



# Cybersecurity for Industry Operational Guidelines

Version 2.2



## Operational Guidelines

---

Operational Guidelines provide recommendations to general security measures for the secure operation of plant and machinery in industrial environments.

Based on these, machine builders and system integrators can evaluate their systems accordingly and apply improvements if necessary.

# Contents

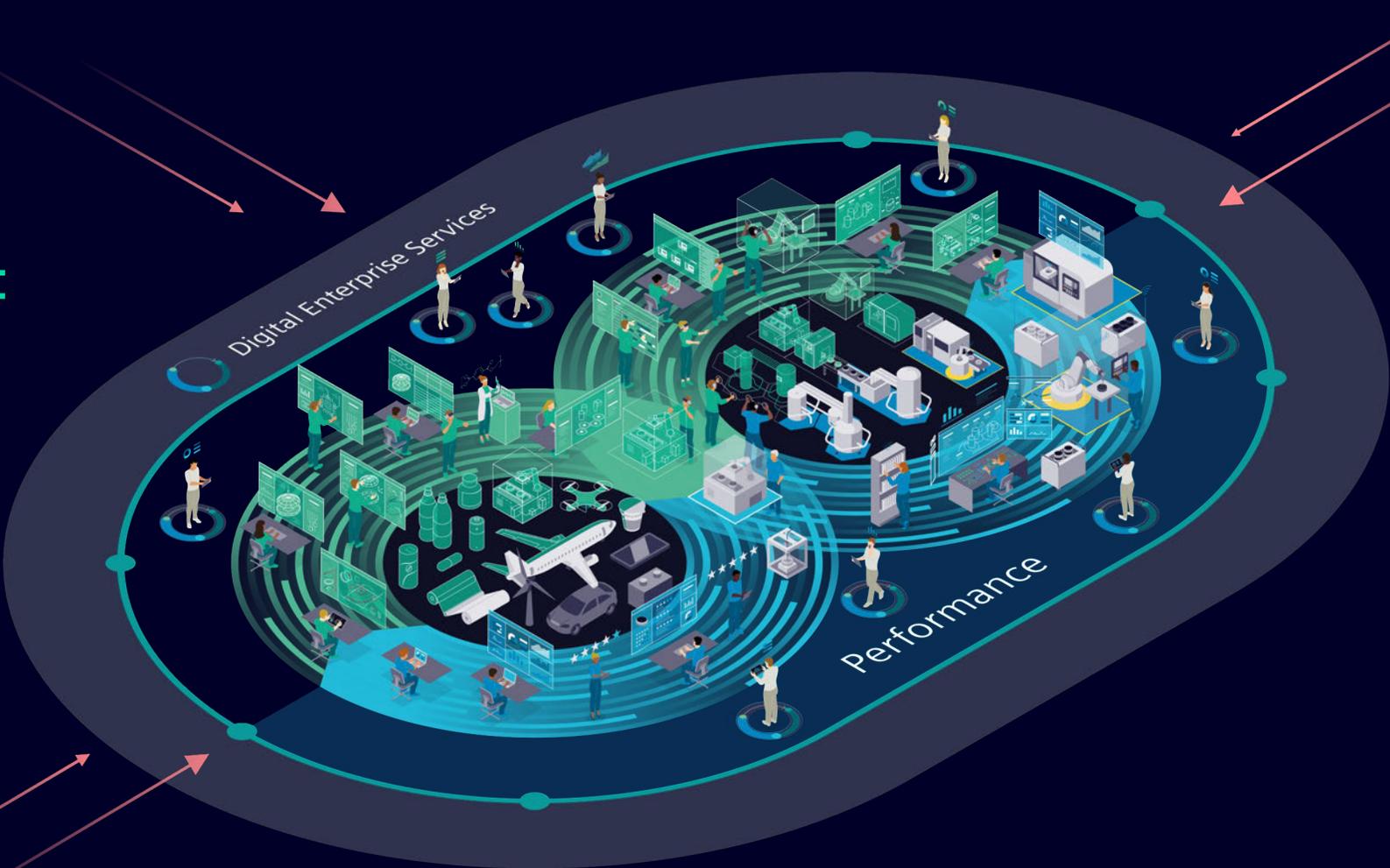
<b>1</b>	<b>Overview</b>	<b>3</b>
<b>2</b>	Risk Analysis	10
<b>3</b>	Security Concept: Defense-in-Depth	12
	• Plant Security	15
	• Network Security	20
	• System Integrity	31
<b>4</b>	Validation and Improvement	44
<b>5</b>	Summary	47

# Machines & automation systems are part of the IoT

That means OT / IT integration at all levels

## OT / IT convergence means:

- 👍 More networking
- 👍 More data
- 👎 New cyber risks!



# Industrial Security

## Risk in industrial automation

### Information technologies are used in industrial automation

- Horizontal and Vertical integration



- Open standards
- PC-based systems



### Increased security threats demand actions to avoid

- Loss of intellectual property, recipes ...
- Plant standstill, e.g. due to viruses or malware
- Sabotage in the production plant
- Manipulation of data or application software
- Unauthorized use of system functions
- Noncompliance with standards and regulations

→ Establishment of security measures required – according to the individual risks

# Protection goals & value added aspects

## Protecting productivity through risk minimization



**Secure Availability, Integrity and Confidentiality at reasonable risk.**

# Industrial Security works only with cooperation between plant operators, system integrators and component manufacturers

## IEC 62443 – Standard for Industrial Security



## Roles

**Product vendor:**  
 Products (Components, Systems) with integrated and configurable security features

**System integrator:**  
 Secure configuration and Integration of products into the entire system

**Plant operator:**  
 Security Management, incl. Maintenance and update of security functionality according to changing circumstances (e.g. new known security vulnerabilities, changes of topology of networks, etc.)

# Only a holistic Industrial Cybersecurity concept can be effective against cyber-threats

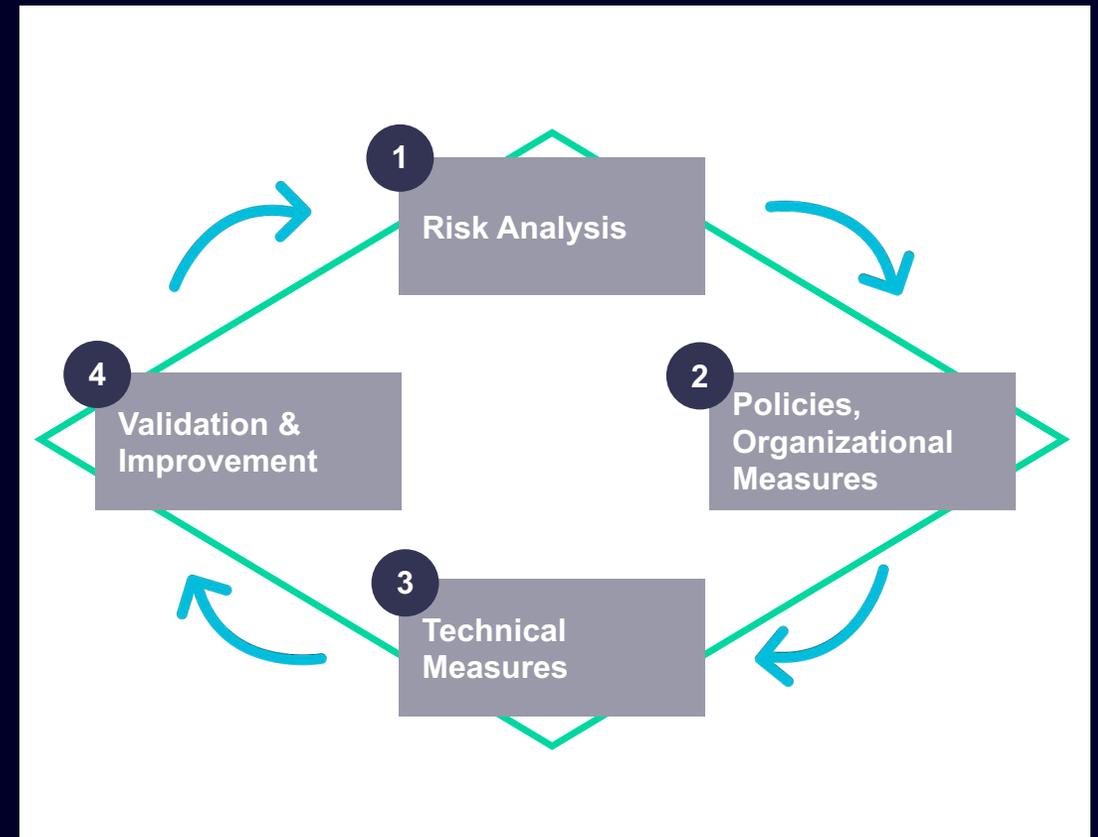


Security solutions in an industrial context must take account of all protection levels.

# Security measures in a plant must be continuously checked and realigned

## Security Management Process

- Security Management forms a **major part of any Industrial Security concept**.
- Definition of Security measures **depending on hazards and risks identified in the plant**.
- Attaining and maintaining the necessary Security Level calls for a rigorous and **continuous Security Management** process with:
  - Risk analysis including definition of countermeasures aimed at reducing the risk to an acceptable level
  - Coordinated organizational / technical measures
  - Regular / event-driven repetition
- Products, systems and processes must meet applicable duty-of-care requirements, based on laws, standards, internal guidelines and the state of the art.



# Contents

<b>1</b>	Overview	3
<b>2</b>	<b>Risk Analysis</b>	<b>10</b>
<b>3</b>	Security Concept: Defense-in-Depth	12
	• Plant Security	15
	• Network Security	20
	• System Integrity	31
<b>4</b>	Validation and Improvement	44
<b>5</b>	Summary	47

# Risk analysis is the first step to determine security measures

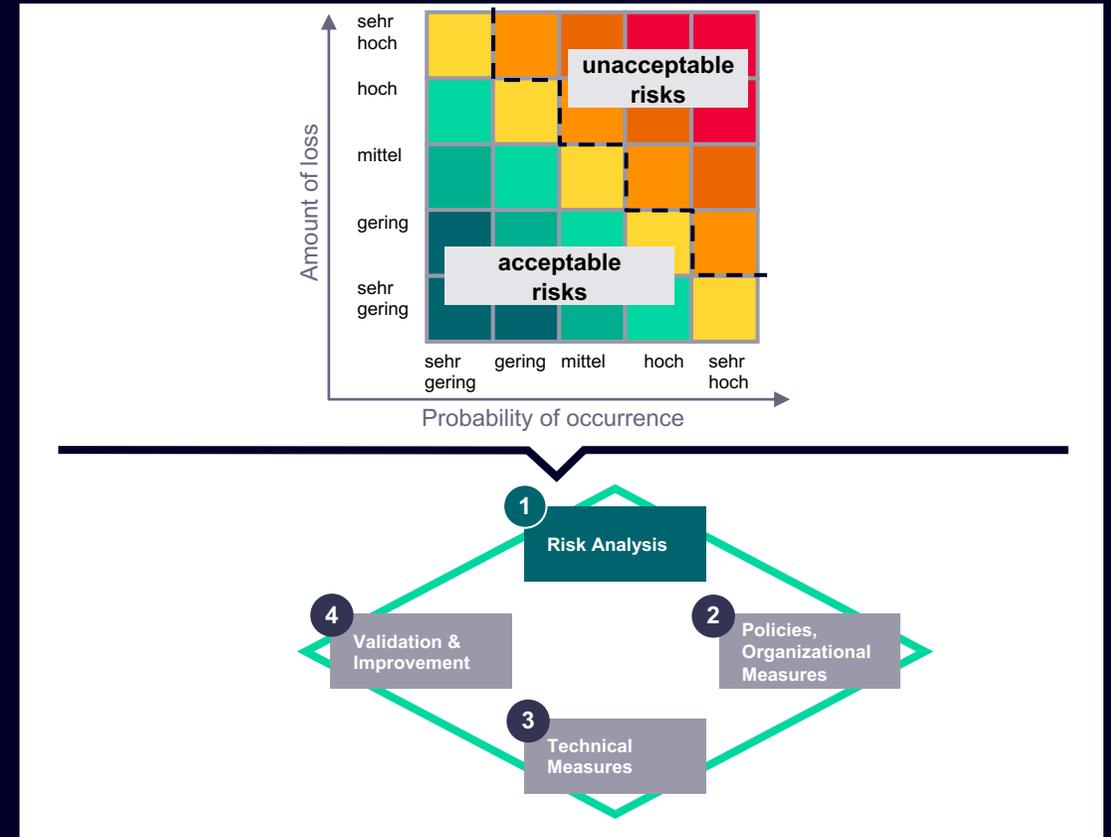
The risk analysis is an important precondition for Security Management relating to a plant or machine, aimed at identifying and assessing individual hazards and risks.

## Typical content of a risk analysis

- Identification of threatened objects
- Analysis of value and damage potential
- Threat and weak points analysis
- Identification of existing security measures
- Risk assessment

The identified and unacceptable risks must be ruled out or reduced by applying compensating measures.

Which risks are ultimately acceptable can only be specified individually for the application concerned.



**However, neither a single measure nor a combination of measures can guarantee absolute security.**

# Contents

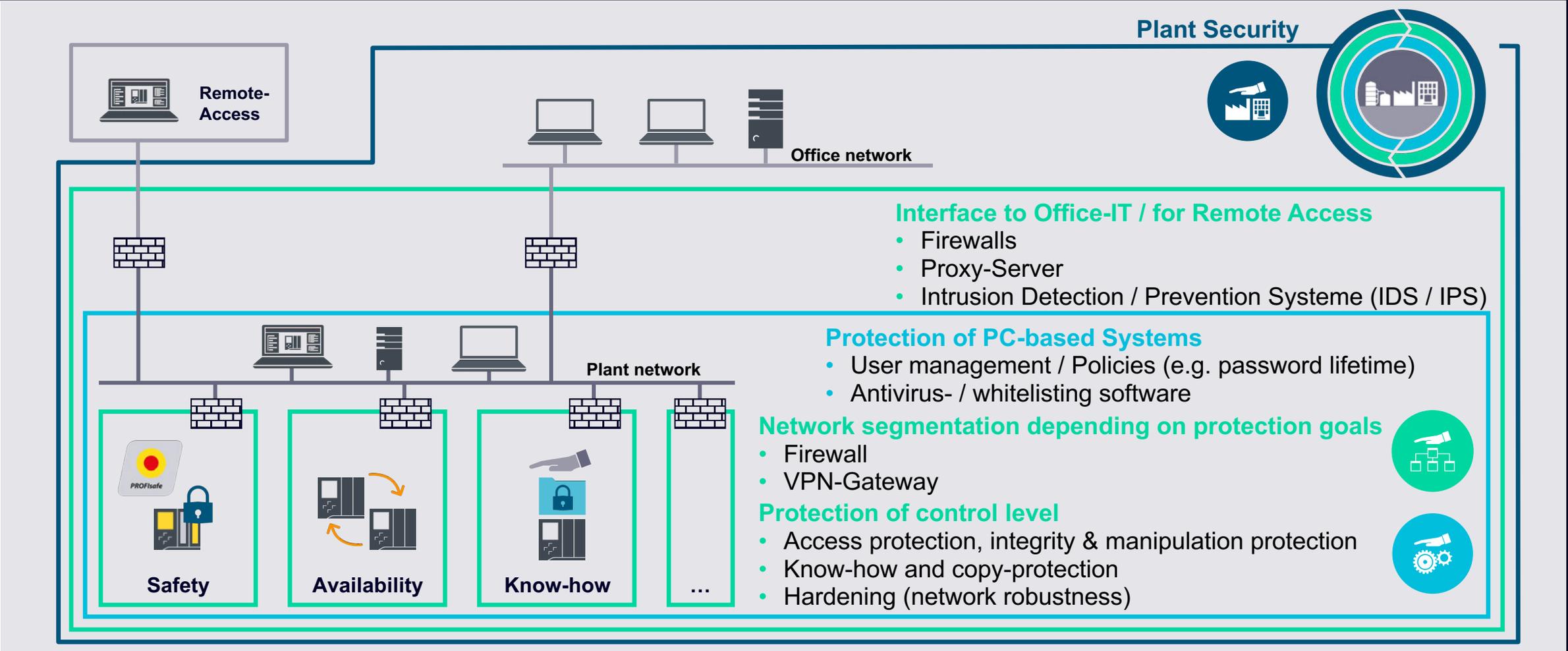
<b>1</b>	Overview	3
<b>2</b>	Risk Analysis	10
<b>3</b>	<b>Security Concept: Defense-in-Depth</b>	<b>12</b>
	• Plant Security	15
	• Network Security	20
	• System Integrity	31
<b>4</b>	Validation and Improvement	44
<b>5</b>	Summary	47

# Only a holistic Industrial Cybersecurity concept can be effective against cyber-threats



Security solutions in an industrial context must take account of all protection levels.

# Defense-in-Depth security architecture to protect automated production plants



# Contents

<b>1</b>	Overview	3
<b>2</b>	Risk Analysis	10
<b>3</b>	Security Concept: Defense-in-Depth	12
	• <b>Plant Security</b>	<b>15</b>
	• Network Security	20
	• System Integrity	31
<b>4</b>	Validation and Improvement	44
<b>5</b>	Summary	47

# Plant Security

## Establishing Security in the organization

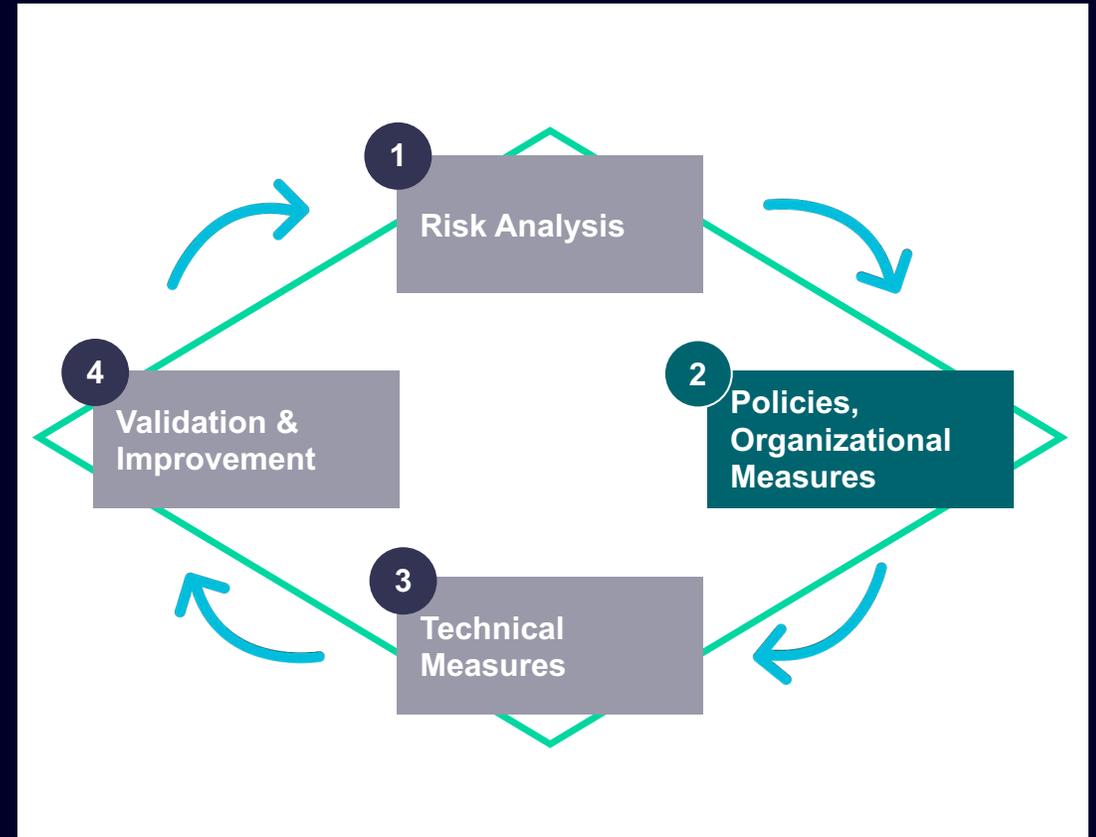
Industrial Security cannot be put into effect by technical measures alone, but has to be actively applied in all relevant company units as a continuous process.

### Industrial Security as a management duty

- Support for Industrial Security by Senior Management
- Clearly defined and agreed responsibilities for Industrial Security, IT Security and physical security in the company
- Establishing a cross-disciplinary organization / network with responsibility for all Industrial Security affairs

### Enhancing Security awareness

- Drafting and regular holding of training programs for production-related Security topics
- Security assessments with Social Engineering aspects



# Plant Security

## Policies and Processes

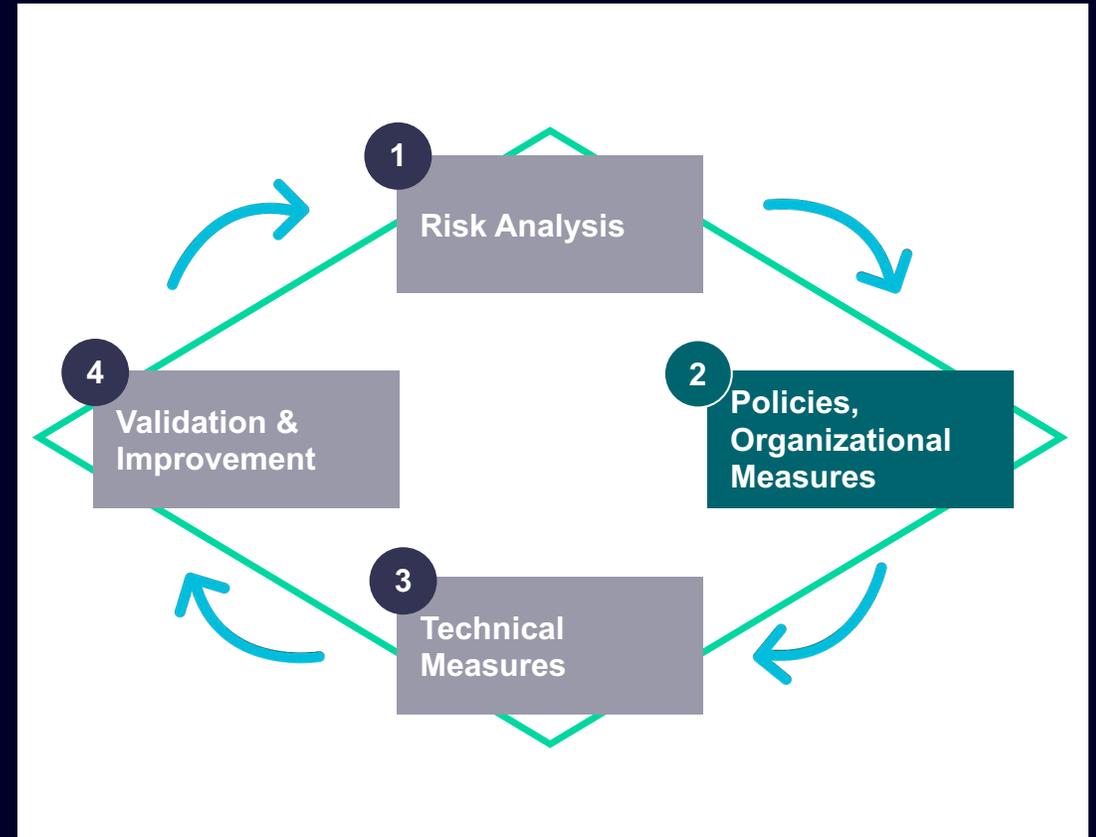
Policies and processes must be defined to ensure a uniform procedure and to uphold the Industrial Security concept.

### Examples of Security-relevant policies

- Uniform stipulations for acceptable Security risks
- Reporting mechanisms for unusual activities and events
- Communication and documentation of Security incidents
- Use of mobile PCs and data storage in the production area (e.g. forbidding their use outside this area / the production network)
- Policies for suppliers of products, solutions or services

### Examples of Security-relevant processes

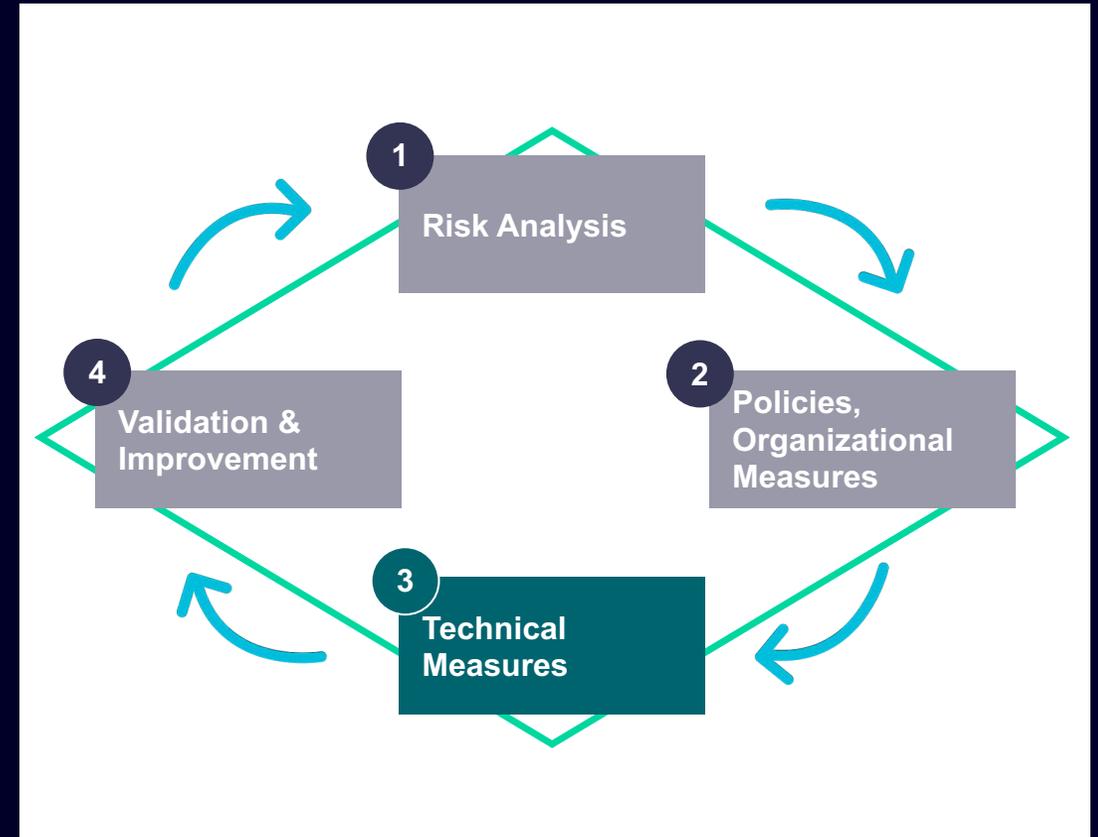
- Dealing with known / corrected weak points in components used
- Procedure in the event of Security incidents (Incident Response Plan)
- Procedure for restoring production systems after Security incidents
- Recording and evaluation of Security events and configuration changes
- Test / inspection procedure for external data carriers before use in the production area



# Plant Security

## Physical access protection of critical production facilities

- Measures and processes to prevent access by unauthorized persons to the plant
- Physical separation of various production areas with differentiated access authorizations
- Physical access protection for critical automation components (e.g. locked control cabinets)
- Coordinated guidelines for physical security and plant IT security required



### Risks

- Access by unauthorized persons to production premises / building
- Physical damage to or changing of production equipment
- Loss of confidential information through espionage

### Measures

#### Company Security

- Company premises fenced off and under surveillance
- Access controls incl. logging, locks / ID card readers and / or security staff
- Visitors / external personnel escorted by company staff

#### Physical production security

- Restricted production areas with limited access
- Critical components in securely lockable control cubicles / rooms including surveillance and alarm facilities

# Contents

<b>1</b>	Overview	3
<b>2</b>	Risk Analysis	10
<b>3</b>	Security Concept: Defense-in-Depth	12
	• Plant Security	15
	• <b>Network Security</b>	<b>20</b>
	• System Integrity	31
<b>4</b>	Validation and Improvement	44
<b>5</b>	Summary	47

# Network Security

## Secure network design for protection of automation systems

Continuous communication from control to field level is more important than ever, reflected in current trends such as digital twin or industrial IoT. However, complete connectivity presents higher levels of risk, which have to be addressed with security measures:

### Separation between production and office networks

- Secure access via demilitarized zone

### Usage of cell protection concept

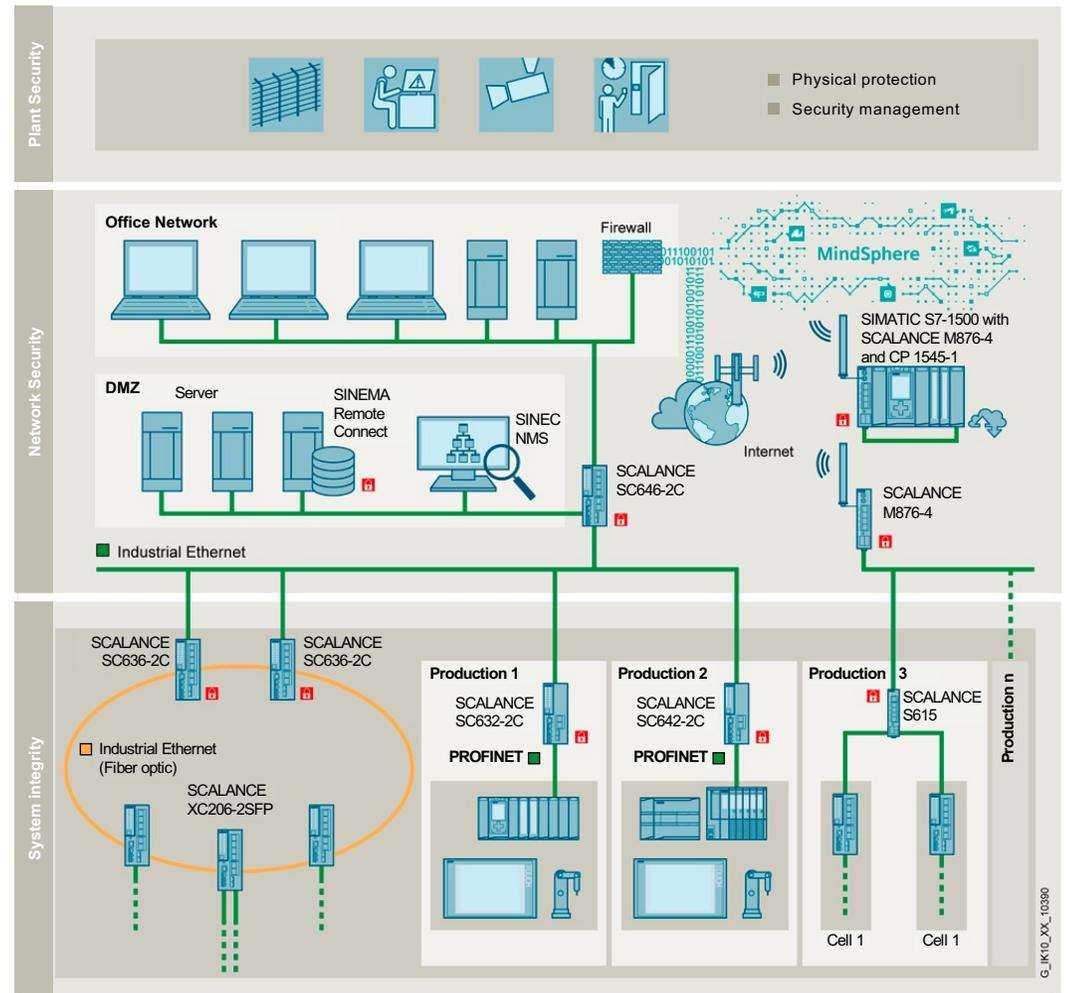
- Segmentation of production in protected cells

### Secured remote control for service and maintenance

- Authenticated and authorized access

### Secured connection to cloud solutions

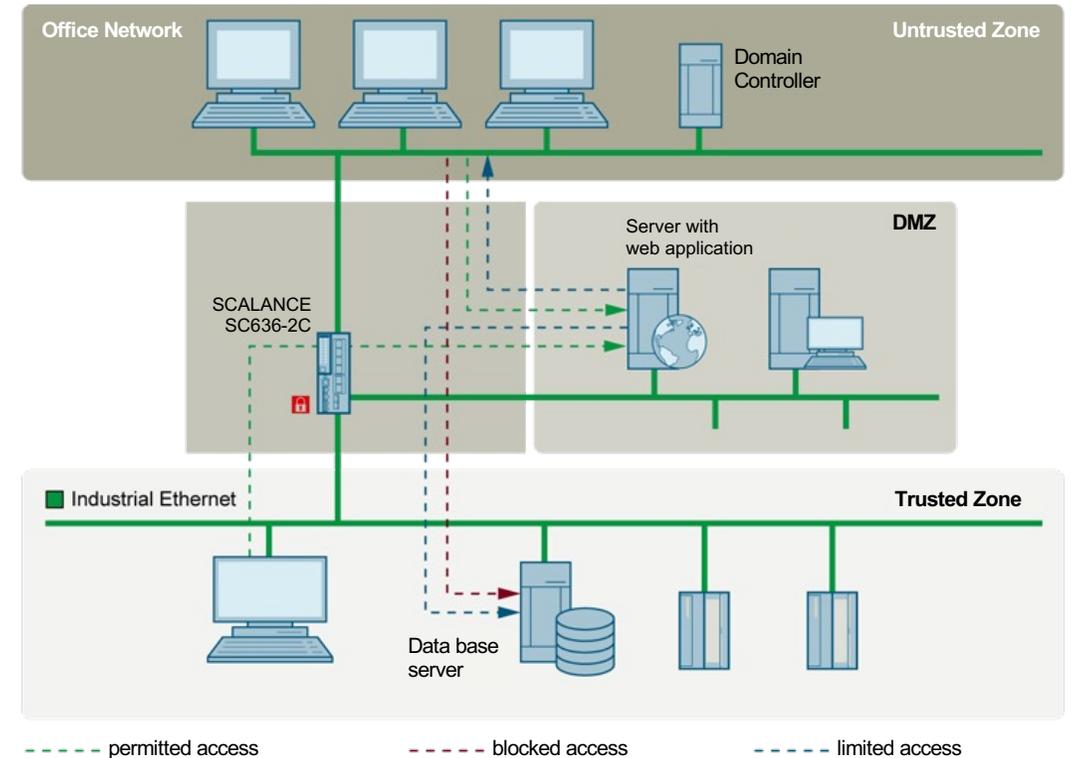
- Access protection and secured data transfer



# Network Security

## Separation of production and office networks

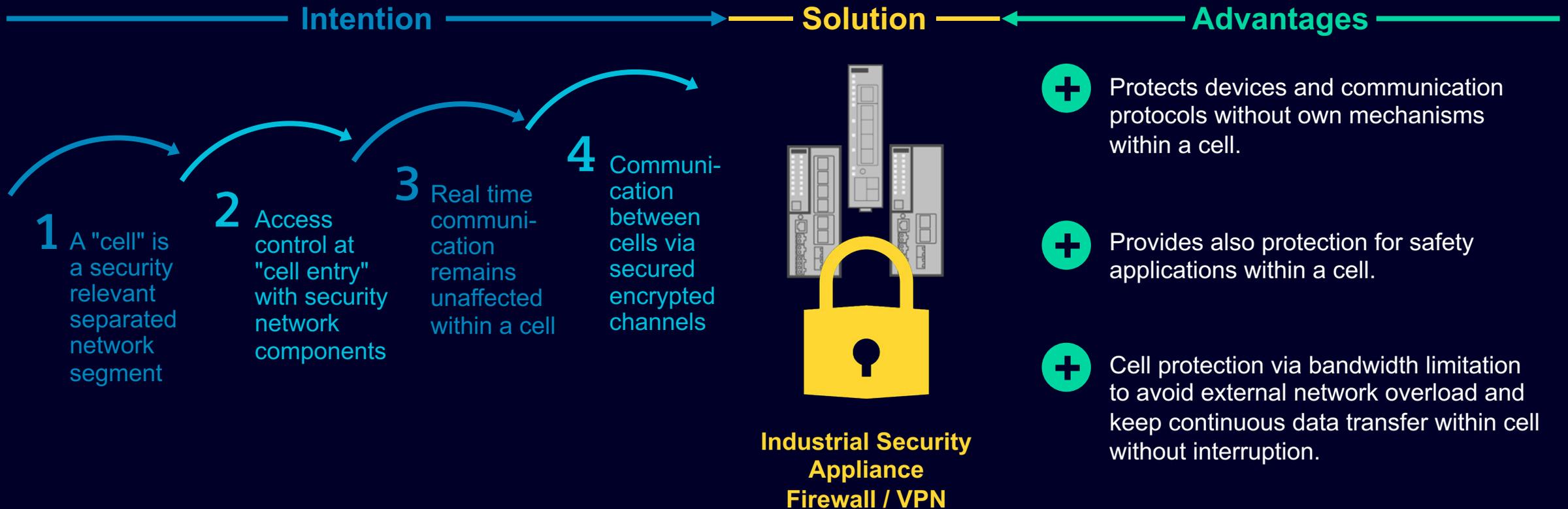
- The first step in network segmentation is strict separation between the production networks and the other company networks
- In the simplest case, separation is provided by means of a single firewall system that controls and regulates communication between the networks
- In the more secure variant, the link is realized via a separate network, the so called demilitarized zone (DMZ), respective perimeter network.
- Direct communication between the production and the company networks is completely blocked by firewalls; communication can take place only indirectly via servers in the DMZ network



# Network Security

## Usage of cell protection concept

Segmentation of production network into multiple secured automation system cells for protection of components against unauthorized access, network overload and other threats:



# Network Security

## Criteria for Network Segmentation

- With a cell protection concept a network segment **is protected from external** unauthorized access.
- Data transfer **within a cell is not controlled** by a Security Appliance and is assumed to be secure or complemented with protection measures within the cell.
- A cell contains only components with the **same protection requirements**.
- Network structure should be **derived from the production process**. This allows for the definition of cells with less communication across cell borders and with minimum firewall approvals.

## Recommendation for network size and network segmentation

---

- All devices of a PROFINET system belongs to a single cell
- Devices with a high rate of communication should be combined in a common cell
- External components that only communicate with devices in a single cell should be integrated into the cell if their protection requirements allow.
- Limit communication based on actual need  
→ „Need-to-connect“ principle

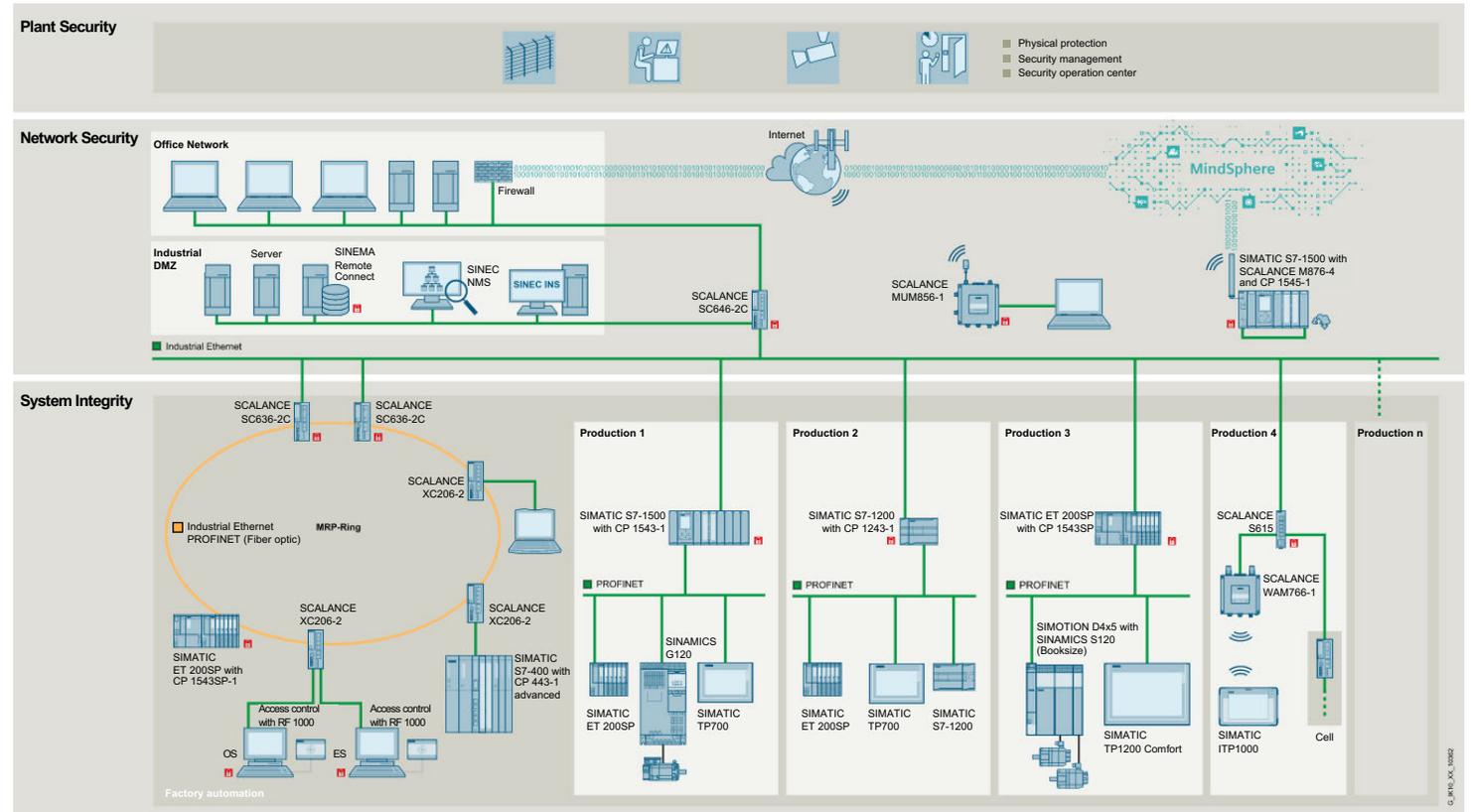
# Network Security

## Example: Network segmentation with Security Appliances

Alternatively or complementary to Industrial Security Appliances, SIMATIC S7 and PC Communication Processors (CP) can be used with **"Security Integrated"** functionality (firewall and VPN) for the protection of automated devices and cells.

S7 communication processors protect underlying networks by an **integrated firewall**.

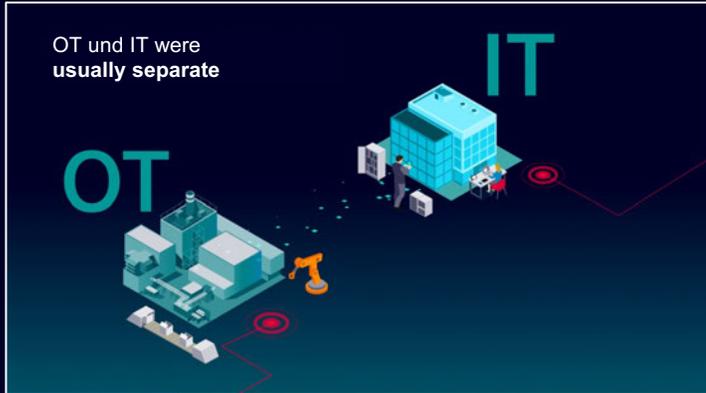
Additionally, **encrypted VPN connections** can be established directly to the SIMATIC S7-1200, S7-1500 or Distributed Controller ET 200SP.





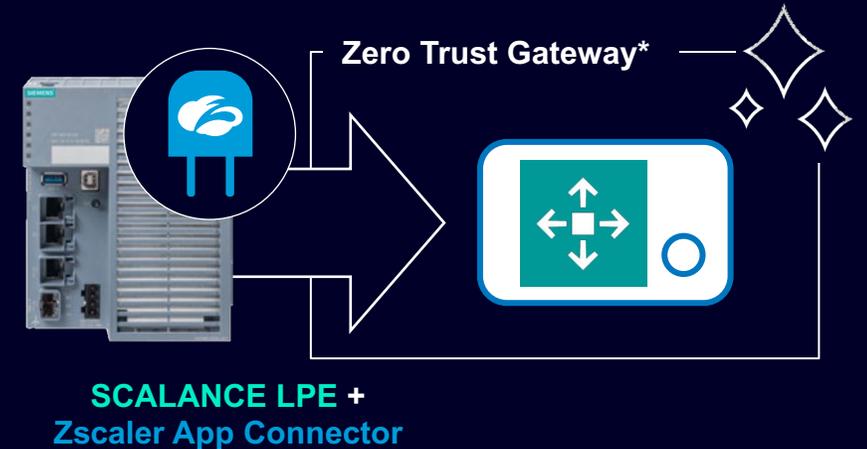
# Network Security

## Secure access to the OT area based on the Zero Trust Concept



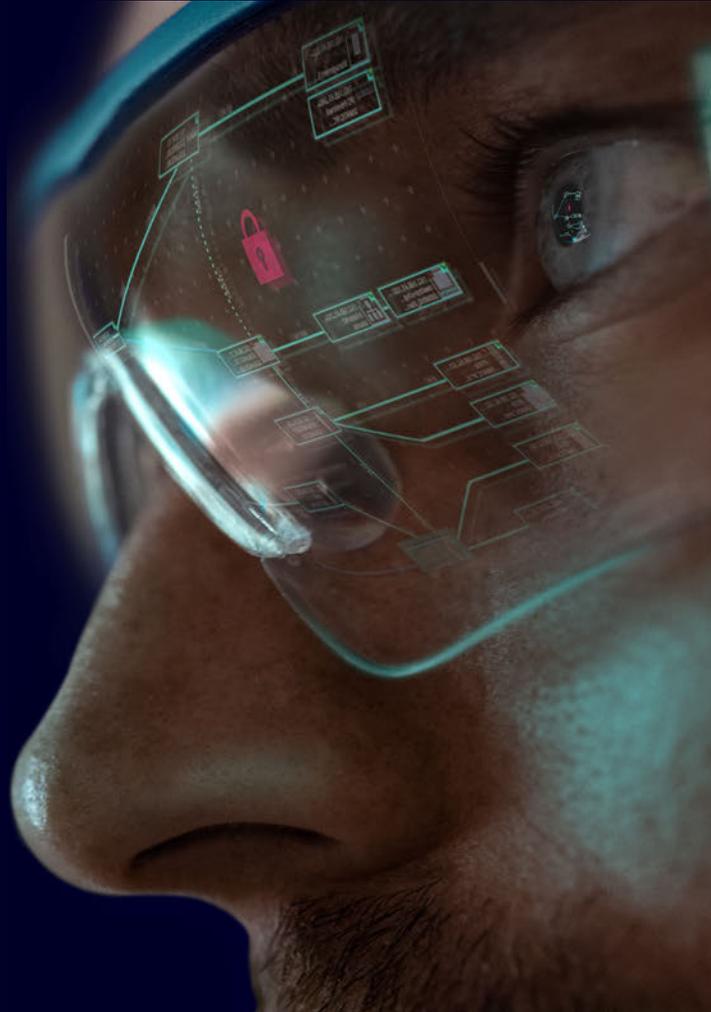
### OT / IT Collaboration

- Secure access with **one unified solution** for OT / IT collaboration that is centrally operated and managed
- Robust solution based on **Zero Trust** principles
- Application-based, device-specific access depending on assigned user rights enabling **secure and transparent access to the OT area**
- **Scalable and flexible** cloud-based solution **adaptable to existing networks** without the need to rip and replace
- Increased employee satisfaction by enabling **mobile working from anywhere**
- Cost optimization through access from office to shopfloor due to **central and holistic management of access policies for OT / IT**



# Network Security

## Benefits of Zero Trust with SCALANCE LPE hosting Zscaler Private Access



### Task

---

Provide access from inside or outside the customer's network to OT areas – even restricted ones – to the machine level without changing the current network infrastructure. Following the rules of IT regarding the Zero Trust Exchange.

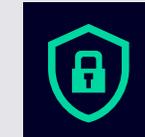
### Solution

---

- SCALANCE LPE hosting Zscaler application as solution for the OT with industrial environment conditions
- Simple Firewall configuration – exclusively utilizing outbound connections
- Application-based and device-specific access depending on assigned user rights
- Remote access to shopfloor without VPN tunnel mechanisms or jump host server for high transparency and reduced risk of, e.g. lateral movement

### Main value drivers

---



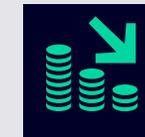
High data protection due to end-to-end encryption and customer owned identity provider

---



Immediate access to OT environment

---



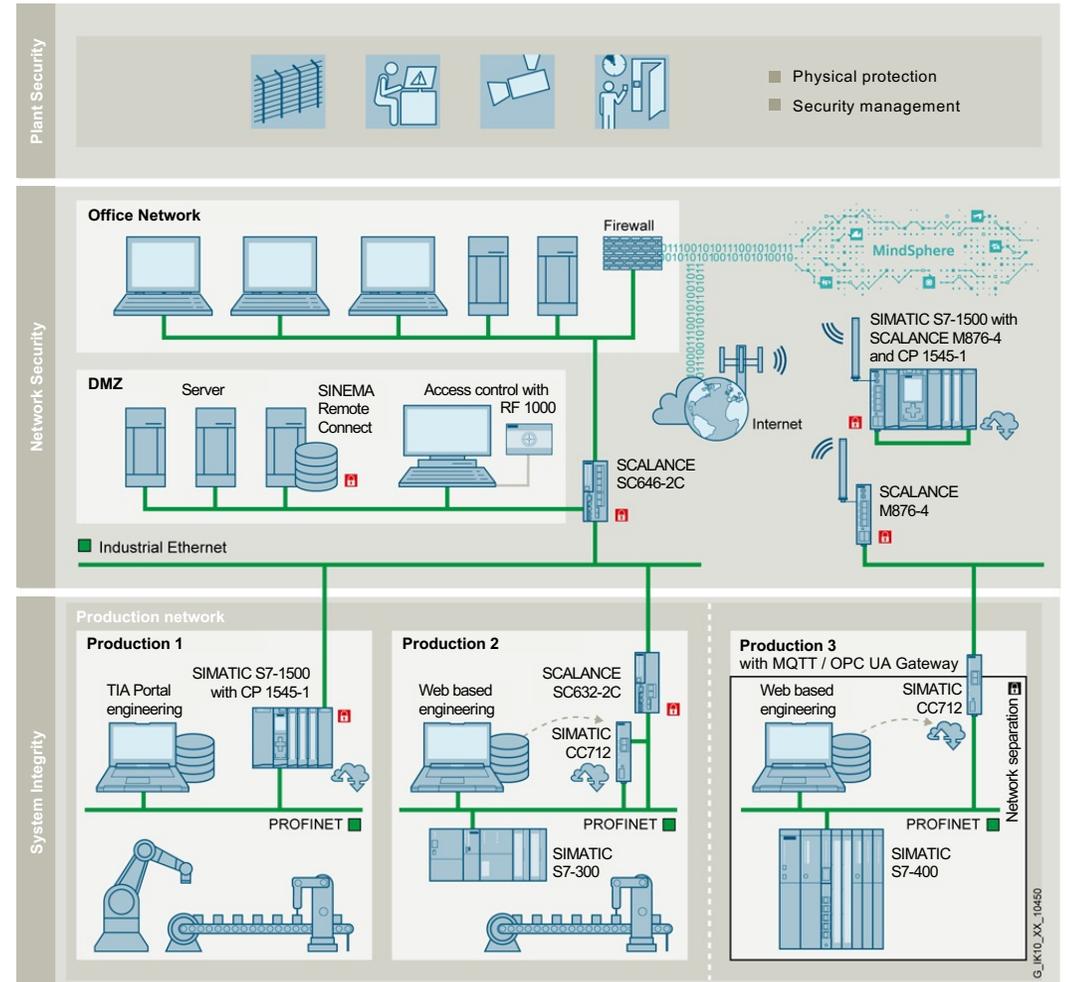
Cloud-based maintenance of security and access policies as well as scalable connectivity

# Network Security

## Secured Cloud Connection

- Only **TLS-based communication protocols**, such as HTTPS or MQTT over TLS, are recommended for device access and data transfer.
- **Authenticated devices and data access** via password or certificates should be used instead of anonymous access.
- Existing **network segmentation** and **cell protection concepts** via firewalls or network separation should be maintained.
- The IIoT gateway **SIMATIC CloudConnect 7** allows existing plants with PROFINET or PROFIBUS to be cloud connected.

Further information: [MindSphere Security Whitepaper](#)



# Network security

## Possible risks and recommended measures

### Risks

- Unauthorized access to automation devices without their own Security Mechanisms
- Deterioration in equipment availability due to network overload
- Espionage / manipulation of data transfer between automation systems

### Measures

- Division of the automation network into appropriate network segments and control of incoming and outgoing data traffic by a firewall (perimeter security). For example, critical network protocols can be blocked.
- Bandwidth restriction, for example in a cell firewall or in switches. Network overload from outside the cell cannot affect devices inside the cell.
- Data transfer via non-secure networks, e.g. between cells or from clients to cells, can be encrypted and authenticated with the Security or VPN Appliance that controls access to the cell.

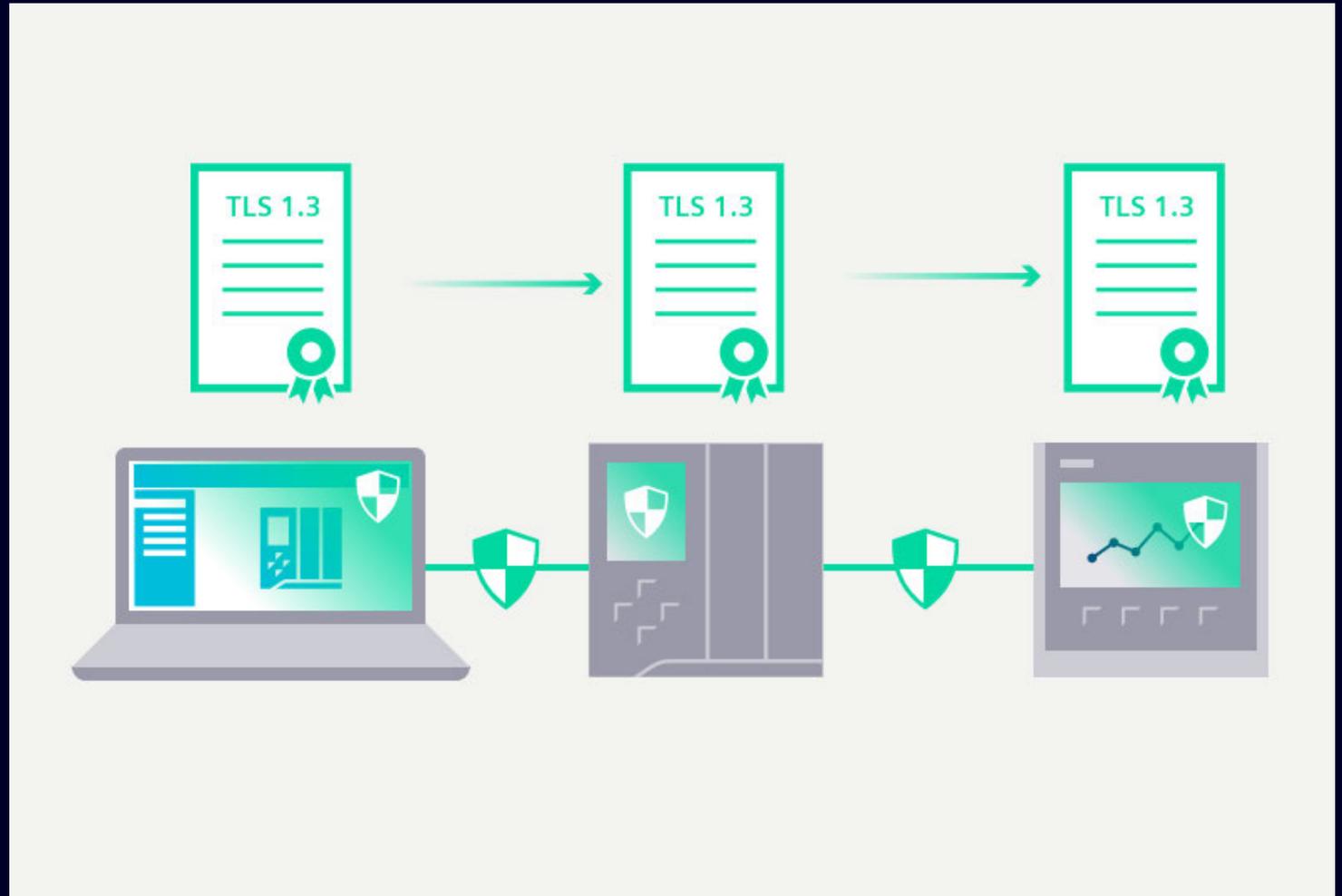
# Contents

<b>1</b>	Overview	3
<b>2</b>	Risk Analysis	10
<b>3</b>	Security Concept: Defense-in-Depth	12
	• Plant Security	15
	• Network Security	20
	• <b>System Integrity</b>	<b>31</b>
<b>4</b>	Validation and Improvement	44
<b>5</b>	Summary	47

# 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



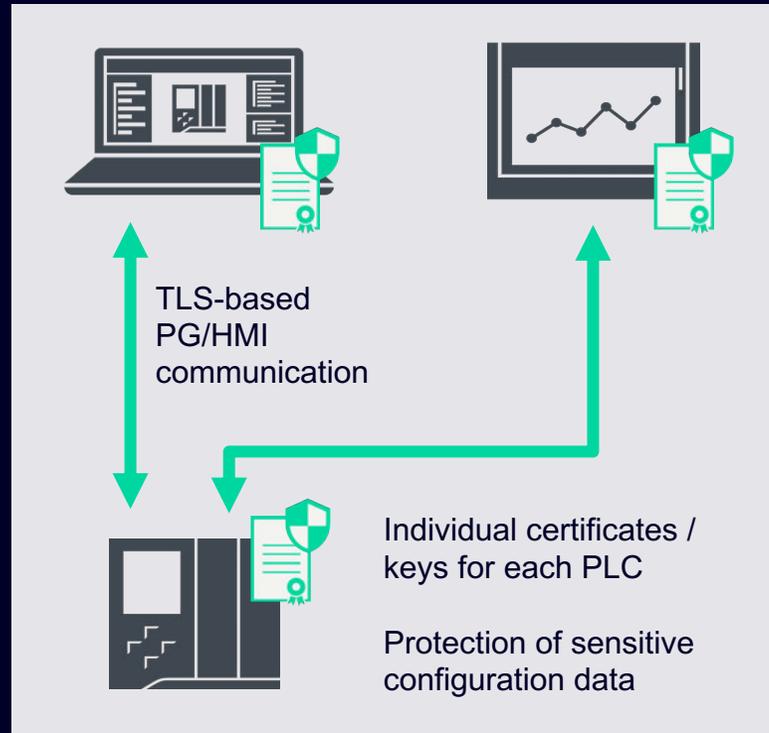
\*) TLS - Transport Layer Security

# Secure 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

# System Integrity

## Access protection for configuration (Engineering)

In order to prevent unauthorized configuration changes to automation components, it is highly recommended to make use of the **integrated access protection mechanisms**.

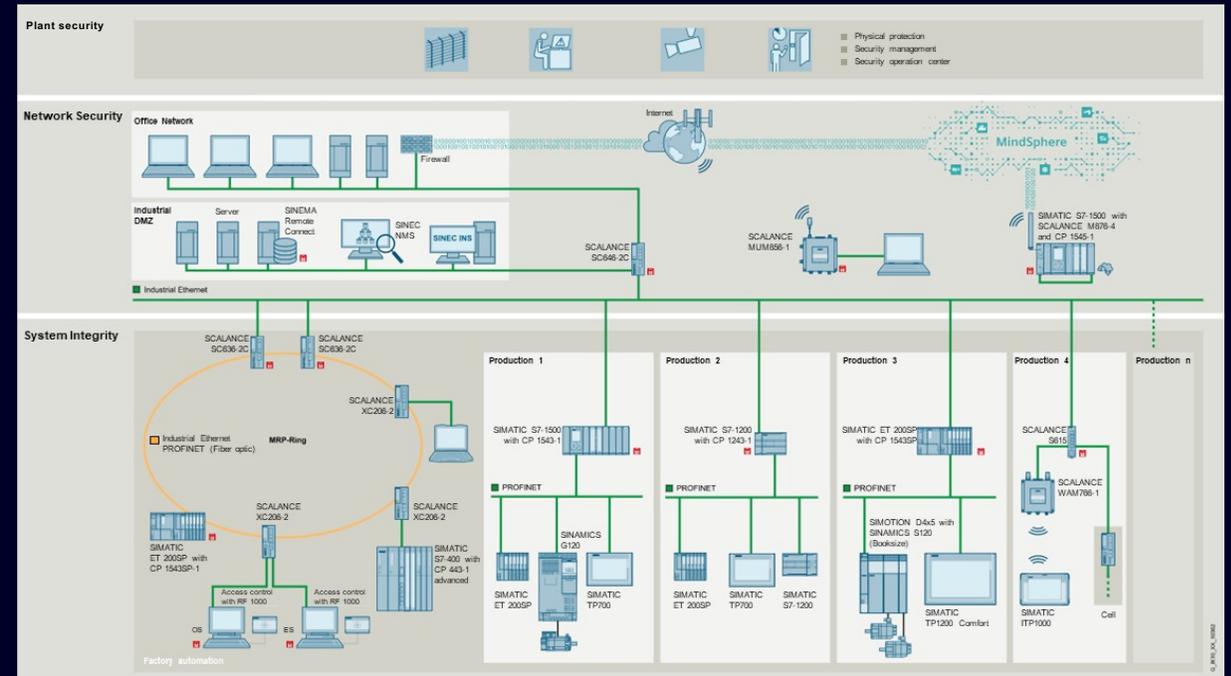
This includes for example:

- Firewalls (User authentication)
- WLAN Access Points (User authentication)
- Managed Switches (User authentication)
- HMI Panels (Access protection for device settings)
- PLCs (Protection levels for configuration and HMI access)
- Drives (Know-how protection).

Use of components with integrated security features such as the S7-1500 controller or SINUMERIK ONE

Use various passwords that are as secure as possible (if possible at least 12 upper- and lower-case characters, numbers and where applicable special characters)

For easier password handling a common password manager is recommended. In case of coordination among multiple persons this one should be stored on a central network share including access rights.



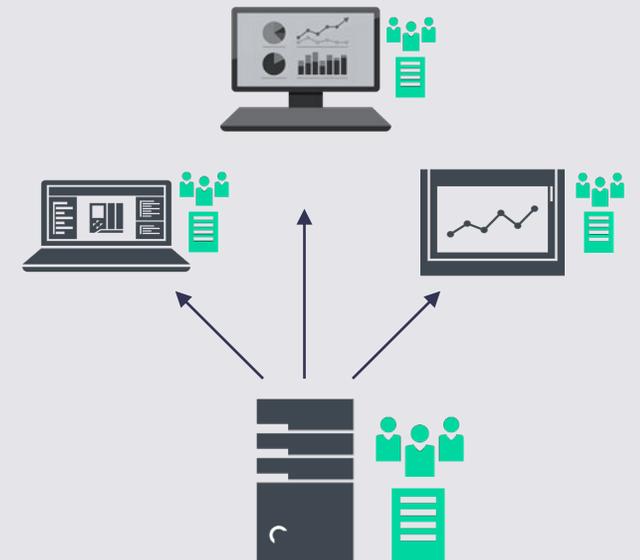
# System Integrity

## Access protection for operations (Runtime)

- Since a plant or machinery is usually operated by more than one person, central user administration is recommended.
- This is based on user accounts of a Windows domain or a Windows Active Directory. SIMATIC (HMI) runtime applications are connected via SIMATIC Logon or UMC.
- Specifying / enforcing security guidelines (e.g. password validity, monitoring of incorrect logging on, etc.)
- Central user administration simplifies regular review of access authorizations (e.g. identifying disused accounts)
- Independent Windows domains can be used to meet the security requirements of segregated networks.
- Depending on required roles (operator, administrator, etc.) user accounts can be restricted to the minimum required operating rights.

### Central administration of

- User accounts / groups
- Policies



## System Integrity

### Access protection for network components (Network)

#### Access protection for networks by means of

- Port Security with Switch Ports: MAC or IP access lists restrict access
- Port Security with central device administration and RADIUS authentication (802.1X)
- Perimeter security of a network in relation to other networks (e.g. Internet) with firewalls

#### WLAN-Security

- Safeguarding of data transfer in accordance with at least WPA2
- Advanced Encryption Standard (AES) for encoding data
- Central device administration with RADIUS authentication (in accordance with 802.1X)
- Protected configuration accesses via HTTPS web interface and SSH sessions

# System Integrity

## System hardening reduces possible attack scenarios

### Network Services

- Active network services are a potential security risk in general
- To minimize risks, only the services that are actually required should be activated on automation components.
- All activated services (especially Webserver, FTP, Remote Desktop, etc.) should be taken into account in the security concept
- Hardening measures (network robustness and security-by-default settings) in automation and drives products enhance security without the need for separate user configuration

### HW & System Interfaces

- Hardware interfaces constitute a risk if unauthorized access via them to equipment or the system is possible. Therefore unused interfaces should be deactivated:
  - USB, Ethernet/PROFINET ports
  - WLAN, Bluetooth, Mobile Comm.
- Protection by deactivation or at least mechanical blocking
- Deactivate booting and Autostart mechanisms of external media
- Activate access protection to BIOS- / UEFI settings
- Only use remote management, like AMT, in a secured manner

### User Accounts

- Every active user account enables access to the system and is thus a potential risk
- Reduce configured / activated user accounts to the minimum necessary
- Use secure access data for existing accounts
- Audit accounts, particularly locally configured user accounts, regularly

**Important:**  
If predefined default passwords are present, they must be changed during system commissioning!

## System Integrity

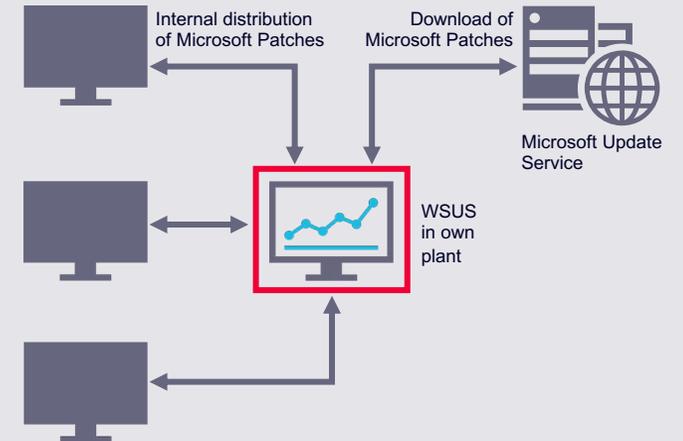
# Patch management fixes security vulnerabilities in operating system and applications

Many security attacks nowadays take place via weak points for which the manufacturers already have patches. Zero day exploits are encountered rarely, where the weak point is not yet known or updates are not available.

- The installation of patches and updates is an important measure to enhance security
- Siemens supports compatibility tests of Microsoft security patches:
  - SIMATIC PCS 7: <http://support.automation.siemens.com/WW/view/en/22754447>
  - SIMATIC WinCC: <http://support.automation.siemens.com/WW/view/en/18752994>
- System-specific compatibility tests recommended
- Patch distribution via central patch server in DMZ and Windows Server Update Services (WSUS).

### [Industrial Security Services](#)

- Set up of update groups and processes for online update simplifies patch distribution (e.g. for redundant systems).



## System Integrity

### Firmware updates for more security within automation devices

- Even such automation components that do not use a standard PC operating system may require software updates to fix security related vulnerabilities.
- Information is available at our Siemens Industrial Security website (<http://www.siemens.com/industrialsecurity>) as well as our product newsletters or RSS feeds.
- As soon as information on a vulnerability becomes available, it should be evaluated for relevance to the application concerned
- Depending thereon, it can be decided whether further measures should be taken:
  - No action, as existing measures provide sufficient protection
  - Additional external measures in order to uphold the security level
  - Installation of latest firmware updates to eliminate the weak point
- The procedure is comparable with a risk analysis, as described earlier in the presentation, but with restricted focus

**Tip: Tools like SIMATIC Automation Tool or SINEC NMS also support software updates for automation and network components.**

# System Integrity

## Identifying / preventing malware with virus scanners

**Suitable antivirus software should be used to identify malware and to prevent further spreading.**

**Depending on the particular case, certain aspects should however be taken into account:**

- Performance loss due to scan procedure (e.g. only automatic scan of incoming data transfer and manual scan during maintenance periods)
- Regular updating of virus signatures – if applicable via central server
- Availability must generally be assured even in the case of infection with malware. This means that the virus scanner must under no circumstances:
  - Remove files or block access thereto or move into Quarantine
  - Block communication
  - Shut down systems

**Siemens supports with compatibility tests \*) with solutions from**

- McAfee



[Industrial Security Services](#)

- Symantec
- Trend Micro

**Further information is available in the Siemens compatibility tool:**  
<http://www.siemens.com/kompatool>

**\*) Please note:** The compatibility must be verified for each specific configuration

# System Integrity

## Identifying / preventing malware by whitelisting

### Basic principle

- Whitelisting mechanisms provide additional protection against undesired applications or malware, as well as unauthorized changes to installed applications
- Whitelisting software creates or contains a list of programs and applications that are allowed to run on the PC
- Software that is not listed in this “white list“ is prevented from running.

### Advantages

- No regular or delayed pattern updates
- Additional protection mechanism
- Higher Protection against specific types of malware

Siemens supports with compatibility tests with \*)

- McAfee Application Control



[Industrial Security Services](#)

Further information is available in the Siemens compatibility tool:  
<http://www.siemens.com/kompatool>

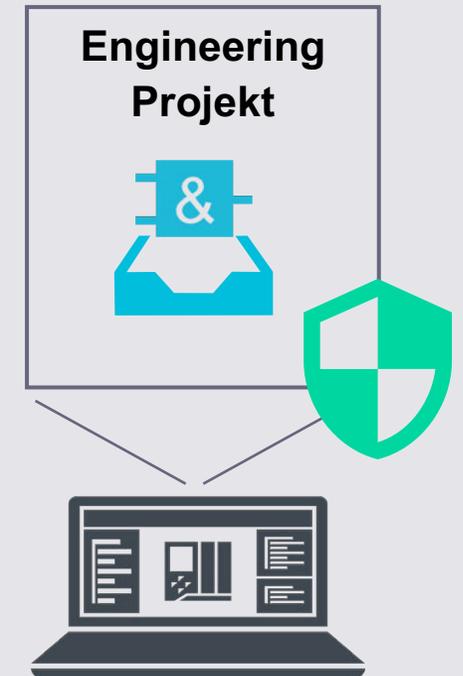
\*) **Please note:** The compatibility must be verified for each specific configuration

# System Integrity

## Access protection of industrial project files

**Project files for industrial automation solutions (e.g. Engineering Project files) often contain internal know-how, which shall not fall into foreign hands. You should therefore protect and prevent from disclosure industrial project files by consider the following guidelines:**

- Protect project files at rest (e.g.: access protection using file system rights; storage in an encrypted drive container)
- Encrypt project files when they are in transit (e.g. via e-mail encryption or encrypted ZIP archives)
- Enforce the need to know principle
- Assess and configure security measures that are connected with online services to test for malicious files carefully. Otherwise industrial project files might be uploaded unintentionally and automatically to external systems. This is for example related to 3<sup>rd</sup> party automated e-mail gateway scanners, Endpoint Protection Systems, DLPs or IDSs.



# System Integrity

## Possible risks and recommended measures

### Risks

- Manipulation / espionage via unauthorized access to devices configuration
- Unauthorized operating activities
- Limited device availability due to malware installation and replication
- Unauthorized / public access to project files

### Measures

- Utilization of access control mechanisms in automation components, which limits access to configuration data and settings to authorized persons only
- Implementation of individual hardening measures for each automation component to reduce targets
- Installation of available updates in case of fixed security vulnerabilities or establishing alternative protection measures
- Usage of antivirus and whitelisting mechanisms as protection mechanism against malware
- Usage of protection mechanism for project files during their whole lifecycle (encrypted storage and transfer; access control; prevent them from being uploaded to online scanning engines; safe deletion of outdated files)

# Contents

<b>1</b>	Overview	3
<b>2</b>	Risk Analysis	10
<b>3</b>	Security Concept: Defense-in-Depth	12
	• Plant Security	15
	• Network Security	20
	• System Integrity	31
<b>4</b>	<b>Validation and Improvement</b>	<b>44</b>
<b>5</b>	Summary	47

# Review of measures

## Reviews and improvements

After implementation of all planned measures a Security Audit is conducted to ensure that

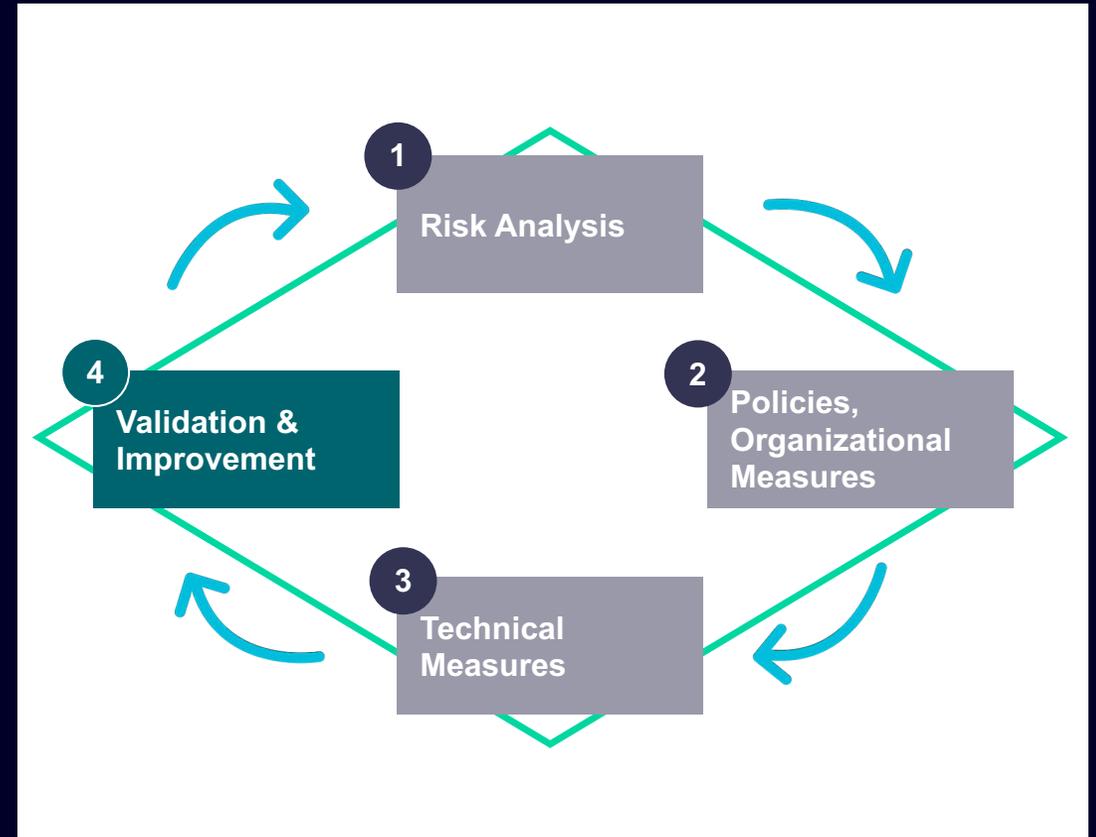
- measures have been put into practice as scheduled,
- these measures reduce the identified risks as expected.

Depending on the results, measures can be changed / added in order to attain the necessary security.

## Repeat the risk analysis

Due to the changes in security threats, regular repetition of the risk analysis is required in order to ensure the security of plant / machinery.

- Following certain occurrences (expansion of or changes to plant / machinery, significant changes in security threats, etc.)
- Annual check of whether a new risk analysis is required.



# Industrial Security

## Siemens ProductCERT

**ProductCERT is a dedicated team of seasoned security experts that manages the receipt, investigation, internal coordination, and public reporting of security issues related to Siemens products, solutions, or services.**



<https://www.siemens.com/cert>

### ProductCERT

- cultivates strong and credible relationships with partners and security researchers around the globe
- acts as the central contact point to report potential Siemens product security vulnerabilities
- coordinates and maintains communication with all involved parties, internal and external, in order to appropriately respond to identified security issues
- publishes Security Advisories, which allows customers to
  - get information about affected products
  - receive detailed vulnerability description (CVE)
  - determine relevance for own solutions, e.g. based on CVSS score
  - obtain information about required steps for a protected plant operation

# Contents

<b>1</b>	Overview	3
<b>2</b>	Risk Analysis	10
<b>3</b>	Security Concept: Defense-in-Depth	12
	• Plant Security	15
	• Network Security	20
	• System Integrity	31
<b>4</b>	Validation and Improvement	44
<b>5</b>	<b>Summary</b>	<b>47</b>

# Our offering for comprehensive Security solutions

## Defense in Depth

based on IEC 62443

Plant Security  
Network Security  
System Integrity



Industrial Security Services

### Siemens products and systems offer integrated security



Know-how and copy protection



Access protection and user management



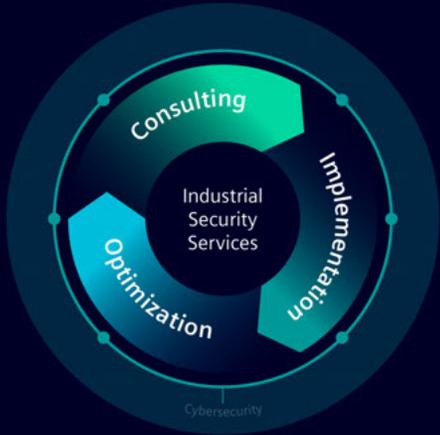
Firewall & VPN (virtual private network)



System hardening

### Siemens Industrial Security Services

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



# Industrial Security Services

## A holistic approach



### Security Consulting

Evaluation of current security status in industrial environment

- Security Assessments
- Scanning Services
- Industrial Security Consulting



### Security Implementation

Risk mitigation by implementation of security measures

- Security Awareness Training
- Automation Firewall
- Endpoint Protection e.g. hardening measures (network robustness)



### Security Optimization

Increased protection by Managed Services

- Industrial Anomaly Detection
- Industrial Security Monitoring
- Remote Incident Handling
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC Security Service Packages

<https://support.industry.siemens.com/cs/en/en/sc/4973>

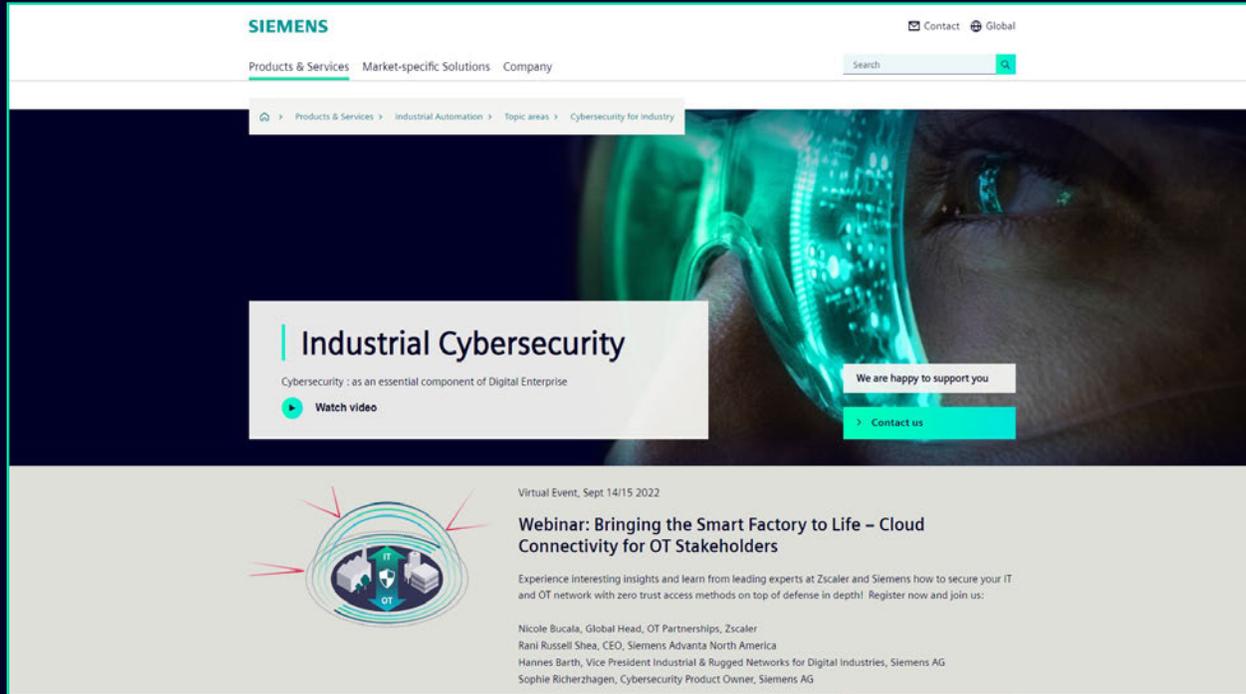
# Summary

## Industrial Cybersecurity



- Industrial Security is not just a question of technical implementation, but rather an ongoing process which also has to be understood as a management task
- Depending on the particular risks inherent in the automation system, appropriate organizational and technical measures must be taken and regularly reviewed
- Maximum security is only possible in close cooperation between all involved parties
- Siemens Industry Automation provides products and systems as well as Security Services, in order to ensure comprehensive Industrial Security solutions for our customers

# Industrial Security – ... discover more – Concepts, Products and News



Further informations on our  
Industrial Cybersecurity Homepage:  
[siemens.com/industrialsecurity](https://www.siemens.com/industrialsecurity)

<b>Report</b>	<b>Analysis</b>	<b>Handling</b>	<b>Disclo- sure</b>	<b>Siemens ProductCERT – Contact for Products, Solutions and Services</b> PGP Public Key and Fingerprint: 7F04 6EDA 338E 6D94 A3AA 4974 BB67 95EA 8E55 D52E Email: <a href="mailto:productcert@siemens.com">productcert@siemens.com</a>	<b>Siemens CERT – Contact for Infrastructure</b> PGP Public Key and Fingerprint: A3D1 8E40 D104 DEAD A112 3FF6 B485 0E2E 1AA2 2CD8 Email: <a href="mailto:cert@siemens.com">cert@siemens.com</a>
---------------	-----------------	-----------------	-------------------------	--	---

## Further Security Guidelines

### **Security guidelines for SIMATIC HMI devices**

<https://support.industry.siemens.com/cs/ww/en/view/109481300>

### **Recommended Security Settings for IPCs in the Industrial Environment**

<https://support.industry.siemens.com/cs/ww/en/view/109475014>

### **Security with SIMATIC S7-Controller**

<https://support.industry.siemens.com/cs/ww/en/view/90885010>

### **SIMATIC Process Control System PCS 7 Security concept PCS 7 & WinCC (Basic)**

<https://support.industry.siemens.com/cs/ww/en/view/60119725>

### **SIMATIC Process Control System PCS 7 Compendium Part F – Industrial Security**

<https://support.industry.siemens.com/cs/ww/en/view/109756871>

### **SINUMERIK / SIMOTION / SINAMICS Industrial Security**

<https://support.industry.siemens.com/cs/ww/en/view/108862708>



# 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>.

# Disclaimer

© Siemens 2022

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.