

Operational Guidelines for Industrial Security

Proposals and recommendations for technical and organizational measures for secure operation of plant and machinery

Version 2.0

Operational Guidelines for Industrial Security

1. Overview

2. Detailed Measures

3. Summary



Why Industrial Security is so important?

Industrial Security is used to protect industrial machines and plants against unauthorized access, sabotage, espionage and malicious manipulation.

Possible consequences of security incidents:

- Loss of system availability
- Impairment of system performance
- Manipulation or loss of data
- Loss of production control
- Environmental disaster
- Risk of death and serious injury
- Damage to company image
- Financial loss



→ Establishing of security measures required – depending on individual risks

Industrial Security

Different requirements in office and production environments

SIEMENS

Requirements that a security solution must meet in an industrial context

- 24/7/365 availability has top priority
- Open standards for seamless communication and functionality
- Common standards, e.g. Microsoft Software as base for automation solutions
- Constant operability and assured system access
- System performance
- Protection against maloperations and sabotage
- Know-how protection
- System and data integrity
- Continuous communication between office and production systems for real-time monitoring and controlling
- Data transfer in real time for efficient production processes
- Support throughout the lifecycle of a plant
- Security trail and change management

Office Security



Confidentiality

Integrity

Availability

Industrial Security



Availability

Integrity

Confidentiality

Industrial Security solutions require a holistic approach based on different protection layers

SIEMENS

Plant security

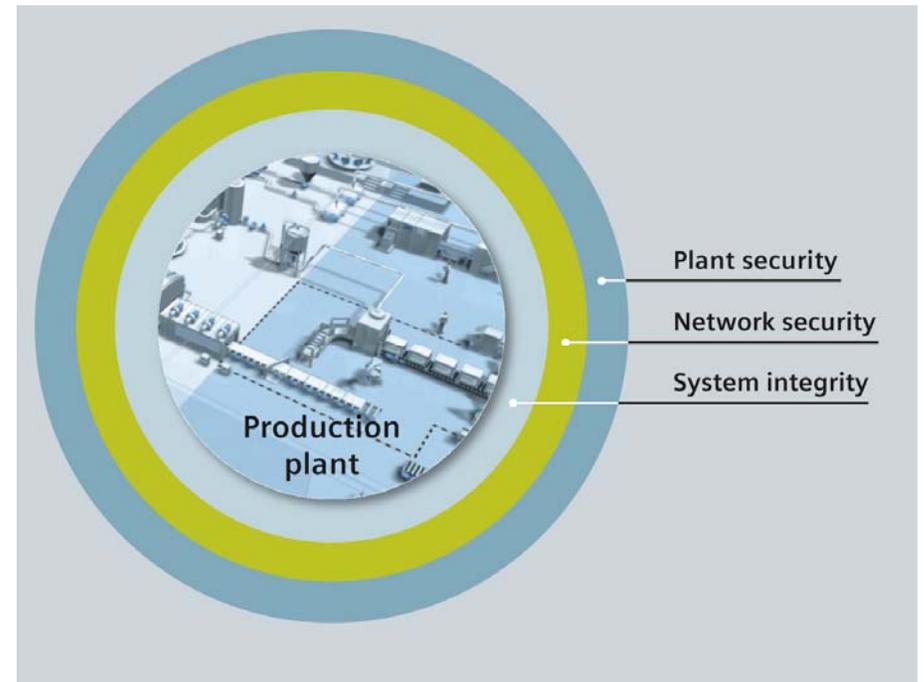
- Access blocked for unauthorized persons
- Physical prevention of access to critical components

Network security

- Controlled interfaces between office and plant network e.g. via firewalls
- Further segmentation of plant network

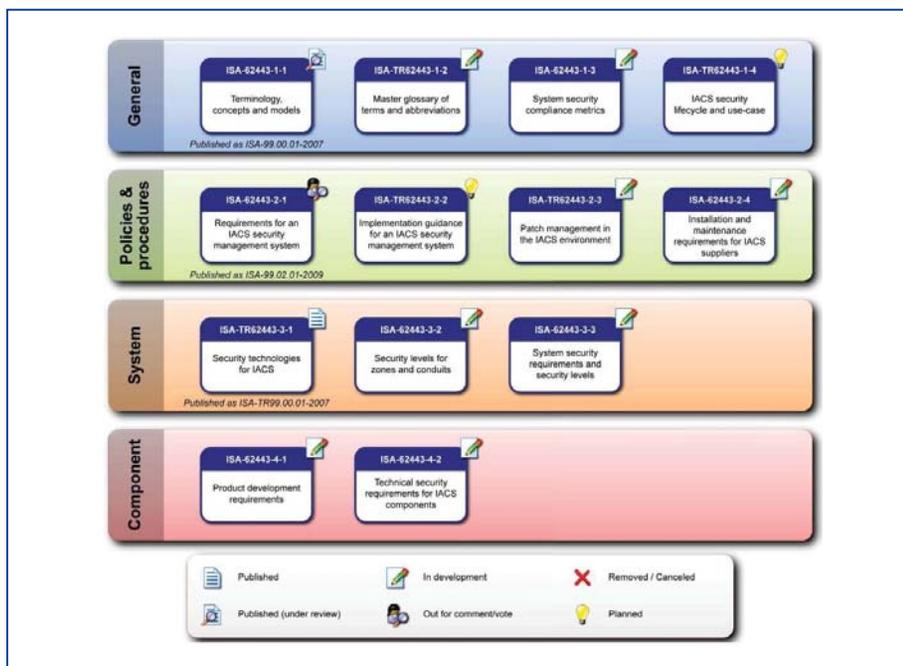
System integrity

- Antivirus and whitelisting software
- Maintenance and update processes
- User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components



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

IEC62433 / ISA99 – Standard for Industrial Security



Example

Component manufacturer:

- Automation products with integrated security features

System integrator:

- Secure configuration and integration of an automation component into the entire system

Plant operator:

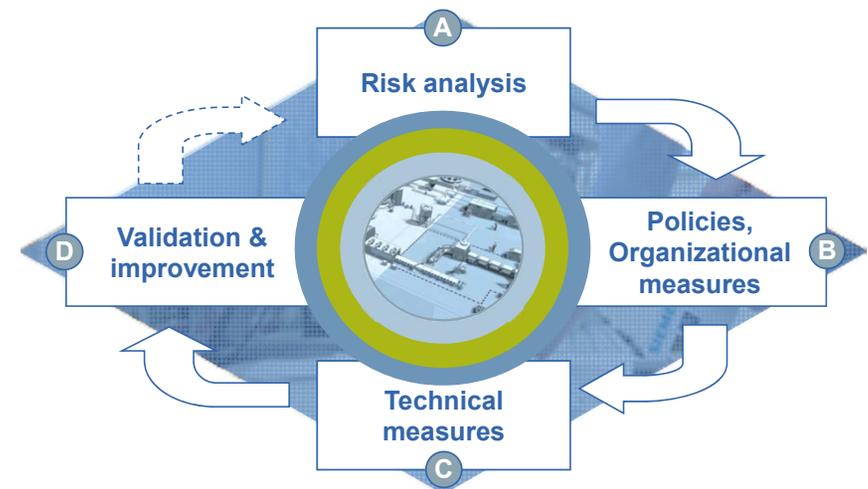
- Maintenance and update of security functionality according to changing circumstances (e.g. new known security vulnerabilities)

Measures must continuously be checked and aligned to an individual plant

Security Management

- 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.

Security Management process



A photograph of an industrial facility. In the foreground, there is a paved road curving to the right, bordered by a chain-link fence. Behind the fence, there are several large, cylindrical industrial tanks and a brick building with large windows. A utility pole with a camera or sensor is visible on the left. The sky is blue with some clouds.

Operational Guidelines for Industrial Security

1. Overview

2. Detailed Measures

3. Summary

Risk analysis is the first step to determine security measures

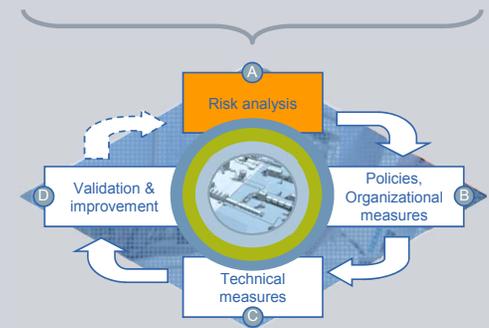
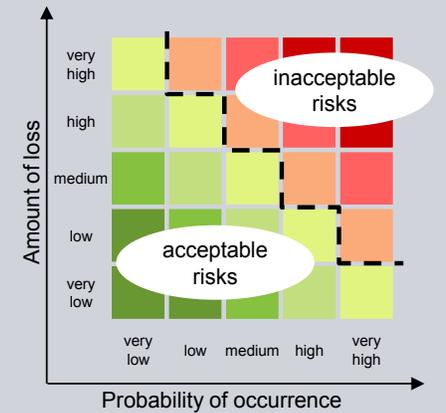
The risk analysis is an important precondition for Security Management relating to a plant or machine, aimed at identifying and assessing individual hazards and risks.

Typical content of a risk analysis:

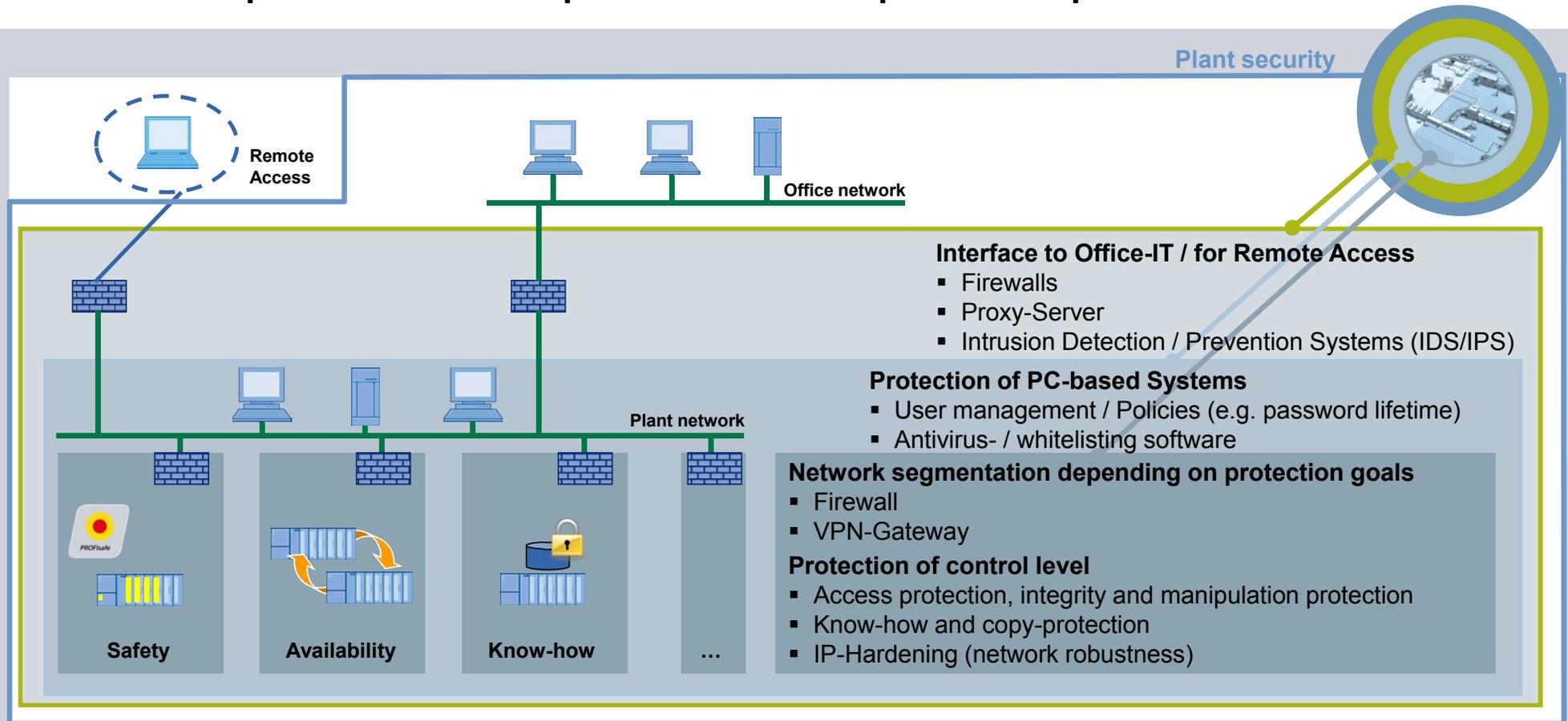
- Identification of threatened objects
- Analysis of value and damage potential
- Threat and weak points analysis
- Identification of existing security measures
- Risk assessment

The identified and unacceptable risks must, by way of suitable measures, be ruled out or typically reduced.

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 100% security.



Defense-in-Depth architecture to protect automated production plants



Overview of security measures

1. Plant security

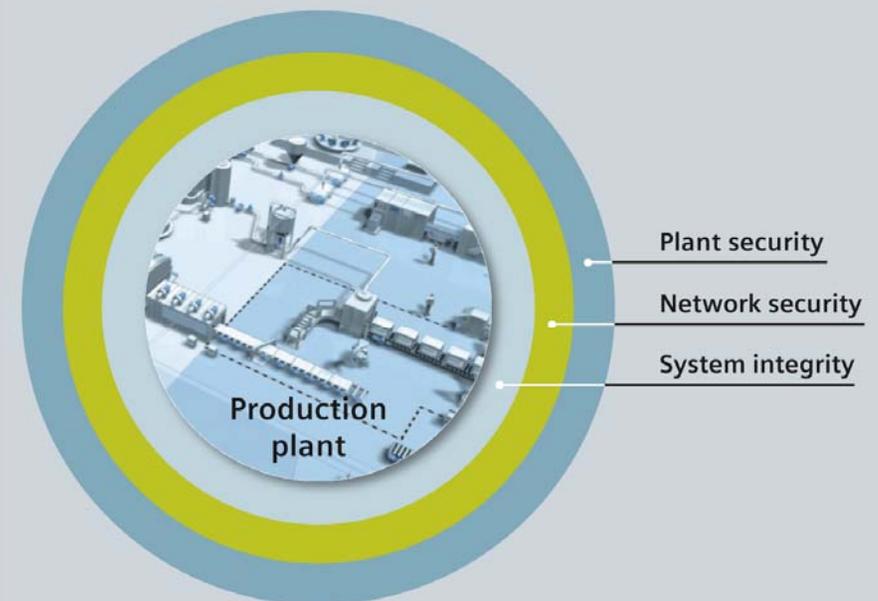
- Security organization and policies
- Physical security

2. Network security

- Network segmentation & DMZ
- Firewalls and VPN

3. System integrity

- Access protection
- System hardening
- Patch management
- Malware protection



1. Security organization and policies

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 in the sense of 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

1. Security organization and policies

Policies and processes

Definition of policies and processes in order to ensure a uniform procedure and to support the upholding of the defined 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, Smartphones and data storage in the production area (e.g. forbidding their use outside this area / the production network)

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

1. Physical 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



1. Physical security

Physical access protection of critical production facilities

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, locks / ID card readers and / or security staff
- Visitors / external personnel escorted by company staff

Physical production security

- Separate access controls for production areas
- Critical components in securely lockable control cubicles / rooms including surveillance and alarm facilities
- Cordoned-off production areas with restricted access

Overview of security measures

1. Plant security

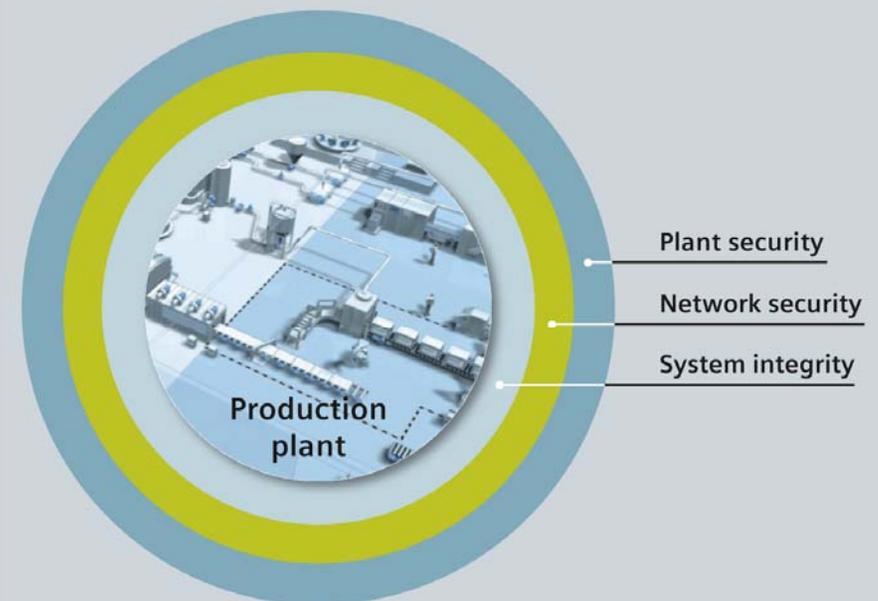
- Security organization and policies
- Physical security

2. Network security

- Network segmentation & DMZ
- Firewalls and VPN

3. System integrity

- Access protection
- System hardening
- Patch management
- Malware protection

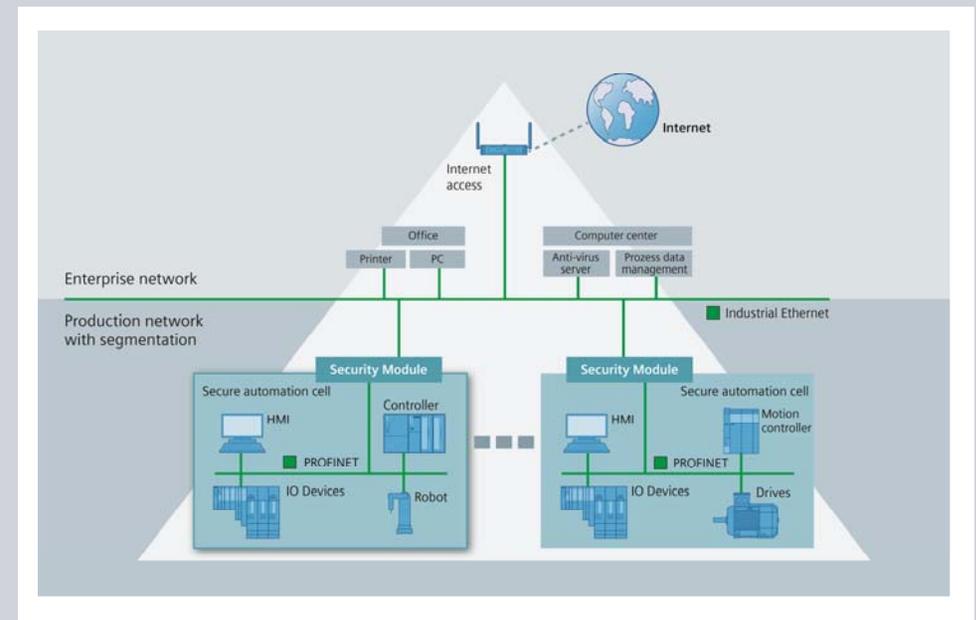


2. Network security

Protection of automation components based on segmented production networks

Ethernet-based fieldbus systems are well established in today's automation solutions because of their advantages like performance and open communication from control level to field level. However this trend also leads to increased risks which have to be addressed by security measures:

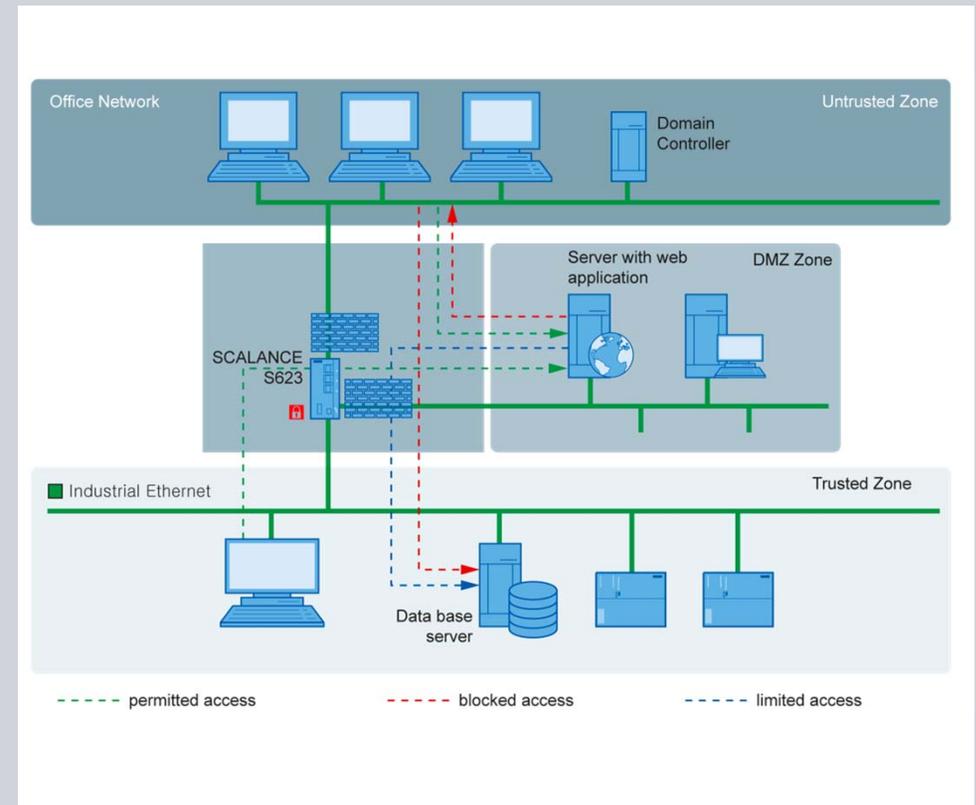
- Network protection mechanism like firewalls, which blocks or regulates communication between office and plant networks
- Segmentation of production networks in different secured automation networks (network cells). This protects automation components within these cells against unauthorized access, network overload, etc.
- Separation of a plant network into different subnets with limited and secure communication between these subnets („Secure Automation Islands“)



© Siemens AG 2013. All Rights Reserved.

2. 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 via a separate 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
- The production networks should likewise be subdivided into separate automation cells, in order to safeguard critical communication mechanisms



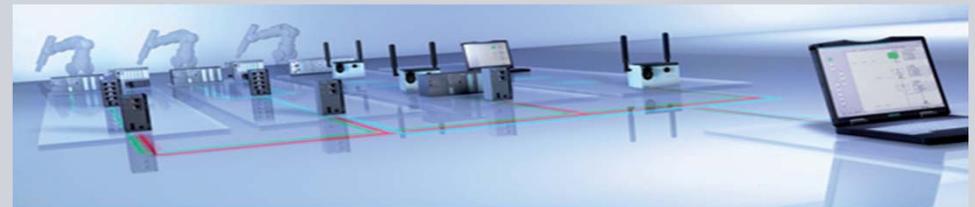
2. Network security

The security cells / zones concept

- A “cell” or “zone” is a network segment sealed off for security purposes
- There are access controls at the “entry to the cell” in the form of security network components
- Devices without their own access protection mechanisms are safeguarded within the cell. This principle is thus suitable for retrofitting in existing installations
- The cell can be protected against network overload by bandwidth restriction, and data traffic within the cell upheld without disturbance
- Real-time communication remains unaffected within the cell
- Provides protection for safety applications within the network cell
- Secure channel and therefore secure communication between cells

Protection of automation equipment and industrial communication by means of:

- Firewall/VPN appliances
- VPN client software for IPCs or PCs, to create secure and authenticated links to the Security Appliances



2. Network security

Criteria for network segmentation

- In the cell protection concept a network segment is safeguarded from outside against unauthorized access. Data traffic within the cell is not controlled by the Security Appliance and must therefore be assumed to be secure or supplemented with protection measures within the cell, e.g. Port Security in the case of switches.
- The size of a Security cell depends primarily on the protection objectives of the components it contains, because one cell may only include components with the same protection requirement.
- It is recommended to plan network structure based on your production processes. This allows the definition of network segments with less communication across network borders and minimal firewall exception rules.
- There are also the following recommendations for network size and network segmentation, resulting from performance requirements:
 - All devices of a PROFINET IO system belong to one cell
 - Devices between which there is much communication should be combined in one cell
 - Devices that communicate only with devices of one cell should, if the protection objective is identical, be integrated in this cell

2. 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

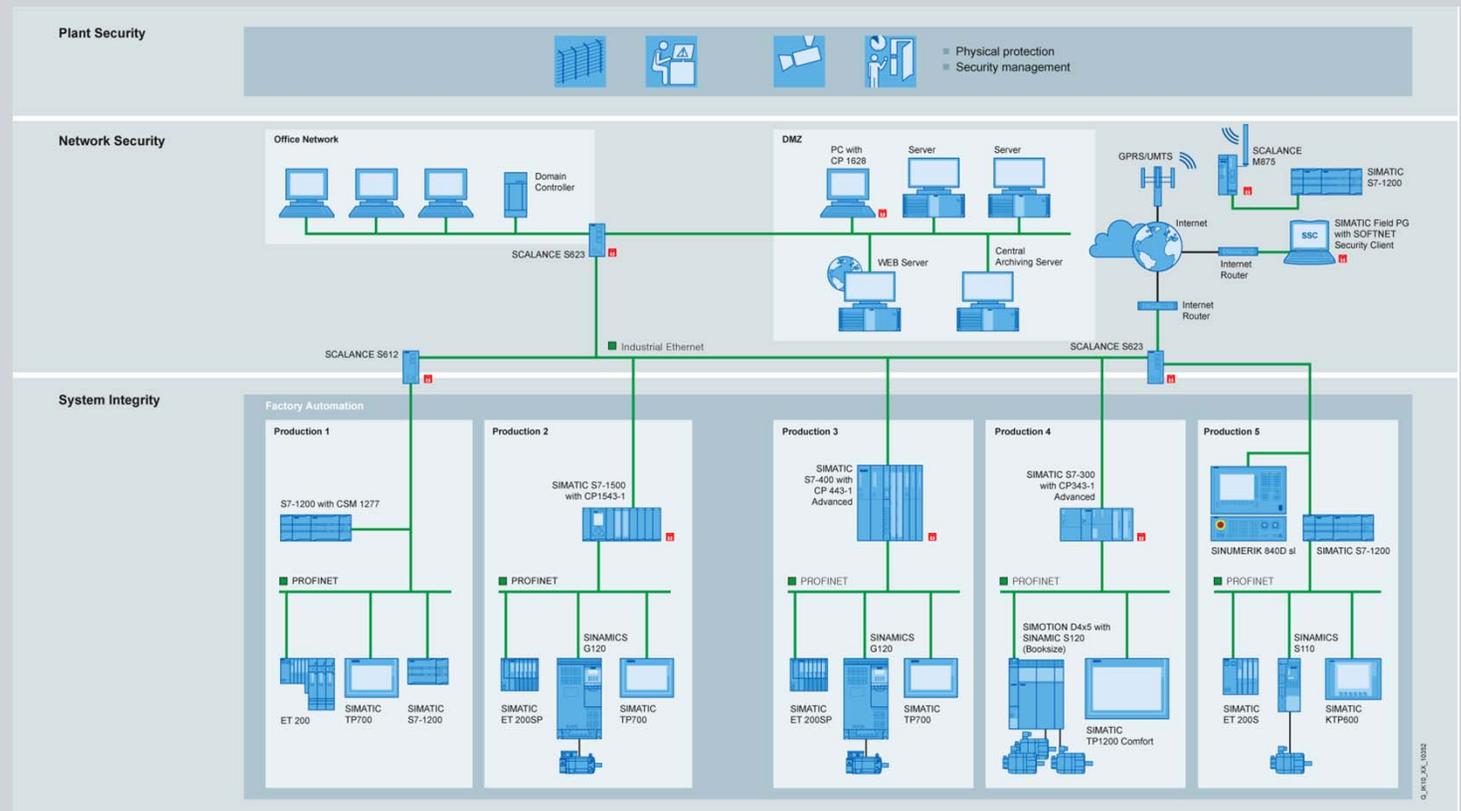
- Division of the automation network into appropriate network segments and control of incoming and outgoing data traffic by a firewall (perimeter security). For example, critical network protocols can be blocked.
- Bandwidth restriction, for example in cell firewall or in switches. Network overload from outside the cell cannot affect those inside.
- 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.

2. Network security

Example: Network segmentation with cell protection concept with security appliances

SIMATIC S7 and PC communication processors (CP) with “Security integrated” (Firewall, VPN) can be used as alternative or extension to security appliances (SCALANCE S) to protect automation devices and networks.

S7 communication processors protect underlying networks by an integrated firewall. Additionally encrypted VPN connections can be established directly to the PLC itself (S7-300, S7-400 or S7-1500).



2. Network security

Example: Secure remote maintenance with SCALANCE S623

Task

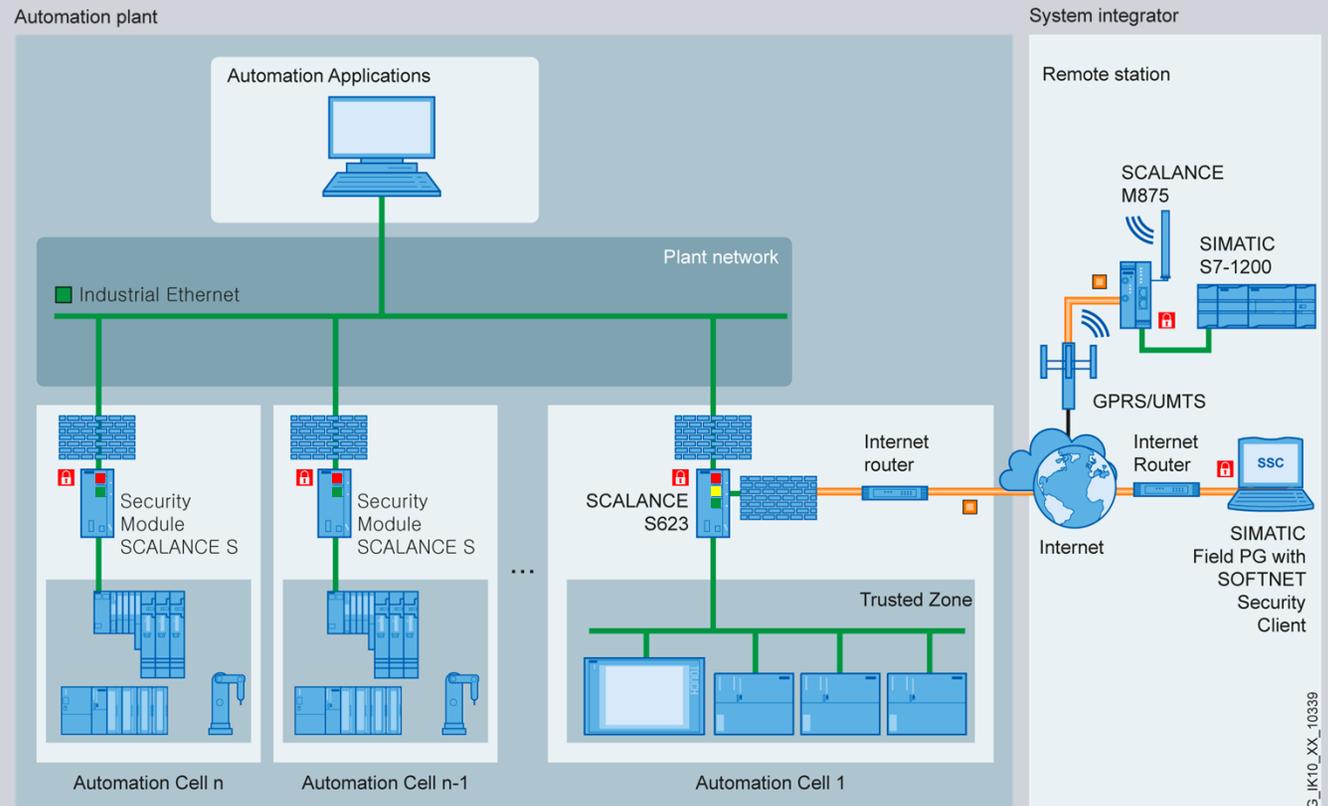
System access via the Internet using an encrypted VPN tunnel.

Solution

Starting point (e.g. system integrator):
e.g. SCALANCE S or SSC as VPN client

End point (e.g. end client system):
SCALANCE S623 as VPN Server

- Red port: Connection to plant network
- Yellow port: Connection of modem / router
- Green port: Connection of secure cells



G_IK10_XX_10339

2. Network security

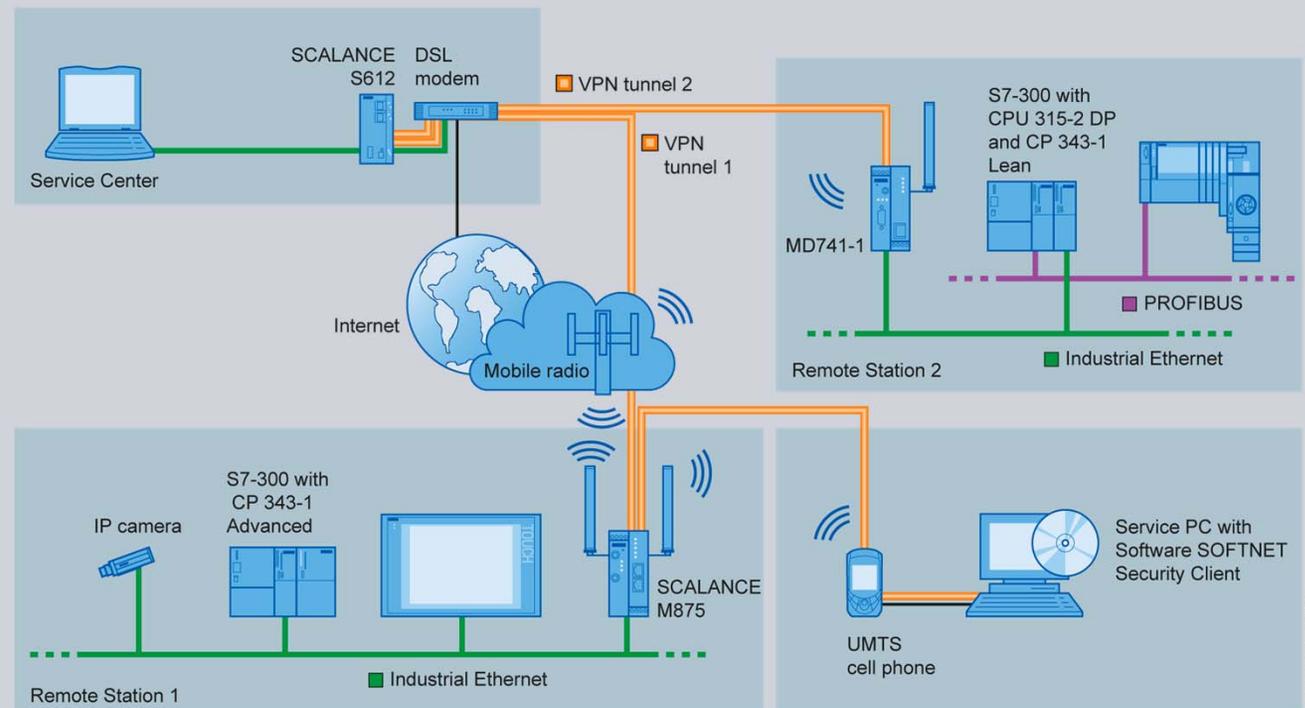
Example: Secure remote maintenance via cellular networks with SCALANCE M875

Task

Classical applications such as remote programming, parameterization and diagnosis, but also monitoring of machines and plants installed worldwide can be performed from a service center that is connected over the Internet.

Solution

Any IP-based devices, particularly automation devices that are downstream of the SCALANCE M875 in the local network, can be accessed. Multimedia applications like video streaming can be implemented thanks to the increased bandwidth in the uplink. The VPN functionality allows the secure transfer of data around the world.



G_IK10_XX_30188

2. Network security

Example: Secure remote maintenance via Siemens Remote Service Platform (SRS)



<http://www.industry.siemens.com/topics/global/en/service/remote-service/Pages/home.aspx>

© Siemens AG 2013. All Rights Reserved.

Overview of security measures

1. Plant security

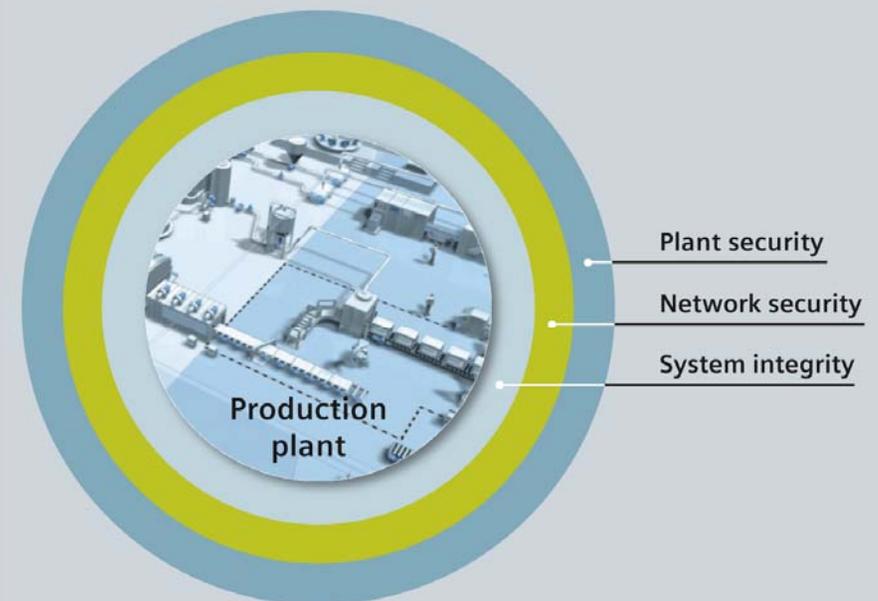
- Security organization and policies
- Physical security

2. Network security

- Network segmentation & DMZ
- Firewalls and VPN

3. System integrity

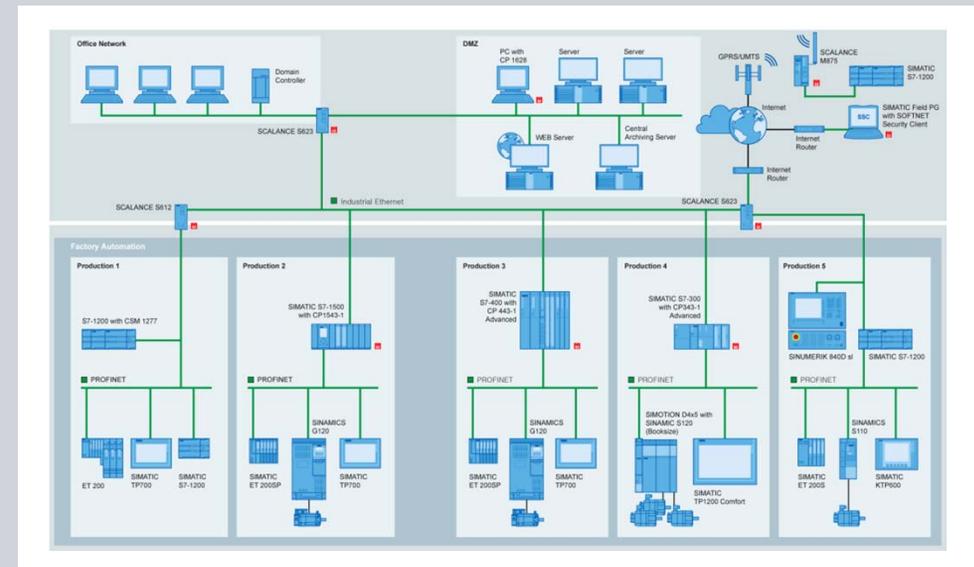
- Access protection
- System hardening
- Patch management
- Malware protection



3. System integrity

Access protection for configuration (Engineering)

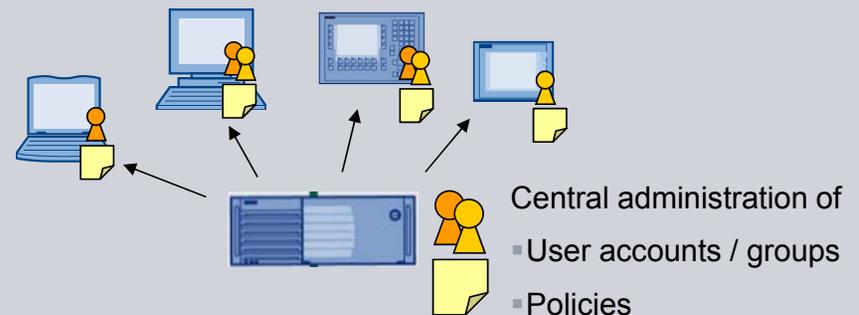
- In order to prevent unauthorized configuration changes to automation components, it is extremely advisable to make use of the integrated access protection mechanisms.
- These include for example:
 - PLCs (“protection level”)
 - HMI Panels („Secure mode“)
 - Managed Switches (Password)
 - WLAN Access Points (Password)
 - Firewalls (Passwords / Certificates)
- Utilization of components with integrated security features like the S7-1500 controller for example
- 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.



3. System integrity

Access protection for operations (Runtime)

- Typically, plant / machinery is operated by various persons; central user administration is therefore advisable
- This is based on the user accounts of a Windows domain or of a Windows Active Directory. The linking of the SIMATIC (HMI) runtime applications is in this case via SIMATIC Logon
- Specifying / enforcing of 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)
- Depending on security requirements separated network segments could also use different Windows domains



3. 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 WPA2 / IEEE 802.11i for Security
 - Advanced Encryption Standard (AES) for encoding data
 - Central device administration with RADIUS authentication (in accordance with 802.1x)
 - Protected configuration accesses to web interface by way of HTTPS and secure logging in via SSH

3. System integrity

System hardening reduces possible attack scenarios

Network services

- Network services are a potential security risk in general
- In order to minimize risks, on all automation components only the services actually required should be activated
- All activated services (especially Webserver, FTP, Remote Desktop, etc.) should be taken into account in the security concept
- IP hardening measures in automation and drives products enhance security without the need for separate user configuration

Hardware interfaces

- Hardware interfaces constitute a risk if unauthorized access via them to equipment or the system is possible
- Unused interfaces should therefore be deactivated:
 - Ethernet/Profinet ports
 - WLAN, Bluetooth
 - USB, Firewire, etc.
- Protection by deactivation or mechanical blocking
- Deactivate booting and autostart mechanisms of external media

User accounts

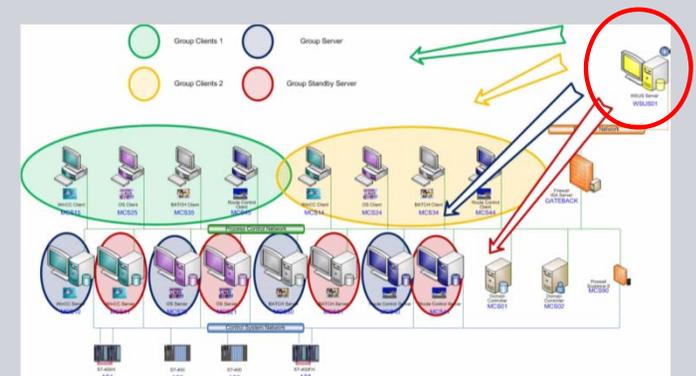
- Every active user account enables access to the system and is thus a potential risk
- Reduce configured / activated user accounts to the really necessary minimum
- Use secure access data for existing accounts
- Regular checks, particularly of locally configured user accounts
- **Important:** Change predefined default passwords during commissioning phase (where available).

3. System integrity

Patch management fixes security vulnerabilities in operating system and applications

Most security attacks nowadays take place via weak points for which the manufacturers already have patches. Only in rare cases are zero day exploits encountered, 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 with 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>
 - SIMOTION P350: <http://support.automation.siemens.com/WW/view/en/22159441>
 - SINUMERIK PCU50/70: <http://support.automation.siemens.com/WW/view/en/19739695>
- System-specific compatibility tests recommended
- Patch distribution via central patch server in DMZ and Windows Server Update Services (WSUS)
- Set up of update groups and processes for online updates simplifies patch distribution (e.g. for redundant systems)



3. 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.
- You will get information 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, the weak point 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 comparable with a risk analysis like at the beginning, but with restricted focus

3. 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 pauses)
 - 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
 - Place files in quarantine
 - Block communication
 - Shut systems down
- Siemens supports with compatibility tests with: *):
 - Trend Micro Office Scan
 - Symantec Endpoint Protection
 - McAfee VirusScan Enterprise
- Further information are available in our compatibility tool:
<http://www.siemens.com/kompatool>

*) Please note the compatibility must be verified for each specific configuration

3. 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
- Protection against unknown malware (zero day exploits)

- Siemens supports with compatibility tests with *) :
 - McAfee Application Control
- For further information go to:
<https://support.automation.siemens.com/WW/view/en/49386558>
<http://www.siemens.com/kompatool>

*) Please note the compatibility must be verified for each specific configuration

3. 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

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

Reviewing 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 eliminate / reduce the identified risks as expected.

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



Repeating 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 fresh risk analysis is required

Operational Guidelines for Industrial Security

1. Overview
2. Detailed Measures
3. Summary



The Siemens Industrial Security Concept is based on five key points which cover the essential protection areas



Implementation of practicable and comprehensive Security Management

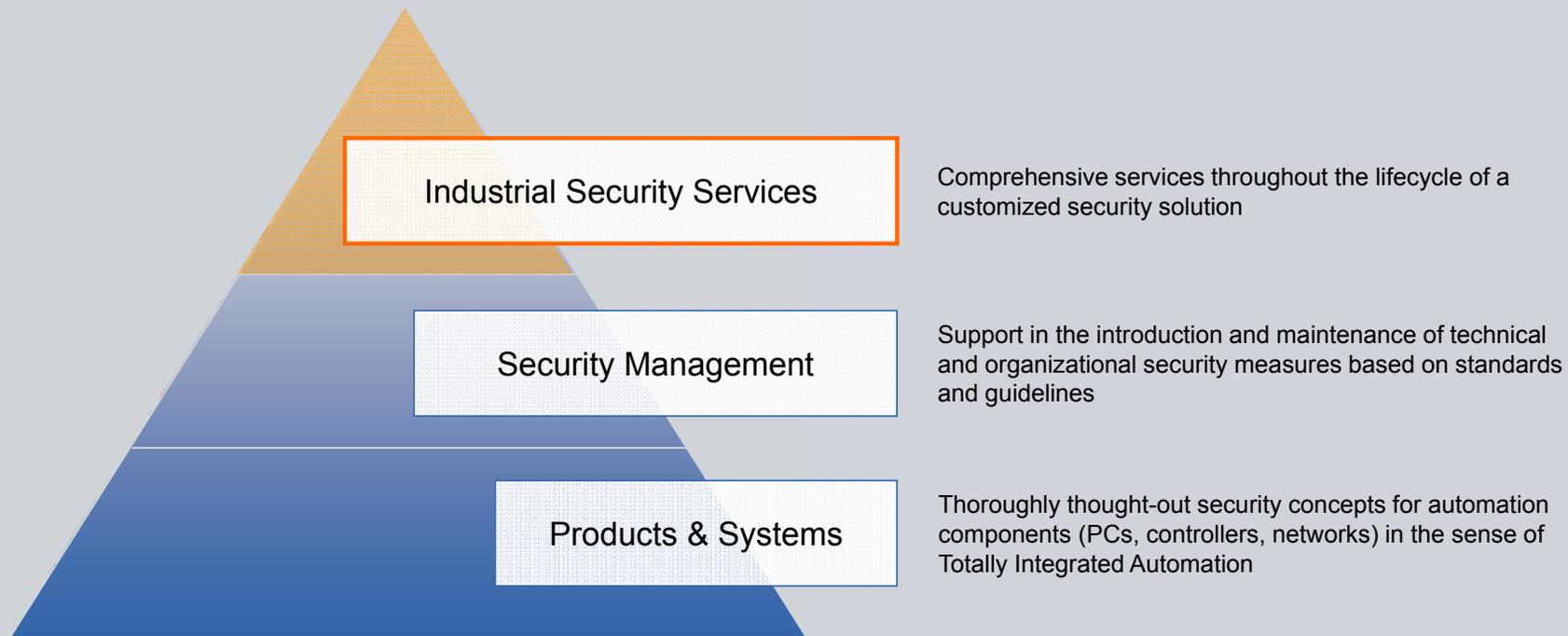
The **interfaces** to office IT and the Internet/Intranet are subject to clearly defined regulations - and are monitored accordingly.

PC-based systems (HMI, engineering and PC-based controls) must be protected with the aid of anti-virus software, whitelisting and integrated security mechanisms.

The **control level** is protected by various integrated security functions within automation and drive components.

Communication must be monitored and can be intelligently segmented by means of firewalls.

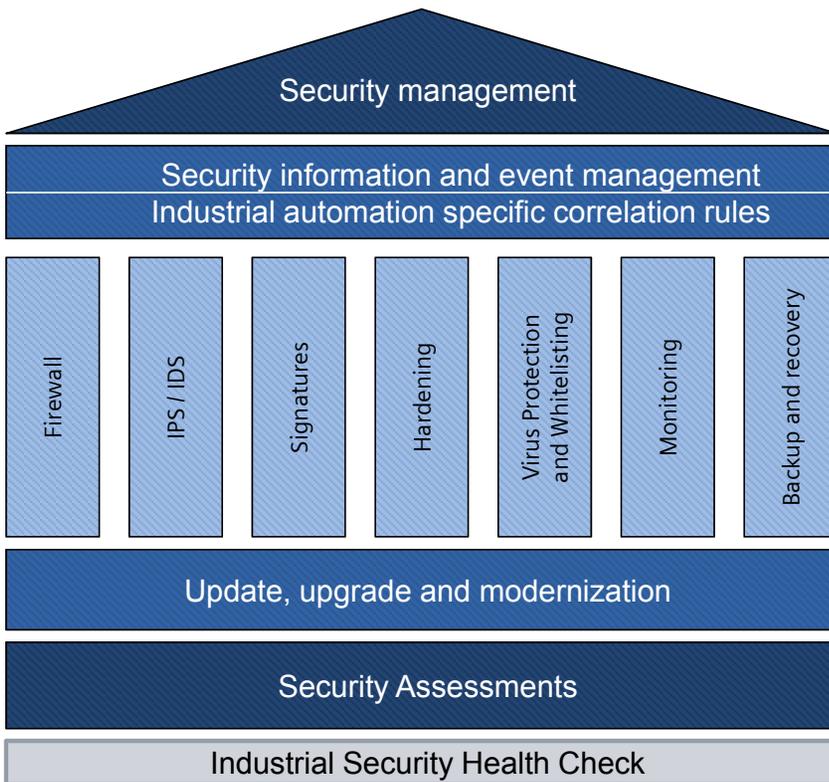
Industrial Security: What we have to offer



Further individual support in planning / implementing an Industrial Security Concept is available from our Industrial Security Services

Industrial Security Services

Technological Overview



Managed Service

Integral Monitoring & Analytics

Professional Packages

Upgrade and Modernization

Consulting

Sales Support

Managed Services
for extensive support

Security Packages
Reduce risk of vulnerabilities through standardized packages

Security Assessment
Identification of risks and definition of mitigations

Industrial Security Services

Security Assessments



Customer requirement

Consultation and review of the current situation, regarding industrial security within the plant.

Analysis and reporting of further steps to reduce security risks.

Our solution

The result of the **security assessment** is a report and the baseline for decisions on next steps.

In this report the current risk level, identified vulnerabilities and the completeness of the implemented security measures will be provided.

Documentation also includes prioritized recommendations how to improve and enhance the security level of the system, depending on the extend of the ordered services.



Summary

Industrial Security

- Industrial Security is not just a question of technical implementation, but rather a 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

Security information

Siemens provides automation and drive products with industrial security functions that support the secure operation of plants or machines. They are an important component in a holistic industrial security concept. With this in mind, our products undergo continuous development. We therefore recommend that you keep yourself informed with respect to our product updates. Please find further information and newsletters on this subject at: <http://support.automation.siemens.com>.

To ensure the secure operation of a plant or machine it is also necessary to take suitable preventive action (e.g. cell protection concept) and to integrate the automation and drive components into a state-of-the-art holistic industrial security concept for the entire plant or machine. Any third-party products that may be in use must also be taken into account. Please find further information at: <http://www.siemens.com/industrialsecurity>

Thank you for your attention!

For further information on
Industrial Security go to:

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

