution approach

Protection of the PLC configuration data against unauthorized access

Siemens solution

SINUMERIK PLC access protection

Password protection for access to the PLC configuration data

Encryption of PLC configuration data

Implementation

System feature of SINUMERIK from a certain release level:

- Activation in new machine tools by the manufacture
- Activation when retrofitting existing machines by Siemens Customer Service

SINUMERIK ONE, SINUMERIK 828D

☑ Encryption of trustworthy CNC data

Threatening situation

Data theft of high-quality or sensitive CNC data (CNC programs) can lead to very high financial losses.

Solution approach

Consistent encryption of user data on CNC storage media for protection during operation of the machine, but also during replacement/disposal in the event of service

Siemens solution

SINUMERIK
SIMATIC IPCs

Encryption of relevant user data on the SINUMERIK ONE SD system memory card.

Protection of relevant user data through Windows bit locker encryption for SINUMERIK ONE applications with SIMATIC IPCs

Implementation

System feature of SINUMERIK equipments from a certain release level:

- Activation in new machine tools by the manufacture
- Activation when retrofitting existing machines by Siemens Customer Service

SINUMERIK ONE, SINUMERIK 828D

☑ Logging and monitoring cybersecurity relevant events

Threatening situation

Cyber attacks often remain undetected for a long time. It is often difficult to subsequently clarify the causes and take countermeasures, including criminal investigations.

Solution approach

Logging of security-relevant events within the CNC

Possibility of connecting the CNC to a higher-level system for Security Information and Event Management (SIEM)

Siemens solution

SINUMERIK Security Eventlog

Recording of security-relevant events with the option of visualization via the CNC user interface.

Forwarding of events via SysLog (RFC 5424) to the central SysLog server (SIEM)

Implementation

System feature of SINUMERIK from a certain release level:

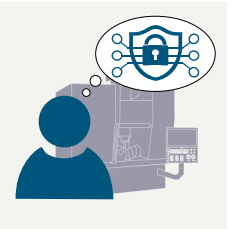
- Provision in new machines tools by the manufacturer
- Retrofit of existing machine tools by Siemens Customer Service
- Connection to SysLog server on the part of the operating companies

SINUMERIK ONE, SINUMERIK 828D

☑ General recommendations for action (1)

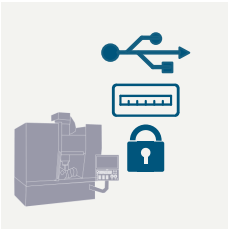
Raising awareness of CNC operating personnel

- Proactively inform your CNC operating personnel about the threat of cyber
  attacks on machine tools.



Safe handling of USB ports on the CNC control

- Do not use the USB ports to charge cell phones.
- If necessary, protect the USB ports with lockable port locks.

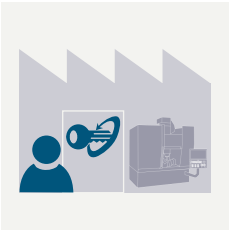


Locking control cabinets

- Make sure that control cabinets cannot be accessed with standard keys.

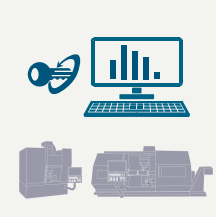
Access restriction to the shop floor

- Ensure that only authorized persons have access to the production facilities.



Access restrictions to control rooms

- Ensure that only authorized persons have access to rooms in which production
  and operational processes are monitored or controlled.

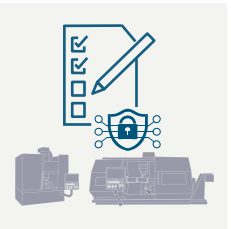


☑ General recommendations for action (2)

Connection to the Internet

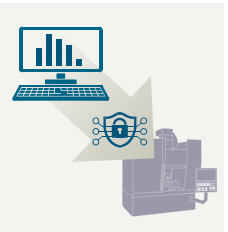
- Machines should not be connected to the Internet without a good reason.
- Disconnect the machine from communication with the unprotected Internet.

Cyber security assessments für OT



- Get an overview of the current cybersecurity status.
  cybersecurity Assessments for OT

Roll out and apply IT processes (ISO 27001) for OT



- Consistently implement the security concepts of the office environment in the production environment as well.

Safe disposal of CNC or PC components

- If possible, encrypt your data while the modules are in operation.
  → ☑ Encryption of trustworthy CNC data
- When disposing of unencrypted data carriers, pay attention to physical destruction
- Follow the instructions for safe disposal in the manual
  SINUMERIK ONE Industrial cybersecurity.

Important notes

- To secure plants, systems, machines and networks against cyber threats, it is necessary to implement a holistic industrial cybersecurity concept.

- The constellation of measures must fundamentally be adapted to the respective security requirements of the operating companies.

- The measures to increase cybersecurity must always be kept up to date to cover newly emerging threats.

- Siemens products and solutions are constantly updated in response to changing threat situations to guarantee maximum security. It is therefore expressly recommended to always only use the current product versions and to apply product updates as soon as they are available.

- To always be informed about product updates and threats or vulnerabilities, subscribe to the
  Siemens Security Advisory Newsletter.

- Further information can be found in the configuration manuals

  SINUMERIK ONE Industrial Cybersecurity

  SINUMERIK / SIMOTION / SINAMICS Industrial Security.

Published by
Siemens AG

DI MC MTS
Version: 1.4.1, 10/2024

Digital Industries
Motion Control
P.O. Box 3180
91050 Erlangen, Germany

General contact:

www.siemens.com/cnc4you

Additional information:

www.siemens.com/sinumerik