



Cybersecurity for Industry

Combine the real and digital worlds securely

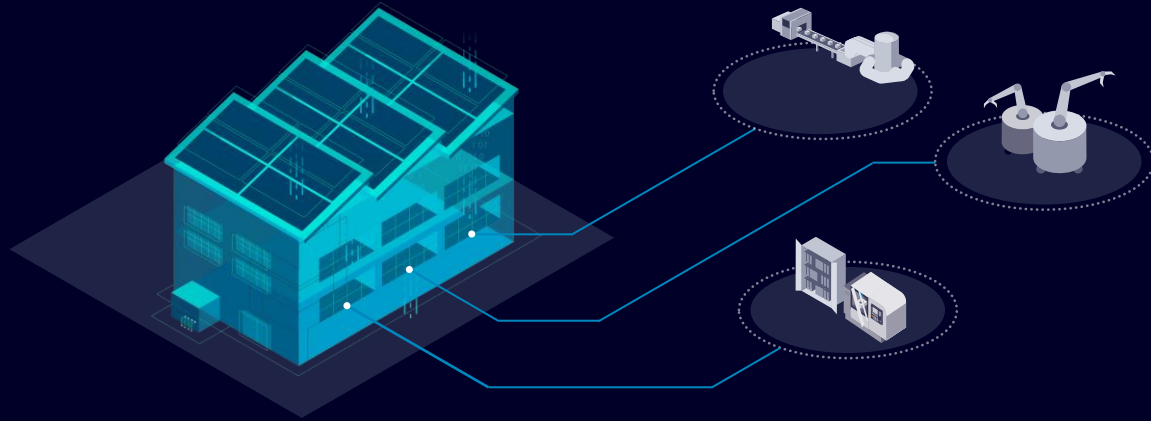
Table of contents

• Why is Cybersecurity such an important topic for industry?	3	• Plant Security	128
• How can the OT be secured?	10	• PCS7 Security	130
• Industrial Cybersecurity Services	15	• PCS neo Security	135
• Plant Security Services	17	• Security Certifications	141
• Network Security Services	20	• Siemens Initiatives to enhance Security for products	146
• System Integrity Services	23	• Security Vulnerability Handling	151
• System Integrity	29	• Security concepts for Industries	155
• Secure SIMATIC PG/HMI communication	30	• Summary	163
• Automation systems with Security Integrated	44	• Attachment: Security Trainings	167
• User Management & Access Control	62	• Contacts	169
• Access Control with RFID Systems	71		
• Security for Motion Control	76		
• Network Security	84		
• Overview: Network Security	86		
• Components for Network Security	91		
• Security Use cases: Network Security	110		

Why is Cybersecurity such an important topic for industry?



Why Cybersecurity is even more important now than before!



Yesterday we had islands of **communication**.



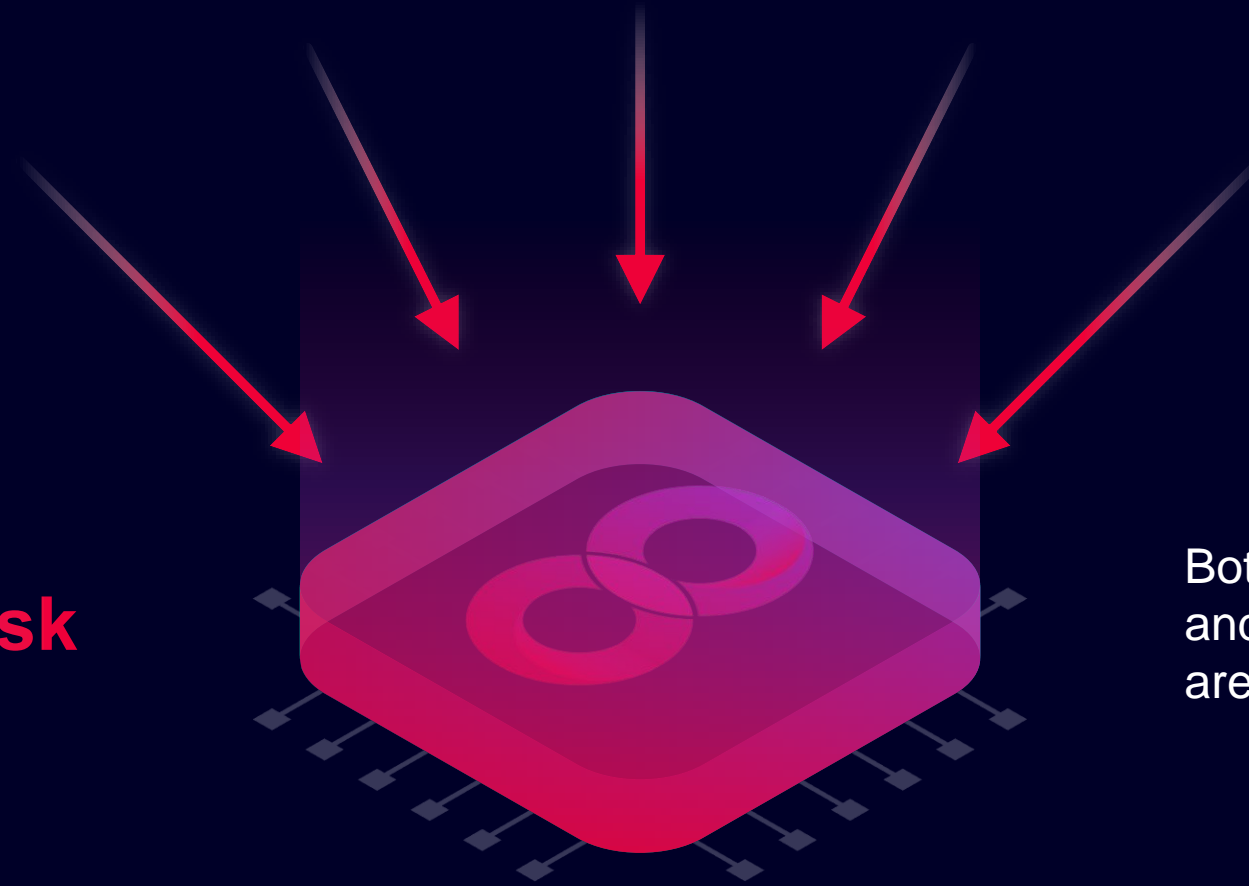
Today everything is **connected** and the risks are growing ...

Digital Enterprise

One of the greatest challenges of becoming a Digital Enterprise is optimally and securely handling data at all times.



**But all this also
increases the risk
of cyberthreats**



Both Information Technology
and Operational Technology
are at risk.

The threat is real and growing

61%

of smart factories have experienced a cybersecurity incident

Source: Manufacturing Automation Growing cybersecurity risks for smart factories

33%

of Cyber incidents occur in manufacturing

Source: PMMI 2021 Assess your risk white paper

65%

of Ransomware attacks occur in manufacturing

Source: Dragos 2021 ICS/OT Cybersecurity year in review

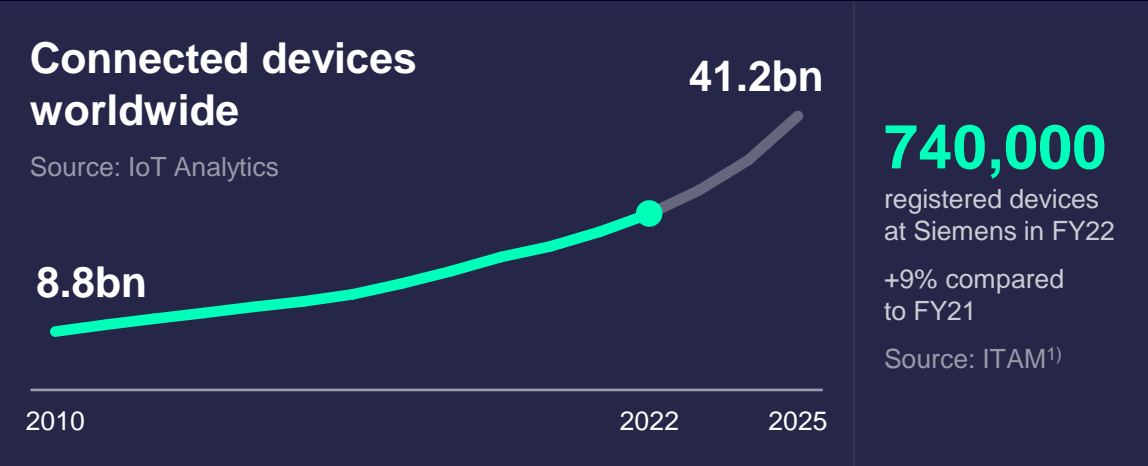
75%

of IT architectures had external connections to OT in 2021

Source: Dragos 2021 ICS/OT Cybersecurity year in review

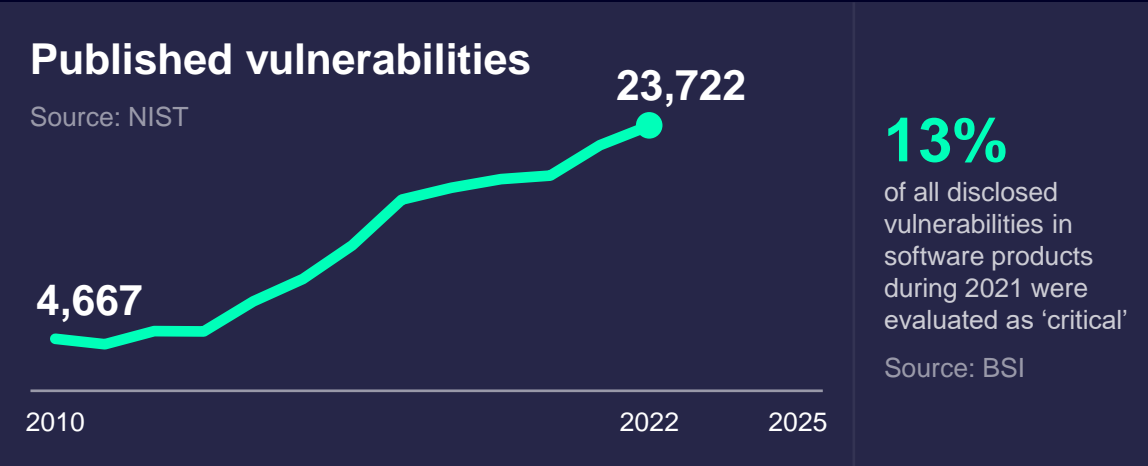
Sources: 1 [Manufacturing Automation – Growing cybersecurity risks for smart factories](#) | 2 [PMMI 2021 Assess your risk white paper](#) | 3 [Dragos 2022 ICS/OT Cybersecurity year in review](#) | 4 [Dragos 2022 ICS/OT Cybersecurity year in review](#)

Exponential growth of vulnerabilities with digitalization increases the attack surface



Connected devices X **Published vulnerabilities**

Although not all vulnerabilities affect all devices, it is fair to assume that combination of increased connectivity and published vulnerabilities has a multiplication effect



Strong need for protection of automation systems and OT against Cyber-threats

 **Cybersecurity for Industry**

¹⁾ IT Asset Management

Graph <https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/>
Text: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2022.pdf?__blob=publicationFile&v=6

Connected factories are ill equipped to defend against cyber attacks

91%

believe that IT and OT should be collectively responsible for the security of machinery ¹⁾

90%

of OT security findings are related to a lack of visibility across OT networks ¹⁾

50%

of OT security audits reveal improper network segmentation ²⁾

81%

of existing SOCs are not sufficiently aligned with business requirements ³⁾

4

Main four reasons why OT security is still poor:

- **Asset lifecycle**
- **Heterogeneity**
- **Focus on availability**
- **Risk based protection**

Clients need help with end-to-end OT security services & solutions

¹⁾ State of Operational Technology and Cybersecurity Report, Fortinet 2020 [2020 State of Operational Technology and Cybersecurity Report \(fortinet.com\)](https://www.fortinet.com/resources/white-papers/2020-state-of-operational-technology-and-cybersecurity-report)

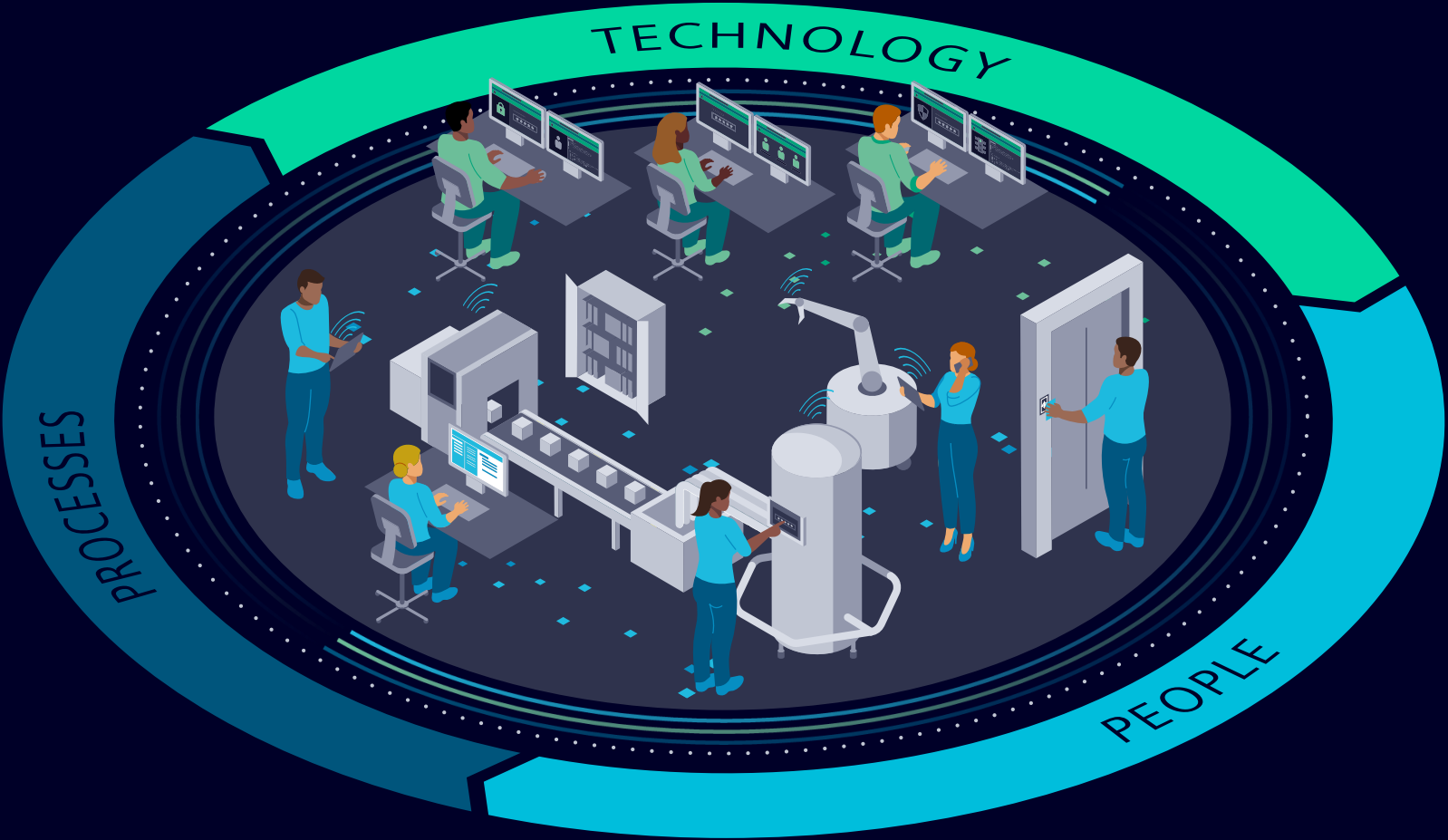
²⁾ ICS Cybersecurity Year In Review, Dragos 2022 [Dragos Year-In-Review-Report-2022.pdf](https://www.dragos.com/ICS-Cybersecurity-Year-In-Review-Report-2022.pdf)

³⁾ Improving the Effectiveness of the Security Operations Center, Ponemon Institute 2019 [Microsoft Word - 2019 Devo Study Final4.docx](#)

How can the OT be secured?



A holistic Cybersecurity approach is guided by three main pillars People, Technology and Processes



Policies and
procedures

Functional security
measures

Competency

Industrial Cybersecurity concept

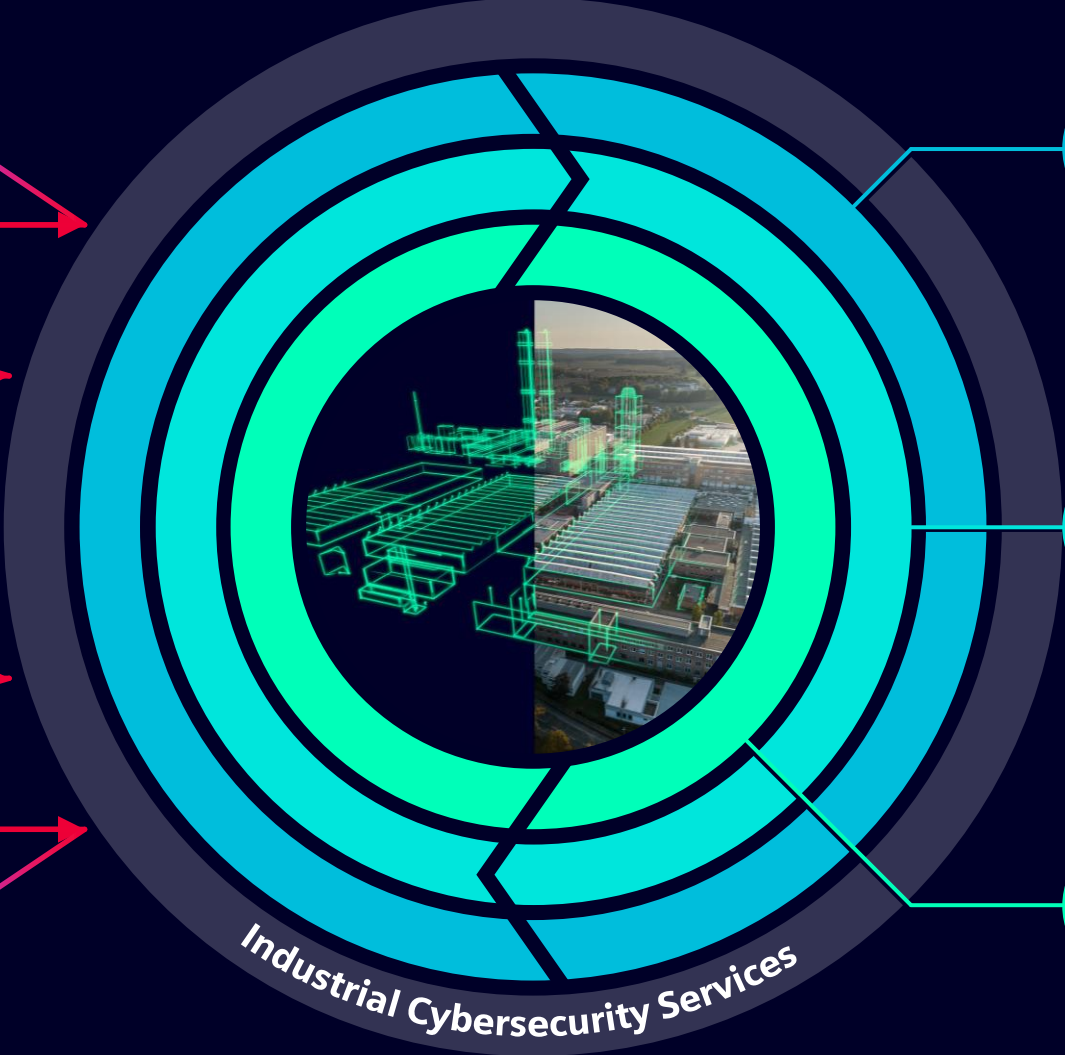


Only a comprehensive security concept based on the defense in depth principle can provide an effective protection



Comprehensive Cybersecurity concept for OT from Siemens

Security threats demand action



Plant security

- Physical access protection
- Security Policies
- Security monitoring



Network security

- Cell protection, perimeter network and trusted zones
- Firewalls and VPN



System integrity

- System hardening
- Patch Management
- Authentication and access protection

Siemens defense in depth at a glance – Three layers to protect automation plants

Description

Added value



Plant security

- Physical access protection
- Security Policies
- Security monitoring

- Systems to prevent unauthorized access to critical components
- Consulting services to define and implement processes and guidelines according IEC 62443-2-1 and 3-3
- Continuous Security monitoring of the plant and network

- Fully scalable plant protection concept
- Standard conform security guidelines tailored to the customer organization
- Identify and react on security threats in daily operation



Network security

- Cell protection, perimeter network and trusted zones
- Firewalls and VPN

- Design, conception and realization of a network security concept, to prevent unauthorized access and to protect the industrial communication

- Prevention of unauthorized access and espionage of data
- Secure remote access and telecontrol services via public networks (internet)
- Increased plant availability
- Easy to operate – time and cost saving



System integrity

- System hardening
- Patch Management
- Authentication and access protection

- Design and implement measures to protect automation systems against a variety of threats and design complete solutions for maximum protection over the system lifecycle

- Increased plant availability
- Identifying threats and vulnerabilities over the lifecycle
- Use of certified secure developed Siemens products according to IEC 62443-4-1
- Comprehensive long-term protection through continuous monitoring and security management

Industrial Cybersecurity Services



Industrial Cybersecurity Services: End-to-end approach



Plant Security Services

- Security Assessments
- Industrial Security Consulting
- Remote Industrial Operations Services

Network Security Services

- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Remote Platform Software as a Service

System Integrity Services

- Endpoint Protection
- Vilocify Vulnerability Services
- Patch Management
- Backup and Restore

Plant-specific security roadmap with Security Assessments



Security Assessments

- Operators of production facilities these days cannot afford to do without effective security measures. But where to start?
- Security Assessments cover a holistic analysis of threats and vulnerabilities, the identification of risks and recommendations to close the identified gaps.

How does it work?

Industrial Security Check	Compact one-day on-site assessment
IEC 62443 Assessment	Assessment based on the best known security standard for automation environment

Main value drivers



Evaluation of the current security status



Plant-specific and risk-based security roadmap



Basis for transparent cost estimates

Immediate access to industrial security expertise with Industrial Security Consulting



Industrial Security Consulting

- Operators of production facilities these days cannot afford to do without effective security measures. But industrial security capacities are rarely available.
- Industrial Security Consulting provides on-site support through experienced consultants regarding security policies and the plant-specific network layout as well as tailor-made implementation support for the industrial security portfolio.

How does it work?

Policy consulting	Network consulting	Implementation support
Review of existing and establishing/ integration of new policies, processes and procedures (e.g. password policy, patch and backup strategy)	Support for cell segmentation of networks, design of a perimeter protection network, review and implementation of firewall rules	Smooth integration of security portfolio from planning over installation and configuration up to commissioning and hands-on training

Main value drivers



Tailored security policies and concepts



Immediate access to expert know-how



No investment for developing own security capacities

Reverse the Operational Domino Effect with Remote Industrial Operations Services



Remote Industrial Operations Services

Increasing system complexity, lack of resources and cybersecurity threats are major risks for productivity losses. The unexpected failure of even the simplest component can lead to a domino effect and shut down operations.

With our Remote Industrial Operations Services, you have experts behind you who remotely manage your IT/OT infrastructure and thus align your IT and OT.

How does it work?

The modular contracting enables you to select only the services you need:

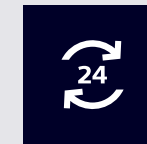
- 24/7 monitoring
- Predictive intelligence maintenance
- IT/OT technical experts support
- Secured by design



Main value drivers



**Proven IT/OT expertise
by our experts**



**Operational continuity
through maximized
availability**



**Compliance with
cybersecurity regu-
lations (e.g. NIS 2)**

Continuous network protection with Industrial Next Generation Firewall

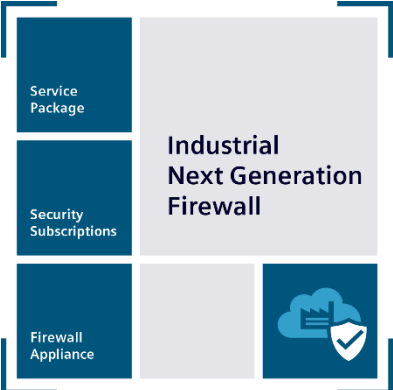


Industrial Next Generation Firewall

- Shop-floor landscape has changed from isolated islands to highly complex networks without any segmentation from untrusted cyber networks (e.g. office or internet).
- Industrial Next Generation Firewall is a perimeter protection solution in line with security requirements for industrial automation, tested and approved for usage with Siemens process control system.

How does it work?

- State-of-the-art Next Generation **Firewall Appliances**
- Additional **Security Subscriptions** for Threat Prevention, URL Filtering and WildFire
- **Service Package** (3 or 5 years) with Premium Support



Main value drivers



Continuous protection against known and unknown threats

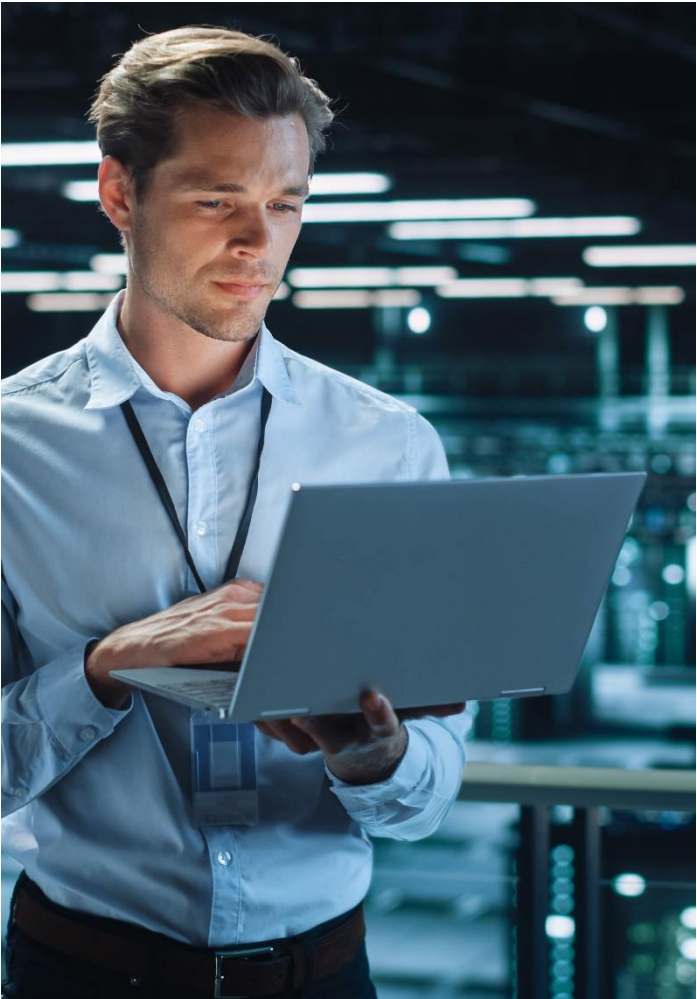


Tested and approved for SIMATIC PCS 7 and SIVaaS



Very good price/performance ratio

Secure data exchange between IT and OT with Industrial DMZ Infrastructure



Industrial DMZ Infrastructure

To protect against cyber attacks, the international security standard IEC 62443 recommends a deeply tiered defense, including network segmentation.

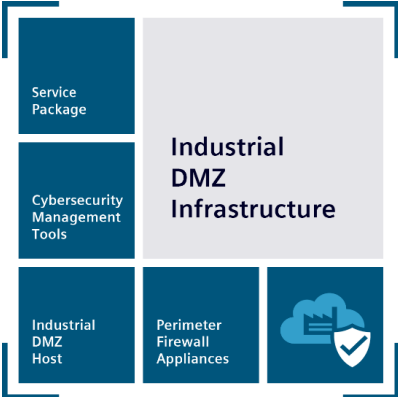
Industrial DMZ Infrastructure is a ready-to-run concept for the segmentation of IT and OT networks with integrated security features in several defense layers.

How does it work?

The concept is based on the principle of the demilitarized zone (DMZ). The applied Next Generation Firewalls protect the automation level from unauthorized access from outside.

Additional highlights:

- Hardware, software and services for network security and system integrity already integrated
- Implementation on the hyper-convergent IT platform Industrial Automation DataCenter



Main value drivers



IT/OT network segmentation based on IEC 62443



Defense in depth with security features out of the box



Hyper-convergent IT infrastructure for high performance computing

Secure remote access to industry devices with Remote Platform SaaS

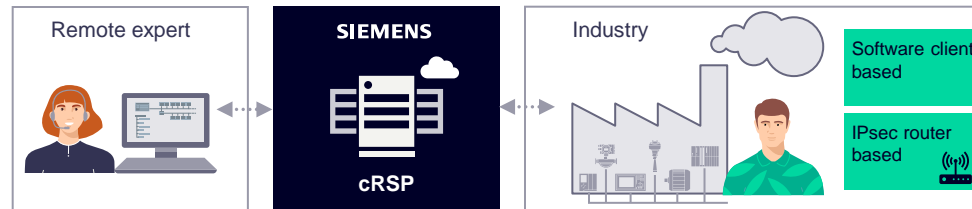


Remote Platform SaaS

Remote Platform Software as a Service (Remote Platform SaaS) provides a highly scalable and secure remote access infrastructure which is operated and maintained by Siemens. The common Remote Service Platform (cRSP) is designed according to industry requirements in line with IEC 62443 and focuses on access to industrial devices.

How does it work?

cRSP is used for implementing remote access and transferring data to IP-based (Siemens and others) devices. The administration and configuration of the remote platform is self-managed or managed by Siemens. Predefined application templates ensure simple workflows for remote experts. After the initial setup, an authorized remote expert can establish a remote connection to the connected devices through secure VPN tunnel via a software client or IPsec router.



Main value drivers



Less travel and reduced downtime lead to cost reduction and contribute to carbon neutrality

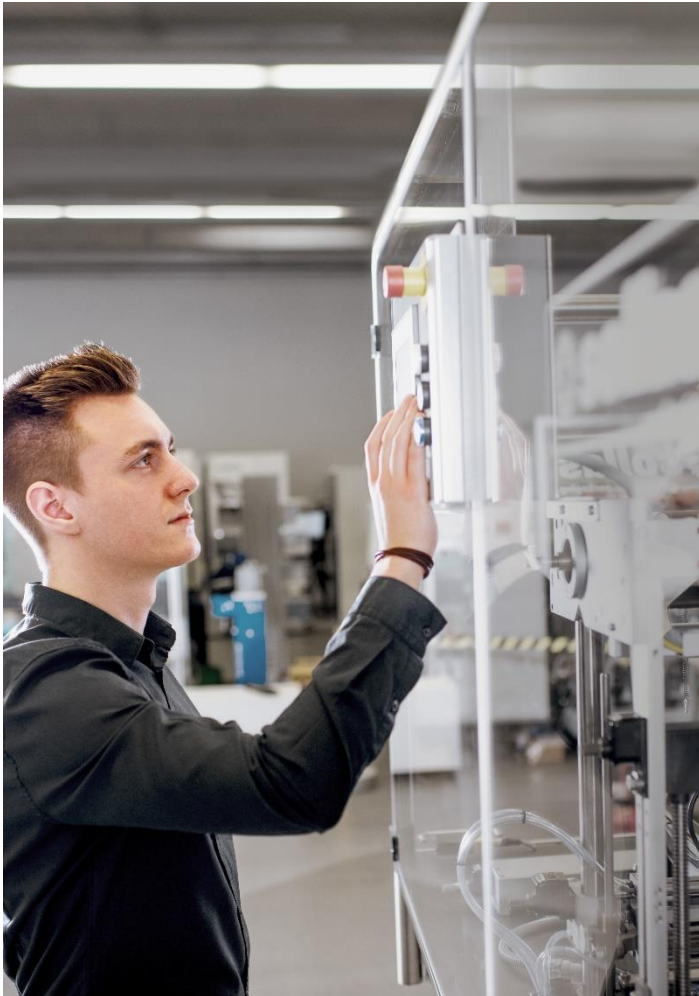


Use of Siemens proven and worldwide available remote platform cRSP



State of the art industrial security

Continuous protection against malware with Endpoint Protection

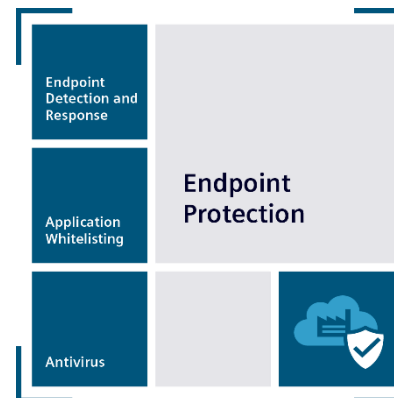


Endpoint Protection

- The threat of malware in form of viruses, rootkits and trojans is growing exponentially – also for endpoint devices in industrial environments (e.g. IPC).
- Endpoint Protection provides different approaches – each has its advantages depending on the use case.

How does it work?

- **Antivirus:** The execution of known malicious applications is blocked based on continuously updated signature files
- **Application Whitelisting:** Only trusted applications are allowed to run based on a positive list
- **Endpoint Detection and Response:** Interoperability test for the specific configuration of PCS 7 version and 3rd party EDR software version



Main value drivers



Protection against known and unknown threats caused by malware



Easy, centralized operation via management server



Approved versions with tailor-made configurations for Siemens products

Efficient handling of vulnerabilities with Vilocity Vulnerability Services



Vilocity Vulnerability Services

Companies need to reduce their exposure to vulnerabilities in the face of a growing number of cyberthreats. Identifying new vulnerabilities as soon as possible is crucial.

Vilocity Vulnerability Services empower you to secure your product development, infrastructure and product portfolio by providing relevant, actionable vulnerability intelligence.

How does it work?

Based on a unique monitoring approach you receive vulnerability alerts for your individual system, enabling proactive management of cyber risks.

There are different options:

Management Portal:

Structured overview of relevant vulnerabilities (basic) plus asset import functions and integrated management tools (extended)

API:

Seamless integration into your existing tools and processes



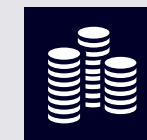
Main value drivers



Instant transparency on vulnerabilities and minimized patch-times



Proactive management of cyber risks – easily integrated into your workflow



Reduced risk of costly exploits

Managing vulnerabilities and critical updates with Patch Management



Patch Management

- The installation of patches is the appropriate reaction to close vulnerabilities in software. Thus, patches contribute to stable plant operation. But patching is manual work and an incompatible patch can cause unplanned downtimes.
- Siemens offers Patch Management of security patches and critical updates in Microsoft products for SIMATIC PCS 7 to simplify the patch process on the plant.

How does it work?

- **Step 1:** The monthly released security patches for Microsoft products are tested and verified for compatibility with SIMATIC PCS 7.
- **Step 2:** This information is published as metadata via a central update server (WSUS – Windows Software Update Services), which sends the information automatically to the local WSUS server in the plant.
- **Step 3:** The customer receives a notification and can download the approved patches directly from Microsoft.

1 Windows Software Update Services

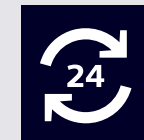
Main value drivers



Save time and cost due to reduction of manual work on-site



Minimize risk of human error



Enhanced plant availability

Pre-configured IT infrastructure for disaster recovery with Backup and Restore (SIMATIC DCS / SCADA Infrastructure)



Backup and Restore

The right disaster recovery strategy is an extremely important factor to restart production after a breakdown and to prevent data loss.

Backup and Restore (as part of SIMATIC DCS / SCADA Infrastructure) provides a powerful and preconfigured IT infrastructure for disaster recovery in industrial environments.

How does it work?

Data Archiving:

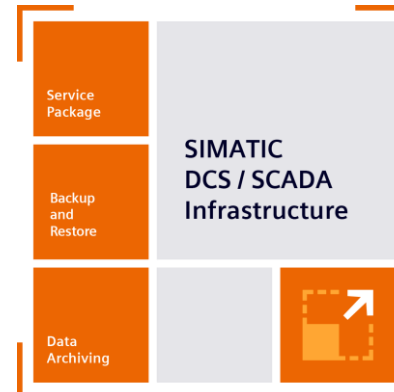
Reliable data archiving and visualization with the Process Historian / Information Server software

Backup and Restore:

Best in class Disaster Recovery Backup solution

Service Package:

3- or 5-year service agreement



Main value drivers



Optimized performance through reliable data archiving and powerful reporting tools



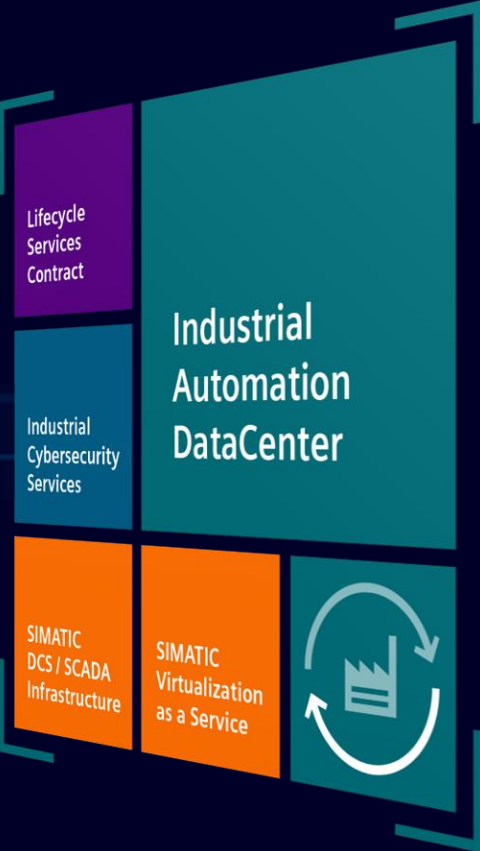
Increased availability thanks to fast disaster recovery and prevented data loss



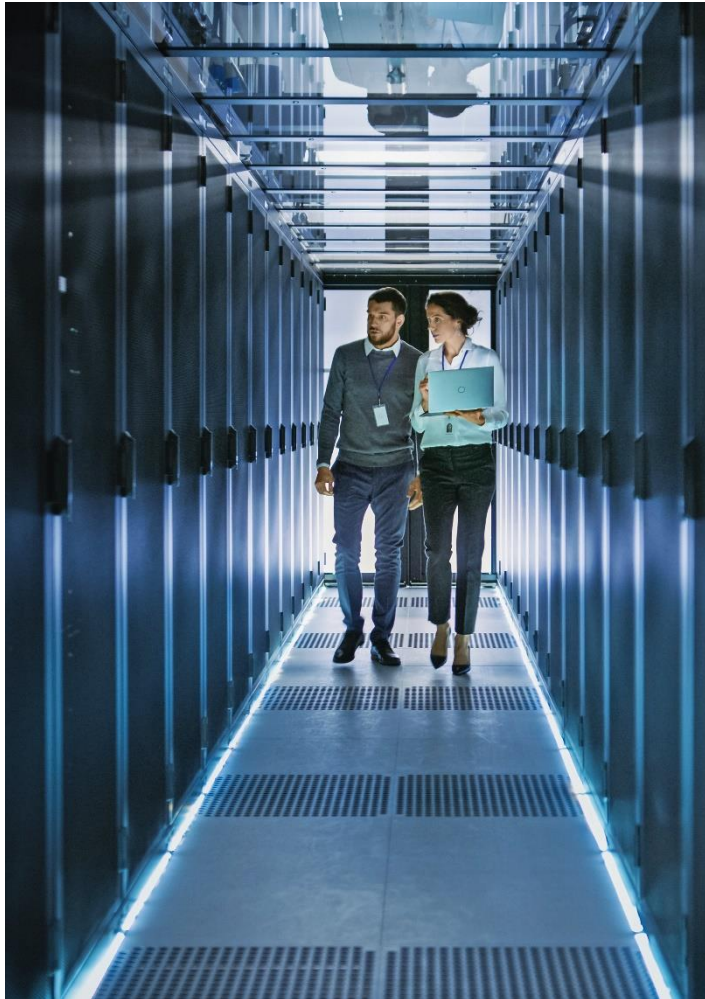
Ready-to-run infrastructure with system-tested, pre-configured components

Industrial Cybersecurity Services @ Industrial Automation DataCenter

Industrial Cybersecurity Services
can be integrated into the
Industrial Automation DataCenter



Bridge the gap between IT and OT with Industrial Automation DataCenter



Industrial Automation DataCenter

System complexity is rising and cybersecurity threats are increasing, whereas there is a lack of know-how and resources when it comes to IT/OT integration.

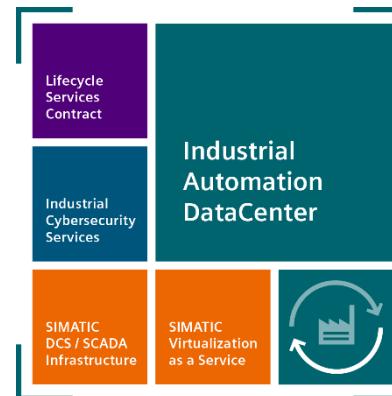
The Industrial Automation DataCenter is a ready-to-run tailor-made IT infrastructure for OT environments – developed by our experts who combine expertise in both fields.

How does it work?

All important core elements of a data center are included:

- High performance computing
- IT/OT network
- Back-up & disaster recovery
- Process data archiving
- Uninterruptible power supply
- IEC 62443 compliant security architecture

The holistic approach covers consulting, configuration and managed services throughout the entire life cycle - from a single source.



Main value drivers



Ready-to-run high available IT/OT infrastructure



High energy efficiency and space savings



Cybersecurity by design

System integrity



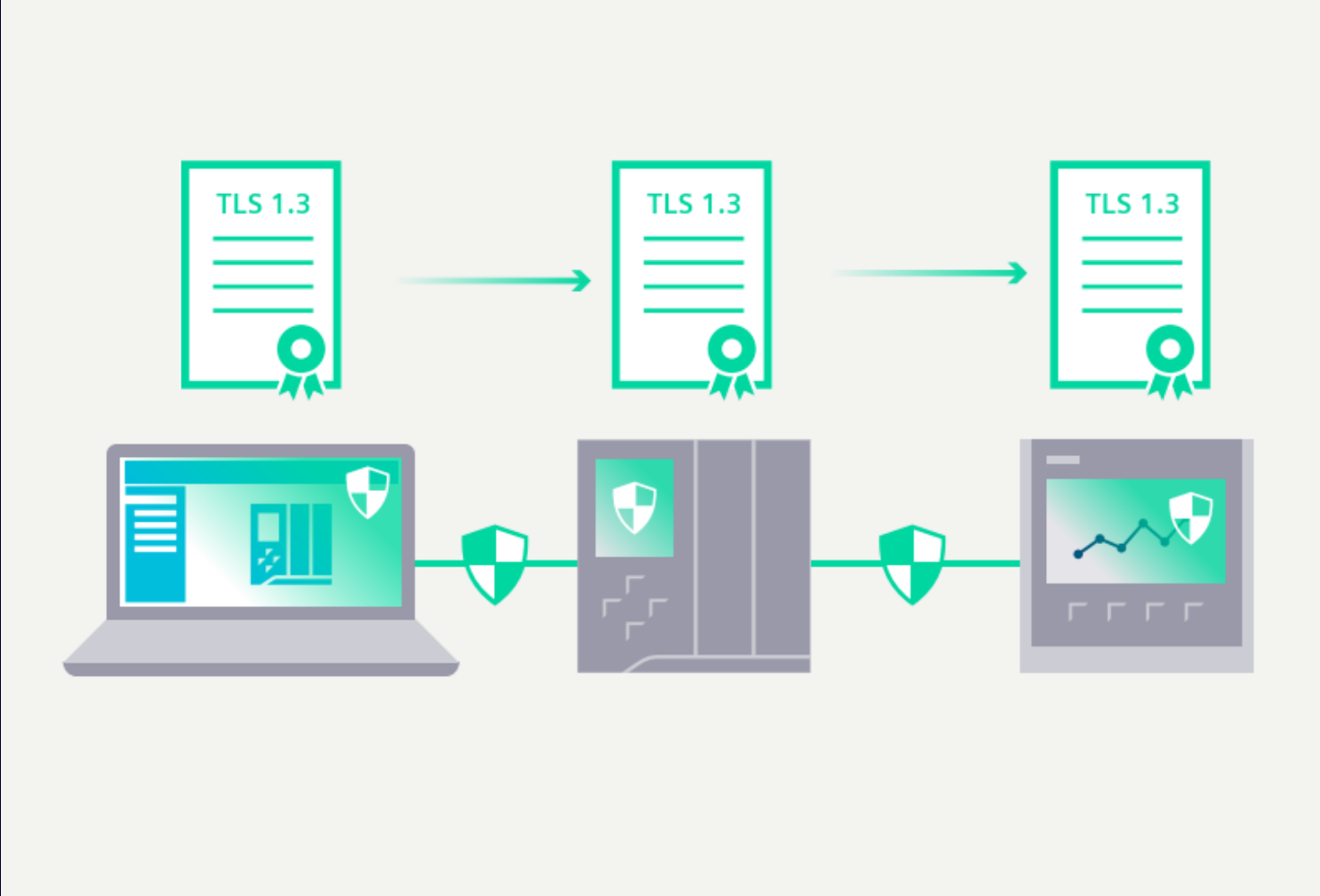
Secure SIMATIC PG/HMI communication



Secure PG/HMI communication with TIA Portal V17

TLS*-based protection of communication between S7-Controllers and Engineering Stations with TIA Portal or HMI-Stations

Encrypts communication by applying **individual** certificates

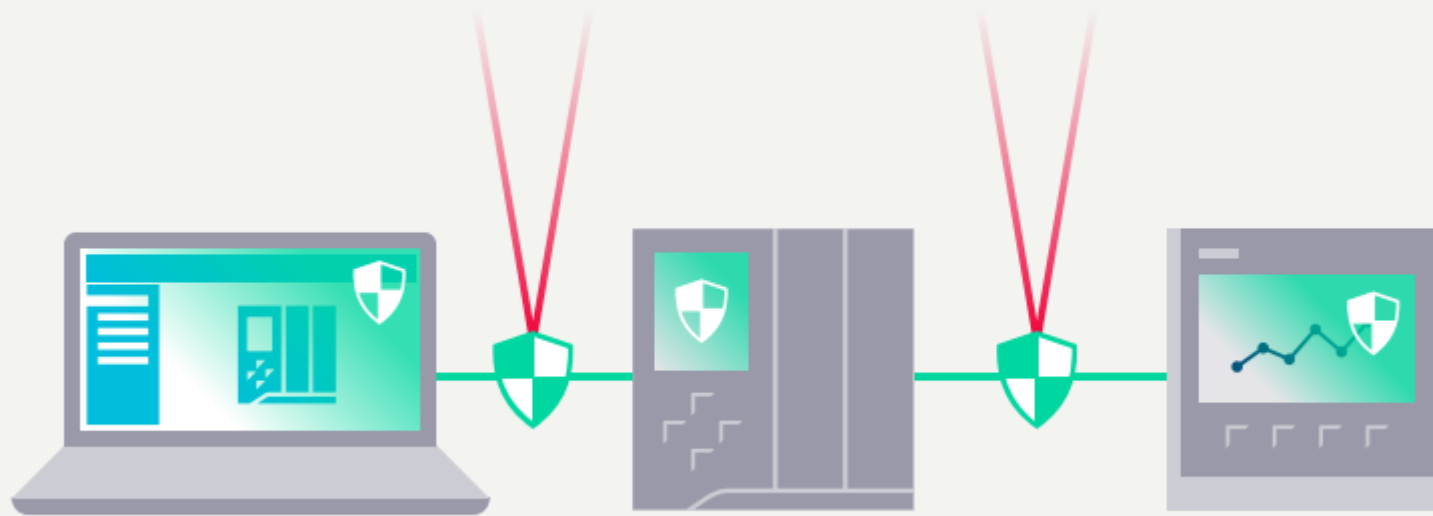


^{*)} TLS - Transport Layer Security

Secure PG/HMI communication with TIA Portal V17

This true **end-to-end encryption** between engineering station or HMI station can prevent any manipulation of the controller program or parameters.

With this state-of-the-art secured communication based on TLS (V1.3) a high-level protection will be provided for the automation systems and avoids production loss, data theft and manipulation or sabotage.

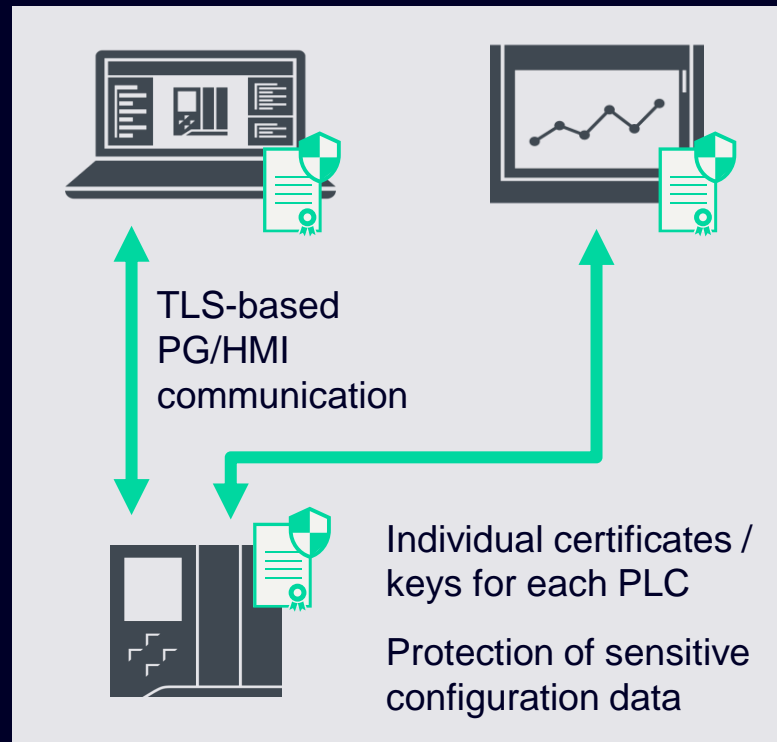


Secure SIMATIC PG/HMI Communication

Improved Communication Security

Security improvements for PG/HMI communication between TIA Portal V17, HMIs and S7-1200/1500 CPUs

- Communication protection is based on the Internet Standard TLS*
- Supports unique identification of each PLC based on individual certificates (e.g. created via TIA Portal)
- Compatibility mode for previous and new TLS-based communication at the same time can be activated
- Provides additional confidentiality protection due to encrypted communication
- Allows protection of sensitive configuration data in TIA Portal and PLCs via user-defined passwords (optional)



Benefit

- Allows unique identification of each PLC based on individual certificates
- Provides additional confidentiality protection due to encrypted communication
- Configuration data protection based on individual passwords

* TLS - Transport Layer Security

Secure SIMATIC PG/HMI Communication

Sivas Compatibility

The following components support the new Secure SIMATIC PG/HMI communication:

Server

- S7-1500 PLCs V2.9
- S7-1200 PLCs V4.5
- S7-PLCSIM Advanced
- Drive Controller V2.9

Clients

- STEP 7 (TIA Portal) V17
- HMI Basic Panels 2nd Generation, V17
- HMI Mobile Panels 2nd Generation, V17
- HMI Comfort Panels, V17
- HMI Unified Comfort Panels V17
- WinCC Runtime Advanced V17
- WinCC Runtime Professional V17
- WinCC Unified PC V17
- WinCC V7.5 SP2 (Update 4)
- SIMATIC NET (OPC UA Server) V17
- WinCC OA V3.18



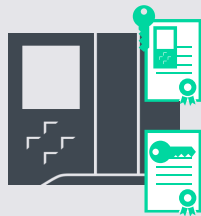
Secure SIMATIC PG/HMI Communication

Improved Communication Security

1. Provisioning phase



TLS-based PG/HMI communication:
Download Project data and Certificate



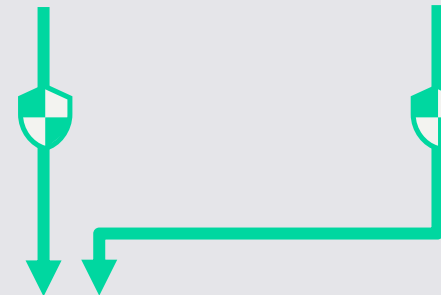
PLC is not configured

PLC has device certificate/
self-signed certificate

2. TLS* based communication



Trusted certificates
of PLCs

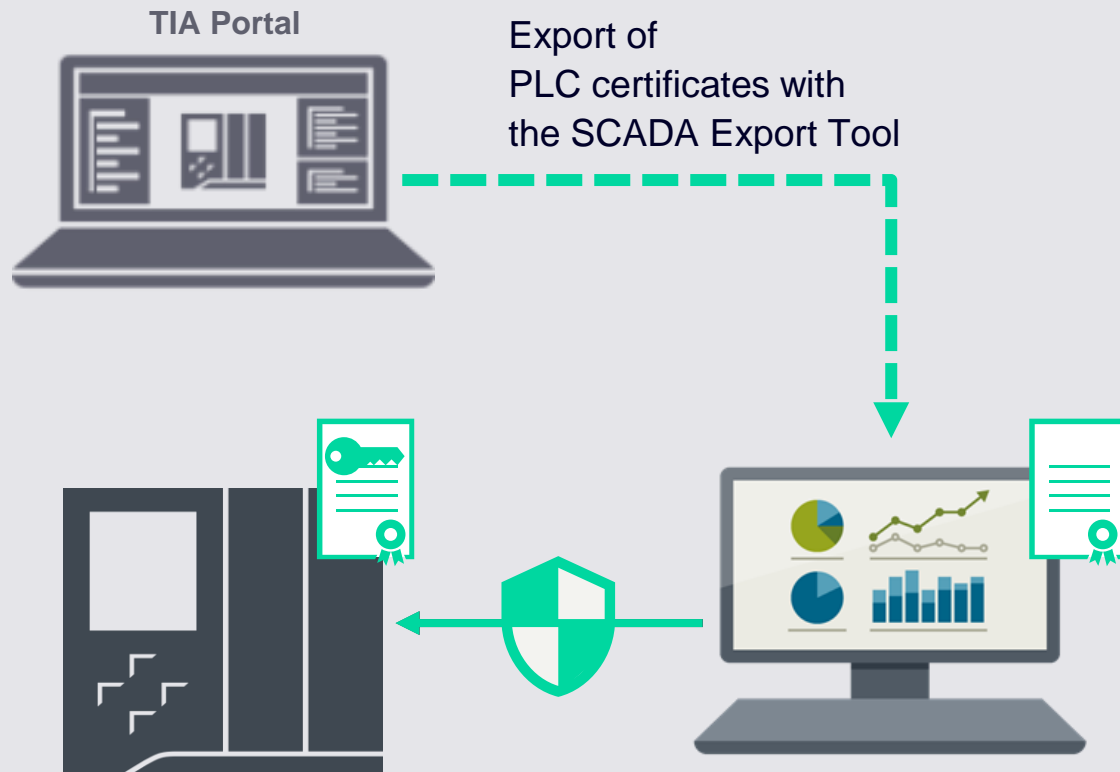


Individual certificates /
keys for each PLC

* TLS - Transport Layer Security

WinCC V7.5 SP2

Improved communication security



SIMATIC SCADA Export für TIA Portal

<https://support.industry.siemens.com/cs/ww/de/view/109748955>

Notes for secure PLC communication with TLS protocol on the SIMATIC S7-1200/S7-1500 channel in WinCC V7.5 SP2 Update 4

<https://support.industry.siemens.com/cs/ww/en/view/109798498>

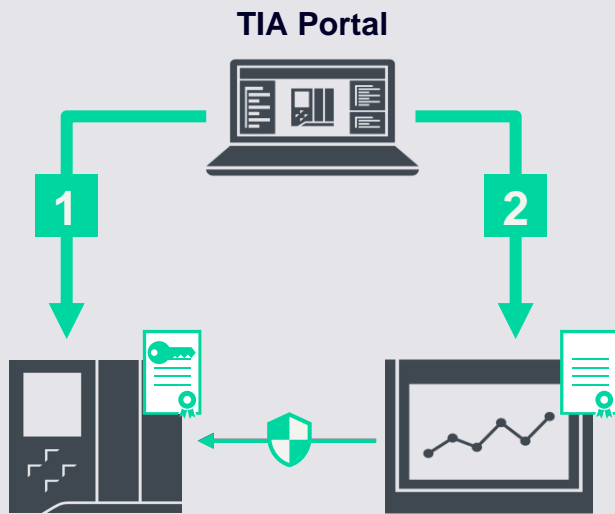


Certificate with private key e.g. for PG/HMI communication

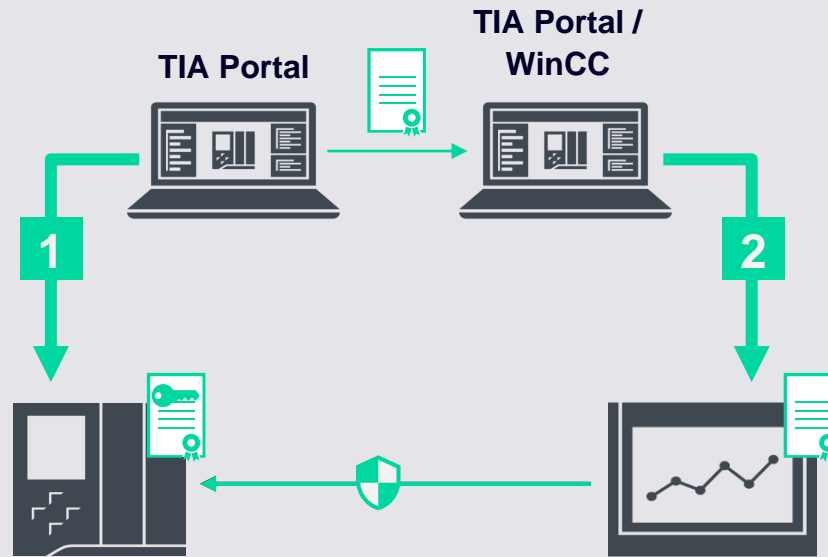
Secure SIMATIC PG/HMI Communication

Improved Communication Security

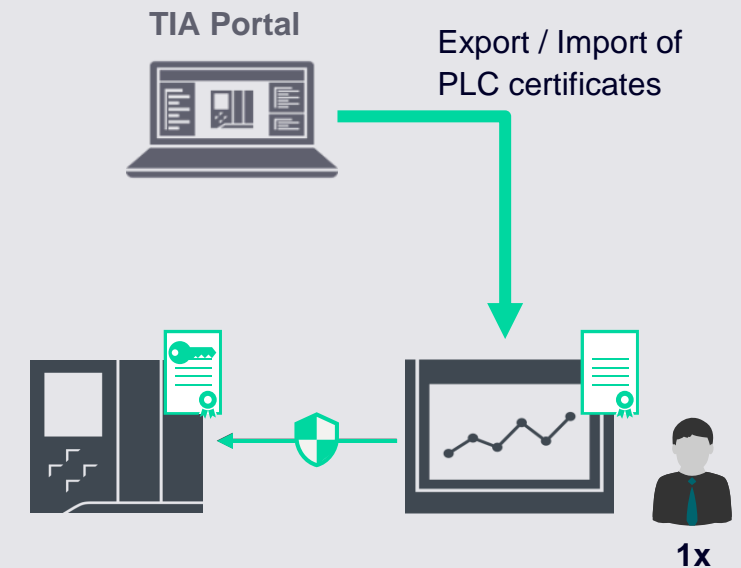
HMI and PLC in the same TIA Portal project




HMI and PLC in separate TIA Portal projects



HMI connection (e.g. WinCC V7) without TIA Portal



 Certificate with private key e.g. for PG/HMI communication

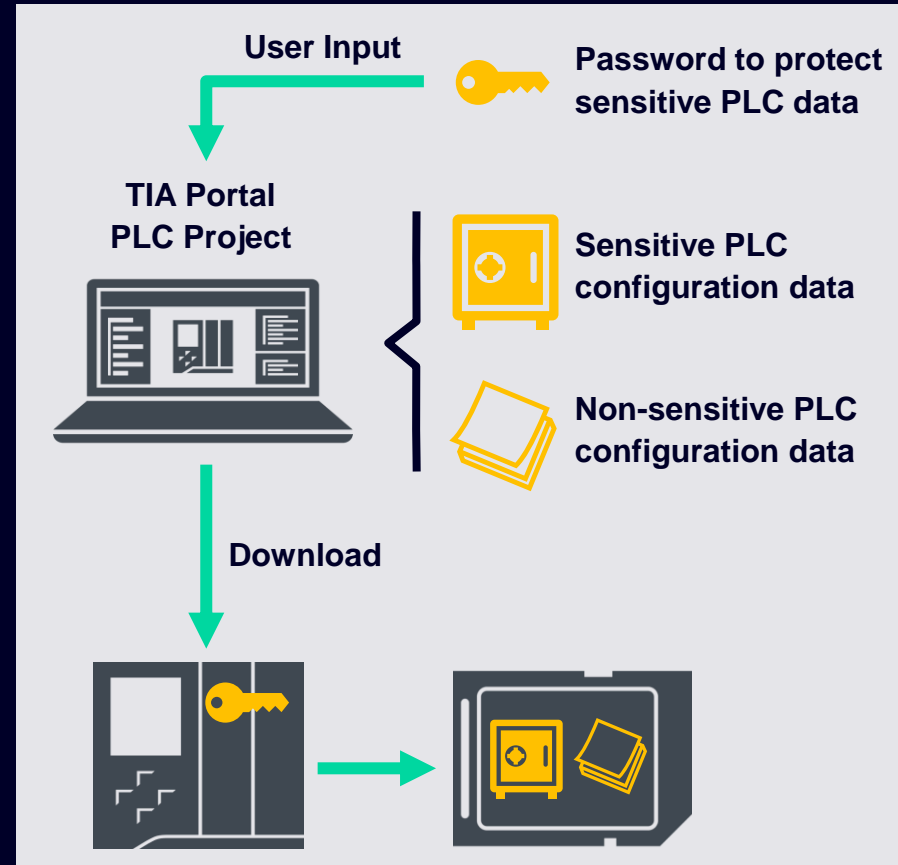
Secure SIMATIC PG/HMI Communication

Improved Communication Security

New mechanism to Protect Sensitive PLC Configuration Data

User defined protection of sensitive configuration data

- Configuration data means private keys from certificates for PG/HMI communication, Webserver, OPC UA etc.
- Data is protected based on a user-defined password per PLC
- This configuration is optional



Benefit

- Configuration of data protection is based on individual passwords

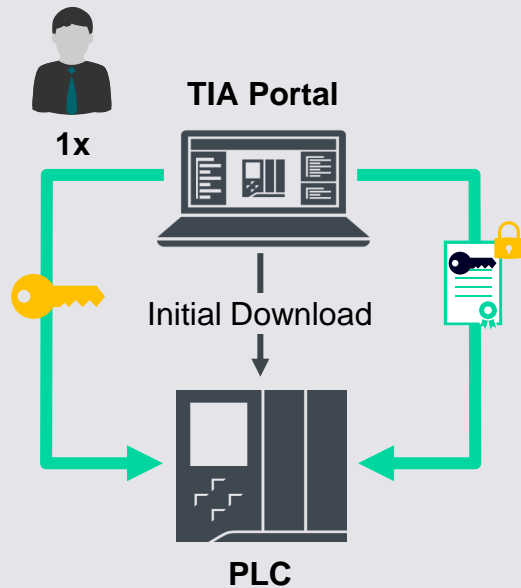
Secure SIMATIC PG/HMI Communication

Improved Communication Security

Device Exchange Scenarios

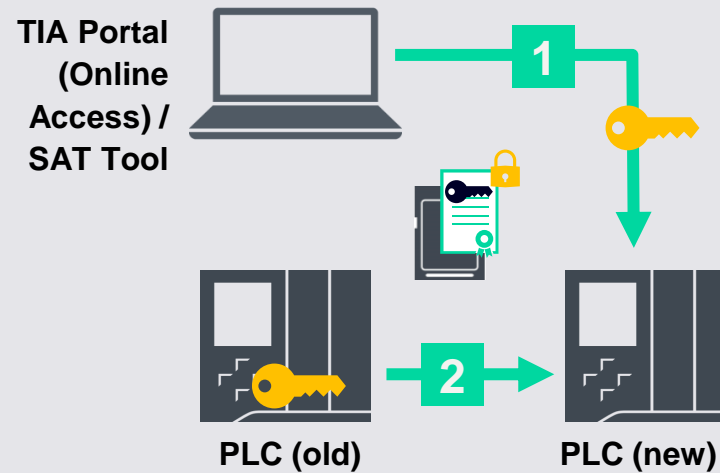
Setting via project download

- Password is set during project download via TIA Portal



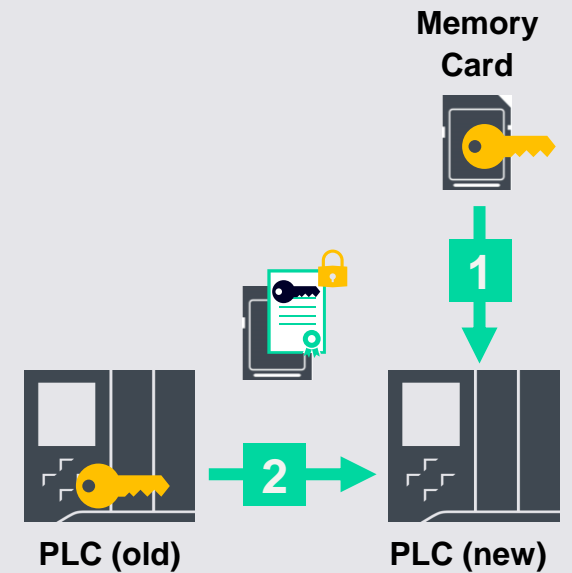
Direct online access


- Password is set / reset via TIA Portal online functions (incl. Openness)
- Also supported by SIMATIC Automation Tool - SAT




SIMATIC Memory Card

- Password is stored on a SMC with a special JOB file
- Additional Memory card needed



 Certificate with private key e.g. for PG/HMI communication

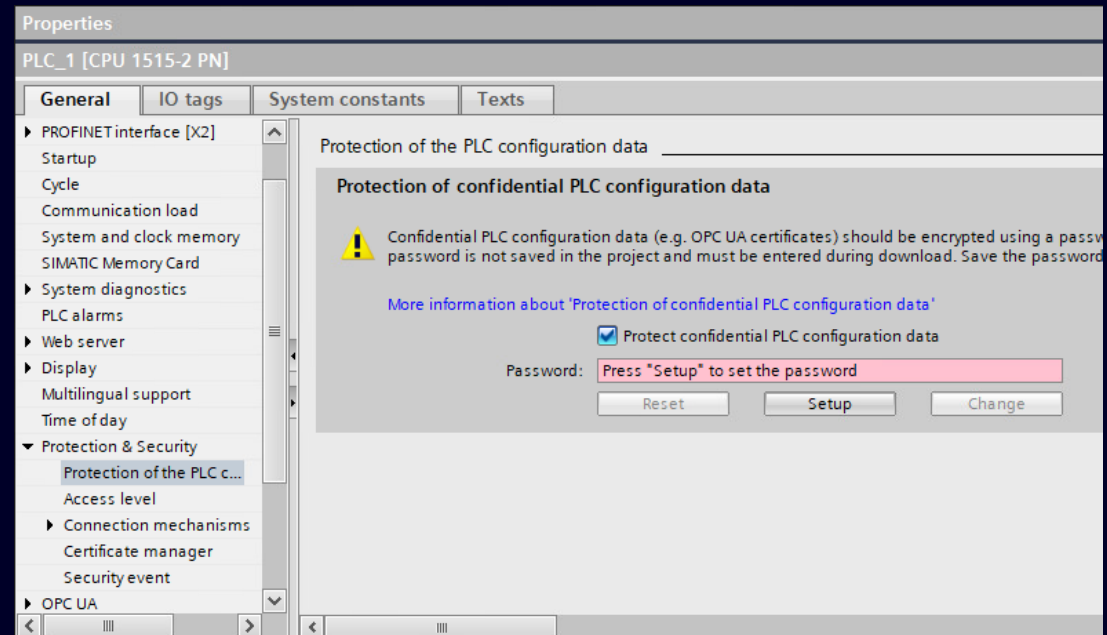
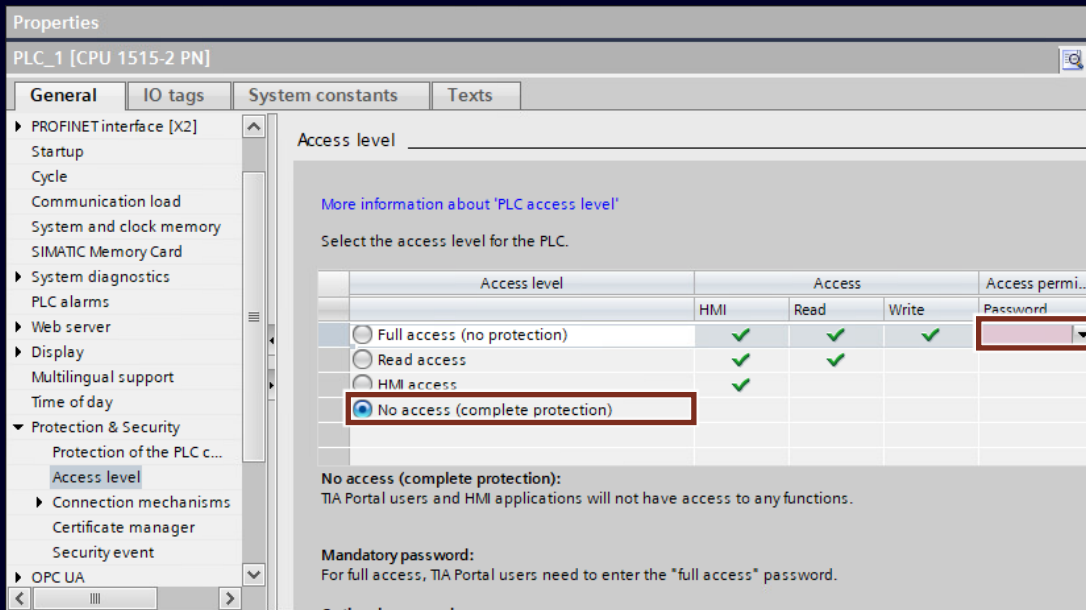
 Password to protect 'confidential PLC configuration'

Secure SIMATIC PG/HMI Communication

“Security-By-Default” Concept

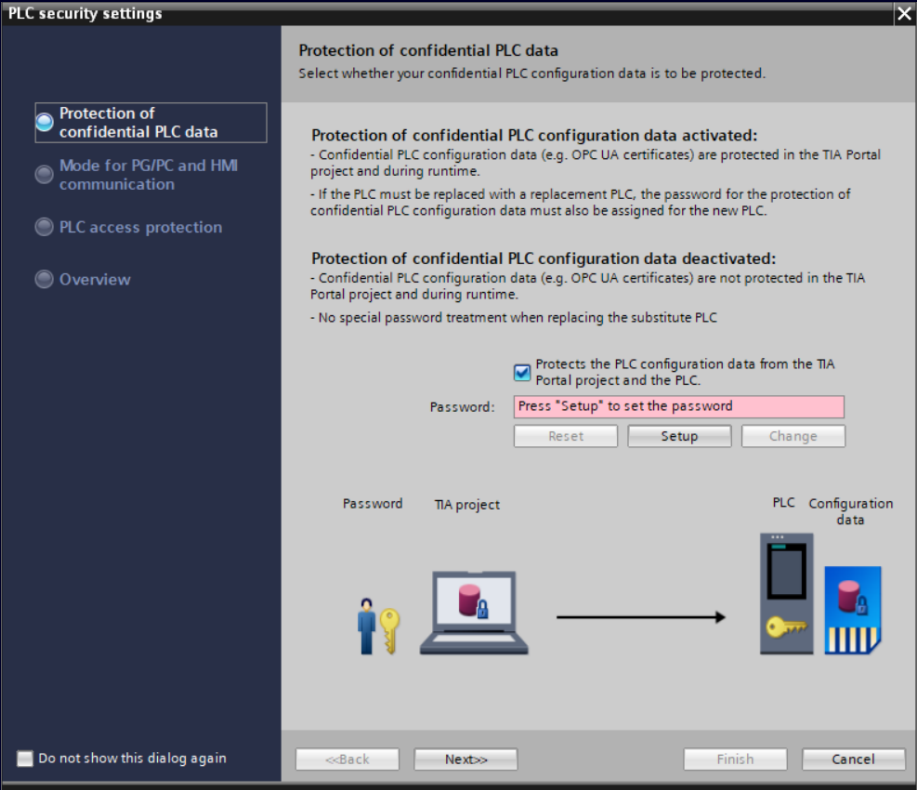
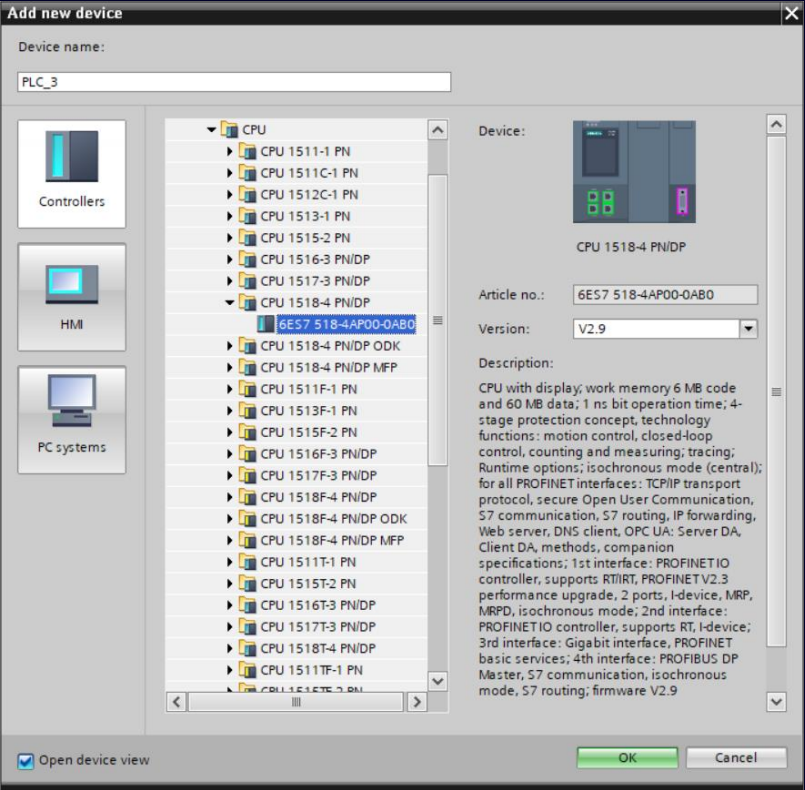
More functionality is predefined in a secure way to support a higher security level for machines and plants. This includes:

- Preactivated PLC access protection (Protection levels)
- Required Password for sensitive PLC configuration data
- Predefined secure PG/HMI communication only (no mixed mode)



Secure SIMATIC PG/HMI Communication Configuration with Security Wizard

Security Wizard in TIA Portal V17

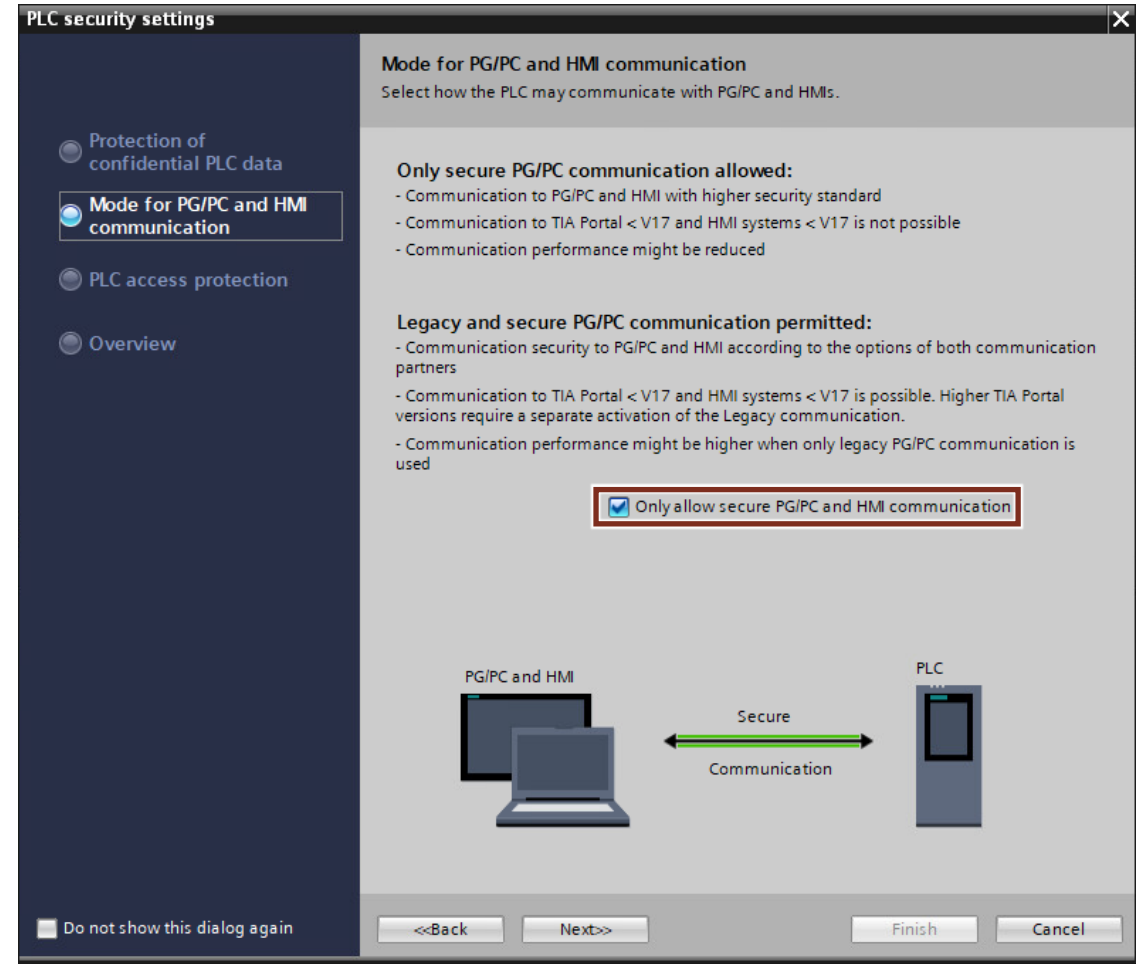


Secure SIMATIC PG/HMI Communication

Simatic Compatibility

Compatibility function

- Improved security measures become active only with TIA Portal V17 related products and relevant configuration
- A PLC with new firmware but old configuration data will work in compatibility mode as configured
- Communication to TIA Portal and HMI systems older than V17 is still possible



Secure SIMATIC PG/HMI Communication

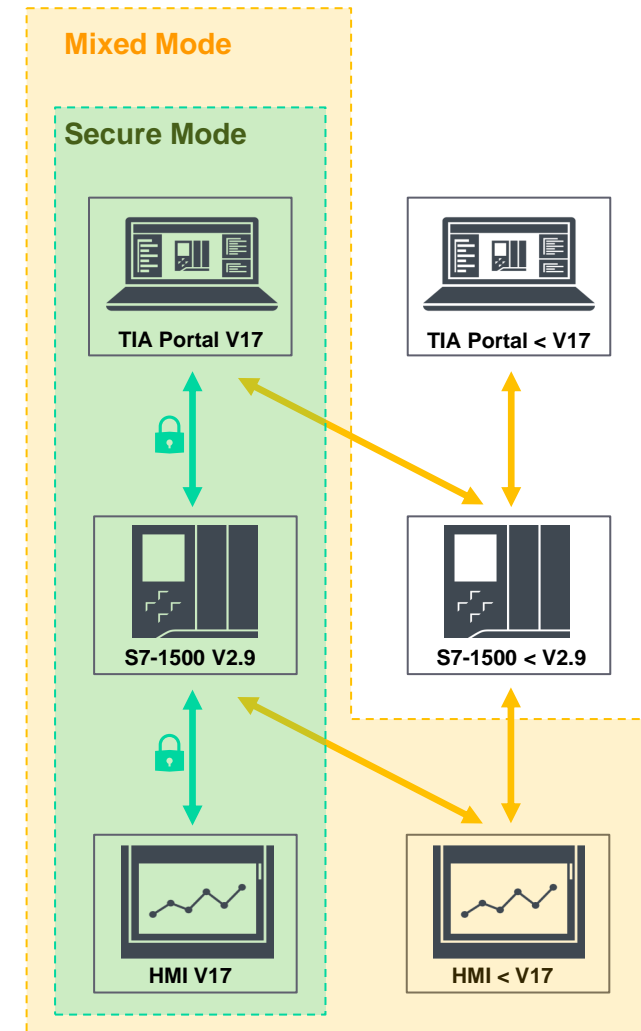
Simatic Compatibility

Supported modes of TIA Portal V17 PLCs

- **Secure Mode:** Allow only secure TLS protected PG/HMI communication
- **Mixed Mode:** Allow TLS protected PG/HMI communication and legacy PG/HMI communication

Compatibility

- Communication of PLCs with ES / HMI clients < V17 is only possible in **Mixed Mode**
- By default, only **secure** TLS-based communication is accepted by V17 related PLCs
- TLS-based communication can be deactivated when needed. In this case, communication is only possible in **Mixed Mode**



Automation systems with Security Integrated



Industrial Security

Security functions overview for SIMATIC Controller

Security Function	S7-300 (>=v3.2)	S7-400 (>=v6.0)	S7-1200 (>v4, V12 SP1)	S7-1500	S7-1500 Software Controller
Increased Know-how Protection					
Know-How Protection for Program blocks	●	●	●	●	●
Copy Protection for Program blocks (as system function)	A)	A)	●	●	●
Improved Access Protection					
Project access protection via Password	●	●	●	●	●
HMI Access Protection for Controllers			●	●	●
Different Access Levels by multiple Passwords			●	●	●
Integrity Protection					
Integrity Protection for Firmware Updates	B)	●	●	●	●
Communication Integrity			●	●	●

A) Realizable via PLC program B) CRC based

Industrial Security

SIMATIC S7-1200, S7-1500 and the TIA Portal



Security Highlights

The **SIMATIC S7-1200 V4, S7-1500 incl. S7-1500 Software Controller and the TIA Portal** provide integrated security features:

- **Increased Know-How Protection in STEP 7**

Protection of intellectual property and effective investment:

- Password protection against unauthorized opening of program blocks in STEP 7 and thus protection against unauthorized copying of e.g. developed algorithms
- Password protection against unauthorized evaluation of the program blocks with external programs
 - from the STEP 7 project
 - from the data of the memory card
 - from program libraries

- **Increased Copy Protection**

Protection against unauthorized reproduction of executable programs:

- Binding of single blocks to the serial number of the memory card or PLC
- Protection against unauthorized copying of program blocks with STEP 7
- Protection against duplicating the project saved on the memory card

Industrial Security

SIMATIC S7-1200, S7-1500 and the TIA Portal



Security Highlights

The **SIMATIC S7-1200 V4, S7-1500 incl. S7-1500 Software Controller and the TIA Portal** provide integrated security features:

- **Increased Access Protection (Authentication)**

Extensive protection against unauthorized project changes:

- New degree of Protection Level 4 for PLC, complete lockdown (also HMI connections need password) *
- Configurable levels of authorization (1-3 with own password)
- General blocking of project parameter changes via the built-in display

- **Expanded Access Protection**

Extensive protection against unauthorized project changes:

- Via Security CP1543-1 by means of integrated firewall and VPN communication

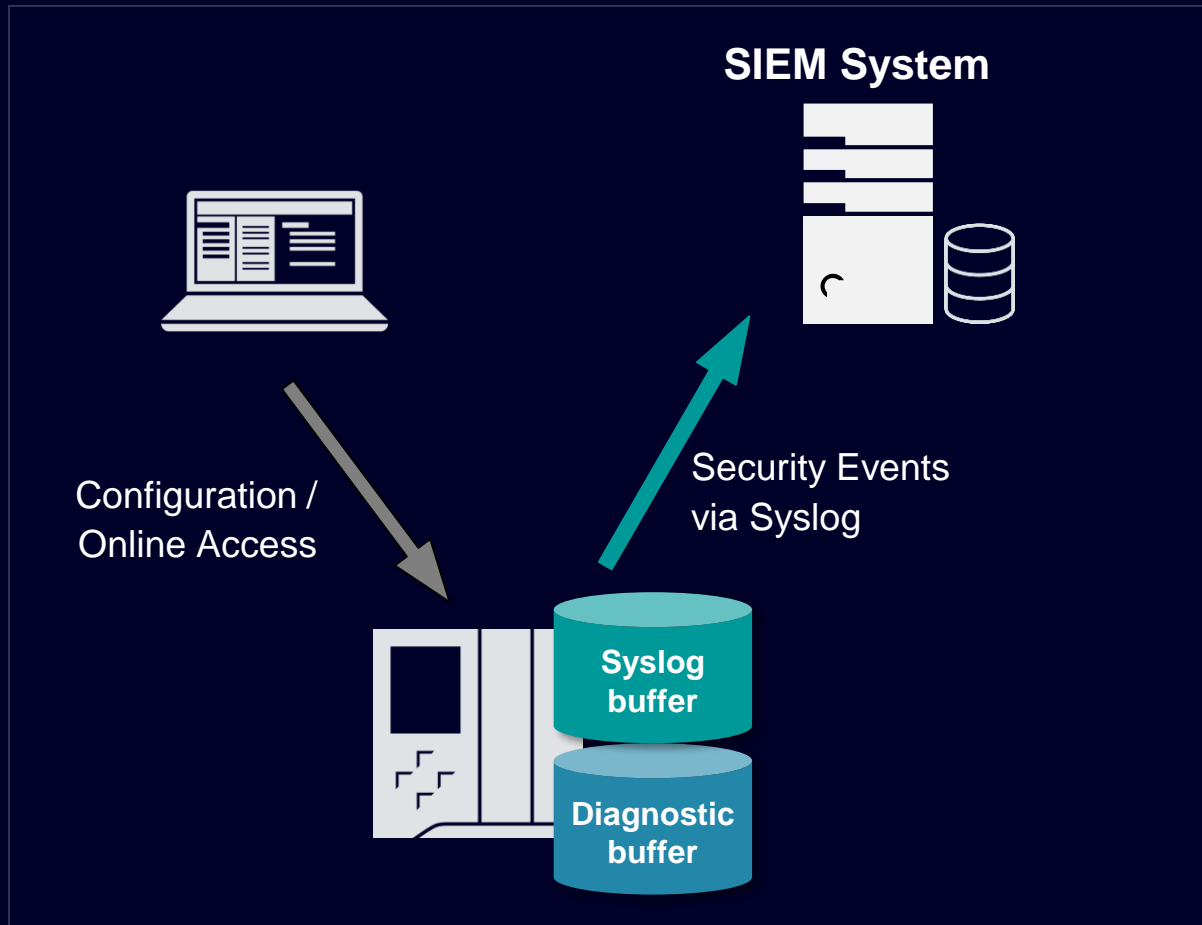
- **Increased Protection against Manipulation**

Protection of communication against unauthorized manipulation for high plant availability:

- Improved protection against manipulated communication by means of digital checksums when accessing controllers
- Protection against network attacks such as intrude of faked / recorded network communication (replay attacks)
- Detection of manipulated firmware updates by means of digital checksums

* Optimally supported by SIMATIC HMI products and SIMATIC NET OPC Server

Security Logging in S7-1500 CPUs and software controller

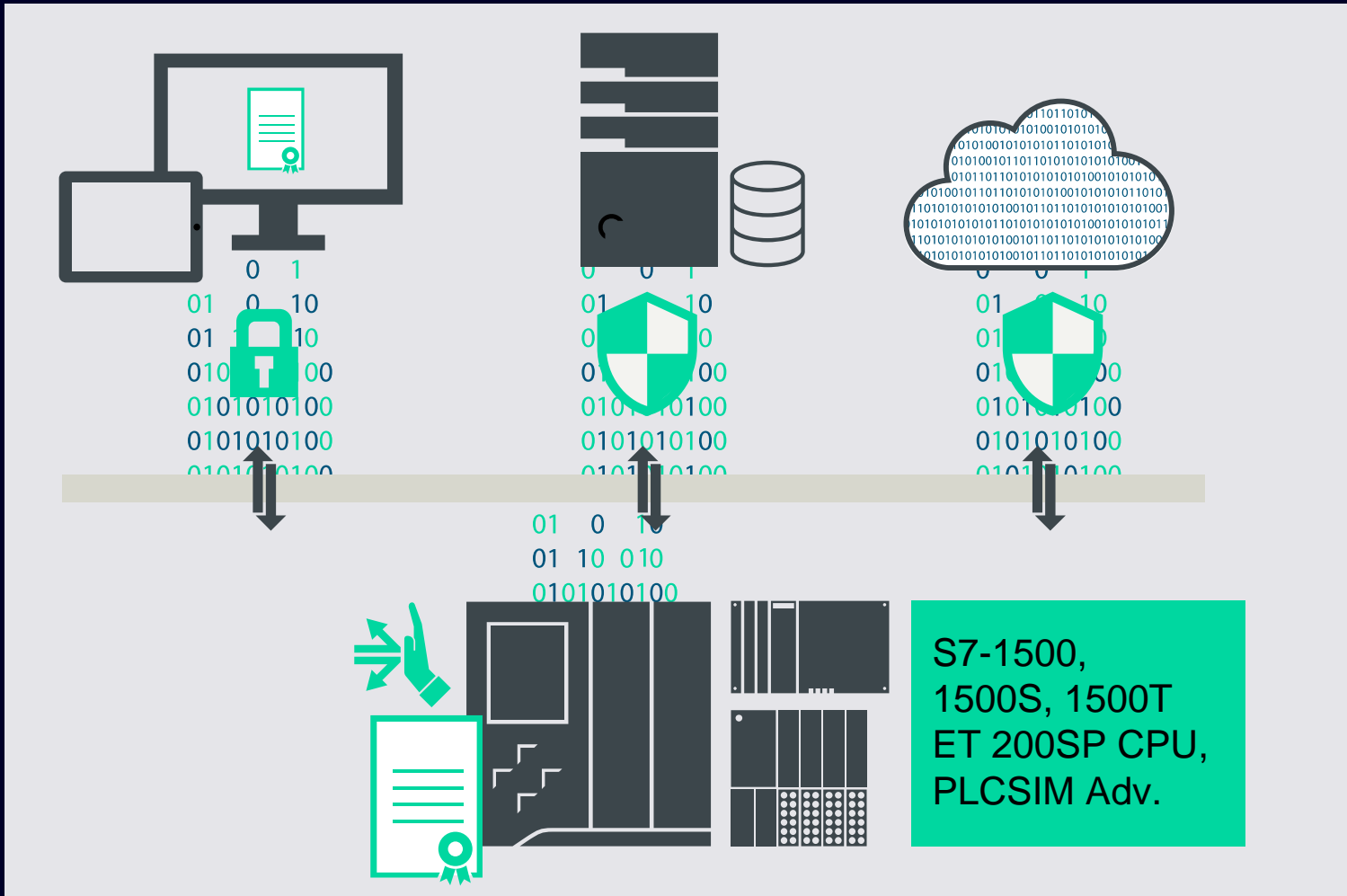


Tracing and monitoring of critical PLC changes / operations with easy integration of into customer Security Monitoring solutions

- Separate security log in PLC for security related events
- Logging contains user information (in combination with UMAC in PLC) to trace who did what and when
- Easy integration into customers Security Monitoring solutions via forwarding to external SYSLOG / SIEM systems via syslog protocol (incl. secure syslog)

OPC UA

Integrated security mechanisms



OPC UA Security



Selectable security policies
in Controller and Clients



Device/application authentication
based on certificates



Integrity protection
and encrypted communication

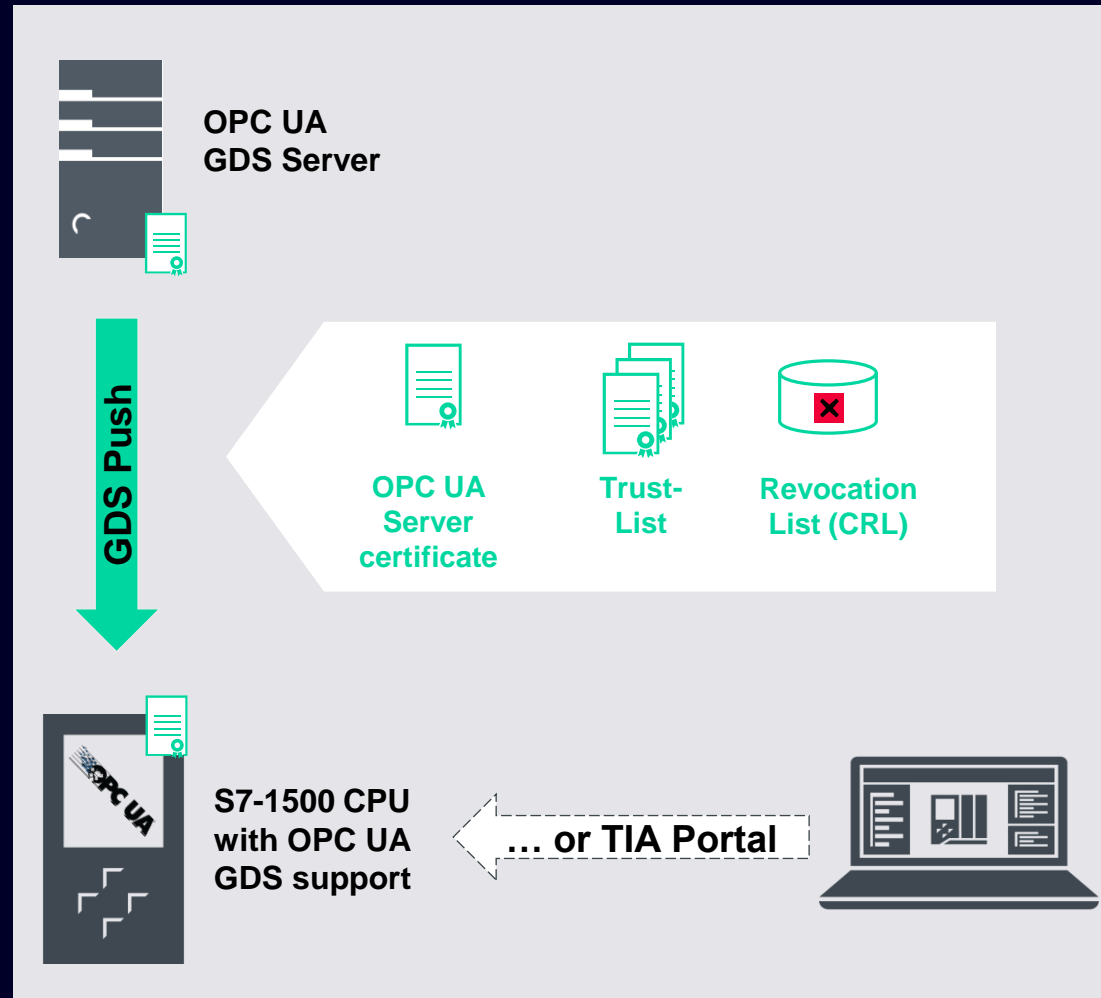


User authentication and restricted
access to PLC tags

Certificate Management via OPC UA for S7-1500 GDS Support

Certificate management is now possible through OPC UA Global Discovery Server - GDS

- Certificate update at **runtime**
- Support of Certificate Revocation Lists - **CRLs**
- Access protection for certificate management



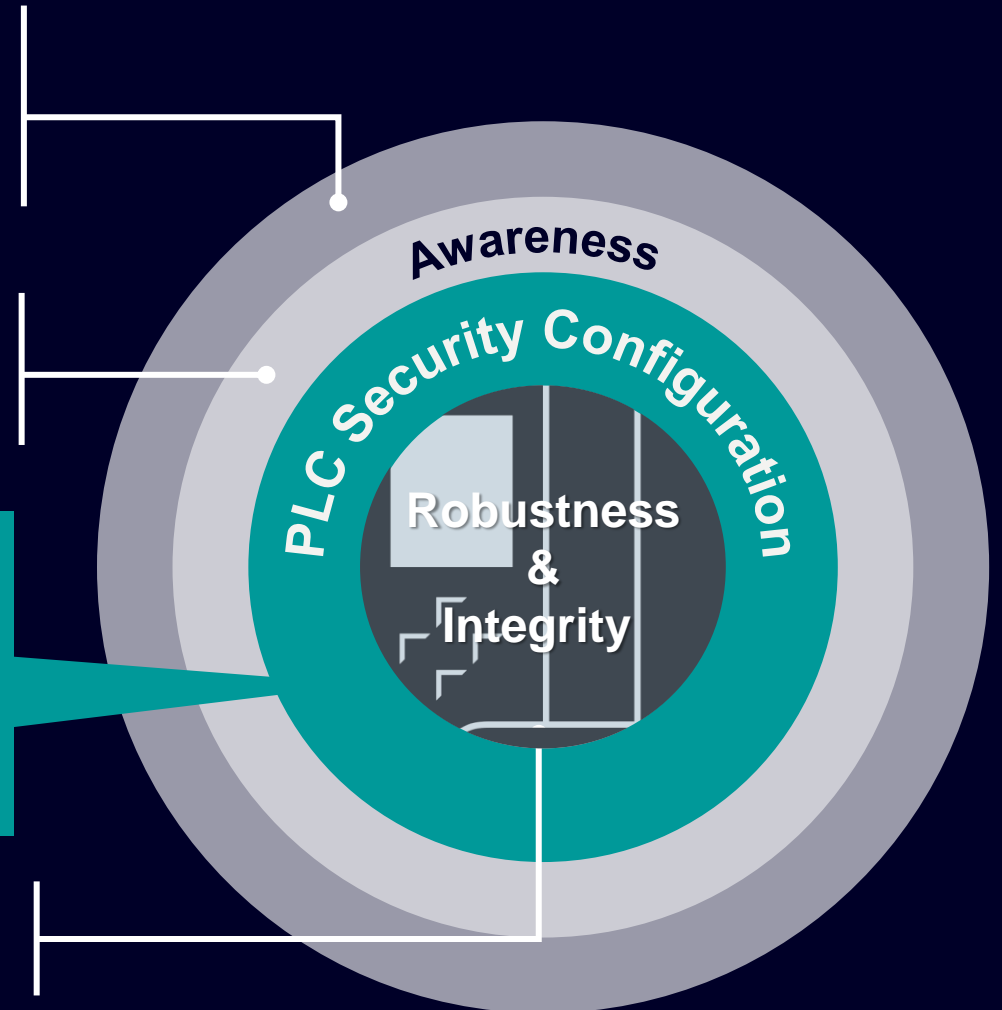
Benefits

- Install or update the OPC UA server certificate during runtime
- Implement security concepts based on short validity period
- Revoke certificates during runtime
- Restrict access when employees leave the company or when the system is compromised

Industrial Security

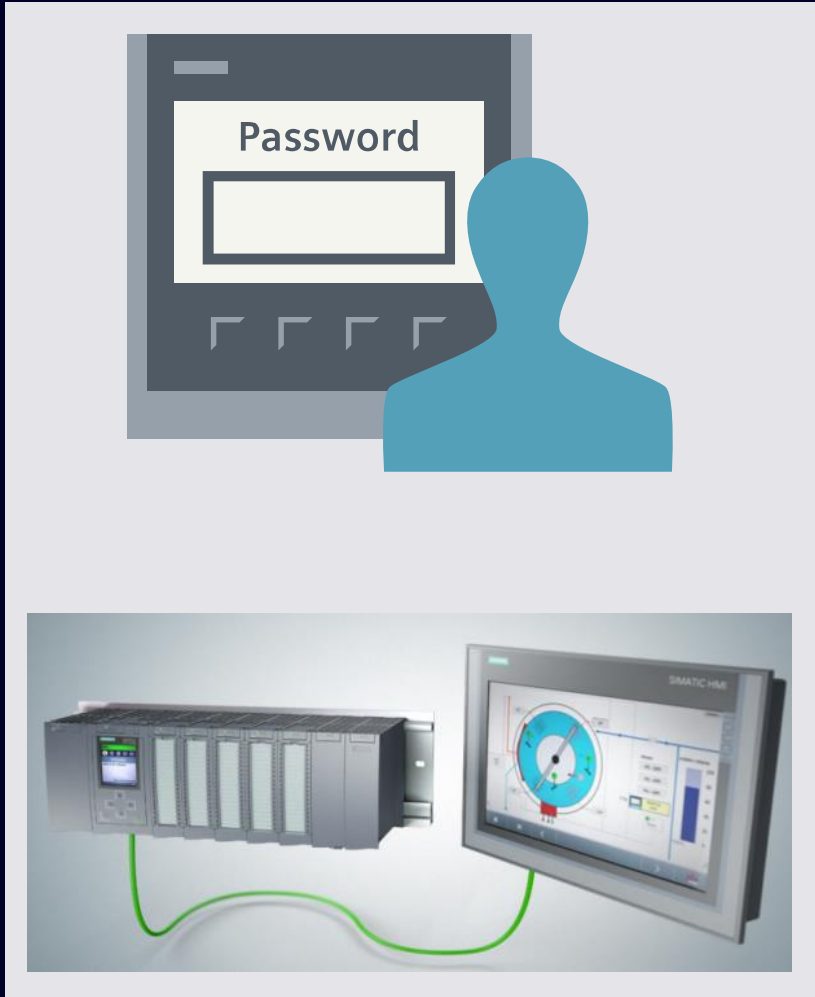
Security measures with SIMATIC S7

- SIMATIC Controllers are one part of an overall defense in depths security concept. The next level of network security protects the local plant network. Siemens Scalance network products offer a broad range of security functions, from VPN to firewalls.
- TIA Portal reminds the engineer to use PLC Security Configuration.
- Controller documentations and guidelines strengthen the customer awareness for the need of security configuration
- The level of security configuration is individual, depending on the required protection level and the overall security concept.
- Following mechanisms are integrated and can be used:
 - 4 level of access protection
 - IP protection and copy protection
- Certified communication robustness
- Manipulation protection of firmware and communication



Industrial Security

Security for HMI Systems



Security Highlights

Panel access protection

Protect device settings of the panels by assigning a password.

User management

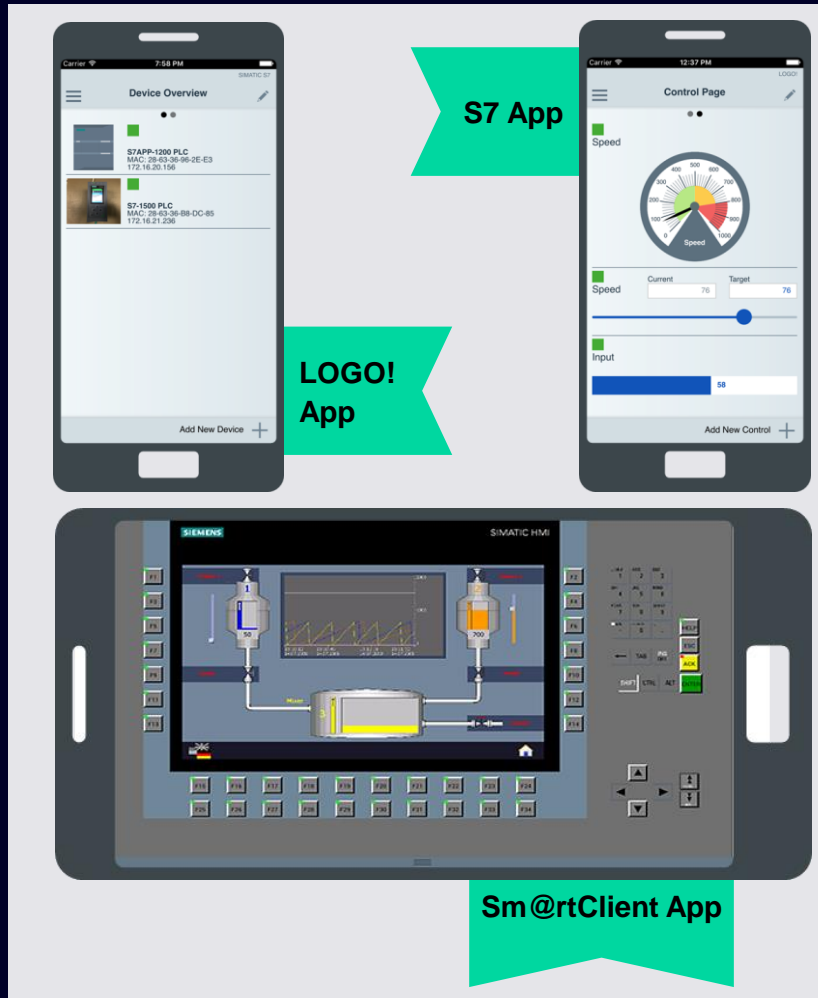
Protect against unauthorized access with permission-based user management

System hardening functions

Increased security with configurable system hardening measures such as locking task switching, Web server authentication

Industrial Security

Simatic Apps



Security Highlights

The SIMATIC Apps provide several security features:

- **Protected communication**
(For Sm@rtClient App: only in full version)
- **Protected profile data**
- **Password needed for startup**
(For Sm@rtClient App: only on iOS)
- **Password needed for connection**

Industrial Security

Protection of IPC Systems



Requirement

Detection and prevention of unauthorized Access and malware

Protection against:

- Manipulation of system / of data
- Malicious or unwanted Software

Solution

Our IPCs support different security functions:

- Boot-/Configuration protection for BIOS/UEFI
- User Management of Operating System (incl. Connection to central Active Directory system)
- EWF (Enhanced Write Filter) Support
- Multiple System Hardening possibilities
→ Guideline available [[Link](#)]
- Disabling of Interfaces
- Locking of Applications
- Support of Antivirus- & Whitelisting Solutions

Industrial Security

Antivirus and whitelisting



Requirement

Detection and prevention of Viruses, Worms and Trojans

Protection against:

- Malicious or unwanted Software
- Manipulation

Solution

Antivirus and whitelisting solutions provide different security functions:

- Protection against Viruses, Worms and Trojans
- Stop unauthorized applications and malware

Industrial Security

Hardening with whitelisting

Example 1

Amongst others, the maintenance of an operating system for a computer, which is important for production, like installing security updates, requires:

- reboot of computer
- and a complete stop of affected part of production during this time period

Example 2

Microsoft Windows XP is end of life since 2014. For Microsoft Windows 7 the support will end in January 2020.

- Due to missing product support even today Windows XP systems are in use. Software update are not possible
- Even after January 2020 many Windows 7 systems will be used in system critical applications

Solution

Carrying out a system hardening on corresponding computers with Whitelisting can increase maintenance cycle.

- As only predefined software can be executed, the demand of installing security updates may be decreased
- In total the amount of stopped production can be decreased

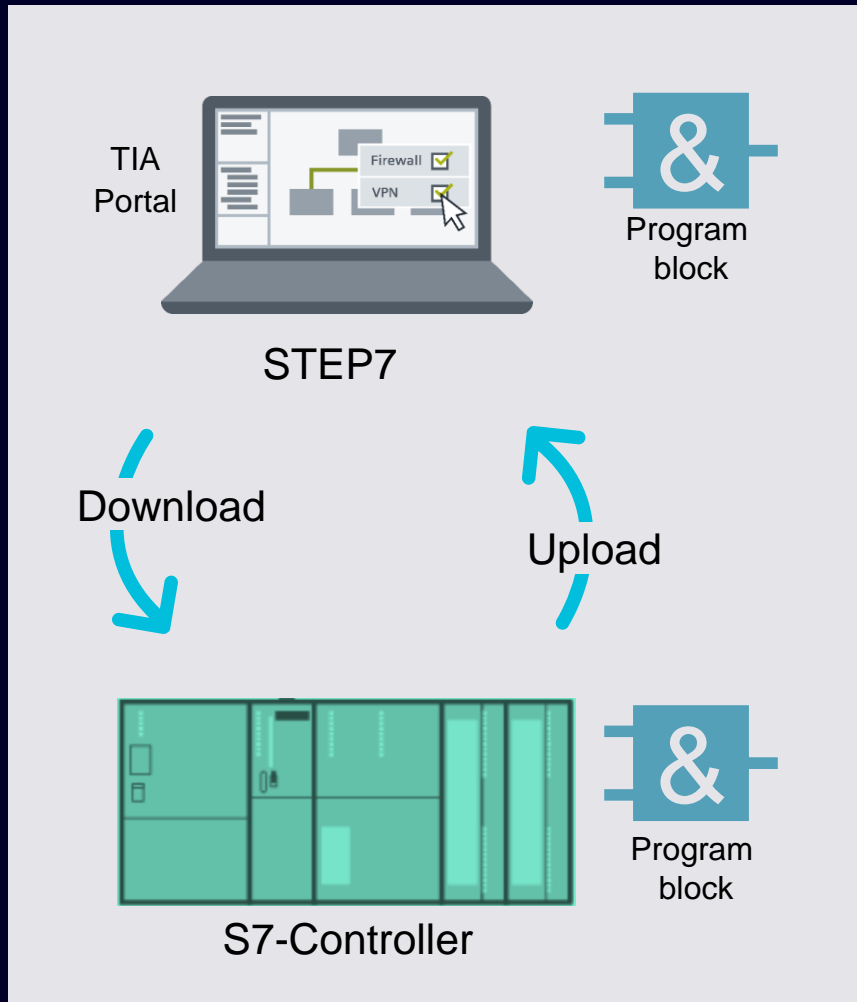
Solution

Carrying out a system hardening on a legacy device with Whitelisting, the time in operation of this device may be increased.

- As only predefined software can be executed, the time until migrating the legacy device to a state-of-the-art device may be increased.
- In total the existing system may be used longer, even if security updates are missing

Industrial Security

SIMATIC S7-300, S7-400 and the TIA Portal



Security Highlights

For **SIMATIC S7-300 and S7-400** the **TIA Portal** provides several security features to protect your investment against unauthorized reading and copying:

Increased Know-how Protection for Programs

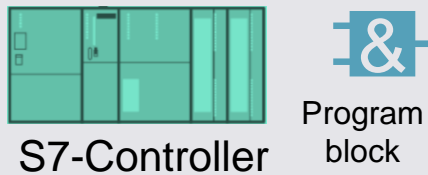
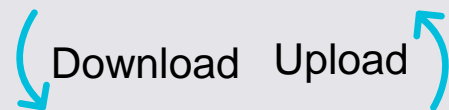
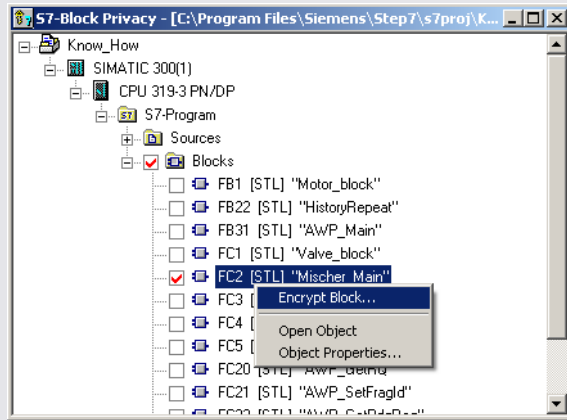
- Prevents reading, content copying and unnoticed changes of program blocks
- Protects program blocks in the engineering project and in the controller
- Program block protection in projects and libraries

Programmable Copy Protection

- Know-how protected programs can be expanded by copy protection
- Comparison with a given serial number of a memory card or CPU

Industrial Security

STEP 7 V5.5 - S7 Block Privacy



Requirement

Know-how and program protection

Protection against:

- Espionage
- Unauthorized access
- Data manipulation

Solution

STEP 7 V5.5 provides several security features:

Increased Know-how Protection

- Protection of program code with password and S7-Block Privacy
- Read and unnoticed changing of block content protection
- Only authenticated user get access to the blocks

Programmable Copy Protection

- Know-how protected programs can be expanded by copy protection
- Comparison with a given serial number of a memory card or CPU

Industrial Security

WinCC V7



Requirement

Secured SCADA environment

Protection against:

- Espionage
- Data manipulation
- System failure

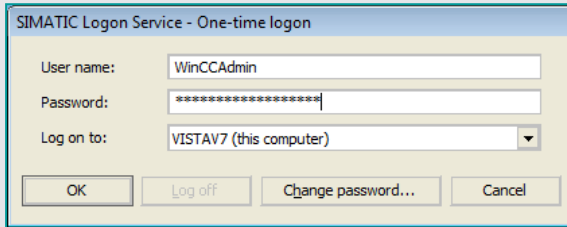
Solution

WinCC V7 offers a broad spectrum of security-promoting features:

- **More secure communication** of the terminal bus via **SSL encryption** and use of **static ports in communication** (Firewalls)
- System tests and result documentation with current virus scanners and patterns
- **WinCC User Administration / SIMATIC Logon**
Only authenticated users obtain access to the system
- **WinCC Runtime**
No access or limited access to the operating system (desktop)
- **WinCC Web Viewer**
Access only to operator screens/no access to Internet pages in order to prevent unintentional download of malware etc.
- **WinCC/WebUX**
Web-based access using an protected connection (HTTPS)
- **WinCC/Audit, WinCC/Change Control**
Logging of operator actions, e.g. with solutions in the FDA environment
- **WinCC/Redundancy**
Higher availability of servers/process connections in the case of an error

Industrial Security

SIMATIC Logon



Requirement

- Central, system-wide user management
- Conforms with the requirements of the Food and Drug Administration (FDA)
- Configuration at runtime (add / lock / remove user accounts)
- High Security through being based on MS Windows
- Supports domain concept and Windows workgroups

User management and authentication for the security of your plant

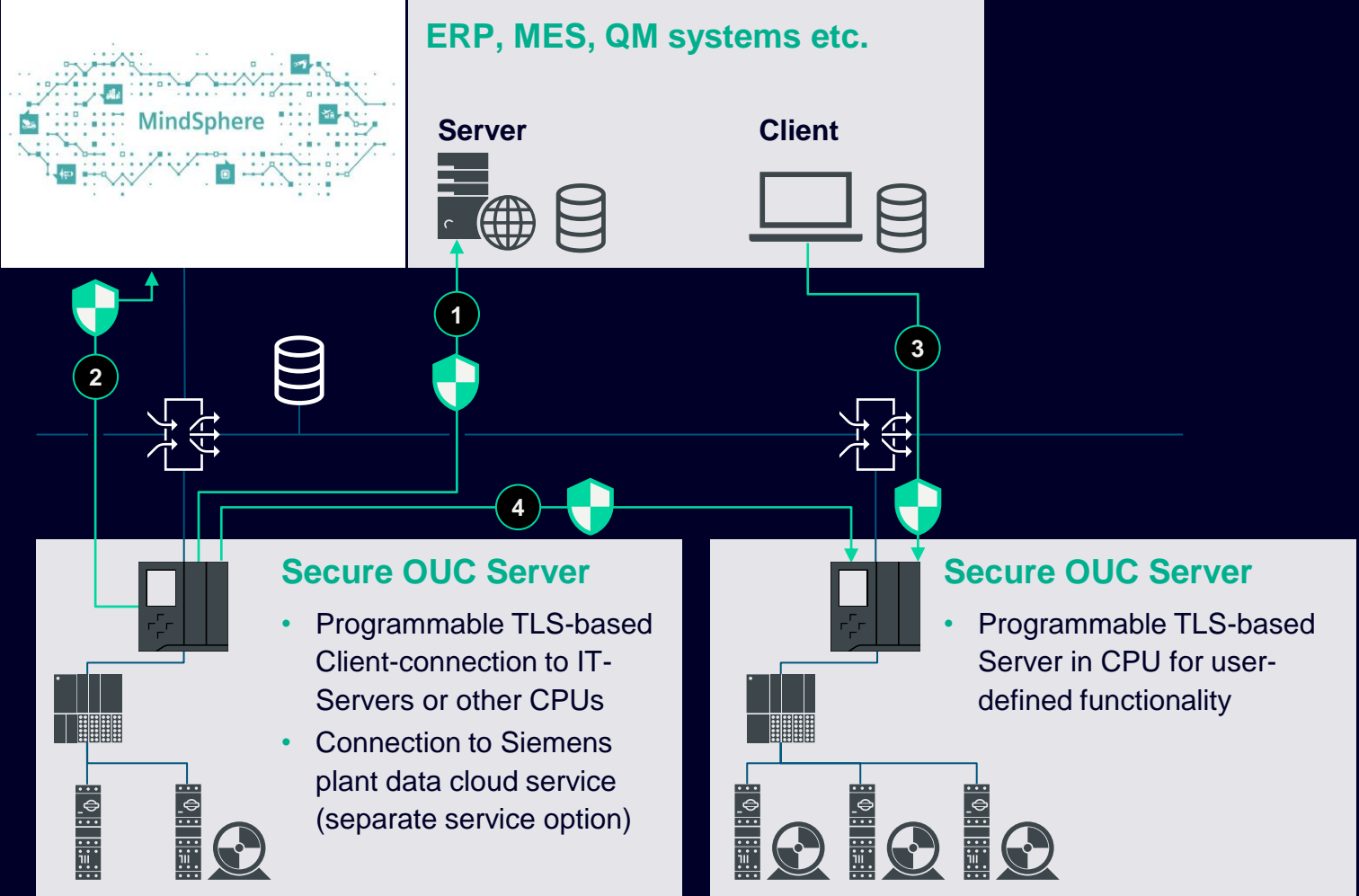
Solution

Secure access control with **SIMATIC Logon**

User Management of WinCC based on SIMATIC Logon with...

- Central administration (incl. password aging, auto logoff after inactivity time or multiple wrong password entries, lock screen)
- Configuration at runtime (add / lock / remove user accounts)
- All WinCC configurations are supported included web
- Supports domain concept and Windows work groups

Secure Open User Communication with the SIMATIC S7-1500 PLC family



Open user communication with system support for SSL/TLS secured communication

- + Allows own HTTPS or FTPS communication (e.g. for production data)

- + Secure Communication (TLS) for own customer defined communication

- + Certificate based authentication of server and client (optionally)

User Management & Access Control

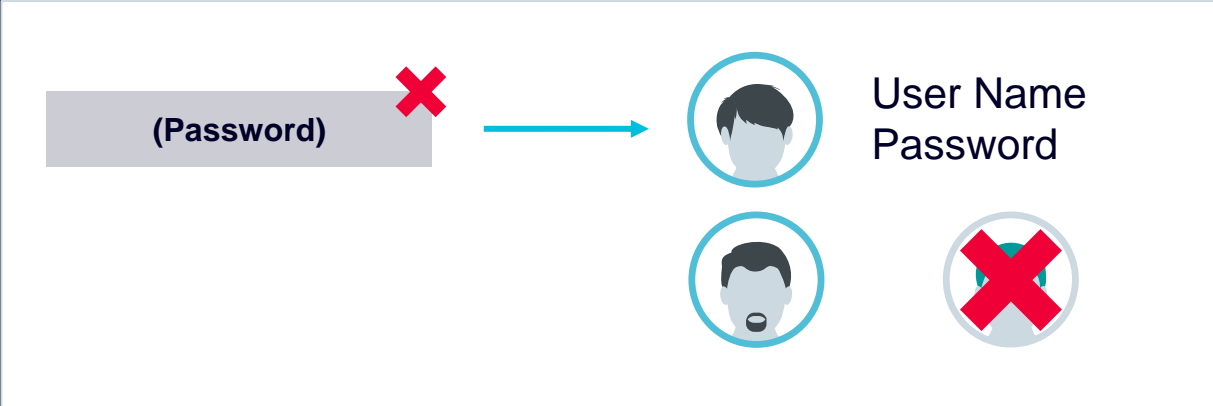


User Management and Access Control UMAC in the TIA Portal

What is it aiming for?

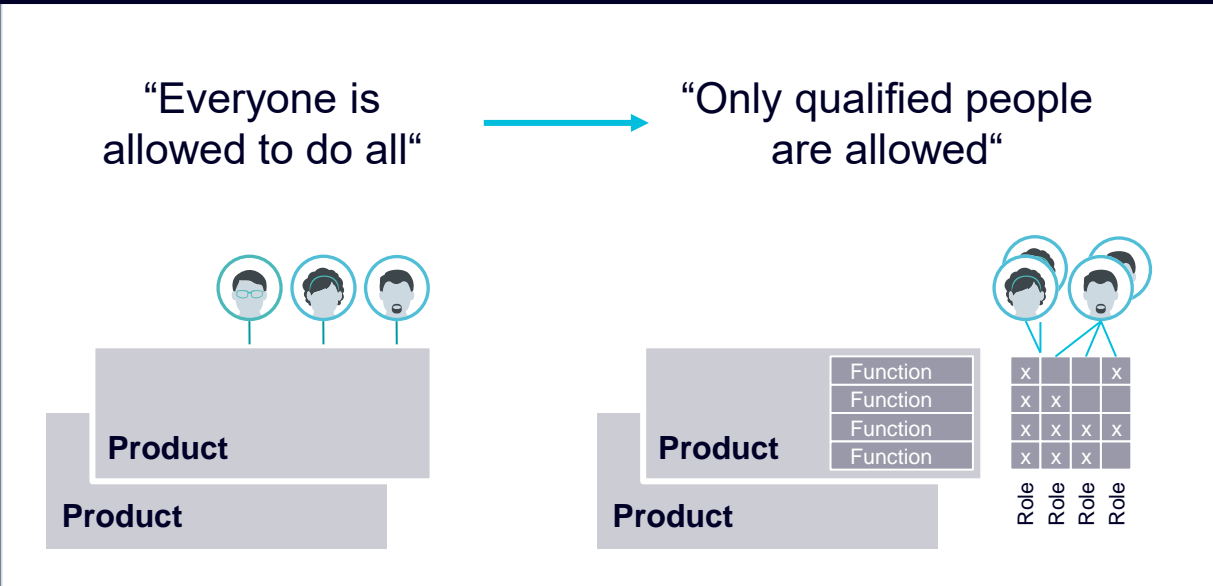
Security: Protection of industrial machines/plants

- Personalized Access instead of Password Access
- Unauthorized Access is prevented



Efficiency: Centralized management

- Of Users in a project or even for multiple projects
- Of Roles summarizing Function Rights of products
- Assignment of Users/Groups to Role/s
- Substitutes product-local solutions



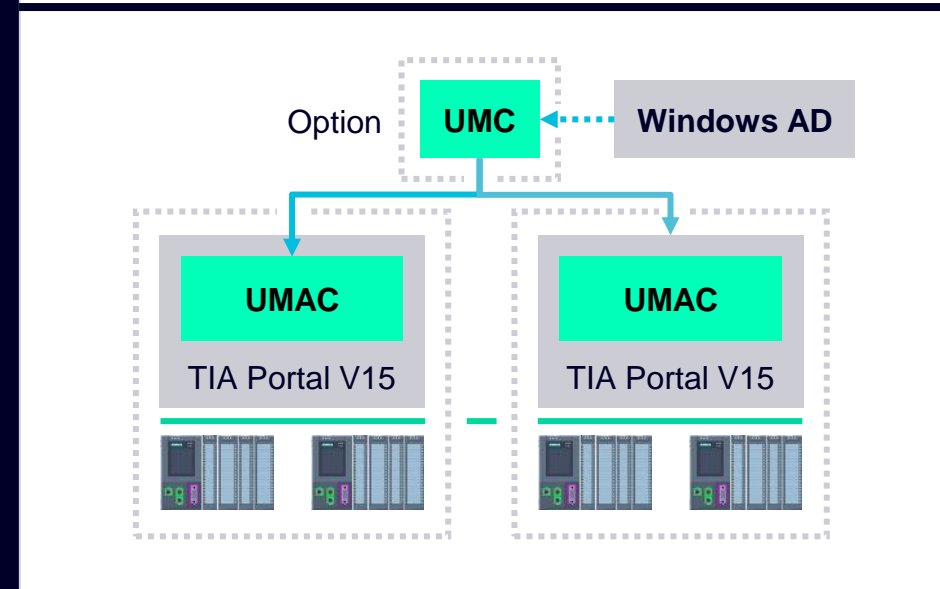
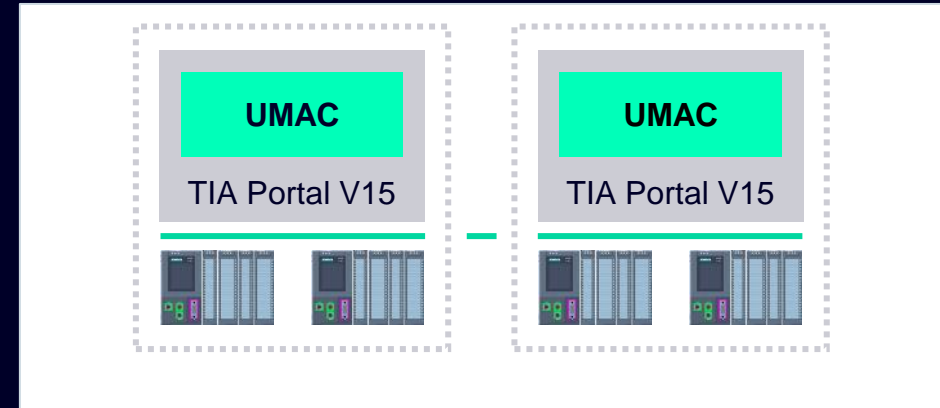
Cooperation of User Management and Access Control UMAC and TIA Portal Option UMC

UMAC: User Management and Access Control

- Built-in functionality in TIA Portal
- Allows personalized access to TIA Portal projects
- Define project users, roles and assign them

UMC: User Management Component

- Extends UMAC by optional use
- Manages users/groups outside TIA Portal projects
- Import of needed UMC users/groups into TIA Portal projects
- Assigning project roles to them
- Authenticates UMC users' logins afterwards



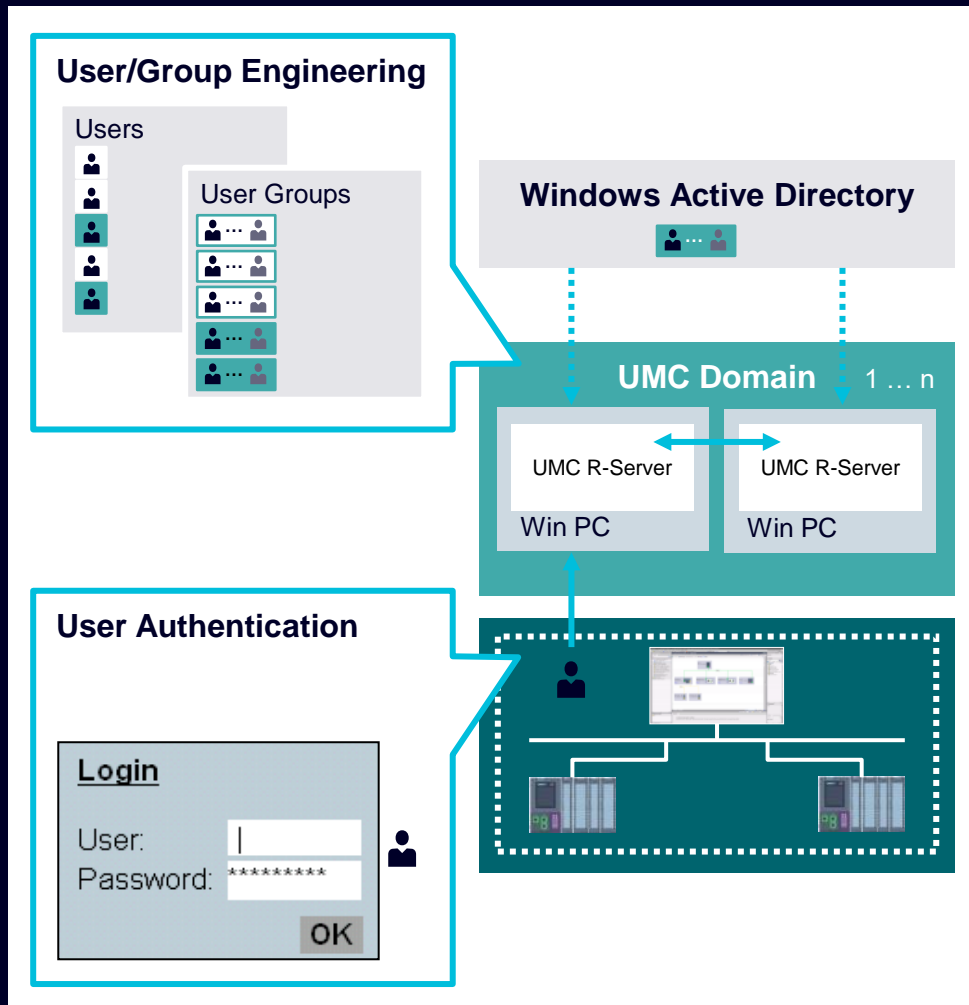
User Management and Access Control UMAC – Classification

User Management and Access Control

- Is an additional TIA Portal >V15 Security Feature
- Is inherent part of each TIA Portal >V15 installation
- Can be used in projects
- Provides personalized access to TIA Projects/Products
- Is an evolutionary extension of the Global Security Setting philosophy, brought in firstly in V12 for network components
- Is a next step in a mid-term development run bringing up more and more access rights from products



TIA Portal Options – System-wide user management UMC



UMC = User Management Component

- Maintenance of users/user groups of a system
- Creation of setup on STEP7/WinCC DVD2
- Project-independent setup with 1... n computers
- Windows users/groups can be imported
- Authentication of login input at runtime

Benefits

- Maintenance of users only once for the system, not multiply across projects or even locally for a product
- UMC users/groups can be imported into projects
- Basis for efficient administration of personalized security in the system
- UMC can be used optionally

User Management & Access Control - UMAC

Features in TIA Portal >V17

Configuration of user-roles

Engineering rights	
Name	Group
<input checked="" type="checkbox"/> Open the project read-only	General
<input checked="" type="checkbox"/> Open and edit the project	General
<input checked="" type="checkbox"/> Monitor PLC program	PLC
<input checked="" type="checkbox"/> Edit online PLC program	PLC
<input checked="" type="checkbox"/> Download to PLC	PLC
<input checked="" type="checkbox"/> Edit PLC program	PLC
<input type="checkbox"/> Modify safety PLC program	CPU
<input type="checkbox"/> Security: Open security devices with write rights	Security
<input type="checkbox"/> Security: Open security devices read-only	Security
<input checked="" type="checkbox"/> Change hardware configuration	General
<input checked="" type="checkbox"/> Maintenance	HMI
<input checked="" type="checkbox"/> Download	HMI
<input type="checkbox"/> Manage users and roles	General
<input type="checkbox"/> Upgrade project	General
<input checked="" type="checkbox"/> Modify project via Openness API	General
<input checked="" type="checkbox"/> Projekttexte importieren	General
<input type="checkbox"/> Download to other devices	General
<input checked="" type="checkbox"/> Change library type versions	General

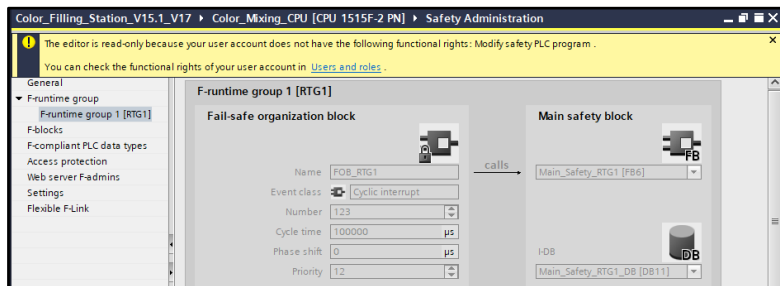
Restricts actions and changes in editors

New Engineering Function Rights

- Following User actions can be restricted by the new function rights:
 - **General Function Rights:** Modify Library type, Change Hardware configuration, Import Project text, Upgrade project
 - **PLC:** Download, Change Program, Modify Safety PLC program, Monitor, Edit online PLC program
 - **HMI:** Download, Configure, Maintenance
 - **Drives:** Modify Drive configuration
 - **Runtime Rights:** Rights for network components

Benefits

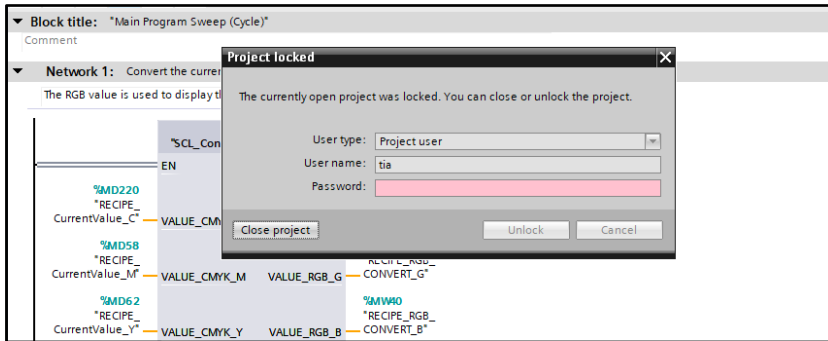
- The previous access protection distinguished between read-only and read/write access.
- With the new function rights user roles can be configured according to the required responsibilities.
- This allows to protect actions and workflows within the engineering against unauthorized access



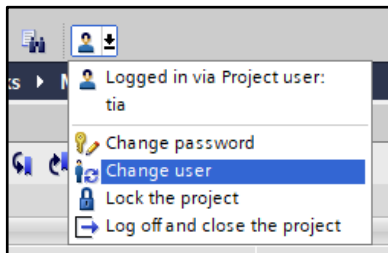
User Management & Access Control - UMAC

Features in TIA Portal >V17

**You leave the station –
project gets locked!**



**You need elevated rights
to change the user!**



Project Lock and Change User

Project Lock:

- An open project can be protected against editing via project lock
- The project lock can be activated manually or automatically after a configurable time of inactivity

Change User:

- Menu entry to change the active user within an opened project

Benefits

- In case of temporal leaving of the engineering station, the project lock prevents the need of project closing
- With the “Change User” functionality, it is possible to continue working at the same project state right before the user change

User Management & Access Control - UMAC

Features in TIA Portal >V17

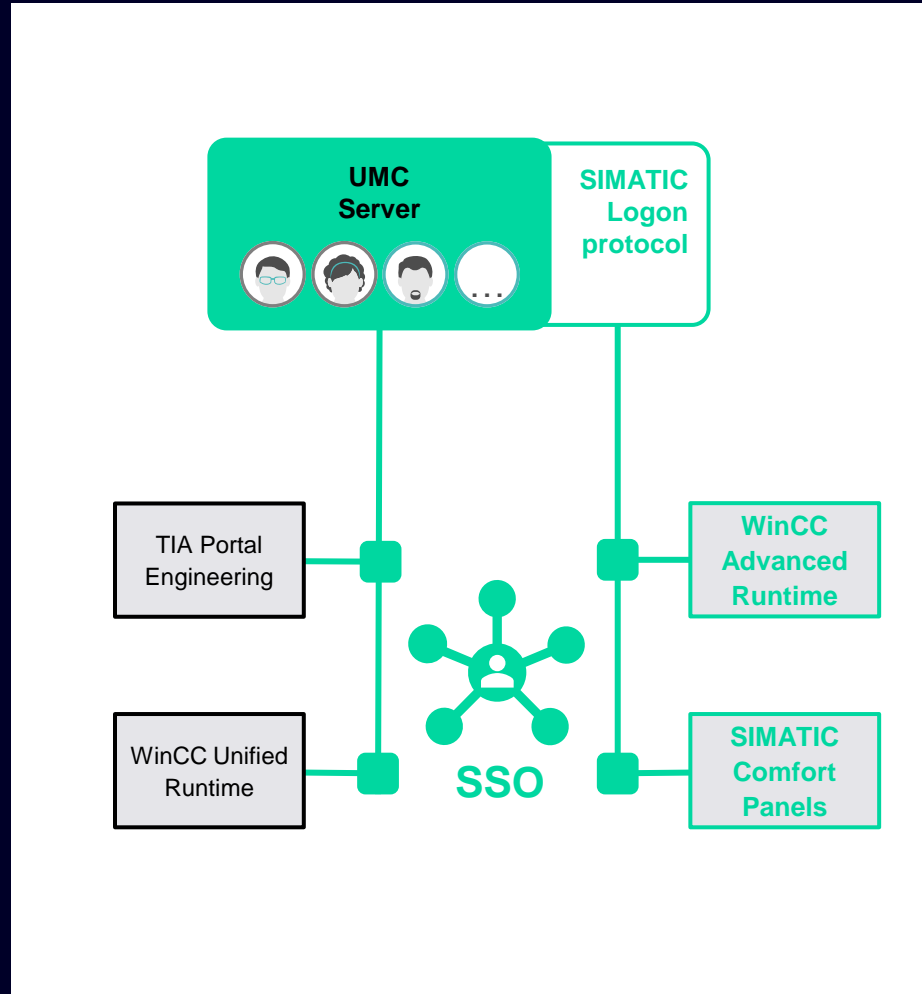
Single Sign-on and SIMATIC Logon Support

Single Sign-on (SSO)

- TIA Portal and HMI Runtimes support Single Sign-on connection (at the same PG)

SIMATIC Logon Protocol

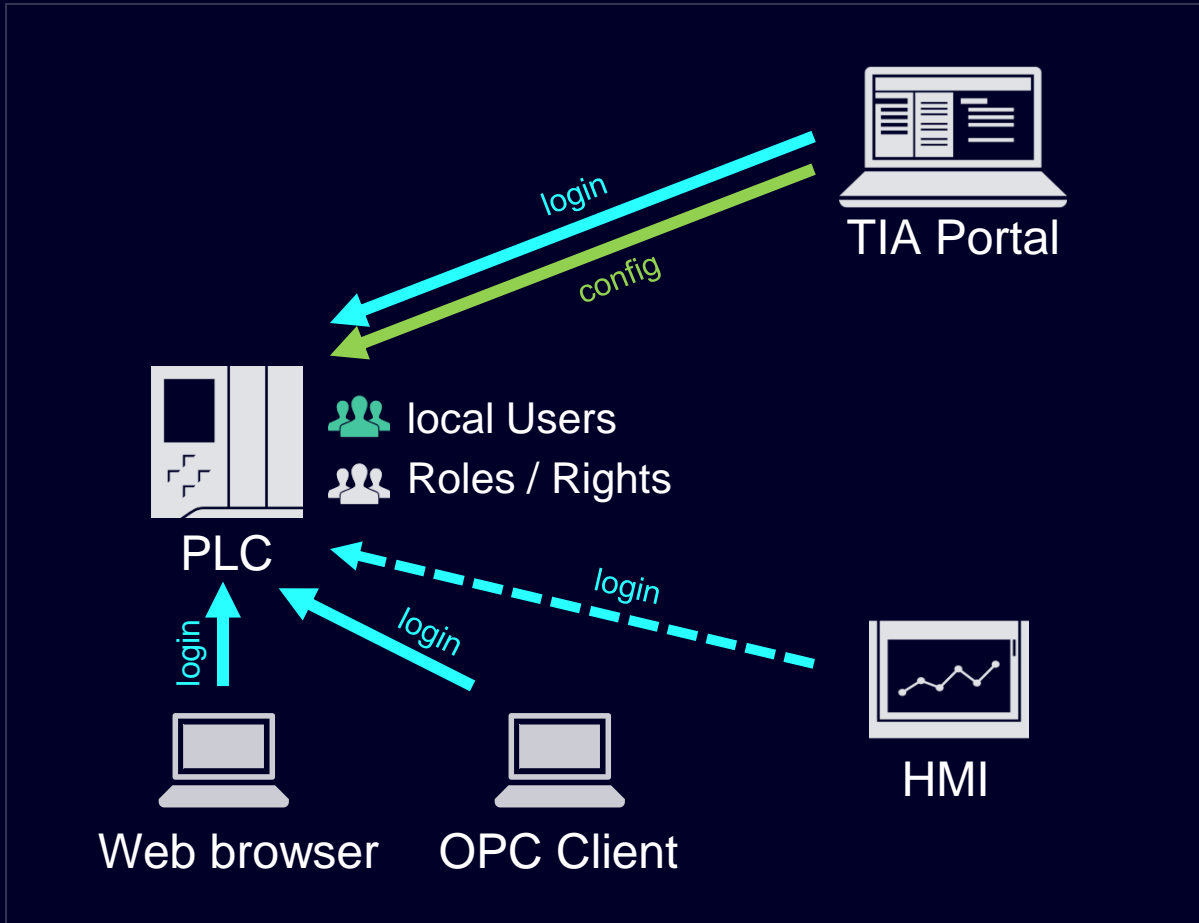
- UMC server supports the SIMATIC Logon Protocol
- This supports a central user management for WinCC Runtime Advanced and Control via UMC



Benefits

- Single Sign-on allows seamless authentication between a protected TIA Portal project and an HMI Runtime on the same engineering station
- SIMATIC Logon Protocol allows the usage of existing HMI Runtime systems within a UMC domain

Unified user and rights management for S7-1500 PLCs and Software Controller



Flexible access control for multiple users, based on individual rights with unified user management in S7-1200/1500 PLCs and Software Controller

- Unique user accounts with individual access rights for suitable access configuration according to users tasks
- Single user account usable for different PLC services (e.g. engineering access, Webserver)
- Roles / Rights concept for different PLC functionality integrated into existing TIA Portal UMAC configuration
- Support of user changes on PLC during runtime

Access Control with RFID Systems



Card reader: Access control with SIMATIC RF1040R



SIMATIC RF1040R

Feature / function

Access control to machines or plant components

Security functionalities:

- Identification of operating personnel
- Tracking of critical activities
- Avoidance of operating errors

Integration options into WinCC, SIMATIC Logon, PM Logon, PCS 7 via USB 2.0 interface

Serial interface **RS 232**

Supported standards:

- ISO 14443 A/B (MIFARE) / ISO 15693, LEGIC Advant, etc.
- HITAG1/2, Cotag, EM4xxx, etc.

Suitable for industrial applications:

- IP65 (front)
- -25 to +55 ° C

Benefit

Flexible authorization levels, e.g. for machine access for each employee by using employee ID cards

Protection of critical components against:

- unauthorized network and device access

Easy integration in existing hardware (HMI devices and panels)

Direct connection to RS232 PTP modules (SIMATIC S7-1200 CM, S7-1500 CM and ET200 SP), SIMATIC RF1xxC/CI, PCs and 3rd party HMI.

The use of existing employee ID cards permits **individual control** of access rights

Card reader: Access control with SIMATIC RF1060R



SIMATIC RF1060R

Feature / function

Access control to machines or plant components

Security functionalities:

- Identification of operating personnel
- Tracking of critical activities
- Avoidance of operating errors

Integration options into WinCC, SIMATIC Logon, PM Logon, PCS 7 via USB interface

Supported standards:

- ISO 14443 A/B (MIFARE) / ISO 15693, LEGIC Advant, etc.

Suitable for industrial applications:

- IP65 (front)
- -25 to +55 ° C (-13 to 131 ° F)
- ATEX II admission

Benefit

Flexible authorization levels, e.g. for machine access for each employee by using employee ID cards

Protection of critical components against:

- unauthorized network and device access

Easy integration in existing hardware (HMI devices and panels)

The use of existing employee ID cards permits **individual control** of access rights

Card reader: Access control with SIMATIC RF1070R



Feature / function

Access control to machines or plant components

Security functionalities:

- Identification of operating personnel
- Tracking of critical activities
- Avoidance of operating errors

Integration options into WinCC, SIMATIC Logon, PM Logon, PCS 7 via USB 2.0 interface

Serial interface **RS 232**

Supported standards:

- ISO 14443 A/B (MIFARE) / ISO 15693
- LEGIC Prime and LEGIC Advant, etc.

Suitable for industrial applications:

- IP65 (front)
- -25 bis +55 ° C (-13 to 131° F)
- ATEX II admission

Benefit

Flexible authorization levels, e.g. for machine access for each employee by using employee ID cards

Protection of critical components against:

- unauthorized network and device access

Easy integration in existing hardware (HMI devices and panels)

Direct connection to RS232 PTP modules (SIMATIC S7-1200 CM, S7-1500 CM and ET200 SP), SIMATIC RF1xxC/CI, PCs and 3rd party HMI.

The use of existing employee ID cards permits **individual control** of access rights

Use Case access control

Machine access with RFID based identification systems

Task

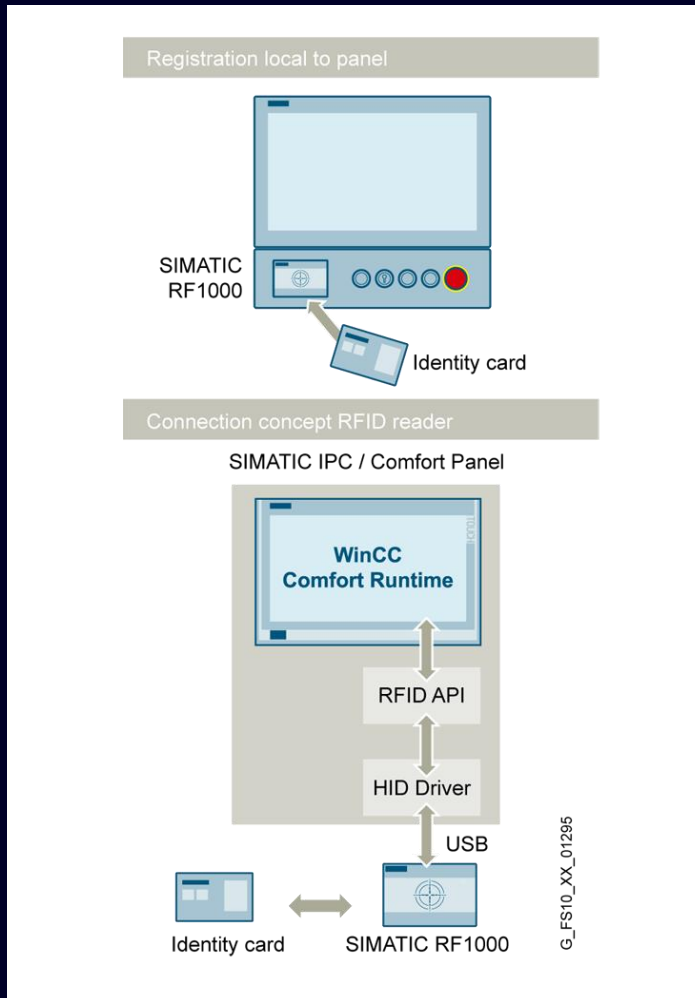
Explicit identification of operating staff at machines and plants, including:

- Access control
- Audit trail

Solution

The access control reader **SIMATIC RF1000R** supports one-time and permanent login with RFID card as well as login with RFID card including user credentials:

- Login with RFID card (one-time)
- Login with RFID card (permanent)
- Login with user name, password and RFID card



Security for Motion Control



Industrial Security

SINUMERIK 840D sl – secure innovative CNC system platform



Requirement

Protection of intellectual property, detection of viruses, secure access and network protection for a high system availability.

Protection against:

- Espionage
- Unauthorized access
- External attacks
- Manipulation

The SINUMERIK 840D sl is a distributed, scalable, open and interconnectable system offering a wide range of functions. It is ideally suited for applications using the most diverse technologies.

Solution

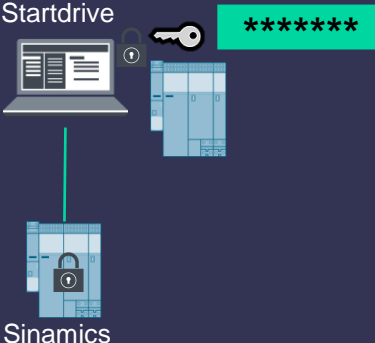
SINUMERIK 840D sl provides several security functions:

- Know-how protection for NCK/HMI Open Architecture and PLC-Program
- CNC Cycle protection
- Role based User authentication
- Anti-Virus scanner support*
- Windows Security patch compatibility*
- Packet Firewall and Interface robustness check

Siemens is your reliable partner to drive secure digitalization

Protecting intellectual property

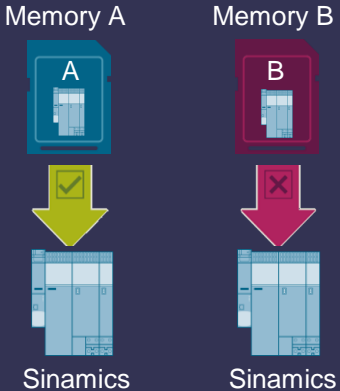
- Encryption of offline project by user management
- Encryption of converter parameterization by Know How protection function



Copy protection

Protection against unauthorized duplication of the converter configuration software

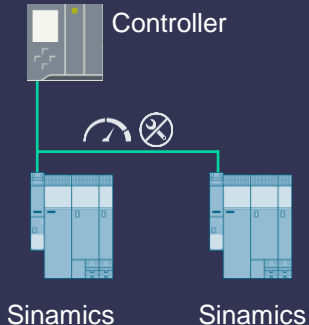
- Linking the converter configuration to hardware serial numbers (memory card and/or Control Unit)



Ruggedness

Protection against malfunction when the network is attacked

- The converter goes into a safe/secure state
- Automatically returns after the attack
- Certified according to PROFINET Netload Class II



Communication integrity

Identifying manipulated communication data

- Encrypted data transfer between the converter and web browser (https)



Industrial Security

SINAMICS know how protection

What?

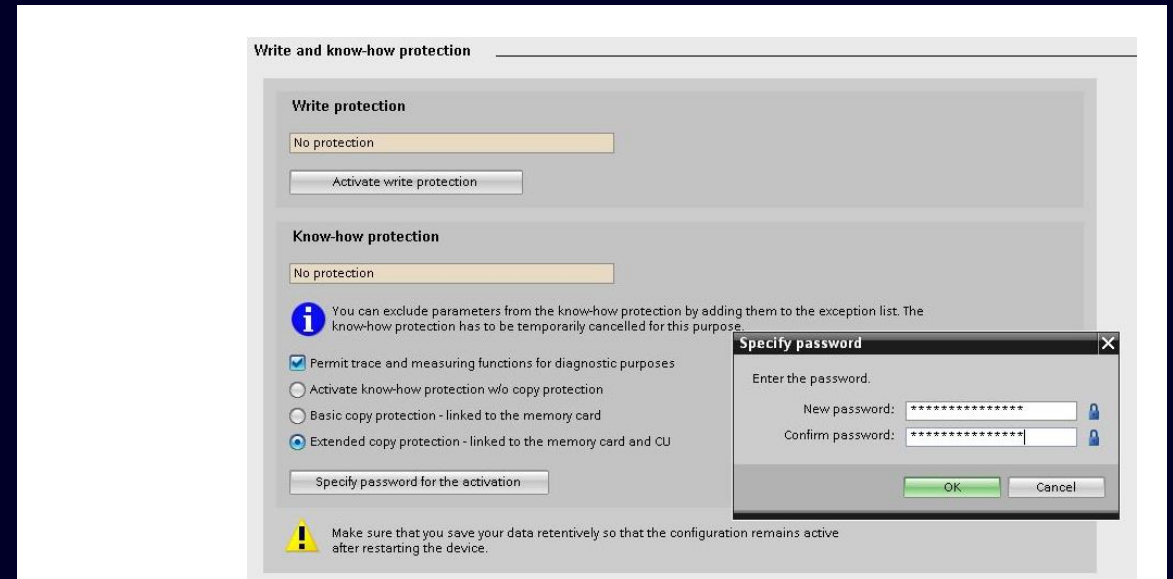
The Know How protection suites to securely **protect** the invested **knowledge** of the machine manufacturer into the SINAMICS project.

How?

- The Know How protection can only be activated at the SINAMICS inverter itself.
- When activated all the parameters, which contain machine builder's Know How, will be hidden.
- The project is safely locked with a **key** (the password).
- Without knowledge of the key the project can only be handled as a „black box“.
- In combination with the **copy protection** the “black box” can only be used within a fixed, predefined **hardware**
- This avoids as well 1:1 clones of the “black box”.



Know How protection functionality protects the drive parameterization from external changes, from theft of intellectual property and makes copying impossible.



Options:

- Exclusively confidentiality protection of parameterization
- **Optional:** additional copy protection – parameterization is coupled fixed to the hardware (Memory Card and/or Control Unit)

Industrial Security

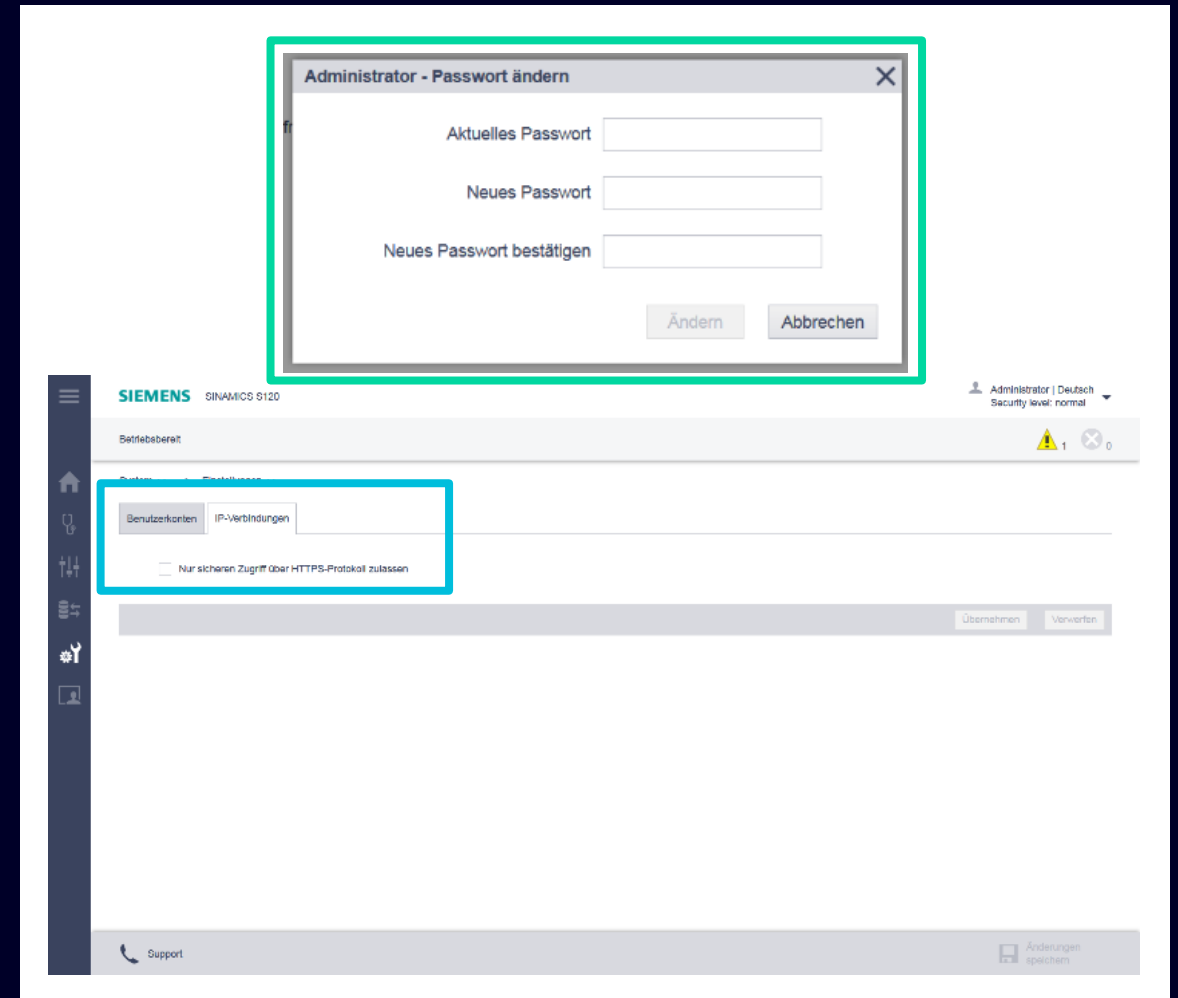
SINAMICS Integrated webserver (S200/ S210/ S120/ G220)

What?

The **integrated** SINAMICS web server enables comfortable access to the inverter for diagnostic purposes, for example, even without an engineering tool.

How?

- For secure **authentication**, the web server provides different **users** with different **access rights** and **passwords**
- **IP connection:**
The web server offers the possibility to make the access possible only by **HTTPS** or also by HTTP.



The protected communication (HTTPS) of the webserver increases security.

Industrial Security

SINAMICS webserver via Smart Access Module (V20 / G120)

What?

The Smart Access Module provides **wireless** access to the inverter. The web server is optimized for mobile devices with a **graphically intuitive interface**. The inverter can thus be comfortably commissioned, parameterised and diagnosed.

How?

- IP connection:
- The connection is established here **uniquely** only directly **point-to-point**.
- The **protected** communication is realized according to **WAP-2** standard



An unwanted parallel access to the encrypted communication between mobile device and inverter is impossible due to the unique point-to-point connection.



Security Integrated: The first steps to make machines more secure against external attacks with the next generation of drives



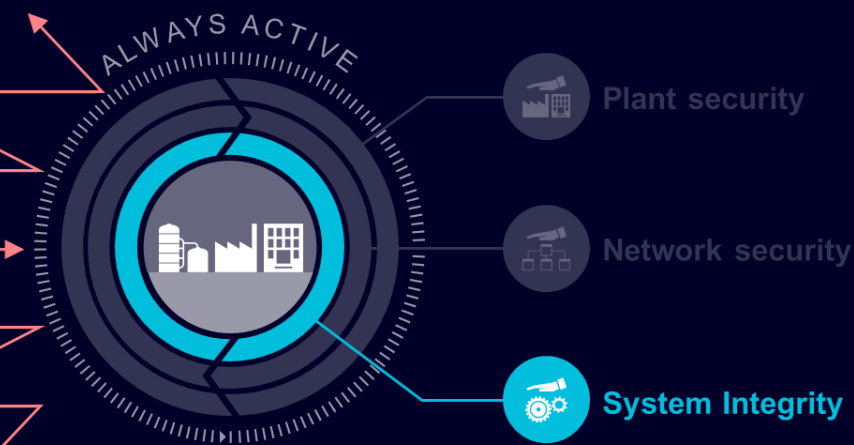
SINAMICS drives support you to make your machine more secure against attacks from the outside!

- **User Management & Access Control (UMAC)**
→ Protects your drive from unauthorized access
- **Secure default settings**
Only necessary functions are enabled and pre-configured with secure settings
- **Secure communication** between drive and TIA Portal / web client
- **Integrity and authenticity check** to prevent the installation of manipulated firmware
- **Drive Data encryption** Encrypts sensitive data in the backup file and on the memory card of the inverter. Sensitive data are UMAC data, e.g. user names and passwords

SINAMICS G220, S200, S210, ...



Defense in Depth Concept



Our products are developed according to a secured development lifecycle process independently certified by TÜV SÜD based on the IEC 62443-4-1 standard.

Our customers are actively informed about known security vulnerabilities and can take countermeasures before attackers exploit these gaps. Remedial actions and / or fixes are provided.

Please find here further information about Cybersecurity for Industry and SINAMICS

Video Tutorials



- [Part 1: General Information](#)
- [Part 2: Security Wizard](#)
- [Part 3: Create custom. User](#)
- [Part 4: Login lost](#)

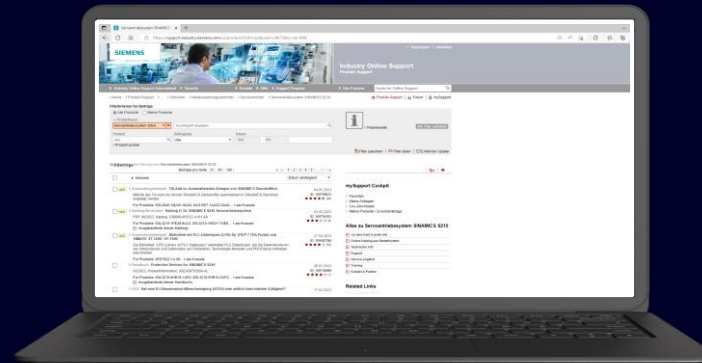
Part 1. General information on cybersecurity in drive technology:
EN: <https://www.youtube.com/watch?v=z8P0K1cKdyY>

Part 2 User Management & Access Control:
EN: <https://www.youtube.com/watch?v=S9GhGug-cZs>

Part 3 Creating a customised user
EN: <https://www.youtube.com/watch?v=bXNaXqKYUzo>

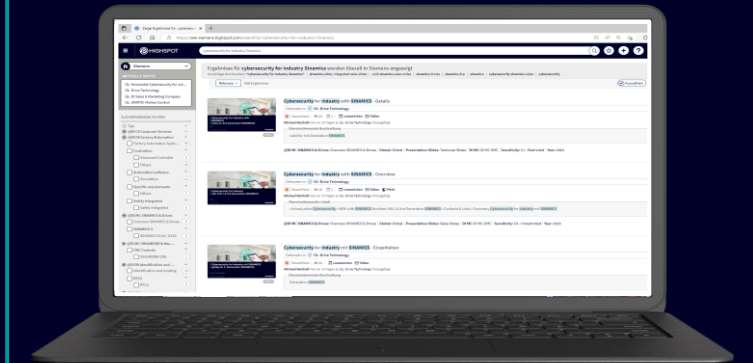
Part 4 Username and Password lost
EN: https://www.youtube.com/watch?v=UDnQtGpLI_s

Documentation



- [SINAMICS Engineering Manual](#)
- Security Application Example
[Entry ID: 109820695](#)
- FAQ: Login lost, how to reset the Drive

Links to further Information



- Sinamics slides
 - [Technical Slides](#)
 - [Sales Slides](#)
 - [Security for beginners](#)
- Horizontal Cybersecurity slides
 - [Horizontal Cyberse. for industry](#)
- Internet: [Industrial Security](#)
- [Customer support](#)

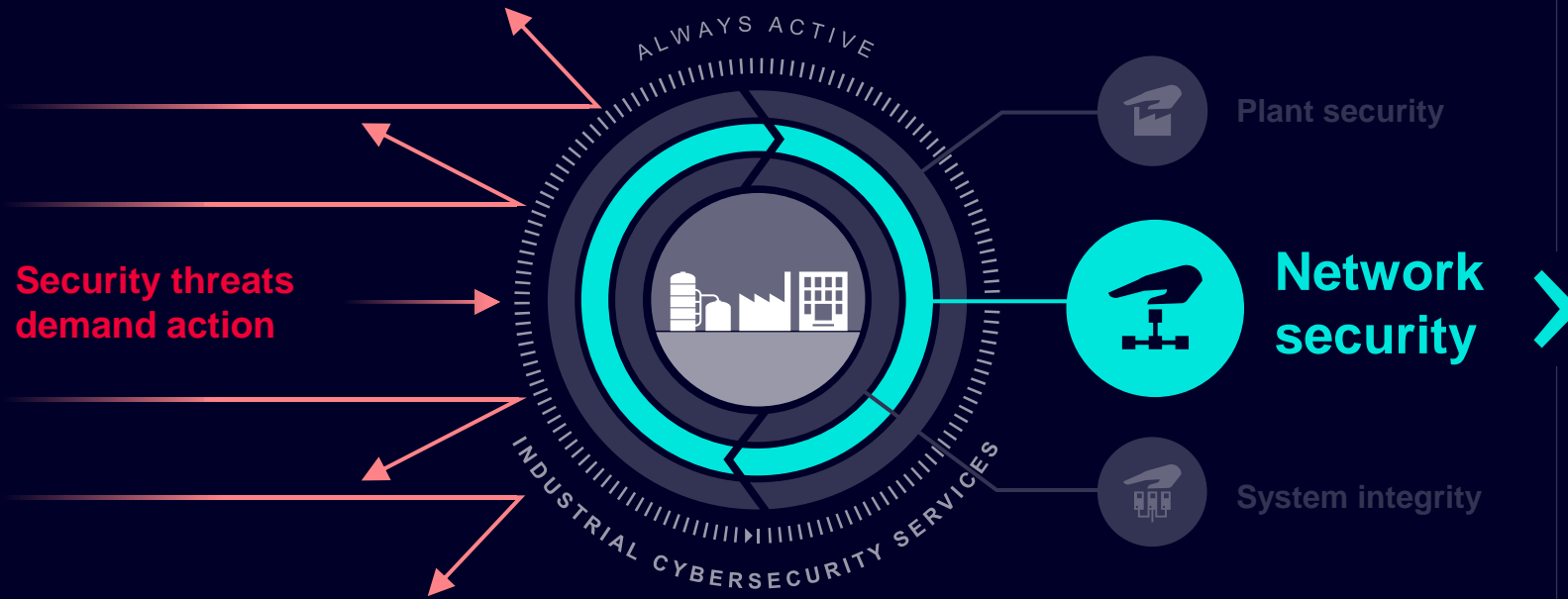
Network Security



Network Security

Combining Zero Trust and perimeter protection principles

Defense in depth remains state-of-the-art, ...



... but classical cell protection ...



... will be enriched by zero trust principles



Overview: Network Security

Adapted measures for production:

Network access control

- Secure interface to IT networks
- Secure architecture with DMZ
- Secure remote access via Internet
- Secure local network access (port security) via device and user authentication
- Secure cloud connection

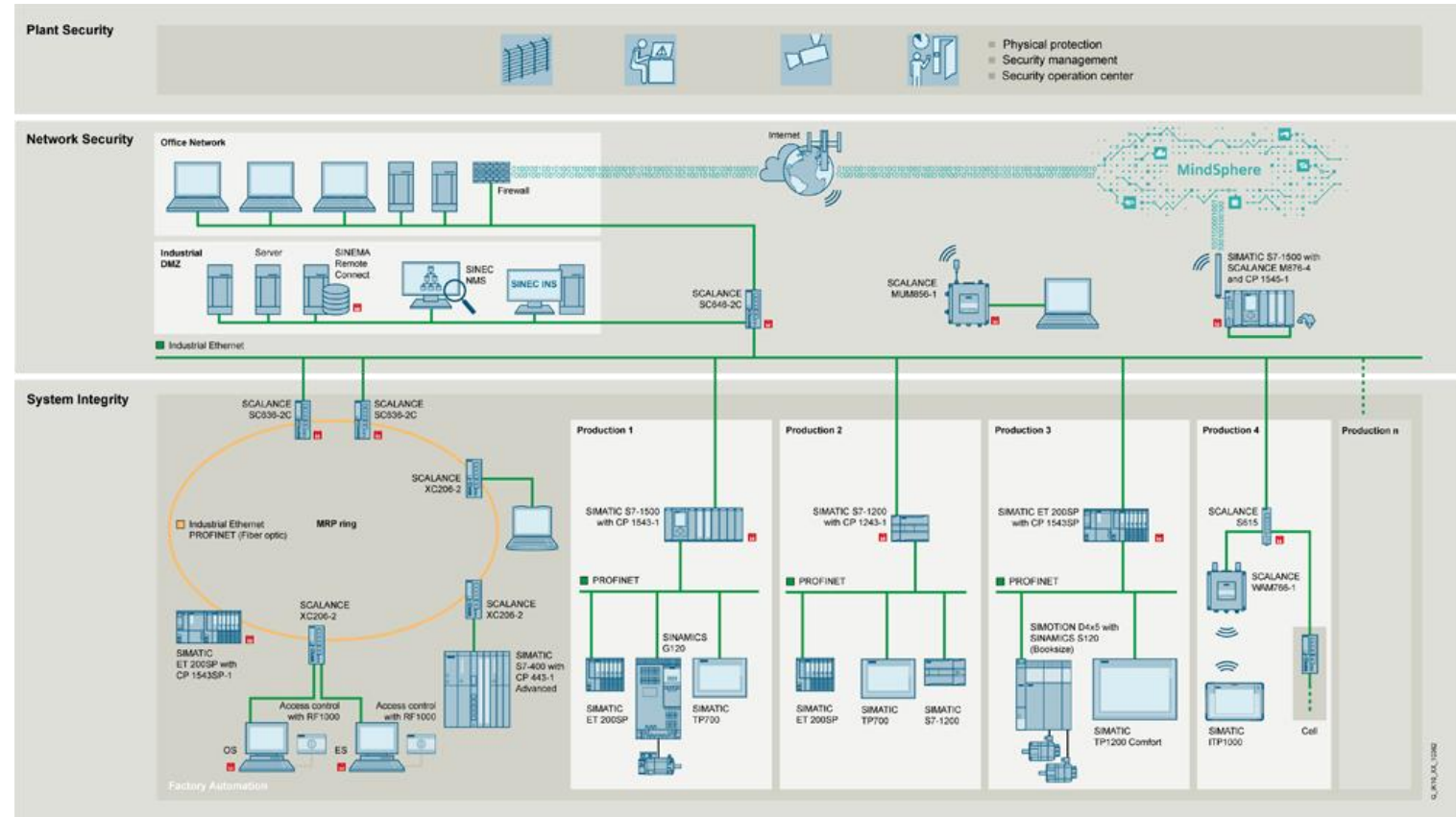
Redundancy

- Protection of redundant network topologies

Cell protection

- Risk mitigation by means of network segmentation
- Extension of cell protection concept by means of:
 - Security communication processors
 - Flexible VLAN configuration

For information on cybersecurity solutions with RUGGEDCOM, visit www.siemens.com/ruggedcom/cybersecurity



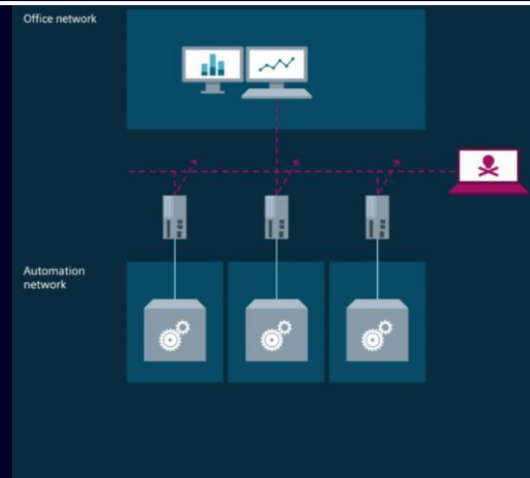
 Products with firewall or VPN functionality

Network Security use cases

Cell protection

Devices without own network security functionality can be protected within an automation cell.

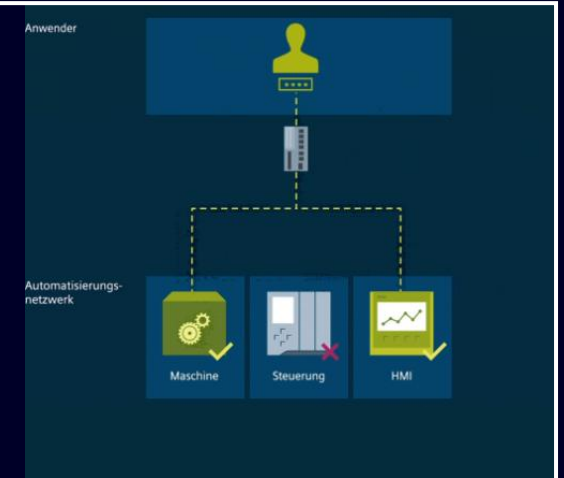
- Industrial Security Appliances SCALANCE S for redundant connections of ring topologies.



Dynamic firewall

Access to network areas and terminals is limited depending on people and roles.

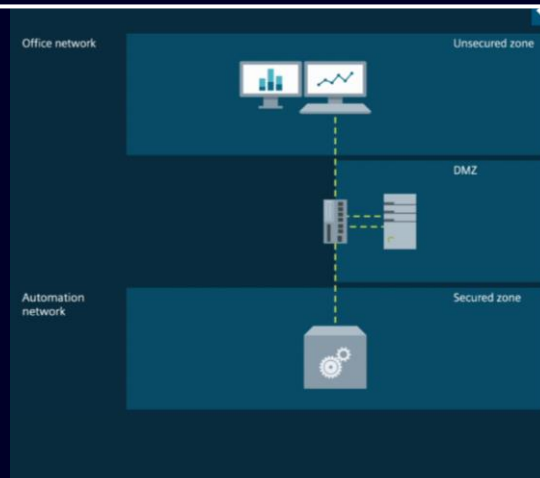
- User-specific firewall rules are temporarily applied with the SCALANCE S industrial security appliances.



Demilitarized zone (DMZ¹⁾)

Increased protection by means of data exchange via DMZ by avoiding direct access to the automation network.

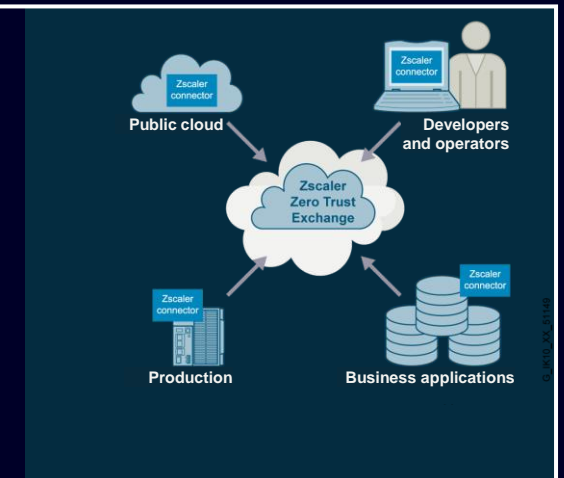
- A firewall controls all data traffic between the different networks and DMZ¹⁾.



Demand-based access to OT networks

More secure and demand-based access to OT applications with zero trust principles.

- Users must be identified and authorized before they gain access to production network systems.



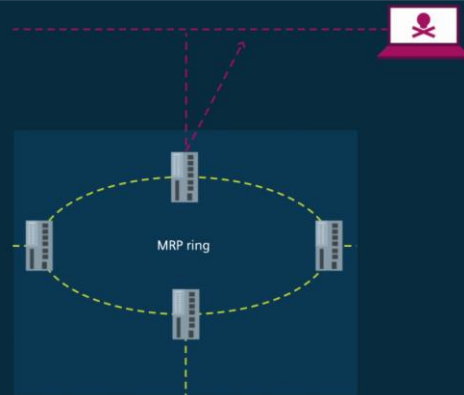
1) Demilitarized zone

Network Security use cases

Redundancy

Increased reliability and availability of segmented networks by means of redundant connections.

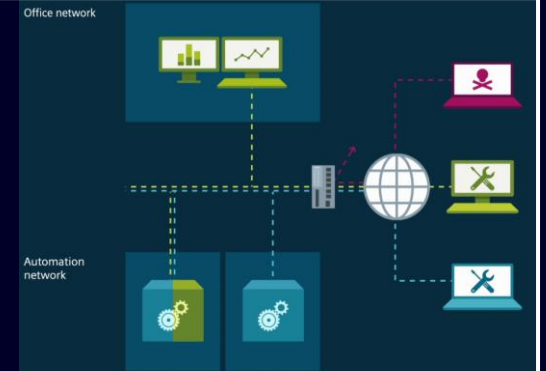
- Industrial Security Appliances SCALANCE S for redundant connections of ring topologies.



Remote access

Secured remote access via the Internet or mobile networks to avoid espionage and sabotage

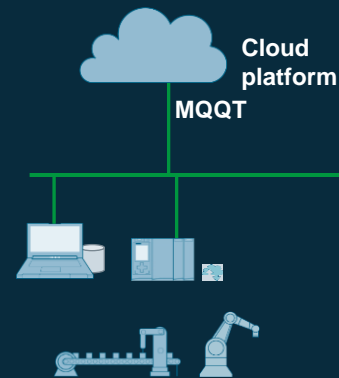
- Encryption of data communication and access control to dedicated end devices.



Secure cloud connection

From the sensor to the cloud: easy and secure connection to cloud platforms

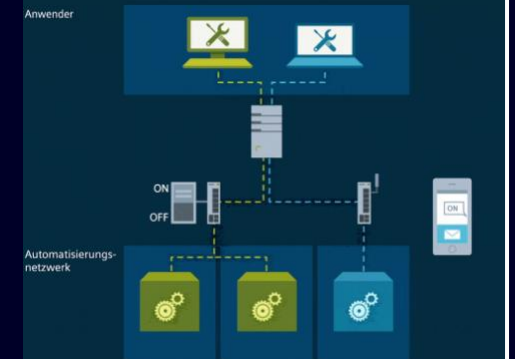
- Secure security concepts with CloudConnect for new and existing plants



Remote access management

Easy and secure remote access for teleservice and remote maintenance

- Secured VPN tunnel connection can be activated with SINEMA Remote Connect via digital input or SMS.

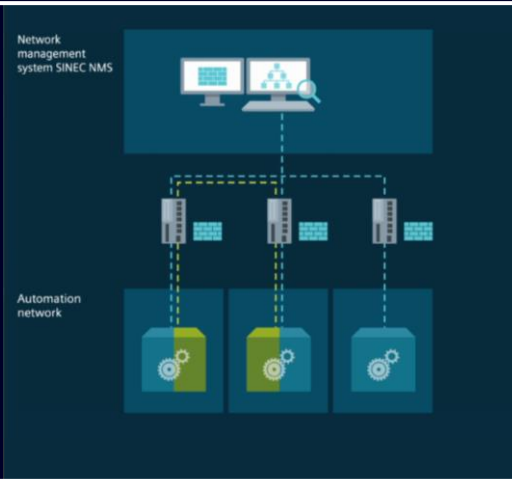


Network Security use cases

Central firewall management

Central configuration and management of the rule sets of decentralized cell firewalls.

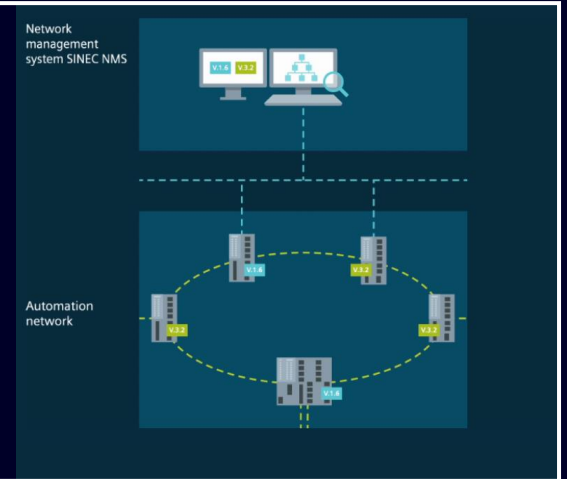
- Graphical and rule-based configuration of all permitted communication relationships at zone transitions



Central firmware updates

Simultaneous distribution of up-to-date firmware independently of devices

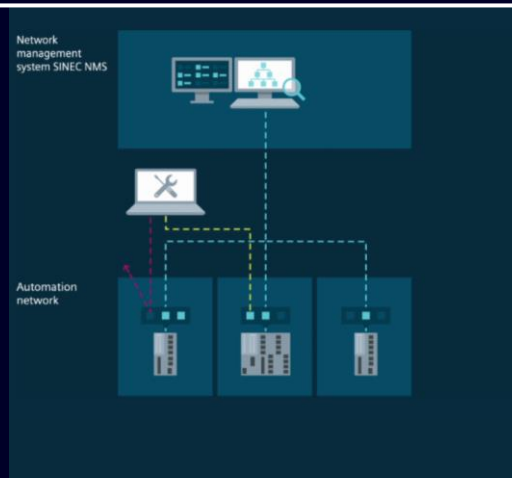
- Elimination of software vulnerabilities through regular firmware update



Device hardening

Rule-based device hardening by disabling unneeded services and ports

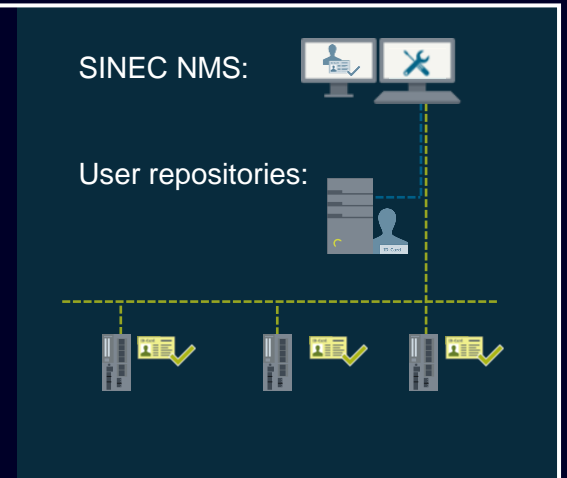
- Reducing the attack surface of monitored network components



Central user administration

Controlled and traceable device access with centralized user administration.

- Integration of existing user databases, such as Active Directory and UMC



Network Security

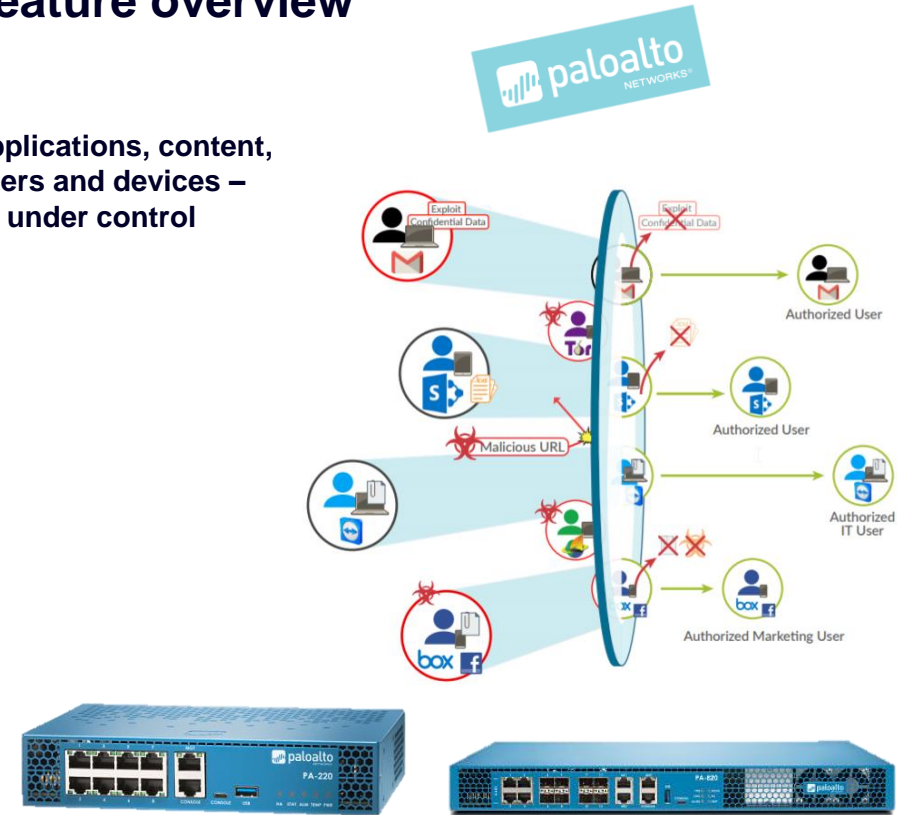
Perimeter protection with Industrial Next Generation Firewall

Our solution

- Based on **Palo Alto Networks Next-Generation Firewall Appliances**
- Palo Alto Networks is a “Gartner Magic Quadrant Leader” for Enterprise Network Firewalls for the 10th consecutive year
- Application layer and stateful inspection firewall
- IPSec VPN gateway
- Threat Prevention (additional subscription required)
- Advanced Malware Protection (additional WildFire subscription required)
- Prevents against known and unknown threats
- High availability (active/active and active/passive) modes
- Redundant power input for increased reliability (PA-220 and PA-850) and fan-less design (for PA-220 model)

Feature overview

Applications, content, users and devices – all under control



Components for Network Security



Network Security

Industrial Security Appliances – SCALANCE S



SC622-2C / SC632-2C

SC636-2C

S615

SC642-2C

SC646-2C

Network Security

Protection of industrial networks with SCALANCE SC-600



SCALANCE SC646-2C

Feature / function

Configuration of **flexible security zones**:

- 2 or 6 electrical ports (RJ45), of them 2 combo ports each
- Free assignment of ports to desired VLANs

Integrated **security functionalities**:

- Stateful Inspection Firewall
- Dynamic Firewall
- Bridge Firewall¹⁾
- Virtual Private Network (VPN)²⁾
- Network Address Translation (NAT)
- Network separation according to PROFI-safe³⁾

Industry-specific **data throughput**:

- 750 Mbps for firewall and routing
- 120 Mbps for IPsec-VPN³⁾

Integrated engineering by means of:

- TIA portal and SINEC NMS

Integration **in SINEMA Remote Connect**

Benefit

Establishment of a **network segmentation** including **DMZ**:

- Combo ports with SFPs for fiber optic topologies
- Protection of network cells

Protection of critical networks against:

- Unauthorized network access
- Espionage or data manipulation
- Inspection and filtering of layer 2 data

High data throughput for **high system availability** and data security in the network

Central configuration and monitoring

Convenient **central administration and auto configuration** of remote access

¹⁾ Only with SCALANCE SC63x-2C and SC64x-2C; ²⁾ Only with SCALANCE SC64x-2C; ³⁾ Only with SCALANCE SC622-2C and SC626-2C

Network Security

Protection of industrial networks with SCALANCE S615 / S615 EEC



SCALANCE S615 / S615 EEC

Feature / function

Configuration of **flexible security zones**:

- Free assignment of ports to desired VLANs

Integrated **security functionalities**:

- Stateful Inspection Firewall
- Dynamic Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)

Industry-specific **data throughput**:

- 100 Mbps for firewall and routing
- 35 Mbps for IPsec VPN

Integrated engineering by means of:

- TIA portal and SINEC NMS
- Integration in **SINEMA Remote Connect**
- **Conformal Coating**¹⁾

¹⁾ Only with SCALANCE S615 EEC

Benefit

Establishment of a **network segmentation** including **DMZ**:

- Protection of network cells

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation

Central configuration and monitoring of industrial security appliances

Central configuration and monitoring of industrial security appliances

Convenient **central administration and auto configuration** of remote access

Usage in **harsh environmental conditions**

Network Security

SCALANCE LPE9403 – local processing engine



Feature / function

- 2x 10/100/1000 Mbps RJ45
- 1x Combo-Port – 10/100/1000 Mbps RJ45 or 100/1000 Mbps SFP
- Enable Zero Trust based remote collaboration with OT environments in combination with 3rd party vendors
- Implementation in brownfield environments relying on “Defense in Depth”
- Connect legacy OT systems with weak security mechanisms
- Open system based on Linux
- Redundant power supply
- Comprehensive approvals: ATEX, IECEx, cULus HazLoc, FM, shipbuilding

Benefit

High data throughput enables fast data processing. Communication and transfer of information over long distances via fiber optic cable.

Siemens hardware platform for installing Zscaler connectors on site for Human-Machine communication.

Customizable access configuration in “Zscaler Zero Trust Exchange” and seamless integration into existing network infrastructures.

Protection of legacy devices as well as secure remote access by means of combination of perimeter protection with Zero Trust.

Zscaler connectors establish direct and encrypted Internet breakouts to Zscaler Zero Trust Exchange. No additional inbound firewall rules are required.

Reliable operation even when a power supply fails.

Use in various applications e.g. in Ex-Zone 2 based on approvals.

Network Security

Industrial routers: Mobile access with SCALANCE M876



M876-4

Feature / function

Secured **connection via mobile networks**:

- 2G / GSM
- 3G / HSPA+
- 4G / LTE

Integrated **security functionalities**:

- Stateful Packet Inspection Firewall
- User Specific Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)

Integrated **engineering** through:

- SINEC NMS

Integration in **SINEMA Remote Connect**

Implementation of a **flexible security zone concept**

Benefit

Secured connection of Ethernet-based networks to **mobile networks of the 2nd, 3rd and 4th generation**:

- Transfer rates of up to 100 Mbps

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation

Central configuration and monitoring

Convenient **central administration and auto configuration** of remote access

Integrated **4-port switch** for easy connection of multiple network cells

Network Security

Industrial routers: Access to PROFIBUS / MPI with SCALANCE M804PB



SCALANCE M804PB



Feature / function

Secured **Ethernet connection** to existing plants with:

- PROFIBUS / MPI

Integrated **security functionalities**:

- Stateful Packet Inspection Firewall
- User Specific Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)

Integrated **engineering** through:

- SINEC NMS

Integration in **SINEMA Remote Connect**

Integrated **TIA Portal Cloud Connector**

Benefit

Direct connection to existing plants with **PROFIBUS / MPI and SINEMA Remote Connect** (without additional devices), for secured remote access to remote machinery and plants

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation

Central configuration and monitoring

Convenient **central administration and auto configuration** of remote access

Easy and **central administration** of engineering software (TIA Portal) at **one server**

Network Security

Industrial routers: Broadband access with SCALANCE M826



SCALANCE M826-2

Feature / function

Secured **wired connection** of remote automation devices via:

- SHDSL

Integrated **security functionalities**:

- Stateful Packet Inspection Firewall
- User Specific Firewall
- Virtual Private Network (VPN)
- Network Address Translation (NAT)

Integration in **SINEMA Remote Connect**

Implementation of a **flexible security zone concept**

Benefit

Secured **2-wire or 4-wire Ethernet communication** for distances of up to 20 km (~ 12.4 miles):

- Transfer rates of up to 15.3 Mbps

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation

Convenient **central administration and auto configuration** of remote access

Integrated **4-port switch** for easy connection of multiple network cells

Network Security

SCALANCE MUM856-1



Feature / function

- High data rates (1 Gbps download/ 500 Mbps upload) thanks to 5G (Rel. 15) and 4G support
- Supported security mechanisms: IPsec, OpenVPN, firewall
- 1 x Gigabit port, 4 x antenna connection
- IPv6
- Support in SINEMA Remote Connect
- Secure boot
- eSIM support
- IP65 protection class, extended temperature range

Benefit

- Transmission of large amounts of data using mobile communications via 5G and 4G thanks to latest mobile wireless technology
- Increased network security through VPN and cell protection concept
- High-performance network connection
- Long-term future-proof design
- User-friendly and secure connection to widely distributed machinery and equipment via remote access
- Support of newest security standards
- Easy change of network provider without SIM card change
- Use in harsh industrial environments, mounting outside cabinet

* The maximum temperature range is expected to be soon specified to up to +70 ° C

Network Security

SCALANCE MUM853-1



SCALANCE MUM853-1

Feature / function

- High data rates (up to 1 Gbps download/ 500 Mbps upload) thanks to 5G (Rel. 15) and 4G support
- Supported security mechanisms: IPsec, OpenVPN, firewall
- 4 x Gigabit port, 4 x antenna connection
- IPv6
- Support in SINEMA Remote Connect
- Secure boot
- eSIM support
- IP30 protection class, extended temperature range

Benefit

- Transmission of large amounts of data using mobile communications via 5G and 4G thanks to latest mobile wireless technology
- Increased network security through VPN and cell protection concept
- High-performance network connection
- Long-term future-proof design
- User-friendly and secure connection to widely distributed machinery and equipment via remote access
- Support of newest security standards
- Easy change of network provider without SIM card change
- Use in harsh industrial environments

Network Security

Communication processors: Secured to Ethernet with CP 1243-1



CP 1243-1

Feature / function

Secured **mobile radio access** to **SIMATIC S7-1200**:

- TeleControl Server Basic
- DNP3
- IEC 60870-5-104

Integrated **security functionalities**:

- Stateful Packet Inspection Firewall
- Virtual Private Network (VPN)
- Clock synchronization (NTP secure)
- Secured web server access (HTTPS)
- Transmission of network analysis information with SNMP V3

Integration in **SINEMA Remote Connect**

Integrated engineering by means of:

- STEP 7 in TIA Portal

Benefit

Network protection and **segmentation** without additional security components and secured connection to a **Telecontrol control center** via telecontrol protocols

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation

Convenient **central administration and auto configuration** of remote access

Central configuration of the communication processor

Network Security

Communication processors: Secured to Ethernet with CP 1543-1



CP 1543-1

Feature / function

Secured **Industrial Ethernet** to **SIMATIC S7-1500**

Integrated **security functionalities**:

- Stateful Packet Inspection Firewall
- Virtual Private Network (VPN)
- Network authentication according to IEEE 802.1X
- Clock synchronization (NTP secure)
- Secured web server access (HTTPS)
- Secure file transfers (FTPs)
- Transmission of network analysis information with SNMP V3

Integrated engineering by means of:

- STEP 7 in TIA Portal

Benefit

Network protection and **segmentation** without any additional security appliances

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation
- Authentication of the SIMATIC S7-1500 via RADIUS

Central configuration of the communication processor

Network Security

Communication processors: CP 1543SP-1 for distributed controller



CP 1543SP-1

Feature / function

Secured connection of **SIMATIC ET 200SP** to **Industrial Ethernet**

Integrated **security functionalities**:

- Stateful Packet Inspection Firewall
- Virtual Private Network (VPN)
- Clock synchronization (NTP secure)
- Transmission of network analysis information with SNMP V3
- Secure authentication of communication partners by means of certificates

Integration in **SINEMA Remote Connect** (from Firmware Version V2.0)

Integrated engineering by means of:

- STEP 7 in TIA Portal

Benefit

Network protection and **segmentation** without any additional security appliances

Protection of critical networks against:

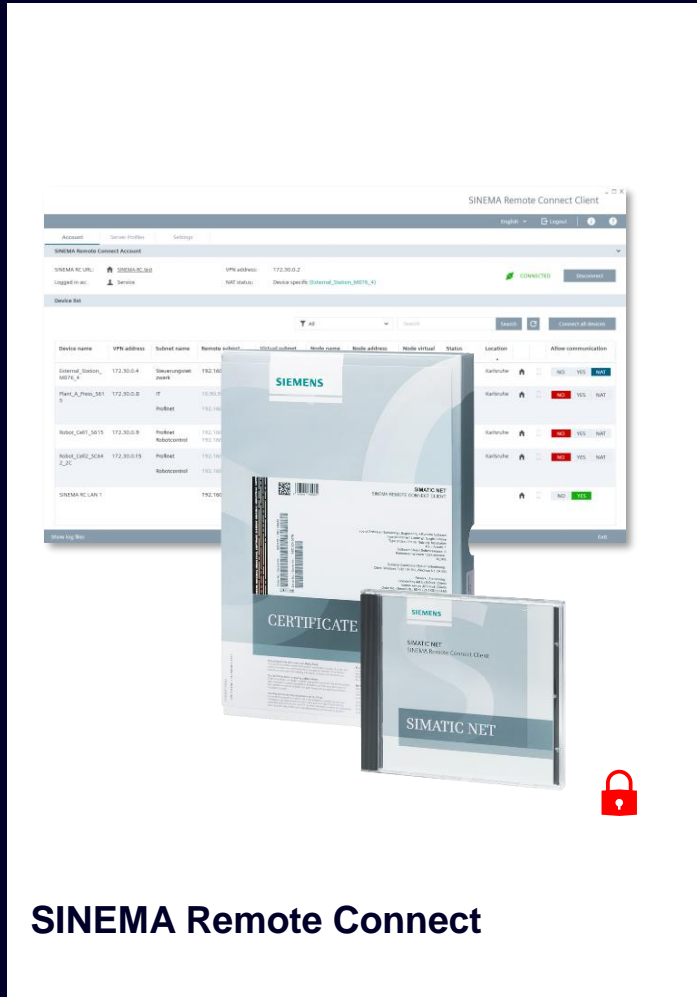
- unauthorized network access
- espionage or data manipulation

Convenient **central administration and auto configuration** of remote access

Central configuration of the communication processor

Network Security

Remote Network Management: SINEMA Remote Connect



Feature / function

Secured management of tunneled connections between a central, the service technicians and the installed systems

Integrated **security functionalities**:

- Virtual Private Network (VPN)
- Dedicated Device Access (DDA)
- PKI smartcard registration for Web-Based Management and SINEMA RC Client
- User management via UMC and AD¹⁾

Integrated security concept for automation technology together with:

- SIMATIC Security CPs
- Industrial Router SCALANCE M
- Industrial Security Appliances SCALANCE S
- Compact SIMATIC RTUs
- Devices of the Siemens Industrial Edge ecosystem
- Local Processing Engine SCALANCE LPE

Benefit

Management of secured remote access

to globally distributed machines and systems

Protection of critical networks against:

- unauthorized network access
- espionage or data manipulation
- User specific access rights for dedicated access to specific IP addresses within a subnet

Communication exclusively via a **rendezvous server**. The service technician and the machine to be serviced each establish a connection to the SINEMA Remote Connect. There, the identity of the participants is determined by exchanging certificates before the machine is accessed.

¹⁾ Active Directory

Network Security

New generation of network management: SINEC NMS



SINEC NMS

Feature / function

Central, **rule-based configuration** and **monitoring** of networks

Central **firewall management** including NAT

Mass configurations and **firmware updates**

Central **user management**

Benefit

Time-saving device configuration and simplified troubleshooting. Reduced misconfiguration thanks to **device-independent rule description**

Graphical definition of permissible communication relationships using **firewall and NAT rulesets**, e.g. for series machines with identical IP addresses

Device-independent firmware update function for single or multiple network components

Integrate and use existing users from **Active Directory** or **UMC**

Network Security

Infrastructure Network Services: SINEC INS



Feature / function

All **services** provided by SINEC INS are **tested in industrial environment**

SINEC INS provides a **web page for configuring** and using the services

SINEC INS delivers **one setup** for initializing all services

Central infrastructure network services

Benefit

Proofed suitability for industrial use cases with Siemens devices and **one service compilation**

Easy configuration and easy use of complex services specialized for Siemens products, without need for deeper IT know-how

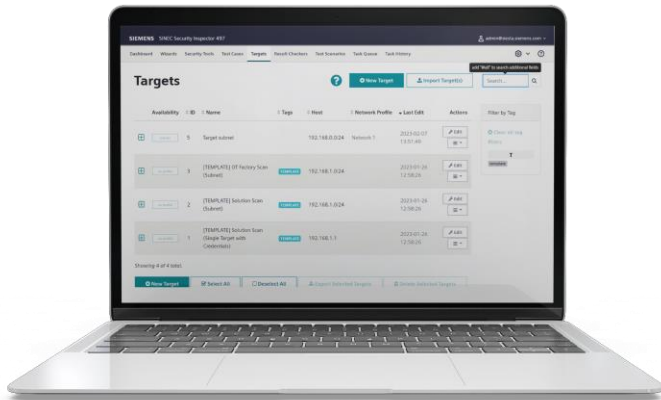
Very **easy and fast installing** and starting of all required services for industrial networks

Services **supporting cybersecurity**. Amongst others:

- RADIUS server for user management
- Syslog server for device monitoring

Network Security

Asset and Vulnerability identification: SINEC Security Inspector



SINEC Security Inspector

Feature / function

Unique **security testing solution for OT/IT** environments

Selection of different **security tests** with wide-ranging capabilities for detecting vulnerabilities

Provides clearly **structured reporting** that summarizes the results of all tests

Simple administration, customized compilation and **automation of test procedures**

Benefit

Intuitive web-based user interface with a wizard supported workflow, tailored to the needs of OT

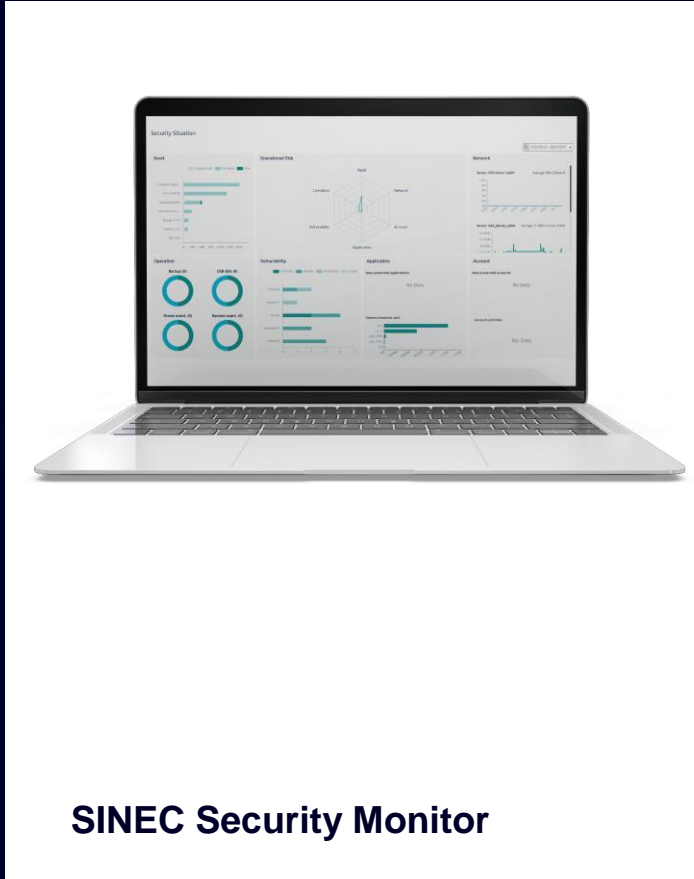
A wide **range of predefined test cases** and supported testing tools to have a broad tool set for increasing insights, **compliance and quality** within your application environment.

Scan and test cases have been adapted to **fit OT network requirements**, involving the experience of the SIEMENS product CERT community.

Enables implementation of **factory and side acceptance tests (FAT)/(SAT)** with ease

Network Security

Security monitoring during production: SINEC Security Monitor ¹⁾



Feature / function

Software for passive, non-intrusive, **continuous on-prem security monitoring** during production

Analysis of **network traffic** allows asset identification, **AI-based anomaly detection** and OT-focused SIEM with interfaces to existing SIEM systems

Modular offering based on amount of monitored assets as well as functional requirements

Used in many Siemens factories – now available for customers in Americas, Asia-Pacific, Europe

Everything you need – from license only to complete server, sensor hardware and services

Benefit

No interruptions of your production
Data stays in your premises

Visibility tailored to the needs of OT and governmental regulations

Flexibility and low entry cost due to term license concept

Benefit from our OT expertise – From OT experts to OT experts!

Holistic offering for detection as well as responding (e.g. with SINEC NMS) from one trusted, long-term available supplier

Passive Asset detection



Vulnerability detection



Anomaly detection



SIEM + Interfaces



¹⁾ Release date: Q3/2023

Network Security

Mechanical closing of unused ports with IE RJ45 Port Lock



Feature / function

- **Mechanical closing** of unused RJ45 interfaces of network components and end devices

Security functionalities:

- RJ45 port can also lock non-configurable network components
- Robust, industrial-suited construction
- Easy installation without additional tools due to RJ45 compatible design
- Removal of port lock only after unlocking with a mechanical key

Benefit

Secures physically open, unused **RJ45 interfaces** to prevent unauthorized network access

Temporary **network disconnections** (plant shutdown for maintenance) can be implemented directly on site

Protection of the critical network components:

- unauthorized network access
- espionage or data manipulation

Security Use cases: Network Security



Use cases for more network security

Network segmentation and „demilitarized zone“ (DMZ)

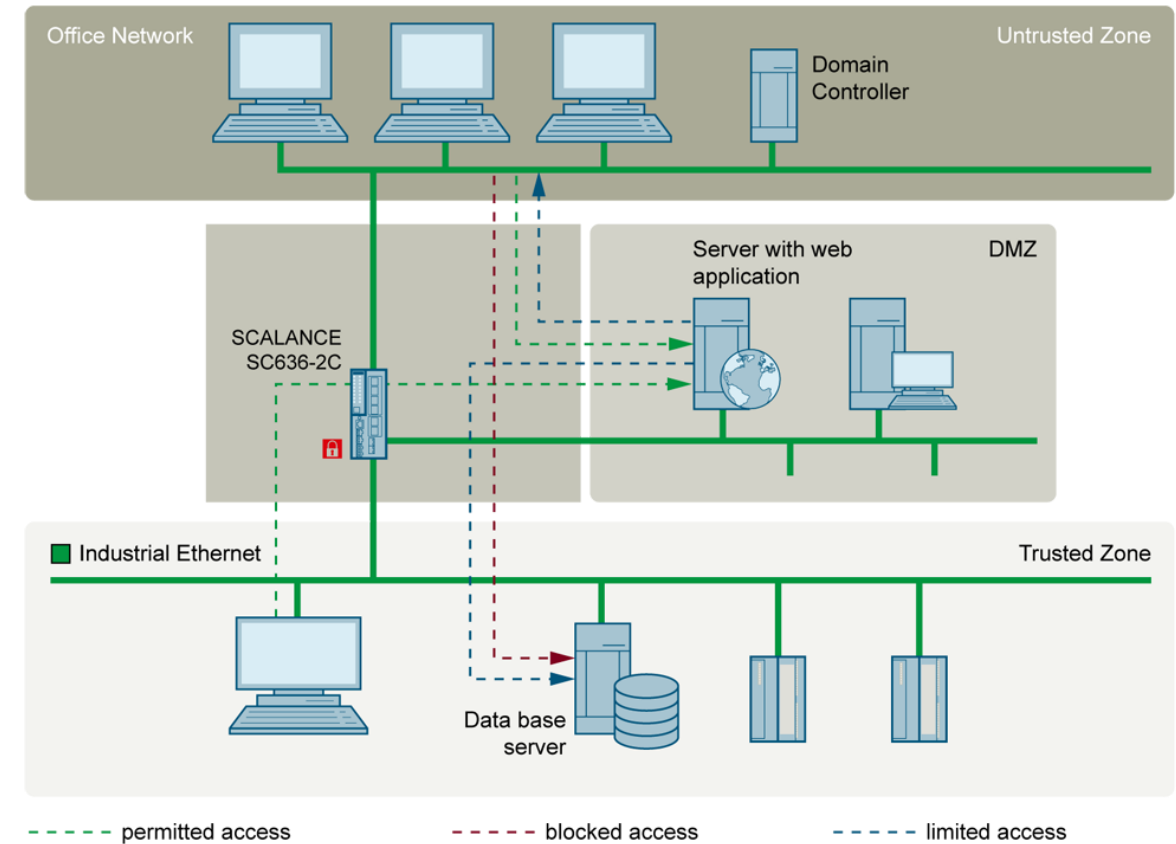
Task

The industrial network shall be divided into several security zones.

Solution

With **SCALANCE S** Industrial Security Appliances a flexible security zone concept can be realized, containing:

- Different security zones such as DMZ, and automation cells
- Remote access only to specific and selected network cells
- Support of 'series machines' by means of NAT/NAPT



¹⁾ Delivery date: 02/2020

Use cases for more network security

Network segmentation and „demilitarized zone“ (DMZ)

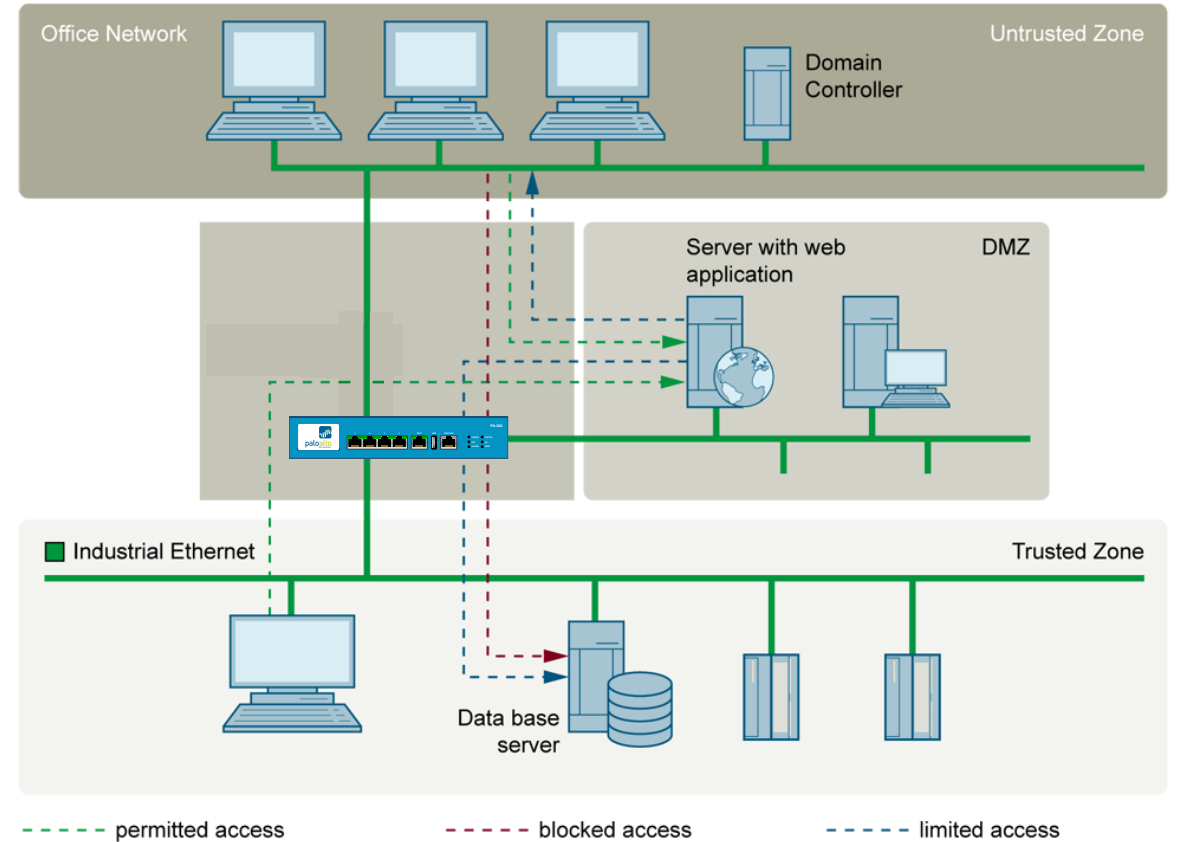
Task

The industrial network shall be divided into several security zones. Also, a deep inspection of the data flow is required.

Solution

With the Industrial Next Generation Firewall based on the firewalls of **Palo Alto Networks** a flexible security zone concept can be realized, containing:

- Different security zones such as DMZ, and automation cells
- Remote access only to specific and selected network cells
- Application Layer Firewall
- Deep Packet Inspection



¹⁾ Delivery date: 02/2020

Use cases for more network security

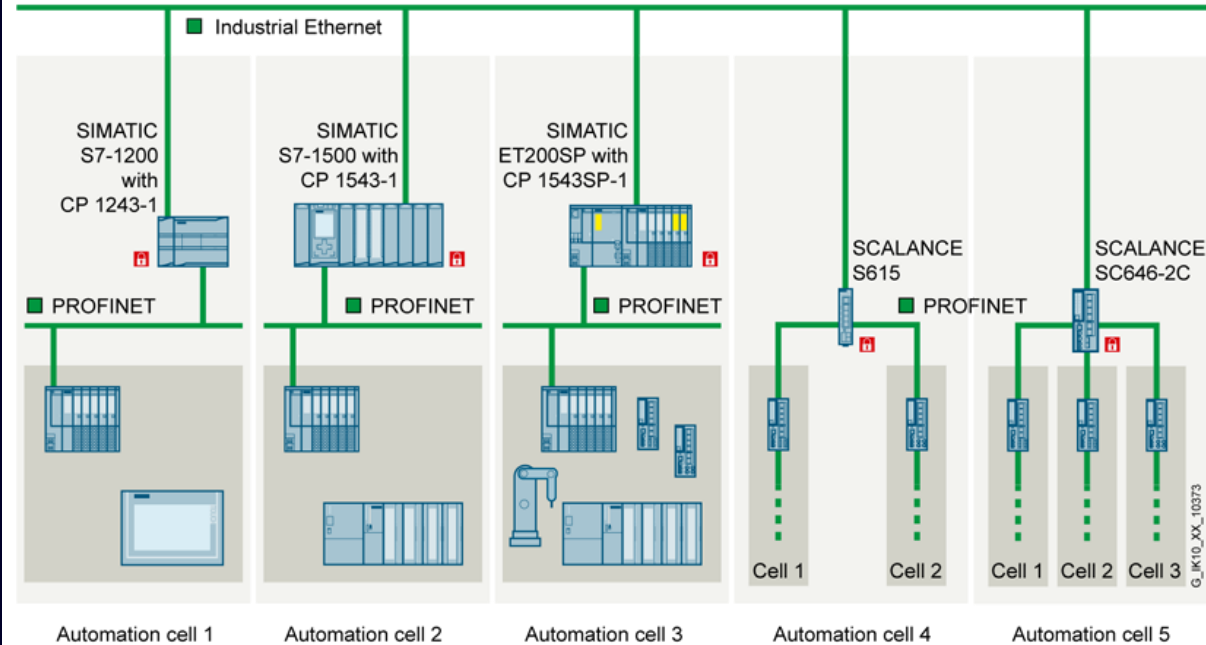
Network segmentation and cell protection

Task

For the purpose of risk mitigation, a large and flat automation network shall be divided into several security-based sections. For each individual segment different requirements may apply.

Solution

The individual network segments will be secured with the **SCALANCE S** Industrial Security Appliances or with specific **security communication processors**. These appliances will control the access and data traffic to the subordinate segment via their integrated firewalls. By means of VLAN, the **SCALANCE S** Industrial Security Appliances can be used to protect several network cells simultaneously.



¹⁾ Delivery date: 02/2020

Use cases for more network security

Use case secure access in OT area based on Zero Trust Concept

Task

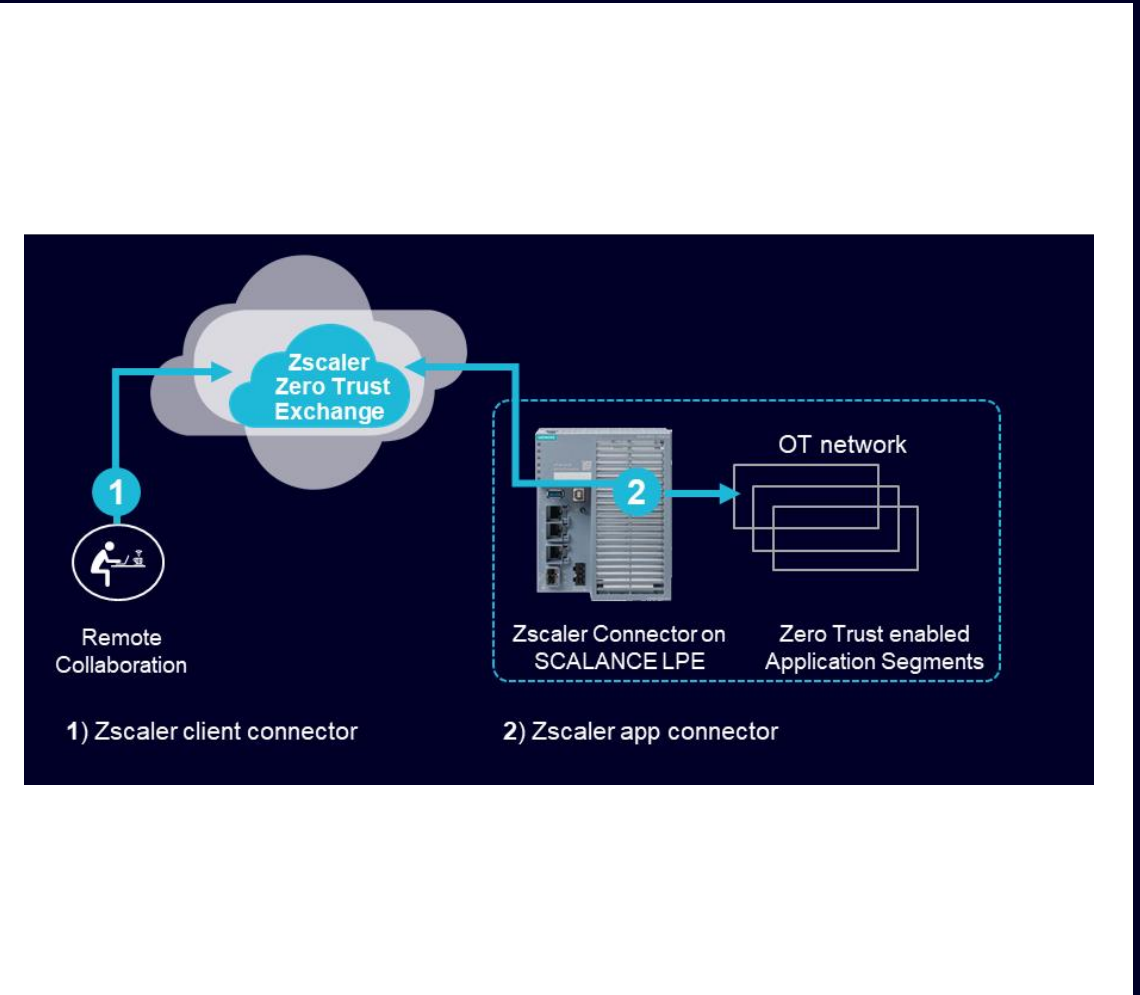
- Provide access from outside or inside the customer
- network to restricted OT areas (machine level) without
- changing the current network infrastructure. Following the
- rules of IT regarding Zero Trust Exchange

Solution

- SCALANCE LPE + Zscaler application as solution for the OT (industrial environment) and as part of the overall existing
- Zscaler architecture

Benefits

- Security with application level
- Simplicity and flexibility granting remote access
- Same infrastructure with IT and OT
- Location independent connectivity



Use cases for more network security

Secured connection with SINEMA Remote Connect Use Case and security mechanisms (VPN)

Task

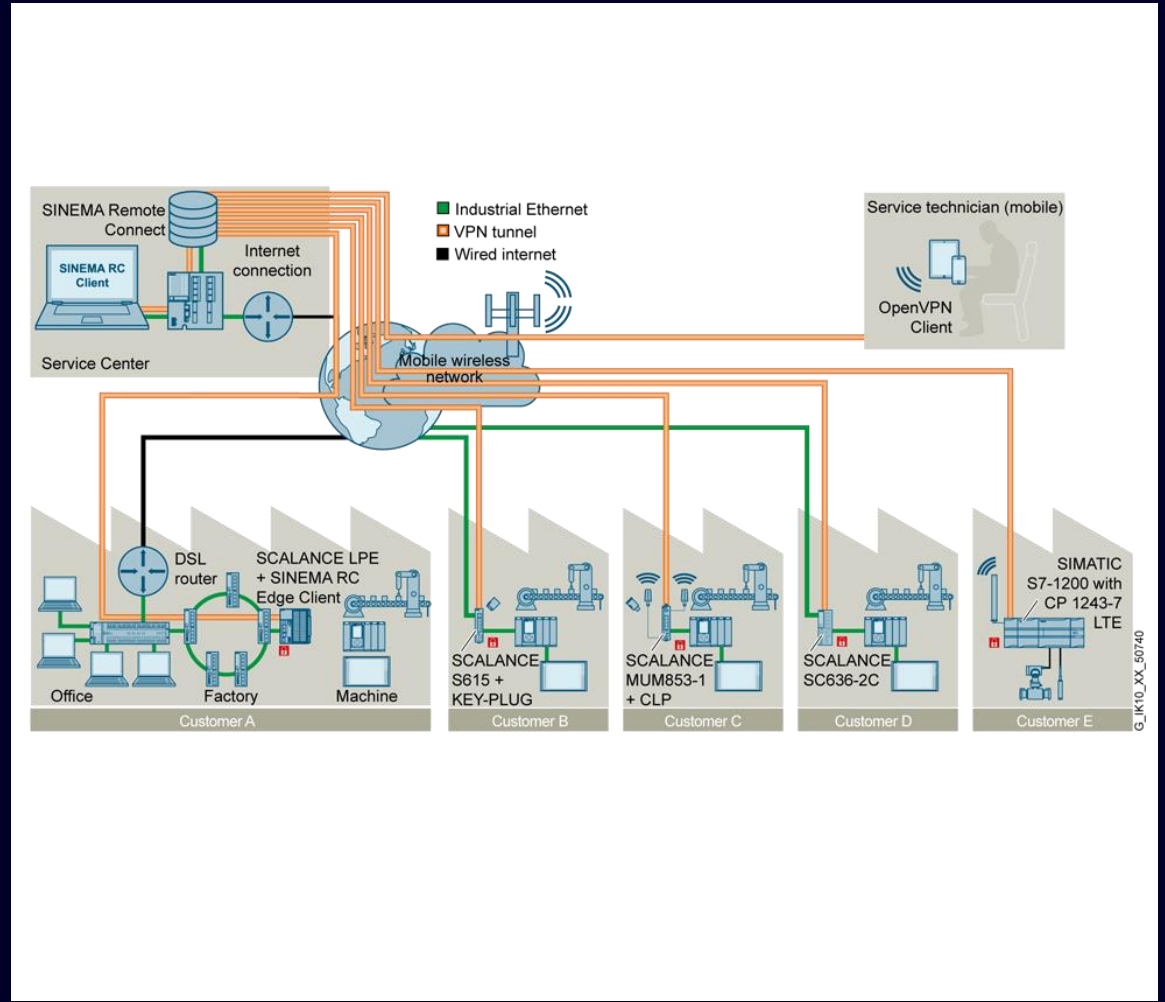
- Remote maintenance of machines and larger plants
- Accesses to the machines/plants/system are protected by security mechanisms (OpenVPN, IPsec)

Solution

- Easy creation of devices with routing/ NAT information in SINEMA Remote Connect
- Simple selection of a device from the list of devices in SINEMA RC Client by mouse click
- Industry routers and service technicians can separately set up a secured connection to the SINEMA Remote Connect server
- SCALANCE M and S devices support firewall and VPN

Benefits

- Time and money saved
- Can be used without specialized IT knowledge
- Flexibility through easy expandability
- Transparent IP communication
- Prevention of manipulation and unauthorized access by means of secured data transmission and authentication



Use cases for more network security

Remote Service for special-purpose machine manufacturers

Task

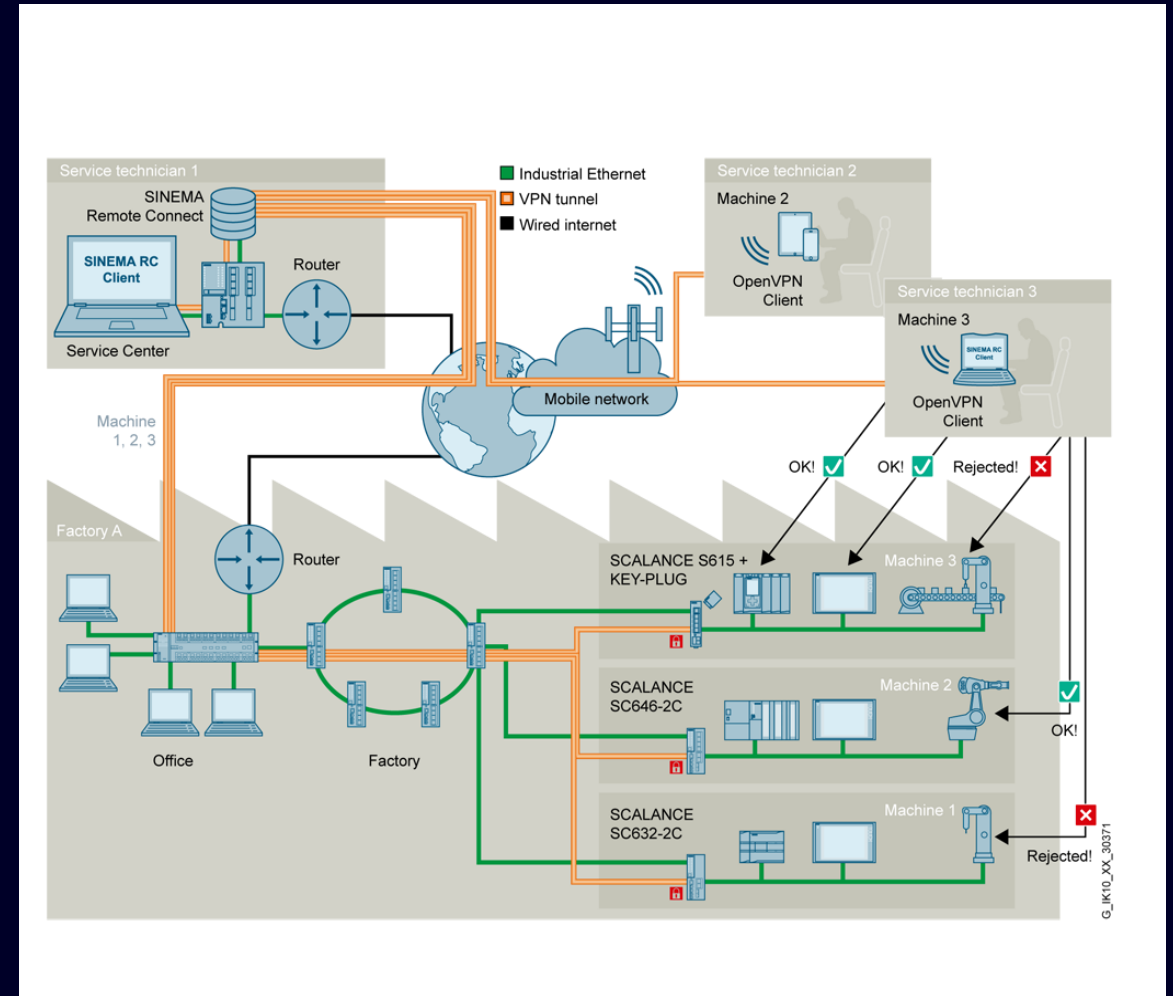
- Secured remote access to special-purpose machines, sensitive areas and individual access restrictions

Solution

- Central management of machines and service technicians in SINEMA Remote Connect
- Assignment and management of user rights and access authorizations
- Logging of accesses

Benefits

- High transparency and security
- Error prevention through explicit assignment of know-how owners to the respective plant sections
- Transparent IP communication
- Secured remote access (via VPN tunnel)



Use cases for more network security

UMC/AD Use Case with Server in the Factory

Task

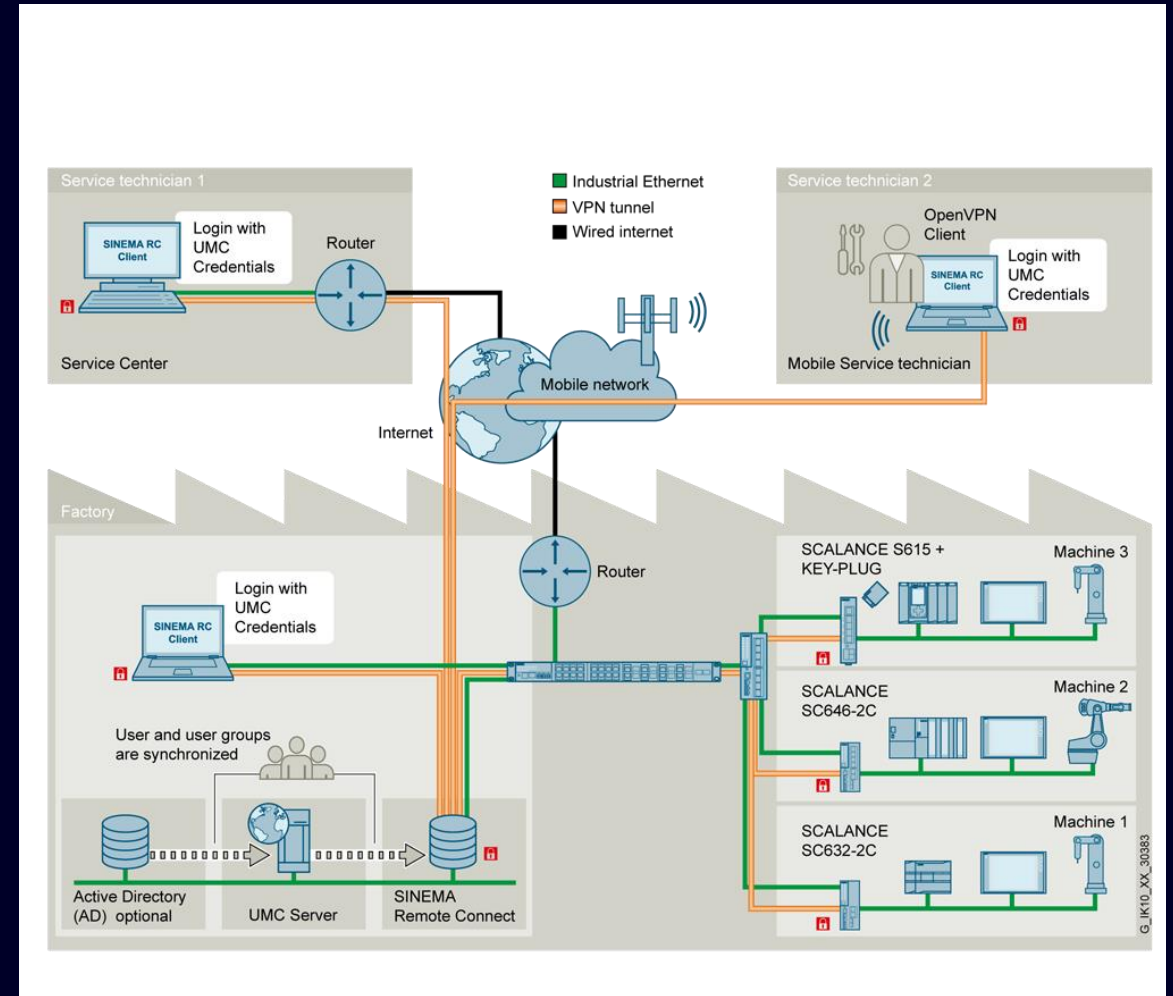
- Secured remote maintenance for series machines and larger systems using central user and permission management

Solution

- Central management of machines and service technicians in SINEMA Remote Connect
- Assignment and management of user rights and access authorizations
- Logging of accesses

Benefits

- High transparency and security
- Error prevention through explicit assignment of know-how owners to the respective plant sections
- Transparent IP communication
- Secured remote access (via VPN tunnel)



Use cases for more network security

Remote Service for series machine manufacturers

Task

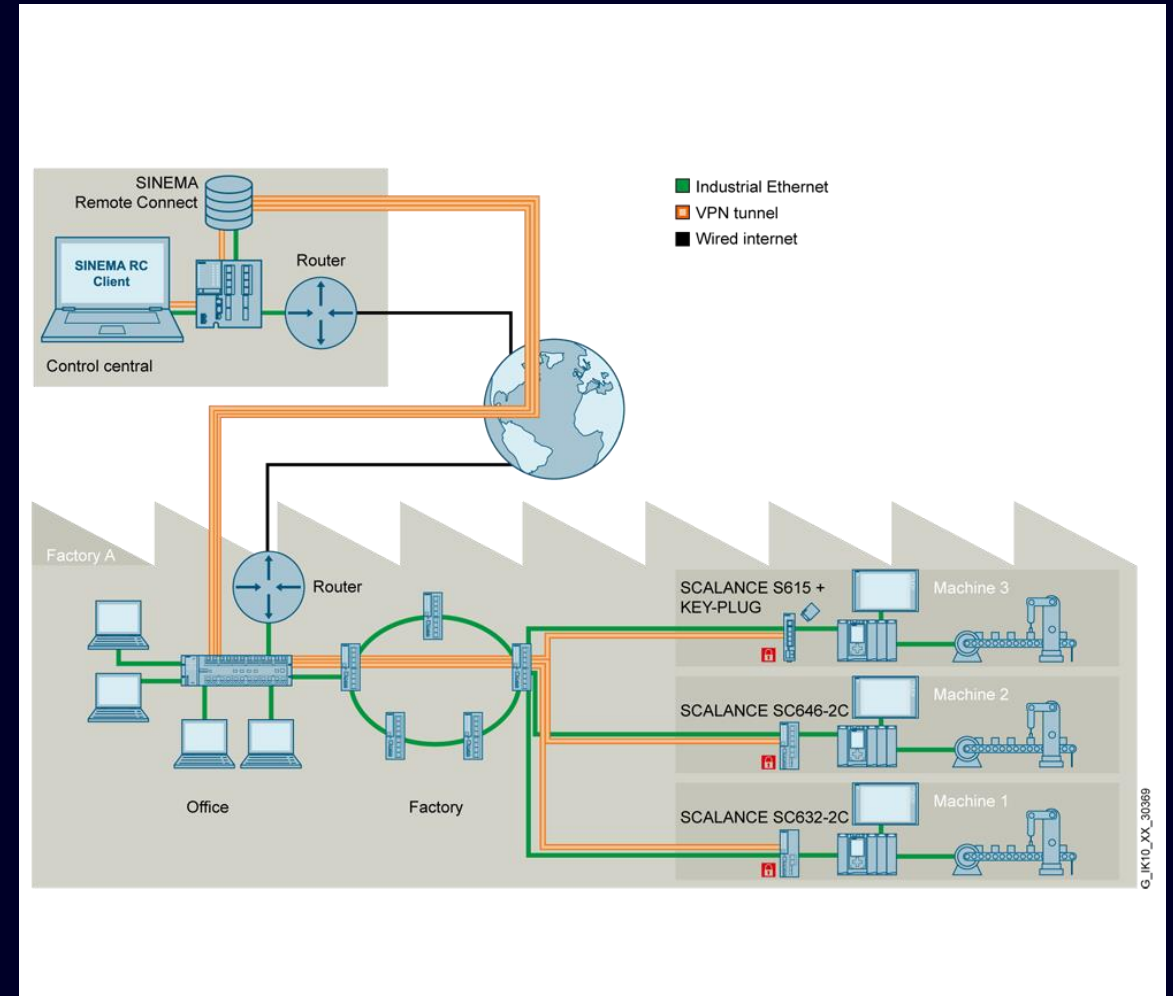
- Secured remote maintenance for serial machines and larger plants with identical subnetworks

Solution

- Easy creation of devices with routing/NAT information in SINEMA RC
- Simple selection of a device from the list of devices in SINEMA RC Client by mouse click

Benefits

- Time and money saved
- Can be used without specialized IT knowledge
- Flexibility through easy expandability
- Transparent IP communication
- Secured remote access (via VPN tunnel)



Use cases for more network security

Remote Service to PROFIBUS/MPI plants with SCALANCE M804PB and Step 7

Task

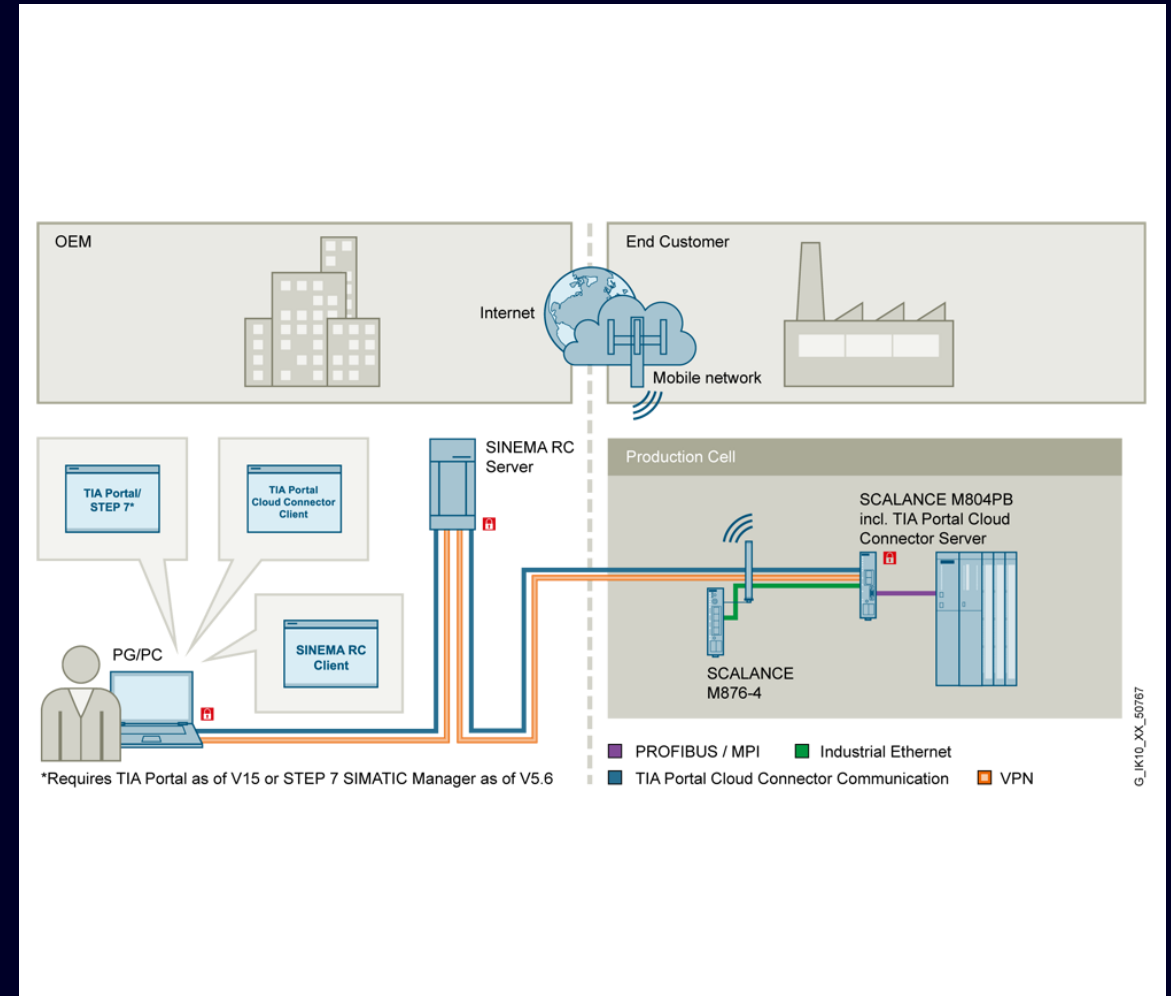
- Remote service with remote access for PROFIBUS via MPI:
A service technician is to access a PROFIBUS plant from outside the company network

Solution

- Connection of PROFIBUS/MPI plants over SCALANCE M804PB that is connected to the production cell over MPI
- Easy configuration and management of the VPN tunnels with the SINEMA Remote Connect management platform enables secure remote access to the plant

Benefits

- Remote Access on machines and plants with PROFIBUS/ MPI reduces time and costs for on-site operation
- Easy connection of consisting plants
- Prevention of manipulation and unauthorized access thanks to secure data transmission and authentication



Use cases for more network security

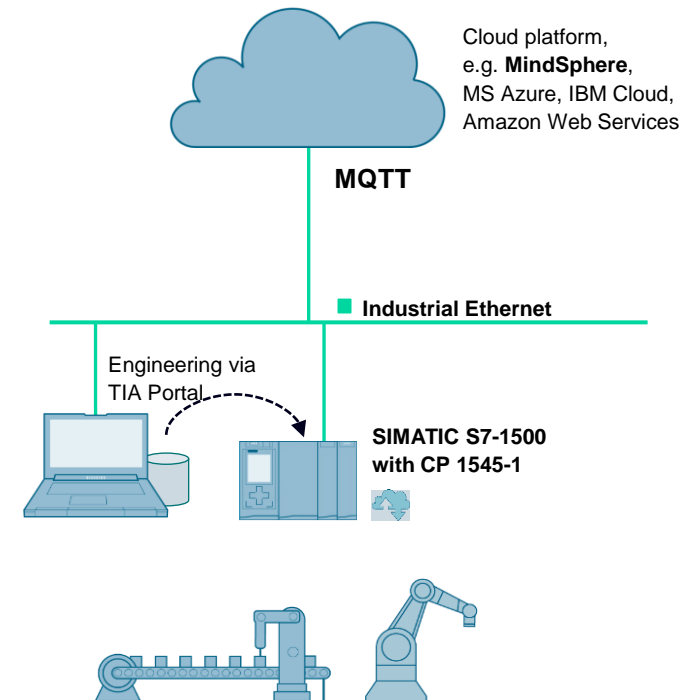
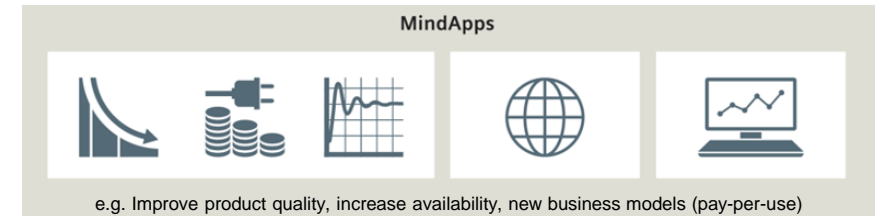
Secure Cloud Connectivity for S7-1500 Controller

Task

Data values of the production process, which is controlled by the S7-1500 system, are to be provided to the cloud-based application.

Solution

CP 1545-1 with CloudConnect to provide the field data of the S7-1500 system in the cloud for further analysis and improvements of the production process. The integrated trigger management with event-driven or cyclic transmission of the data offers an easy way of configuration.



Use cases for more network security

Security concepts for the path to the cloud

Task

Every careful design of a company network requires a multi-level protection concept from the field level to the internet and cloud.

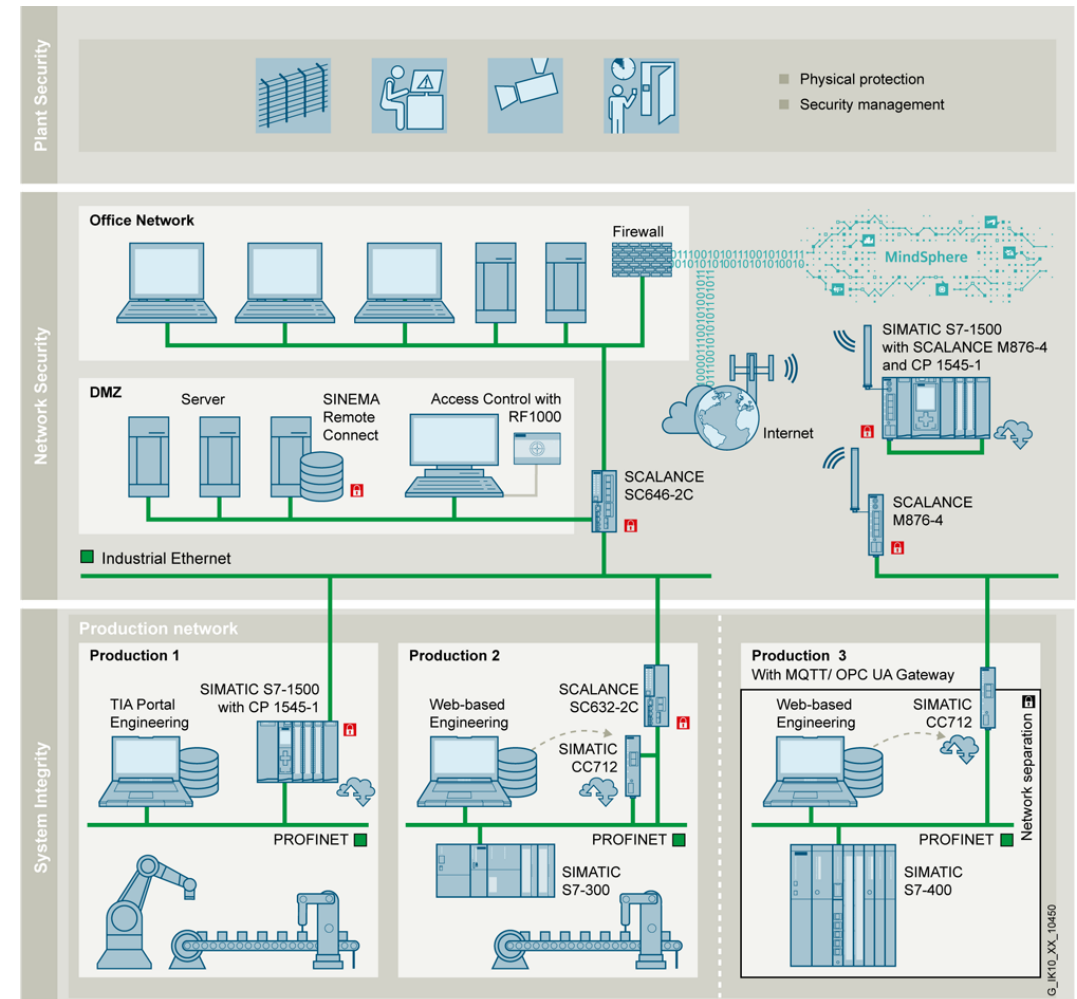
Solution

Cell protection – protection of each individual protection cell

- Production 1: CP 1545-1 with integrated firewall for SIMATIC S7-1500.
- Production 2: Firewall of SCALANCE SC632-2C protects both, the IP address ranges of PROFINET communication and the MQTT communication of SIMATIC CC712.
- Production 3: Network separation by SIMATIC CC712 and protection on the higher level by a firewall of SCALANCE M876-4.

Network security – controlled separation of all networks

- The production networks only access the servers in the demilitarized zone (DMZ), set up by the SCALANCE SC646-2C. Individual communication channels from production to the Internet are specifically opened in one direction (e.g. the MQTT communication of the SIMATIC CC712).
- The office network is strictly separated from the production networks and only connect to the servers in the DMZ and via firewall to the Internet.



Use cases for more network security

Holistic security engineering

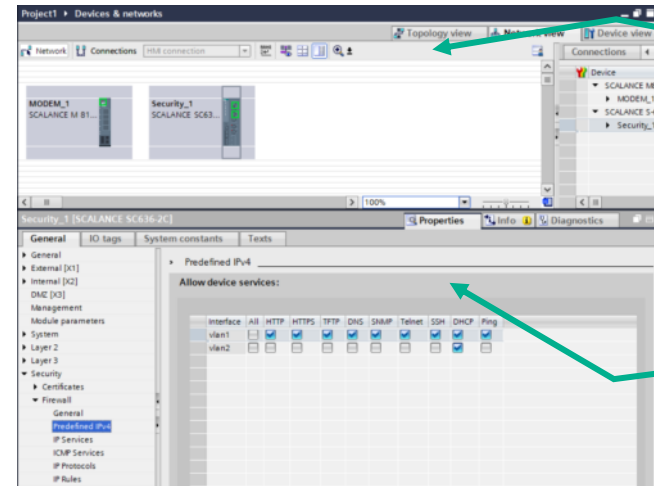
Task

The security components used in the network shall be configurable both via decentral standard engineering paths and from a central point.

Solution

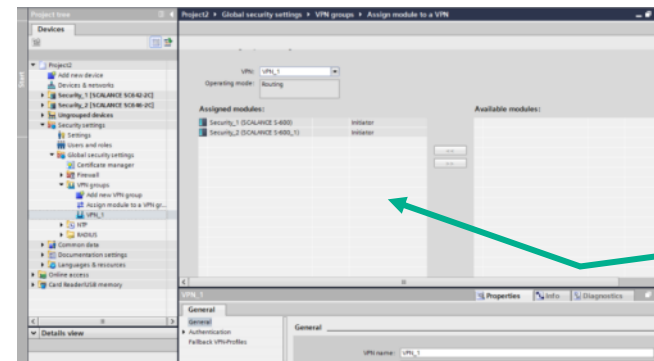
The Industrial Security Appliances **SCALANCE S** supports the popular standard paths and can also be centrally engineered:

- Decentral configuration and administration by means of WBM, CLI or SNMP
- Central configuration and administration by means of TIA Portal



Network view

Setup of firewall rules



Creation of VPN connections

Use cases for more network security

Network management and -diagnostics

Task

All Ethernet parameters of SCALANCE S devices should be managed and diagnosed centrally in a network management system.

Solution

The network management system SINEC NMS is optimized for the integration of SCALANCE network components. NMS provides central monitoring, firmware update and device configuration for SCALANCE S.

The screenshot displays the SIEMENS SINEC NMS interface for network monitoring. The top navigation bar includes 'SIEMENS', 'SINEC NMS', and user information 'SuperAdmin'. The main area shows a network topology diagram with various devices connected. A left sidebar lists device categories and status. A right sidebar shows details for a selected device, including 'Redundancy information' and 'Pending events'. A bottom table lists event logs.

Event status	Event	Event class	Time stamp	Event details	IP address - affected
No	Pending	Wireless interface quality: critical high signal strength to the connection	2018-08-26 19:25:57.595	MAC address: 00:1b:1b:37:a4:f9, value: -34	192.168.120.82
No	Resolving automat	Wireless interface quality: normal signal strength to the connection	2018-08-26 19:20:57.431	MAC address: 00:1b:1b:37:a4:f9, value: -43	192.168.120.82
No	Resolving automat	Wireless interface quality: critical high signal strength to the connection	2018-08-26 19:15:57.544	MAC address: 00:1b:1b:37:a4:f9, value: -31	192.168.120.82
No	Resolving	Wireless interface quality: normal signal strength to the connection	2018-08-26 19:10:57.505	MAC address: 00:1b:1b:37:a4:f9, value: -41	192.168.120.82
No	Resolving automat	Wireless interface quality: risky signal strength to the connection	2018-08-26 19:05:57.608	MAC address: 00:1b:1b:37:a4:f9, value: -36	192.168.120.82

Use cases for more network security

Central firewall / NAT management with SINEC NMS

Task

With the industry's growing concern on cybersecurity, an efficient and secure way to create, maintain and document firewall and NAT configurations is becoming an essential task in network management.

Solution

Instead of managing firewall devices separately, **SINEC NMS** offers a centralized Firewall management:

- Definition of centralized communication relations with graphical interface
- Access control with central and role based user management
- Documentation of all changes and configurations at firewall settings with so-called audit trail

The screenshot displays the SINEC NMS configuration interface for a Communication Relation. The top section, 'Primary details', shows the relation named 'NAT - Area 1' with a description of 'NAT only', 0 firewall rules, a flag, and version 1.0. Below this is the 'Communication Relation Chain' diagram, which illustrates the flow from 'Communication Partner 1*' (containing an object group 'All Devices in Area 1') through a 'Firewall group' (labeled 'Cell Firewall Area 1') to 'Communication Partner 2*' (containing an object group 'Any'). The 'Firewall group' configuration is expanded, showing 'Internal' and 'External' interfaces, 'Common capabilities', and 'NAT' settings. A tooltip points to the 'NAT' dropdown, which is set to '1:1 Destination NAT (Internal network on the right)'. Other settings include 'Log level' and 'Digital Input'. At the bottom, the 'Allowed Services*' section lists various services such as 'SNMP_SNMP', 'SIMATIC_123', and 'HTTPS_HTTP', with an 'Add services' button. The interface concludes with 'Cancel' and 'Apply' buttons.

Use cases for more network security

Asset identification / SINEC Security Inspector

Task

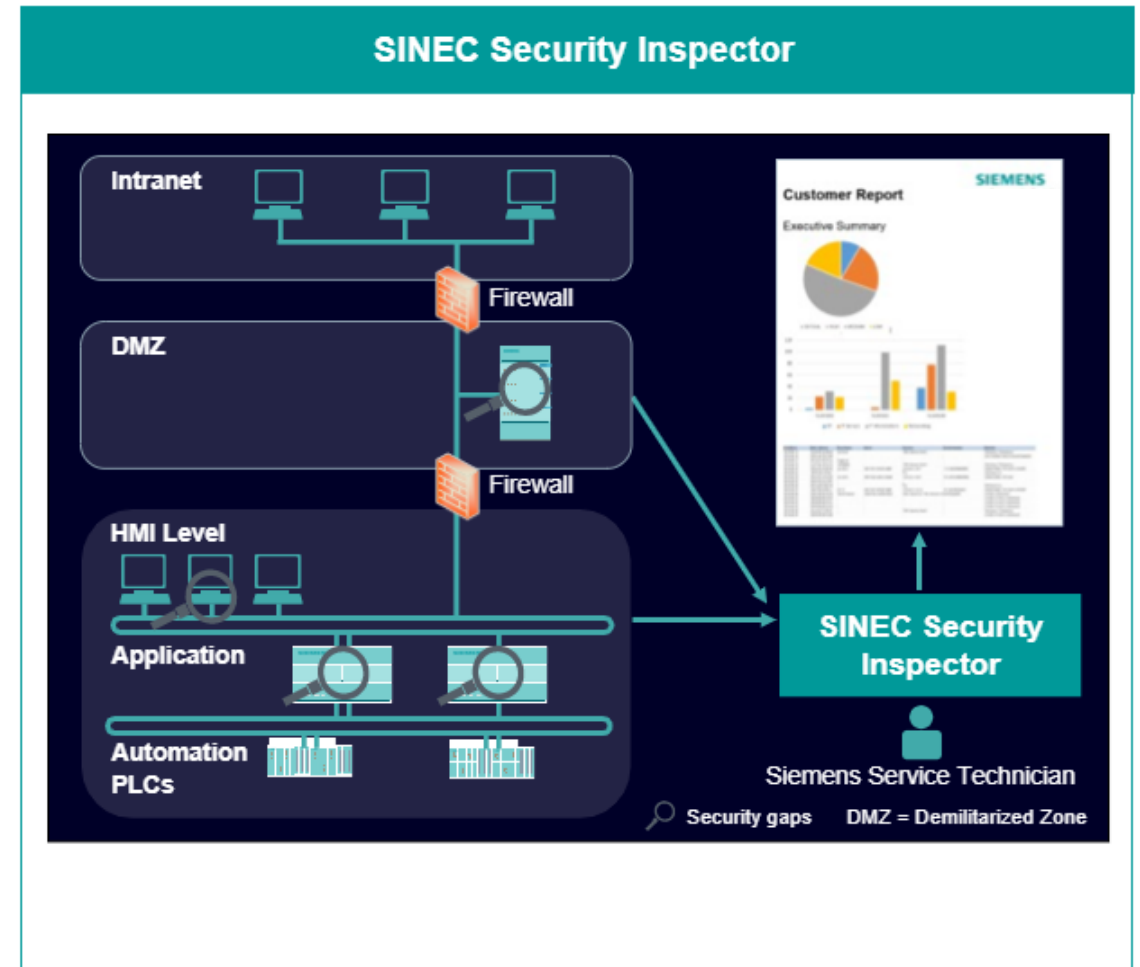
A factory structure with different machine providers using a vast vendor variety has been grown over years. This generates the demand to gain transparency and system identification within the factory environment to ensure a total cyber security approach.

Solution

SINEC Security Inspector offers a framework performing different possibilities to identify assets. This bandwidth of usable protocols increases the identification rate, especially for OT specific assets.

Benefits

- Discover multi-vendor assets of the entire network.
- Asset information can be shared with external systems using software interfaces (REST API) or the possibility of exports in standardized formats.
- Possibility of soft/non-intrusive OT optimized scans, which are also supporting OT specific communication protocols.



Use cases for more network security

Vulnerability identification / SINEC Security Inspector

Task

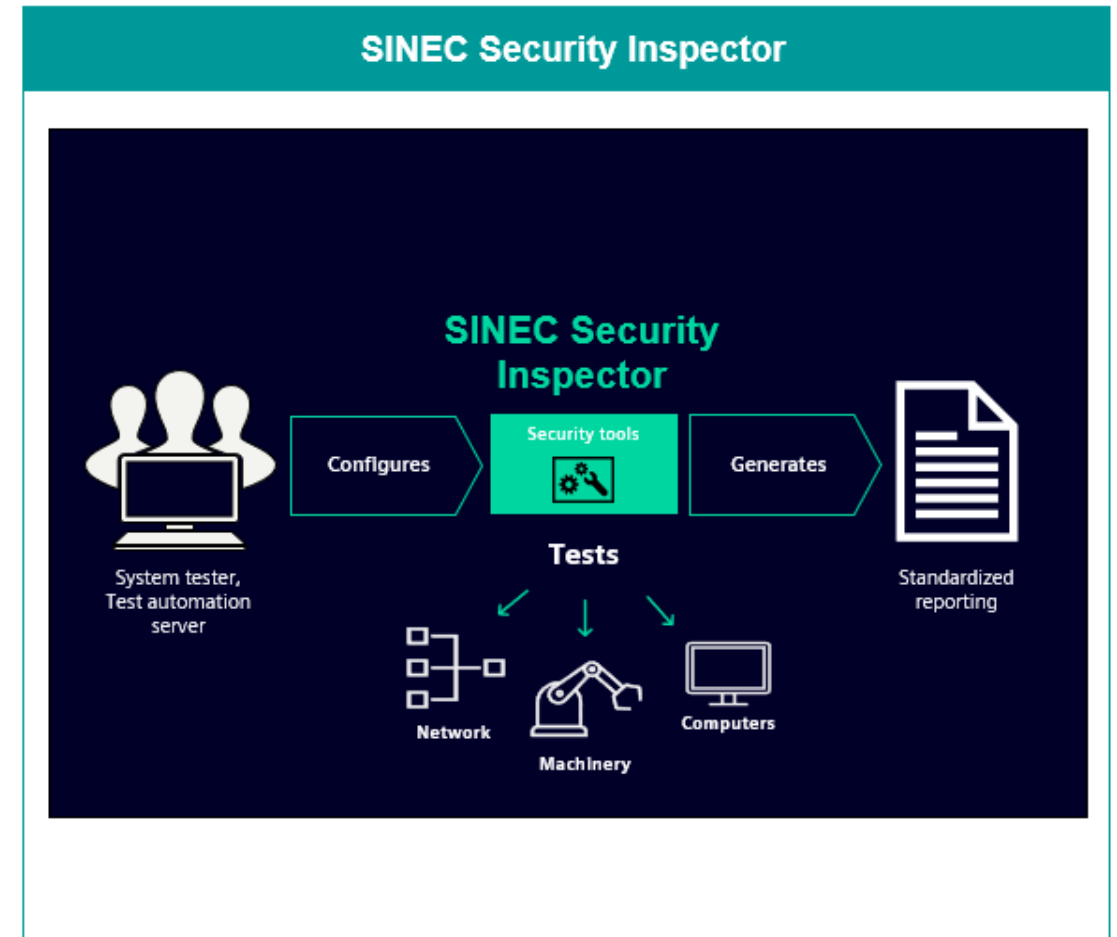
A factory structure with different machine providers using a vast vendor variety is the basis. To ensure a cyber security concept asset transparency and a dedicated vulnerability management is needed. On top of this a centralized patch management is missing as well.

Solution

SINEC Security Inspector offers a framework performing different test cases to identify vulnerabilities. According to these found vulnerabilities mitigation proposals are made to increase the overall cyber security.

Benefits

- Discover multi-vendor vulnerabilities of the entire network.
- Vulnerability information can be shared with external systems using software interfaces (REST API), the possibility of exports in standardized formats or summarized vulnerability reports.
- Up to date solution proposals to mitigate discovered vulnerabilities.



Exemplary Use cases

Security Monitoring for OT networks

Task

- Create transparency about all ports, network participants and network topology
- Check installed Firmware Versions on devices against recommended or company standard
- Identify known vulnerabilities of devices in use
- Detect Anomalies and Intrusions to react fast

Solution

- Identify Assets including firmware and topology by traffic analysis and smart probing using SINEC Security Monitor¹⁾ Basic package and sensor
- Monitoring down to segmented network zones e.g. in aggregation and cell level can be realized with the optional “Distributed sensor Add-On”
- Monitoring of Windows based PCs using the optional “Agent Add-On” for example: USB-storage plugged in, application installed
- Correlation of devices with known vulnerabilities from leading intelligence databases
- Detection of anomalies and intrusions using AI based anomaly detection

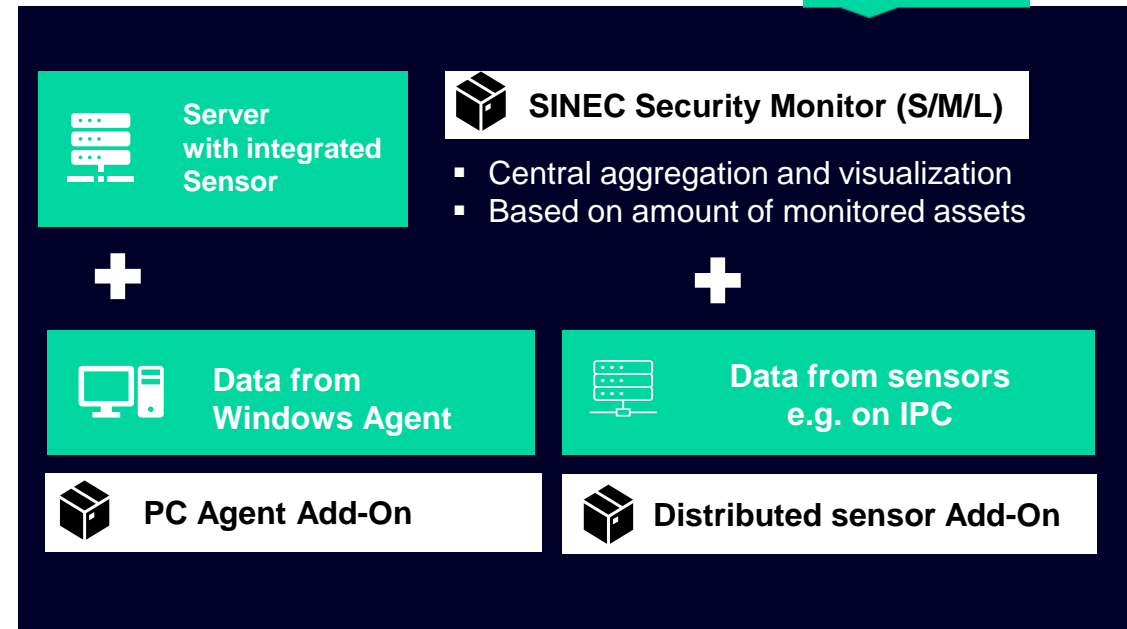
Additional Benefits

- Passive, non-intrusive solution
- Fully on premises solution (No internet connection required except for updates)

¹⁾ Sales release in Q3/2023



Term licence



Plant Security



Industrial Security

Admission management

Security Management Process

- Risk analysis with definition of mitigation measures
- Setting up policies and coordination of organizational measures
- Coordination of technical measures
- Regular / event-based repetition of risk analysis



Security Management is essential for a well thought-out security concept

SIMATIC PCS7 Cyber Security



SIMATIC PCS 7 V9.1

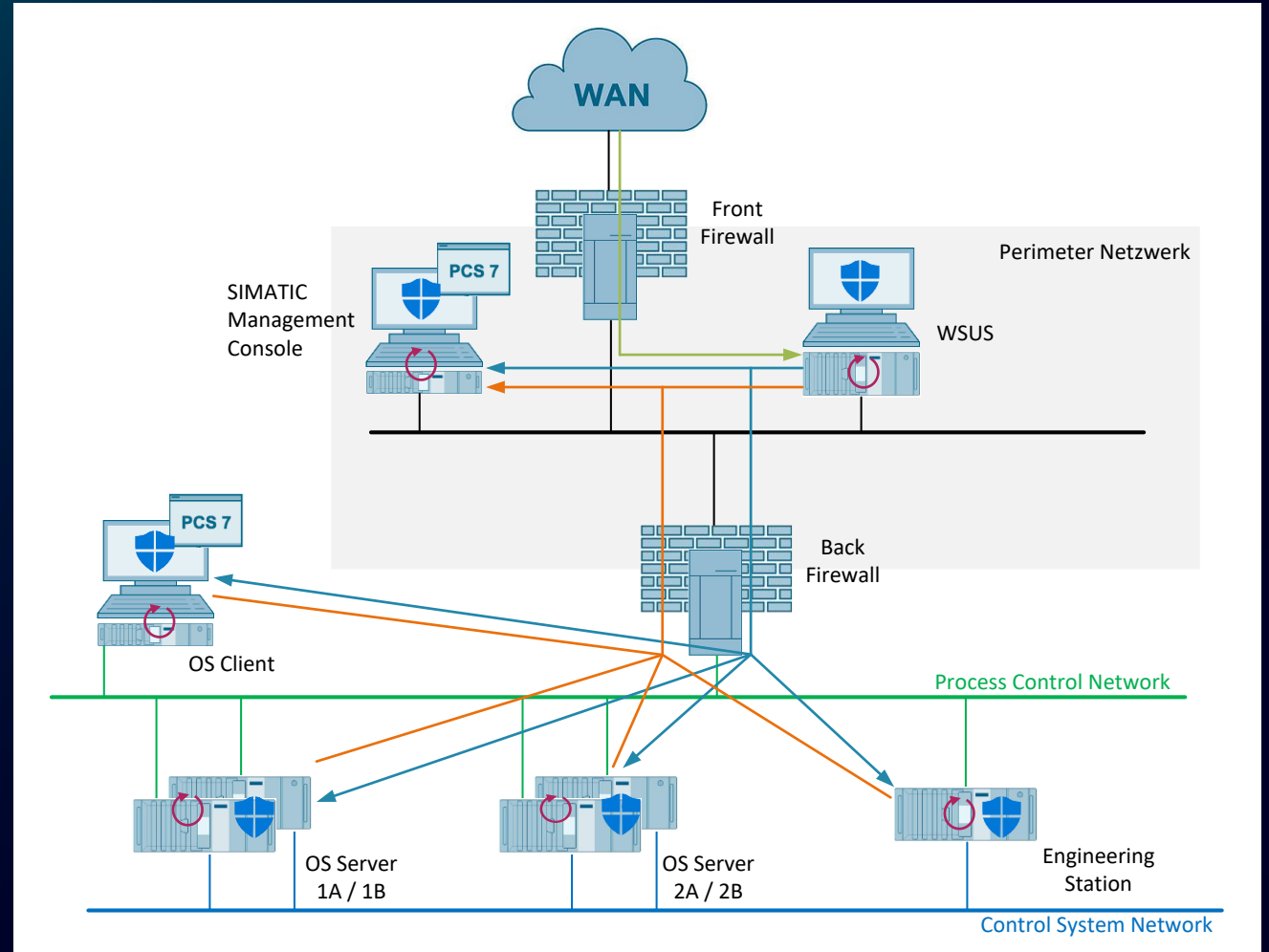
Antivirus Solution based on integrated Microsoft Windows Defender Antivirus

- + Integrated antivirus solution provided with Microsoft operating system
→ No additional licenses required
- + Ongoing virus protection based on Microsoft Windows Defender Antivirus
- + Automatic download of Defender definition updates based on WSUS¹
(WSUS already used for operating system updates)
- + SIMATIC Management Console collects Defender Antivirus events from all computers
- + Reduced hardware footprint and maintenance costs
 - No additional update server for antivirus software required
 - Existing WSUS used for Defender updates
 - Reduced effort for firewall configuration

Definition update sequence

- ➔ Definition updates are downloaded from the Internet to the WSUS
- ➔ Clients download automatically new Defender definition updates on a daily basis
- ➔ Important Windows Defender events will be available on SIMATIC Management Console
- ➔ After successful download: Clients install the Defender definition updates automatically (no reboot required)

¹ WSUS – Windows Server Update Services



Industrial Security in SIMATIC PCS 7 V9.1

Supported Firewalls

Features



- Automation Firewall NG (Next Generation) based on Palo Alto Networks Firewall as system tested solution for front and back firewall (successor to the SecureGuard firewall)
- SCALANCE SC6xx-2C as system tested firewall for remote OS client stations and for bridged connections between different CSNs (most actual firmware V2.1.1 and later required)

Key Benefits



- Next Generation firewall with data analyses at the application level. This process filters malware out of network-based communication
- SCALANCE SC with state of the art security for industrial environments

Industrial Security in SIMATIC PCS 7 V9.1

Backup & Recovery

Features



- SIDS Backup & Restore – Professional (SIMATIC DCS/SCADA Infrastructure) is a system tested backup & restore solution
- Easy setup of PCS 7 compliant backup plans
- Backup Recovery Verification Tests

<https://support.industry.siemens.com/cs/ww/en/sc/4784>

Key Benefits



- Turn key solution with holistic support approach covering all hard- and software components
- State of the art backup and recovery solution for virtualized and non-virtualized environments



Industrial Security in SIMATIC PCS 7 V9.1

Security Measures

Features



General security improvements:

- “Secure-by-Default”, e.g., secured communication on PCN is enabled by default
- SIMATIC OpenPCS 7: Possibility to use advanced encryption and digital signature algorithms for OPC UA communication
- Release of an updated PCS 7 compendium part F in accordance to the security improvement

Key Benefits



Continuous improvement of the SIMATIC PCS 7 security.

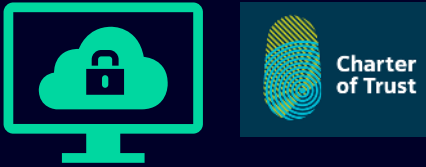
SIMATIC PCS neo Cyber Security



SIMATIC PCS neo – Industrial Security

... in a nutshell

State-of-the-art security is already an integrated part of SIMATIC PCS neo – Right from the start



The functions which are required for the system are securely preconfigured (secure by default) – According to Charter of Trust, principles 3



Only the necessary functions are installed (least functionality)



Users and applications have only as many rights as they actually require for their tasks (least privilege)

... because all these measures are implemented, Defense-in-Depth can be implemented consistently

System integrity

...provided by SIMATIC PCS neo

Authentication & access protection

Provides control, overview and easy administration of access to the system



- Central user management with SIMATIC PCS neo User Management Component
- Possible integration in Windows Active Directory user management
- Single Sign on for all SIMATIC PCS neo servers
- Possibility to define the user rights on each SIMATIC PCS neo object
- Two Factor Authentication (2FA)
- Users and applications have only as many rights as they actually require for their tasks (Least Privilege)

System hardening

The **secure by default** configuration of SIMATIC PCS neo helps to harden the system



- Due to the modularity of PCS neo, unused functions are deactivated/not installed, existing functions are secure configured (secure by default)
- No additional installation on web clients required, no data stored locally on web clients
- Secure configuration and hardening guideline for SIMATIC PCS neo
- Integrity and Authenticity protection of SIMATIC PCS neo software with digital signature
- Additional Whitelisting software with configuration guide



System integrity

Recognize and avoid attacks

Patch Management

Provides an overview about current patch level



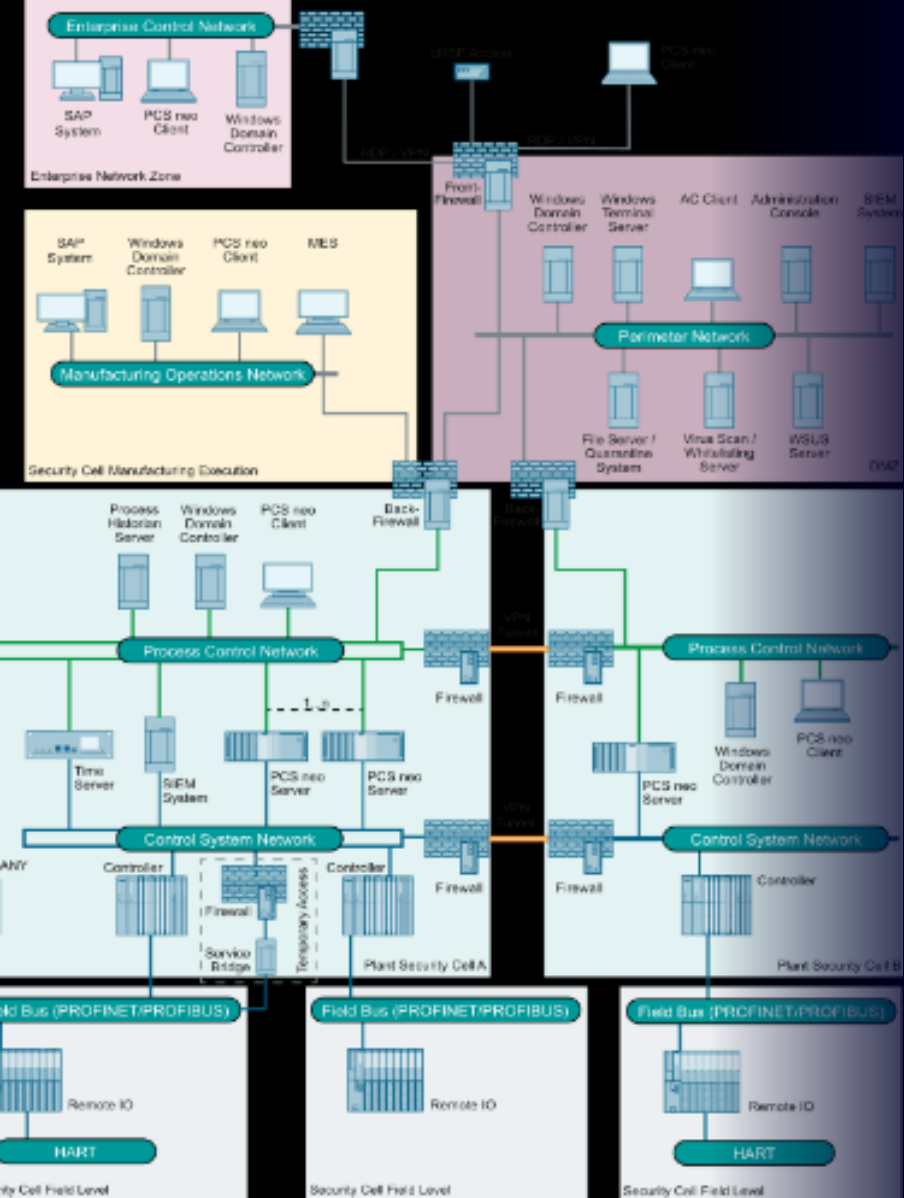
- SIMATIC PCS neo integrated central patch management with Administration Console allows to fix security vulnerabilities “quickly and without effort”
- Use of Windows Server Update Services (WSUS) for installation and management of Microsoft updates which are compatibility tested with SIMATIC PCS neo

Detection of attacks

Early detection of attacks allows to take countermeasures and reduces the potential damage



- Integrated generation of security events on all SIMATIC PCS neo systems allows an early detection of attacks
- SIMATIC PCS neo generates security events for a SIEM system
- Additional protection with support of optional systems like Security Information and Event Management (SIEM), Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
- Compatibility tested with antivirus software, application whitelisting and next generation firewall



Network Security

Network cells, Firewalls and VPN

Separation in network cells

SIMATIC PCS neo is designed to operate in separated network cells which is made possible by simple cross-firewall communication

The communication within and across network cells, e.g. between PCS neo servers and clients, is secured by using HTTPS.

Multiple firewall layers

- Front firewall to control and restrict the data exchange with the office network
- Perimeter network (DMZ) to allow service and support access to the plant with controlled and restricted data exchange with the process control network
- On every host Windows firewall automatically configured by SIMATIC PCS neo

Virtual Private Network (VPN) as a solution for manipulation protection, e.g. when transferring data via untrusted networks.

PCS neo provides proven add-on partner products which are tested on compatibility.



Plant Security

Industrial Security cannot be put into effect by technical measures alone but has to be actively applied in all relevant company units as a continuous process.

SIMATIC PCS neo supports this!

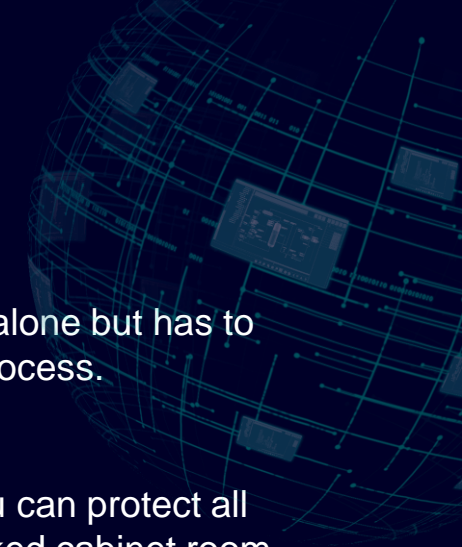
Thanks to the usage of web clients in a web-based architecture you can protect all critical components like server and controller in a separate and locked cabinet room (**physical access protection**).

SIMATIC PCS neo provides security related events which are used for regular evaluation and incorporated into a **holistic security monitoring**.

The provided SIMATIC PCS neo security documentation supports with the planning of a plant, operation and maintenance.

Based on that, plant individual guidelines can be elaborated and implemented in a continuous process (**processes and guidelines**) to ensure the security within a complete plant lifecycle.

SIMATIC PCS neo facilitates an overall plant security with its web-based architecture and a comprehensive security documentation.



Security Certifications



Industrial Security

Granted certificates

Development process

- Certification of “Secure Product Development Lifecycle” for Siemens Digital Industries based on IEC 62443-4-1

Find more information:

<https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security/certification-standards.html>



S7- 1500 Controllers SCALANCE XM408-8C

- First security level certification (CSPN – Certification de Sécurité de Premier Niveau)

Find more information:

http://ssi.gouv.fr/certification_cspn/simatic-s7-1518-4-version-du-micrologiciel-1-83/,
http://www.ssi.gouv.fr/entreprise/certification_cspn/scalance-xm408-8c



Industrial Security – Certification based on IEC 62443-4-1 of development processes for industrial products of Siemens

Siemens



Security by design



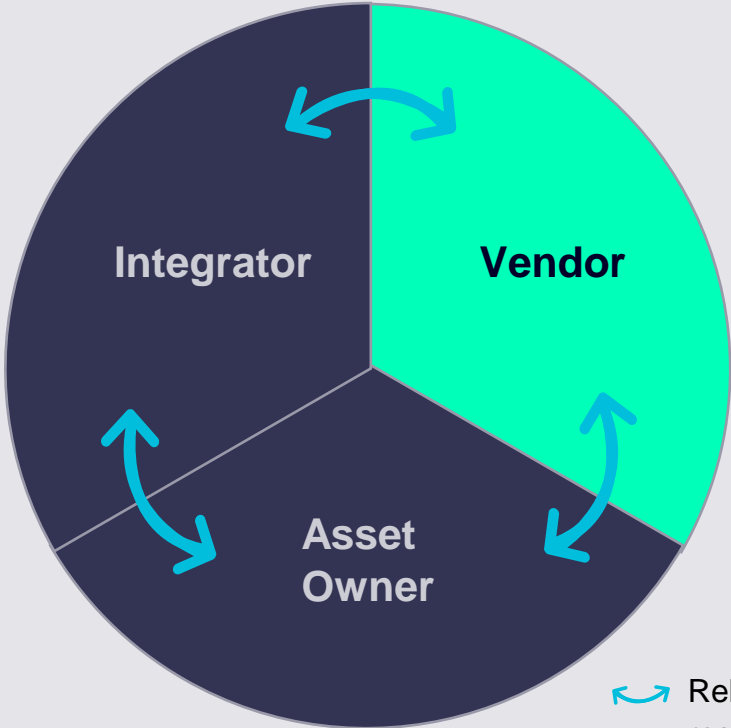
Security verification and validation testing



Security update management



Stakeholders according to IEC 62443



Industrial Security

Certification for the process control system SIMATIC PCS 7

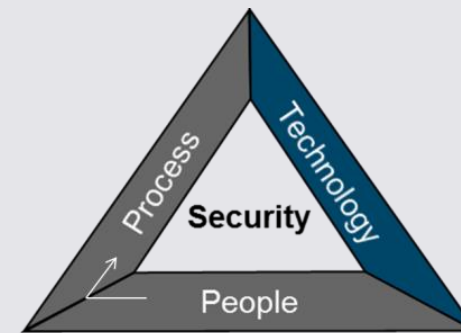
First product certification according to IEC 62443

TÜV SÜD certifies that the SIMATIC PCS 7 process control system conforms with the security standards IEC 62443-4-1 and IEC 62443-3-3



Highlights

- With this certificate, the company documents its security approach to automation products, and gives integrators and operators a transparent insight into its industrial security measures.
- The process control system offers comprehensive security measures and functions to protect plant operation



4-1

Product Development Lifecycle of SIMATIC PCS 7

3-3

Functional security capabilities of SIMATIC PCS 7

Security law for Critical Infrastructure Protection (CIP) in Germany

Industries

Part 1:

- Energy
- Water, wastewater
- Food
- Information technology and telecommunications

Part 2:

- Health
- Transport and transportation
- Finance and insurance industry, media and culture

All sites with 500,000 or more customers are affected

1 Mandatory reporting requirements

- Mandatory reporting requirements related to the Federal Office for Information Security for IT security incidents
- Including the requirement to establish a point of contact with the Federal Office for Information Security
- Fines up to EUR 50,000

2 Minimum standards for IT security

- Minimum standards are currently being worked out
- Compliance with the minimum standards will be regularly reviewed by the Federal Office for Information Security
- Fines up to EUR 100,000

Siemens proposal

Industrial Security Monitoring

→ Continuous security monitoring of facilities



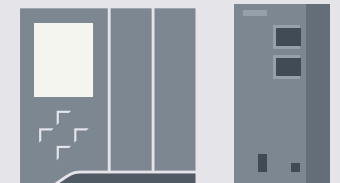
Assess security

→ Security status and development of a security timetable



Security integrated portfolio

→ Implementation of the minimum standards to reduce costs



Integrated engineering

→ Efficient implementation in the automation project



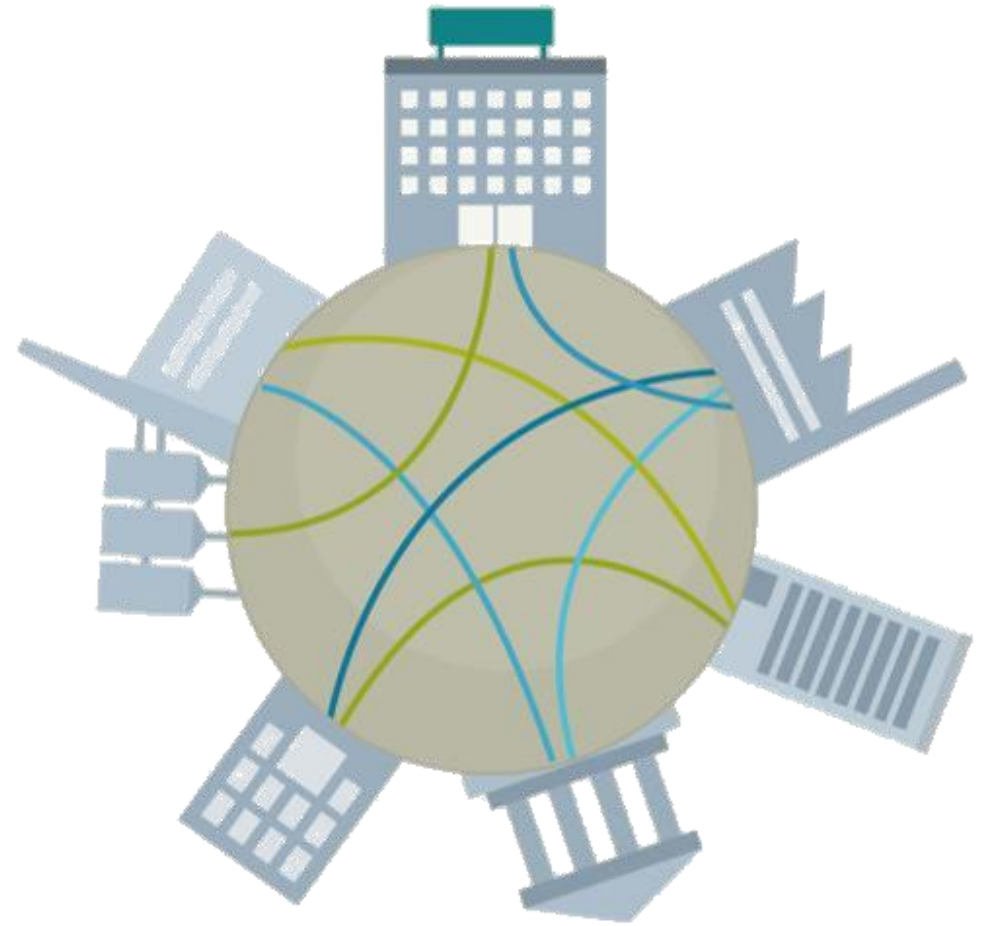
Siemens Initiatives to enhance Security for products



Industrial Security

Security-related expertise

- We collaborate intensively with **CERT organizations** (e.g. FIRST, ANSSI, and ICS-CERT)
- We are member of the **Software Assurance Forum for Excellence in Code** (SAFECode)
- We maintain partnership with **Security researchers** around the world



Industrial Security

Security concepts for industry

- Siemens brings its experience into the relevant **committees**
- Siemens **internal security measures** are based upon the requirements set by **IEC 62443**
- We offer **specific security solutions** for the manufacturing and process industry



Industrial Security

Security of Siemens Products

- We do **product design** for fundamental system hardening
- We adapted **PLM, SCM, and CRM** processes to fulfil **IEC 62443** requirements
- We do 3rd party product **certifications**



Industrial Security

Security in Siemens Production

- We defined a **Holistic Security Concept** (HSC) on the basis of IEC 62443
- We protect the **integrity** and safeguard the **confidentiality** of the manufacturing using HSC
- We monitor HSC measures in **development and production departments**



Security Vulnerability Handling



Industrial Security

Security Vulnerability Handling

- We created a sophisticated **team of security experts** and Product Computer Emergency Response Team (ProductCERT)
- We maintain **open communication** with customers
- We make advisories and **updates** available on a public website



Siemens Vulnerability Handling and Disclosure Process

Handling of Security Vulnerabilities in Siemens Products

Reporting of Vulnerabilities

To report a security vulnerability affecting a Siemens product, solution or infrastructure component, please contact Siemens CERT (contact information, see below). Siemens usually responds to incoming reports within one business day (reference: Munich, Germany).

Everyone is encouraged to report discovered vulnerabilities, regardless of service contracts or product lifecycle status. Siemens urges reporting parties to perform a coordinated disclosure, as immediate public disclosure causes a 'zero-day situation' which puts Siemens' customer systems at unnecessary risk.



How to find Information about Security Incidents?

Security advisories are official statements

Security Publications

Siemens Security Advisories

Siemens ProductCERT investigates all reports of security issues and publishes Security Advisories for validated security vulnerabilities that directly involve Siemens products and require applying an update, performing an upgrade, or other customer action. As part of the ongoing effort to help operators manage security risks and help keep systems protected, Siemens ProductCERT discloses the required information necessary for operators to assess the impact of a security vulnerability.

SSA-232418	5.3	Vulnerabilities in SIMATIC S7-1200 and SIMATIC S7-1500 CPU families		V1.0	2019-08-13	PDF TXT
SSA-307392	7.5	Denial-of-Service in OPC UA in Industrial Products		V1.3	2019-07-09	PDF TXT
SSA-254686	7.9	Foreshadow / L1 Terminal Fault Vulnerabilities in Industrial Products		V1.5	2019-06-11	PDF TXT
SSA-179516	5.9	OpenSSL Vulnerability in Industrial Products		V1.5	2019-04-09	PDF TXT

<https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications>

Subscribe to Security Advisories

Subscriptions

Stay Informed

Follow us on Twitter, register to our advisory mailing list, or subscribe to our RSS feeds to stay informed with Siemens ProductCERT. Our Twitter handle is @ProductCERT. Register to our advisory mailing list and we will notify you via email on newly released or updated Security Advisories:

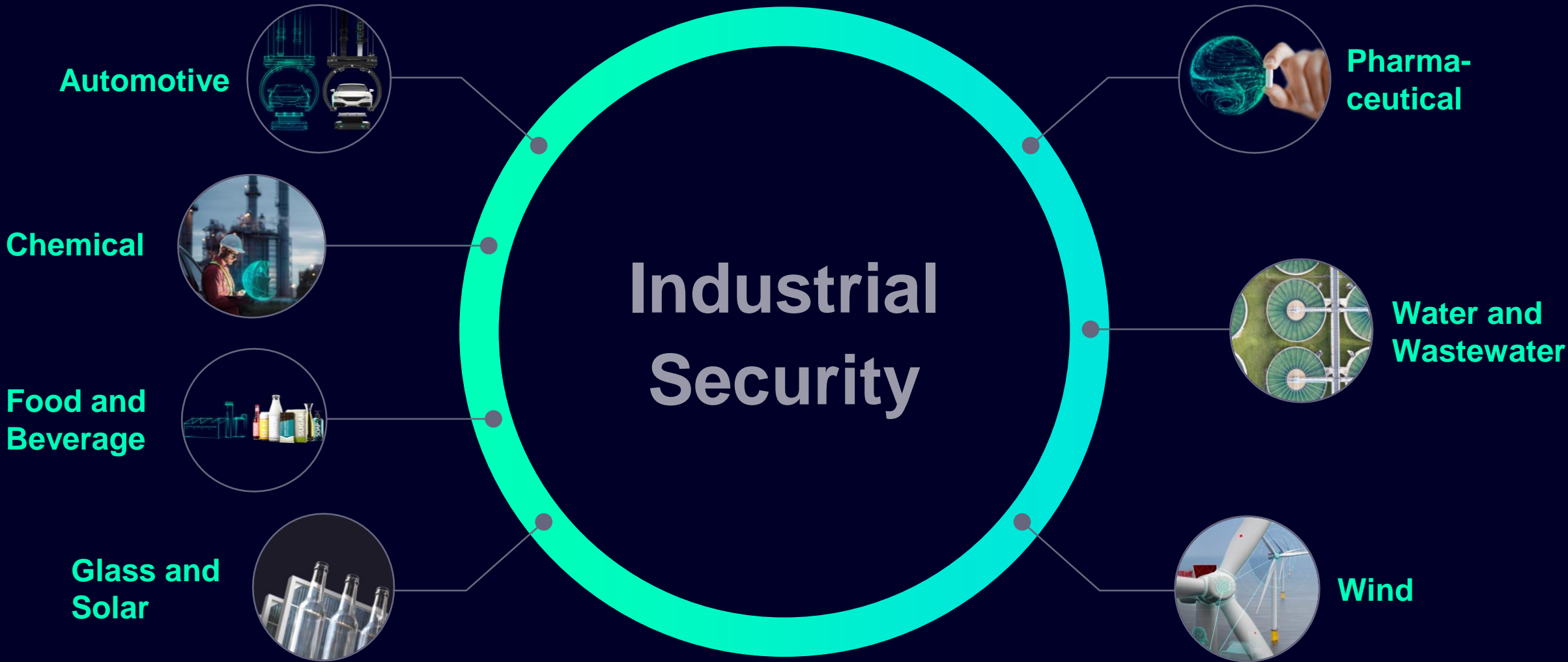
<https://new.siemens.com/global/en/products/services/cert.html#Subscriptions>

Security concepts for Industries



Industrial Security

Siemens Vertical Expertise



Industrial Security

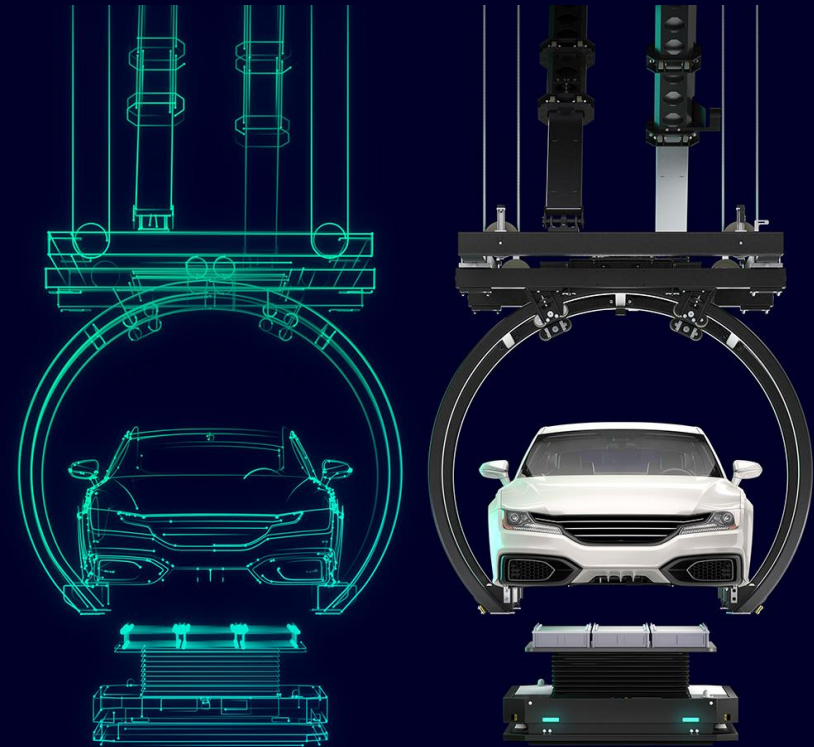
Siemens Vertical Expertise: Automotive

Chemical Environment

- High degree of Automation
- Horizontal and Vertical Integration
- Different Machine Suppliers
- Real-time Communication

Industrial Security provides

- Secured Plant Uptime
- Segmented and Monitored Communication
- Secure Remote Access
- Real-time Communication in Secure Cell Concept



Industrial Security to keep your plant running securely

Industrial Security

Siemens Vertical Expertise: Chemical

Chemical Environment

- Chemical Environment
- Production Flexibility
- Operational Efficiency
- Product Quality

Industrial Security provides

- Increased Plant Availability
- Secure User Access



Industrial Security to keep your plant running securely

Industrial Security

Siemens Vertical Expertise: Food and Beverage

Food and Beverage Environment

- High Quality and Hygiene Standards
- Strong Regulation through FDA and Others
- High Integration of MES and ERP Systems
- Highly 'Confidential Recipes'
- Consistent Traceability through whole Production Process

Industrial Security provides

- Secured Traceability through Production
- Secure Vertical Integration of Software
- Secured Plant Uptime
- Segmented and Monitored Communication



Industrial Security to keep your plant running securely

Industrial Security

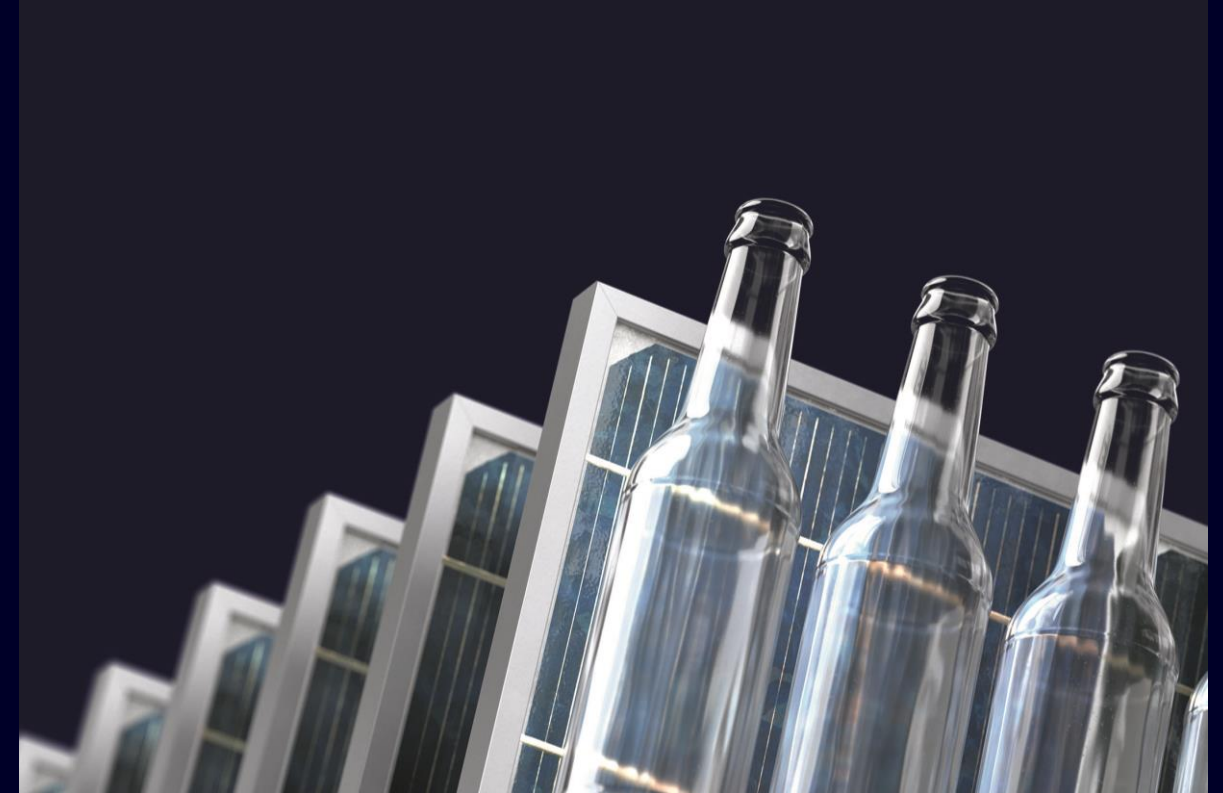
Siemens Vertical Expertise: VSS Glass and Solar

Glass and Solar Environment

- Cost Effective Production Processes
- Horizontal and Vertical Integration of Production
- Different Machine Suppliers
- Hybrid Processes in Production

Industrial Security provides

- Secured Plant Availability
- Sophisticated Malware Detection
- Secure Remote Access
- Real-time Communication in Secure Cell Concept



Industrial Security to keep your plant running securely

Industrial Security

Siemens Vertical Expertise: Pharmaceutical

Pharmaceutical Environment

- Product Quality
- Reduced Time-to-Market
- Production Flexibility
- Different Equipment Suppliers
- Meeting Regulations (FDA)

Industrial Security provides

- Increased Plant Availability
- Secure User Access
- Secure Plant Communications



Industrial Security to keep your plant running securely

Industrial Security

Siemens Vertical Expertise: Water and Wastewater

Water and Wastewater Environment

- Efficiency
- Reliability & Plant Availability
- Investment Protection
- Regulations for critical infrastructure

Industrial Security provides

- Increased Plant Uptime
- Secure User Access
- Fulfillment of security laws



Industrial Security to keep your plant running securely

Summary



Our offering: Industrial Security

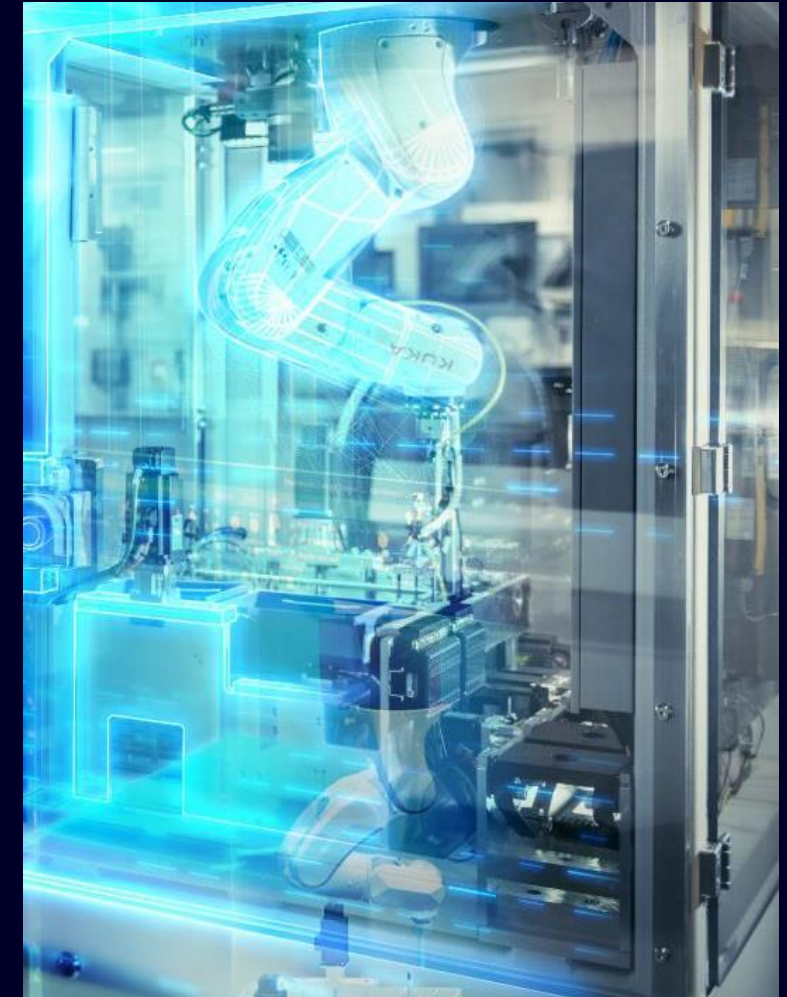
Your benefit: Risk down, ready for Digitalization

Holistic Security concept provides comprehensive protection

Cybersecurity has become crucial for the success of the digital economy. Increasing threats and risks affect Industrial production plants and require effective Security measures. Avoiding Security Incidents means saving money, protecting sensitive data and intellectual property as well as preventing damage for people, machines and reputation.

As complete vendor of automation systems, Siemens offers also a comprehensive portfolio with Security products and services to implement a holistic Security concept, which provides appropriate protection for industrial plants and enables Digitalization at full scale.

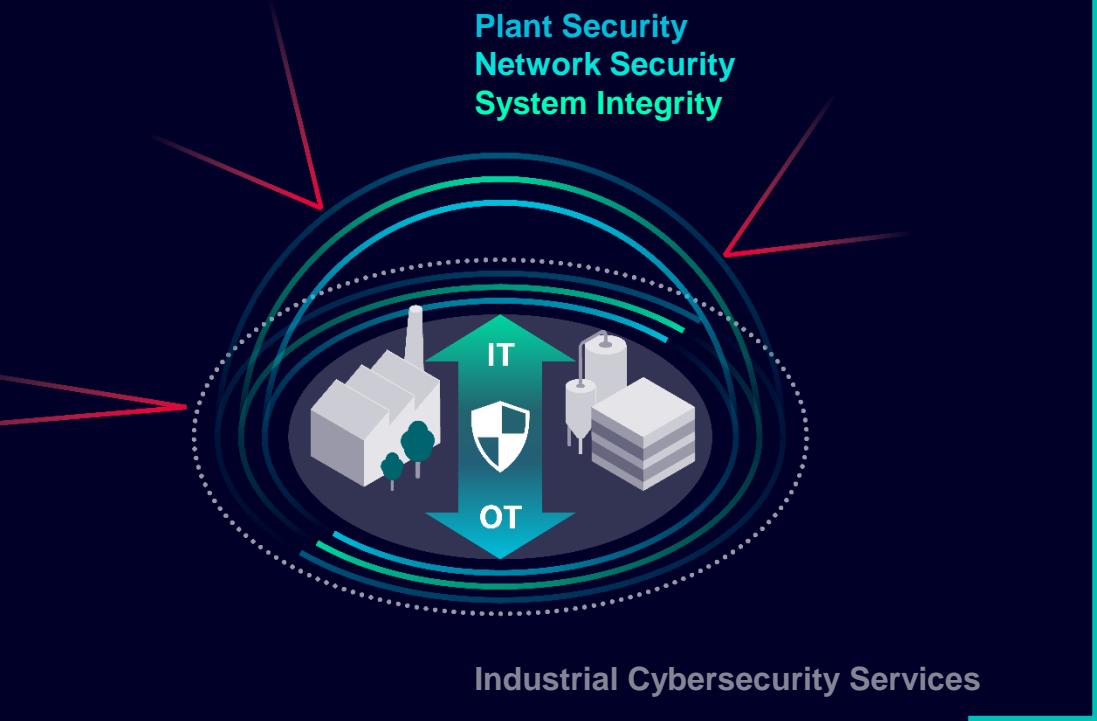
Plant Security	<ul style="list-style-type: none">• Includes Processes and Guidelines, physical access protection and Security Monitoring, supported by Cybersecurity Services
Network Security	<ul style="list-style-type: none">• Protection of Industrial communication and networks against unauthorized access with Industrial Firewalls and Appliances
System-integrity	<ul style="list-style-type: none">• Integrated Security functionalities in automation systems protecting access and data
Defense-in-depth	<ul style="list-style-type: none">• Holistic approach based on different Security layer to mitigate the risks and increase the protection level
Industrial Security	<ul style="list-style-type: none">• Cybersecurity for Industry, which meet the specific requirements in OT, automation systems and production plants



Cybersecurity for Industry: Offering from Siemens

Defense in Depth

based on IEC 62443



Siemens products and systems offer integrated security



Know-how and copy protection



Authentication and user management



Firewall and VPN



System hardening, continuous monitoring and anomaly detection

Siemens Industrial Cybersecurity Services

- Transparency about the current security status
- Increased security level by closing security gaps
- Long-term protection through continuous security management



Siemens is your reliable partner to drive secure digitalization

We are the automation experts with specific industry know-how



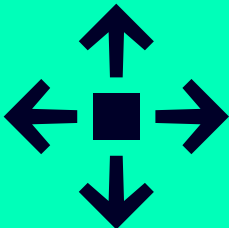
We drive digitalization



We understand industrial security



We offer state-of-the-art technology and end-to-end services from a single source



Our processes and products are proven and certified



“We make sure that you can focus on your core business.”

Attachment: Security Trainings



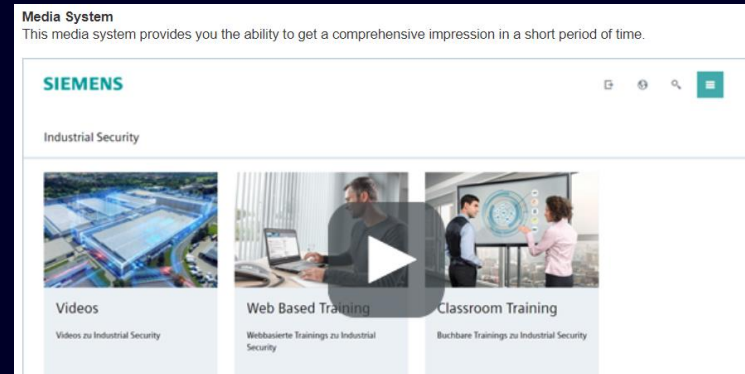
Industrial Security Trainings

Industrial Security Information Center

Entry Associated product(s)

This media system provides you with comprehensive, visually appealing information with numerous general and technical videos of Industrial Security.

- [Industrial Security Information Center](#)
Web based & classroom trainings (EN)
- [V17 News Workshop in Saba](#)
- [SSP Webinar V17 Security](#)



Contacts



Industrial Security

Support & Service for Industrial Security

Information about Industrial Security

www: <http://www.siemens.com/industrialsecurity>

E-mail: industrialsecurity.i@siemens.com



SIMATIC System Presales Support Factory Automation

E-mail: simatic.industry@siemens.com

Phone: +49 (911) 895-4646



SIMATIC System Presales Support Process Automation

E-mail: pcs7.industry@siemens.com

Phone: +49 (721) 595-7117



Industrial Security

Support & Service for Industrial Security

SIMATIC NET support for Network Security

Email presales.ci.industry@siemens.com

Phone: +49 (911) 895-2905



Customer Support

www: <http://support.automation.siemens.com>

Phone: +49 (911) 895-7222



Industrial Security

Security Information

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

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

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

For additional information on industrial security measures that may be implemented, please visit <https://www.siemens.com/industrialsecurity>.

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

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under <https://www.siemens.com/industrialsecurity>.

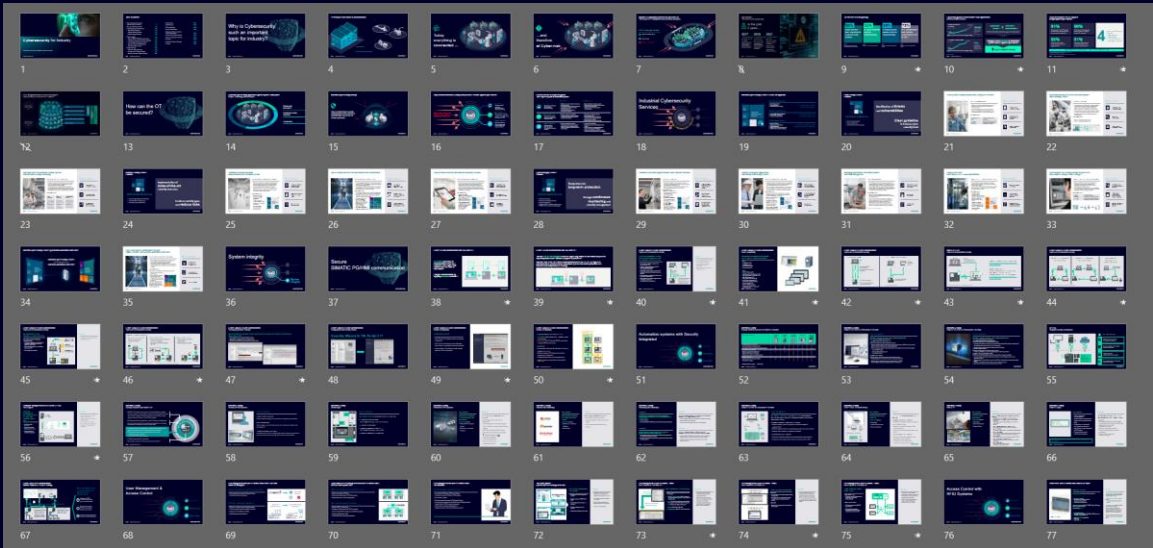
Usage recommendation

Recommendations for usage:

This slide deck contain a comprehensive overview concerning Industrial Security topics including a security portfolio overview, use cases, concepts and many other information. These slides can be used for Siemens presentations by choosing the specific needed slides individually from this slide deck.



Individually used slides



Technical slide deck

Disclaimer

© Siemens 2024

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations may be trademarks or other rights of Siemens AG, its affiliated companies or other companies whose use by third parties for their own purposes could violate the rights of the respective owner.

Contact

Published by Siemens AG

First name Last name

Job title

Group / Region / Department XY

Street 123

12345 City

Country

Phone +49 123 45 67 89

Mobile +49 123 45 67 89 0

E-mail firstname.lastname@siemens.com