SIEMENS

Industrial Security

Network Security

Brochure

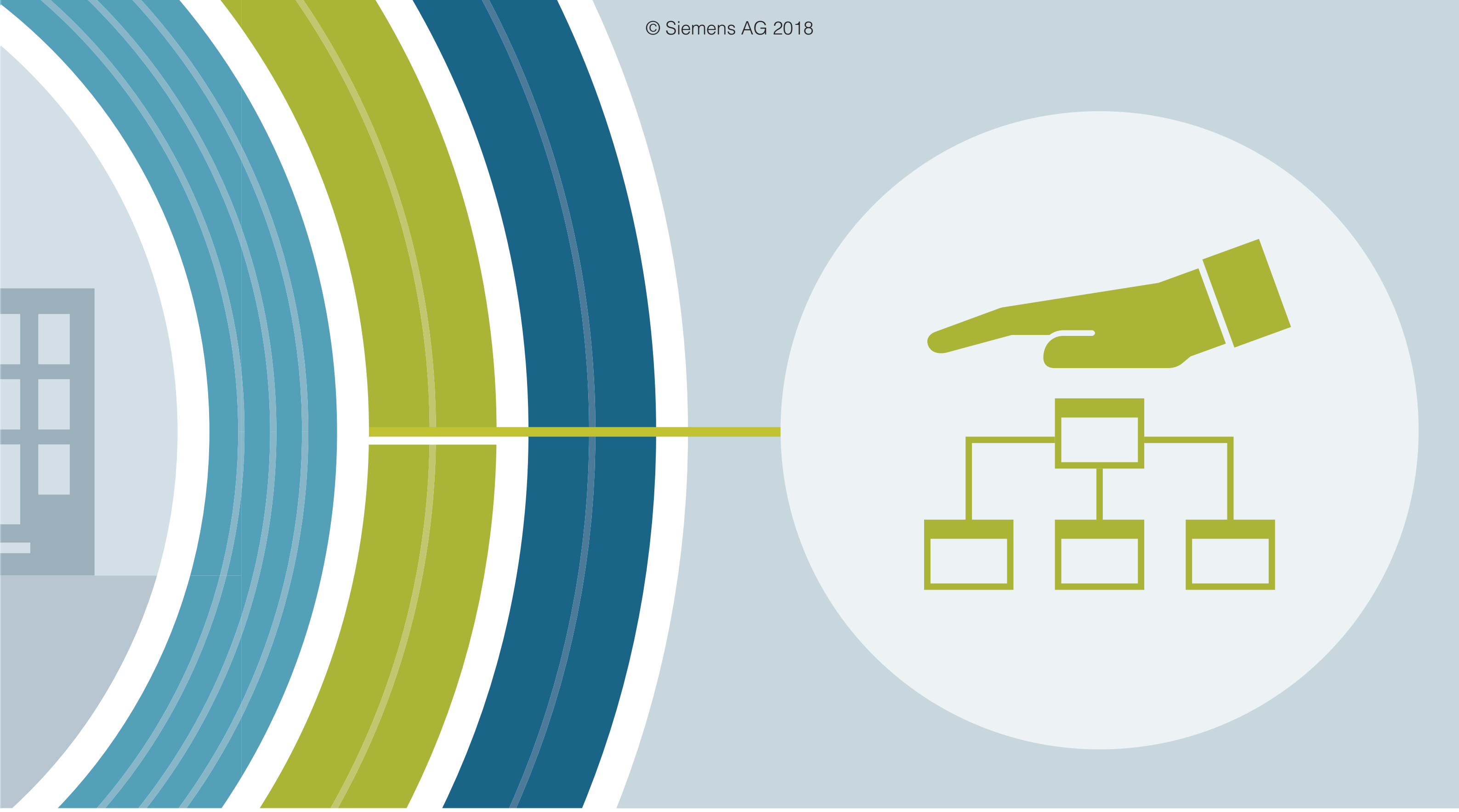
Edition 04/2018

siemens.com/networksecurity

The Internet serves as an enormous accelerator of business processes and has revolutionized business operations around the world. The resulting changes in the production industry can also be described as a revolution – the 4th Industrial Revolution. Industry 4.0 affects all aspects of the industrial value chain, including the very important aspects of industrial communication and security.

Key here is that in light of digitization and the ever increasing networking of machines and plants, data security is always taken into account. The use of industrial security solutions precisely tailored to the needs of industry is therefore of fundamental importance – and should be inseparably linked with the industrial communication.

The topic of cybersecurity is also becoming increasingly important due to the constantly growing number of convergent networks. Cybersecurity has long been the subject of attempts for standardization in which international committees ensure that uniform standards are specified and developed for cybersecurity.
Moreover, security is now also regulated by laws addressing critical infrastructures in particular in order to accommodate increased security requirements. Examples include the IT Security Act in Germany, the ANSSI Certification in France, NERC CIP in the USA or a TÜV SÜD certification based on IEC 62443-4-1. After all, open communication and the increased networking of production systems involve not only huge opportunities, but also high risks. To provide an industrial plant with comprehensive security protection against attacks, the appropriate measures must be taken. Siemens supports you here in the targeted implementation of these measures – as part of an integrated portfolio for industrial security.



Content

Industrial Security

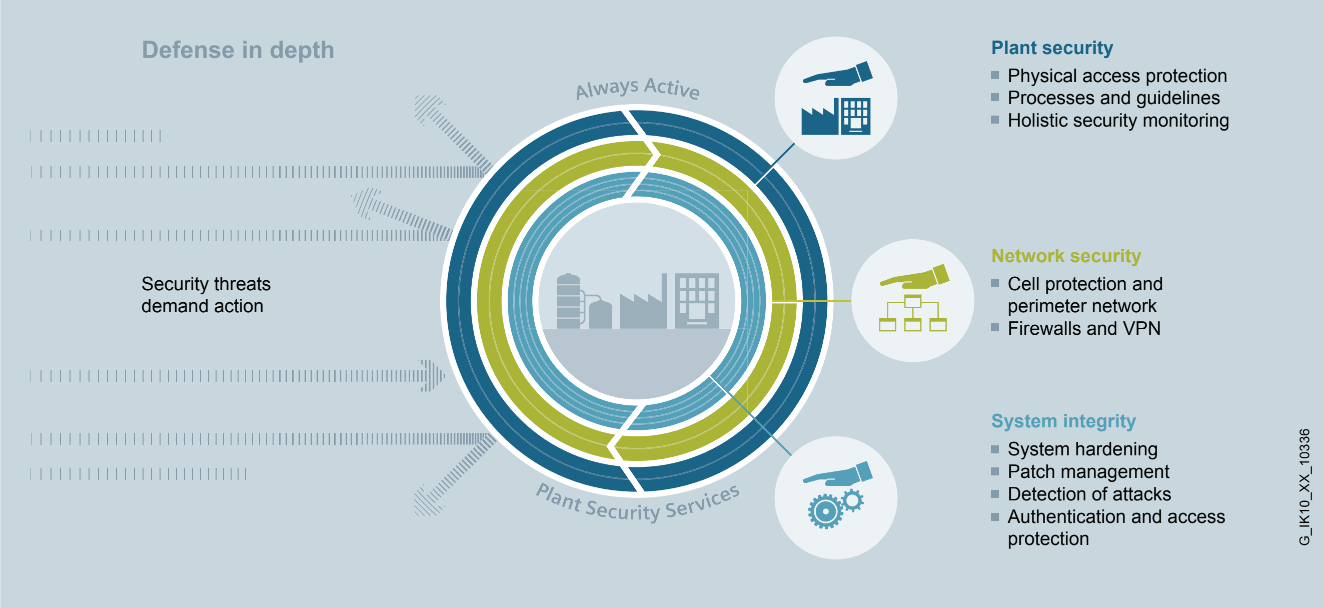
Why industrial security is so important

No.	Threat	Explanation
1	Social Engineering and phishing	Social Engineering is a method of gaining unauthorized access to information or IT systems through mostly non-technical actions in which human traits such as helpfulness, trust or fear or respect of authority are exploited. An example of this are fraudulent emails (phishing emails). These entice employees into opening attachments containing malware or contain links to manipulated websites.
2	Introduction of malware via removable media and external hardware	Removable media such as USB sticks are subject to unnoticed malware infection. The use of notebooks containing external data and maintenance software that may have been used in other companies poses a comparable danger.
3	Malware infection via Internet or intranet	Standard IT components such as operating systems, web servers and databases generally contain errors and vulnerabilities that can be exploited by attackers.
4	Intrusion via remote maintenance access	External access to ICS installations for maintenance purposes is a widespread practice. And when one system is accessed for maintenance, other systems can be easily reached. Often the lack of authentication and authorization as well as flat network hierarchies are causes for security incidents.
5	Human error and sabotage	Personnel working in an ICS environment occupy a special position when it comes to security. This applies both to a company's own employees as well as all external personnel involved in maintenance or construction work. Security can never be guaranteed by technical measures alone. Organizational regulations are always required too.
6	Control components connected to the Internet	Insecure ICS components such as programmable logic controllers are often connected directly to the Internet contrary to manufacturer recommendations without adequate accompanying security measures.
7	Technical malfunctions and force majeure	Failures due to extreme environmental influences or technical defects are always possible – the risk and the potential for damage can only be minimized here.
8	Compromising of extranet and cloud components	The widespread trend in conventional IT toward outsourcing of IT components is now finding its way into ICS. For example, remote maintenance solution providers are placing client systems for remote access in the cloud, but this leaves system owners with only very limited control over the security of these components.
9	(D)DoS attacks	(Distributed) denial of service attacks can be used to disrupt network connections and required resources and cause systems to crash, e.g. to disrupt the functionality of an ICS.
10	Compromising of smartphones in the production environment	The ability to display and change operating and production parameters on a smartphone or tablet is an additional product feature that is being promoted and used for more and more ICS components. This represents a special remote maintenance access case in which the use of smartphones creates an additional attack target.

Threat overview

Source:
Industrial Control System Security: Top 10 Threats and Countermeasures Version 1.20
Publication date: August 1, 2016
Note:
This list of threats was compiled in close cooperation between BSI (German Federal Office for Information Security) and representatives of industry.
Using BSI analyses, the Federal Office for Information Security (BSI) publishes statistics and reports on current topics dealing with cybersecurity. Please direct all comments and notes to:
cs-info@bsi.bund.de

Defense in depth



Network security as a central component of the Siemens Industrial Security concept

With defense in depth, Siemens provides a multi-faceted concept that gives your system both all-round and in-depth protection. The concept is based on plant security, network security and system integrity – according to the recommendations of IEC 62443, the leading standard for security in industrial automation.

Plant security

Plant security uses a number of different methods to prevent unauthorized persons from gaining physical access to critical components. This starts with conventional building access and extends to securing sensitive areas by means of key cards. Comprehensive security monitoring leads to transparency with regard to the security status of production facilities. Thanks to continuous analysis and correlation of existing data as well as the matching of industrial security monitoring against threat intelligence information, security-relevant events can be detected and classified according to risk factor. Based on this, plant owners receive an overview of the current security status of their production facilities in the form of monthly status reports, enabling them to react swiftly to threats.

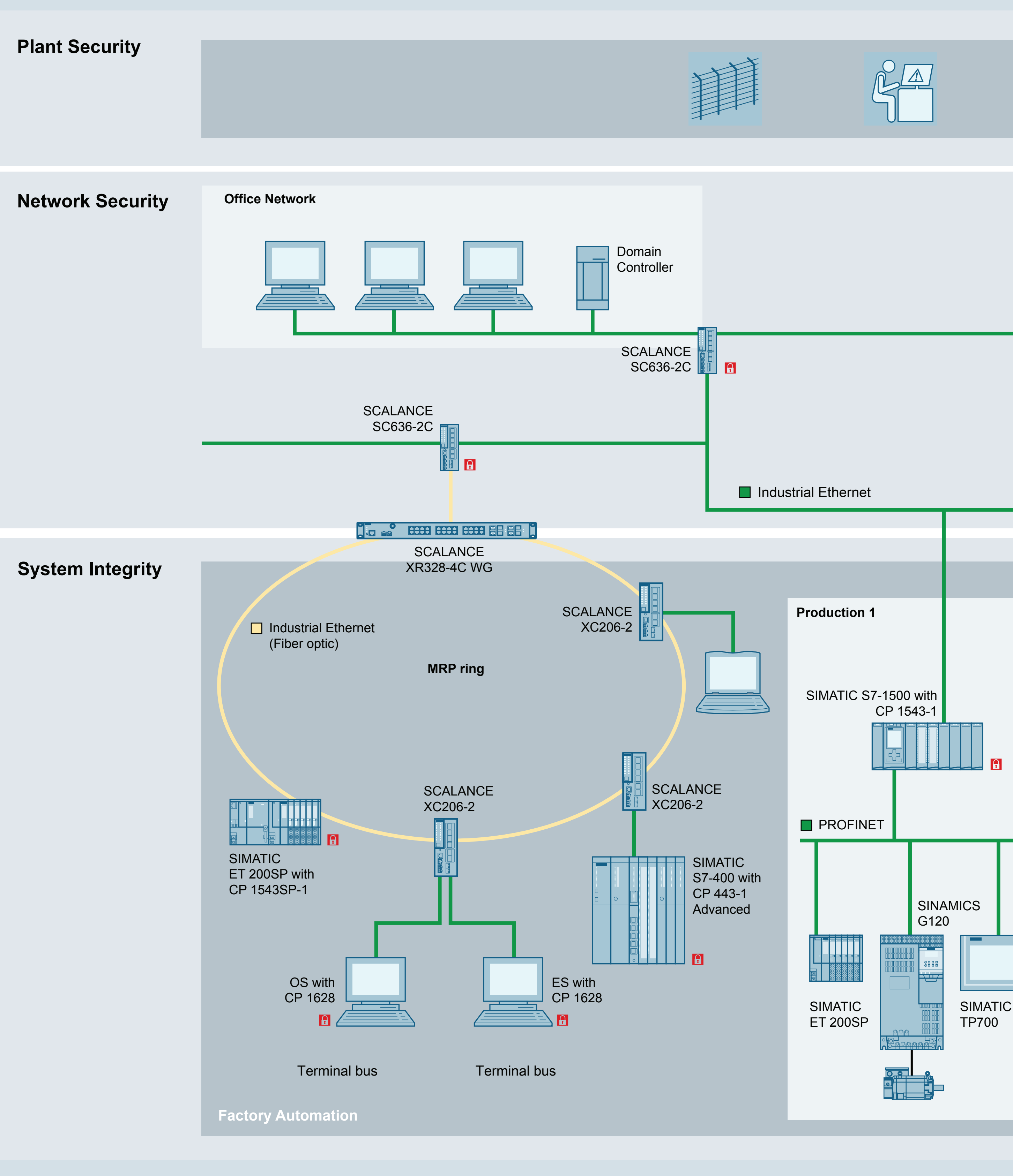
Network Security

Network security means protecting automation networks from unauthorized access. This includes the monitoring of all interfaces such as the interfaces between office and plant networks or the remote maintenance access to the Internet. It can be accomplished by means of firewalls and, if applicable, by establishing a secured and protected "demilitarized zone" (DMZ). The DMZ is used for making data available to other networks without granting direct access to the automation network itself. The security-related segmentation of the plant network into individually protected automation cells minimizes risks and increases security. Cell division and device assignment are based on communication and protection requirements. Data transmission can be encrypted using Virtual Private Network (VPN) and thus be protected from data espionage and manipulation. The communication nodes are securely authenticated. Automation networks, automation systems and industrial communication can be made secure with SCALANCE S Industrial Security Appliances, SCALANCE M Internet and mobile wireless routers and Security communications processors for SIMATIC.

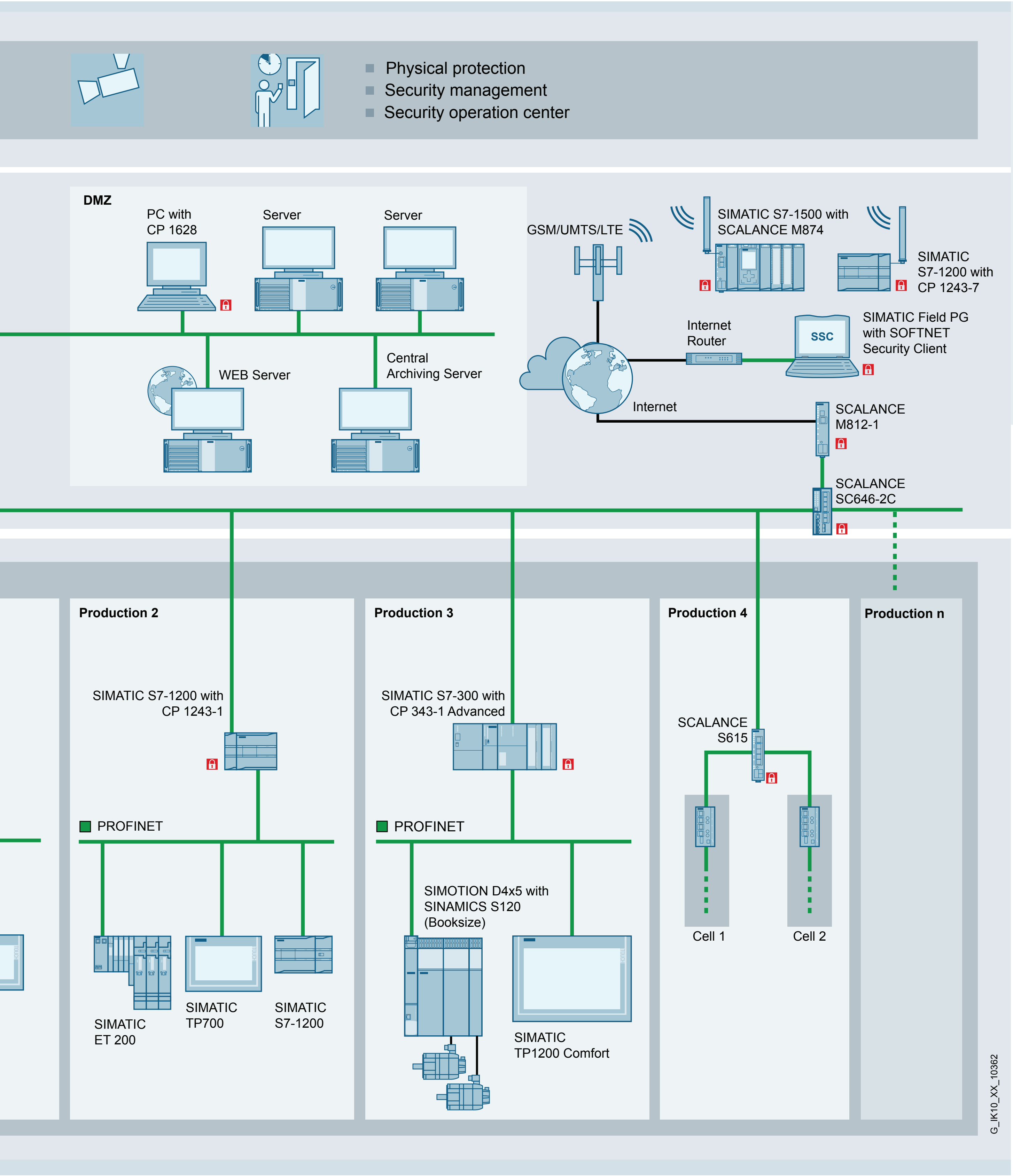
System integrity

The third pillar of defense in depth is the safeguarding of system integrity. The emphasis here is on protecting automation systems and control components such as SIMATIC S7-1200 and S7-1500 as well as SCADA and HMI systems against unauthorized access and on meeting special requirements such as know-how protection. Furthermore, system integrity also involves authentication of users, access and change authorizations, and system hardening – in other words, the robustness of components against attacks.

Industrial security at a glance

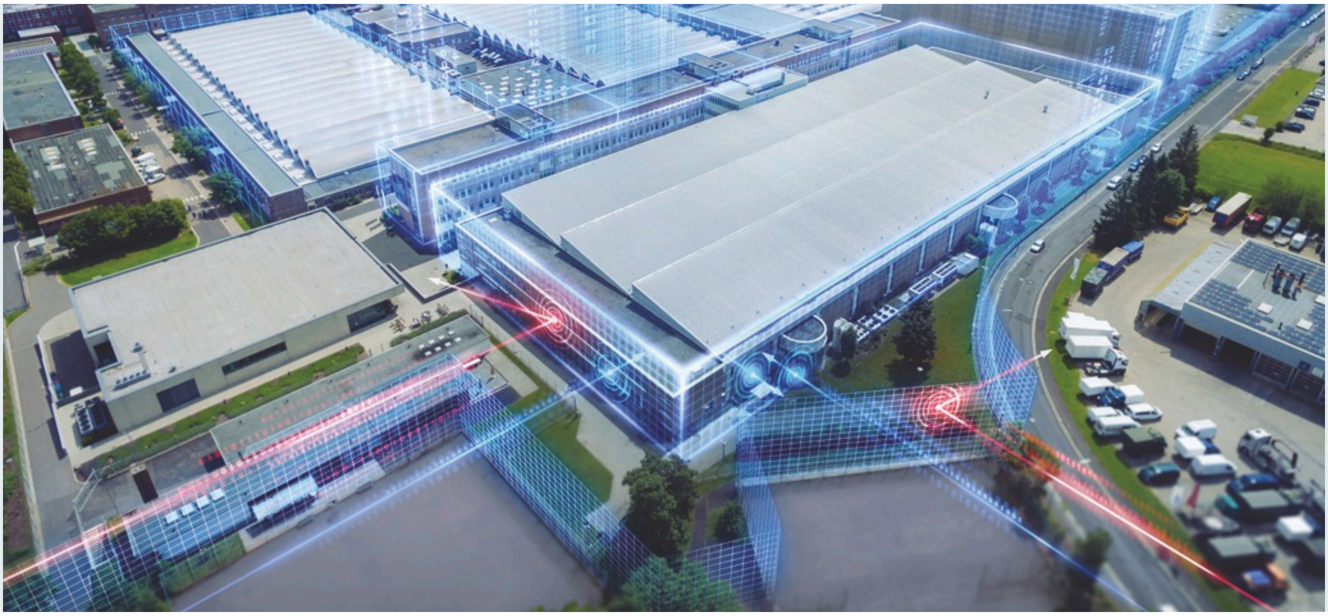


Secured communication, network access protection and network segmentation with Security Integrated components



- Physical protection
- Security management
- Security operation center

Industrial security – Prerequisite for digitization



The increasing digitization of companies and accompanying networking of practically all areas is creating significant economic potential. At the same time, however, digitization trends are producing new opportunities for attack and vulnerabilities due to increased communication, the transmission and storage of large data quantities and more open standards, which call for fast and consistent reactions. Cybersecurity and industrial security are therefore just as essential for digitization of companies as industrial communication and identification.

Industrial security as part of Totally Integrated Automation

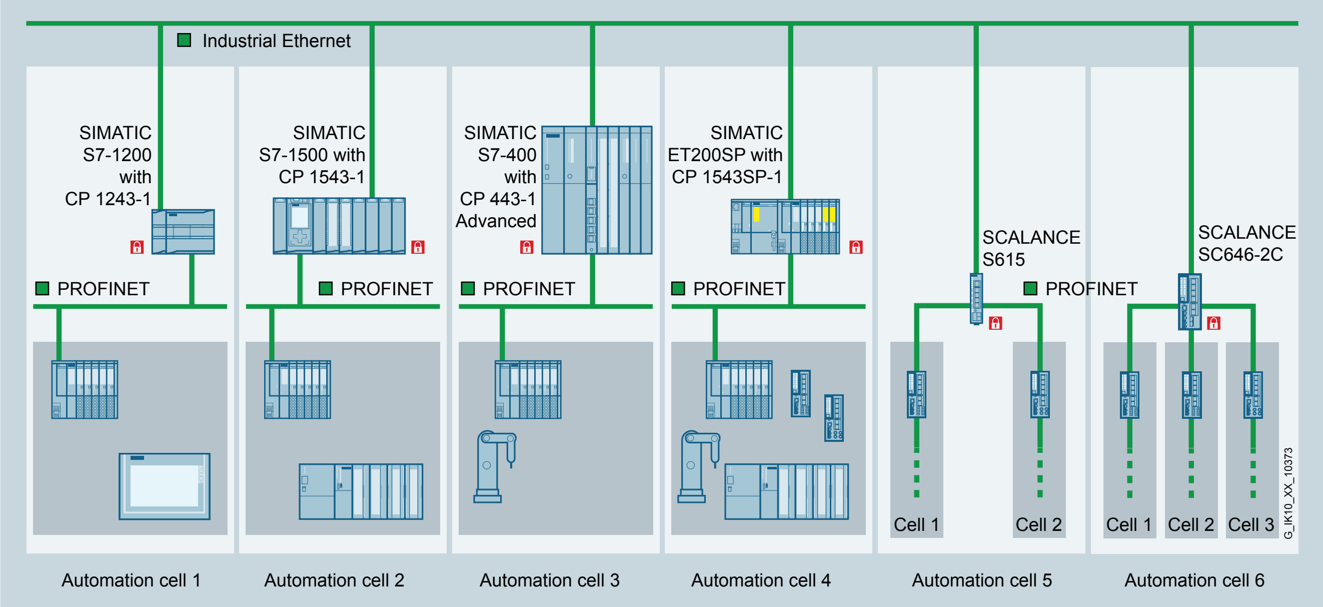
Totally Integrated Automation:
Efficient interaction between all automation components

With industry-compatible security products for network security and system integrity integrated in the TIA Portal, your automation solutions can be efficiently safeguarded and the defense-in-depth concept for protection of industrial plants and automation systems can be implemented.

All industrial security appliances and remote networks components are integrated in the TIA Portal and can be engineered there. In addition, the security communications processors are automatically assigned the firewall rules via the TIA Portal.

Network Security

Cell protection concept



Secured communication between components with Security Integrated in separate automation cells

Industrial communication is a key factor for corporate success – as long as the network is protected. For realization of the cell protection concept, Siemens partners with its customers to provide Security Integrated components, which not only have integrated communication functions but also special security functions such as firewall and VPN.

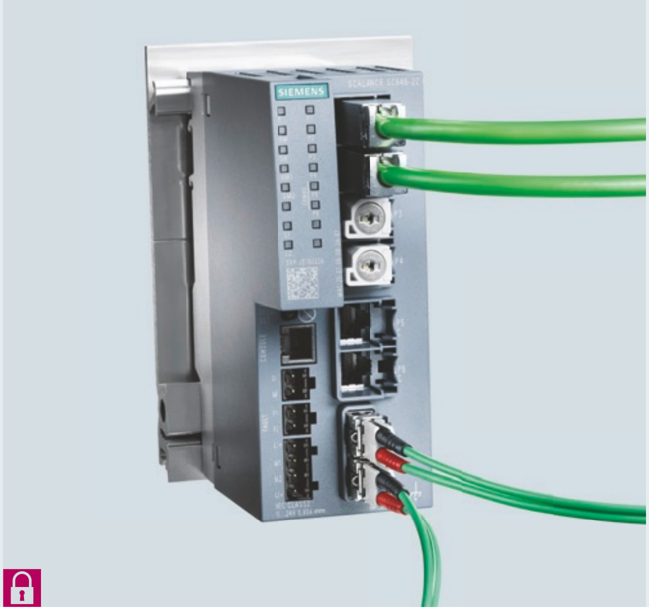
Cybersecurity - comprehensive security mechanisms

Siemens helps its customers benefit from technological progress while keeping risks in areas such as cybersecurity as low as possible. A security solution can only be implemented optimally when it is continuously adapted to new threats. Siemens is therefore vigilant regarding potential threats to itself, as well as those encountered by its customers.
Products, solutions and services from Siemens for cybersecurity offer proven protection in industrial plants, automation systems as well as in mains operation.

Cell protection concept

With the cell protection concept, a plant network is segmented into individual, protected automation cells within which all devices are able to securely communicate with each other. The individual cells are connected to the plant network in a secured manner with VPN and firewall. Cell protection reduces the susceptibility to failure of the entire production plant and thus increases its availability. Security Integrated products such as SCALANCE S Industrial Security Appliances and the SIMATIC S7/PC communications processors can be used for implementation.

SCALANCE S Industrial Security Appliance



The SCALANCE S Industrial Security Appliances offer protection of devices and networks in discrete manufacturing and in the process industry, and protect industrial communication with mechanisms such as Stateful Inspection Firewall as well as Virtual Private Networks (VPN).
The Industrial Security Appliances are suitable for industry-related applications and, depending on the requirement, are available with different port configurations (2 to 6 ports) and range of functions (firewall or firewall + VPN).
All versions enable configuration over Web Based Management (WBM), Command Line Interface (CLI), Simple Network Management Protocol (SNMP), network management SINEMA server as well as TIA Portal (V15 and higher).
All Industrial Security Appliances have a digital input (DI) for connection of a key-operated switch for controlled setup of a tunnel connection.

Industrial Firewall Appliances

SCALANCE SC632-2C and SCALANCE SC636-2C

- Firewall or encryption performance approx. 600 Mbit/s
- Network Address Translation (NAT), Network Address Port Translation (NAPT) for communication with series-produced machines with identical IP address bands
- Fiber optic for large distances (up to 200 km)
- Console port for direct access via programming device
- Secured remote access via SINEMA Remote Connect
- Simple device replacement with C-PLUG

Industrial VPN Appliances

SCALANCE S615

- Firewall and Virtual Private Network VPN (IPsec; OpenVPN as client and for connection to SINEMA Remote Connect)
- Up to five variable security zones per port-based Virtual Local Area Network (VLAN) allow configuration of security zones and firewall rules as needed between security zones
- Auto-configuration interface for easy configuration of a connection to SINEMA Remote Connect
- Connection via 10/100 Mbit/s ports
- Simple device replacement with C-PLUG

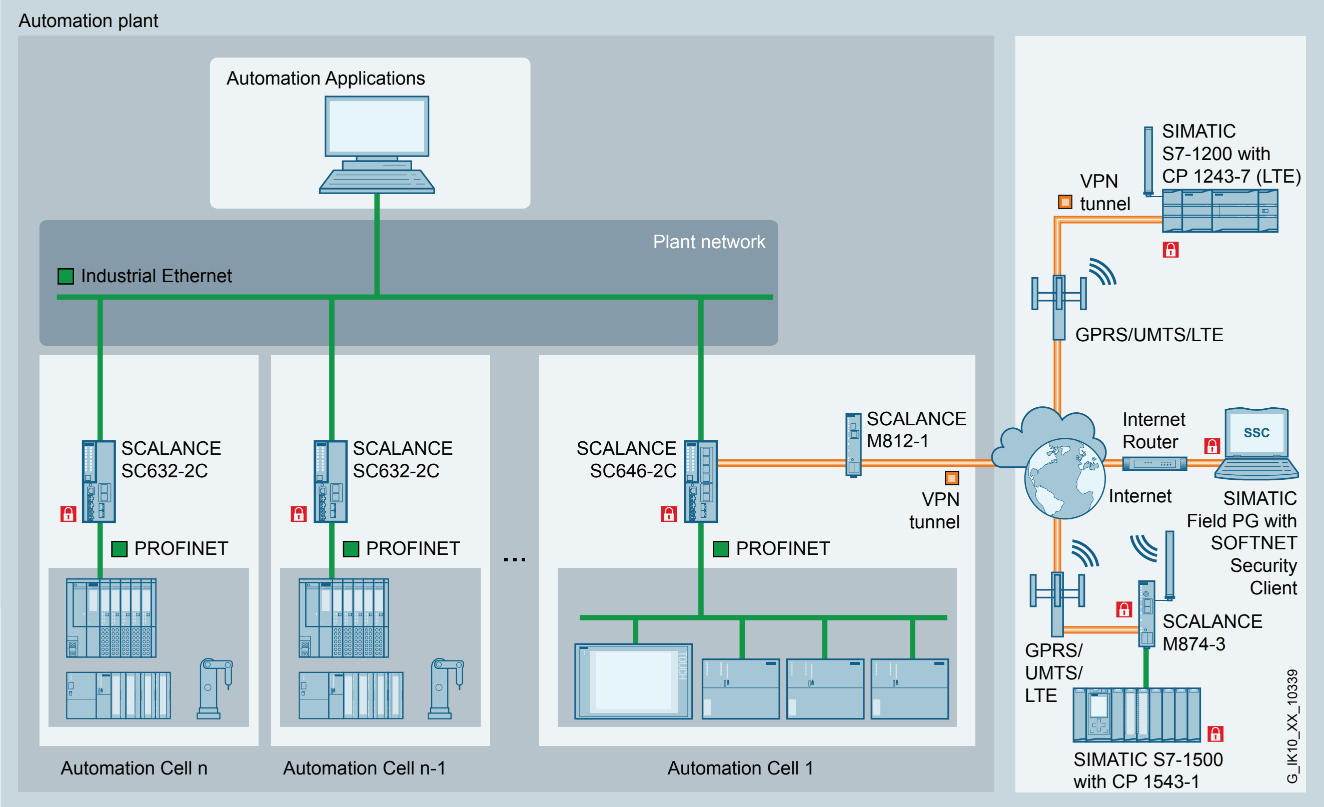
SCALANCE SC642-2C and SCALANCE SC646-2C

- Firewall or encryption performance approx. 600 Mbit/s
- Management of up to 200 VPN connections with a data rate of up to 120 Mbit/s
- Network Address Translation (NAT), Network Address Port Translation (NAPT) for communication with series-produced machines with identical IP address bands
- Fiber optic for large distances (up to 200 km)
- Console port for direct access via programming device
- Secured remote access via SINEMA Remote Connect
- Simple device replacement with C-PLUG

For more information on Industrial Security Appliances visit:
siemens.com/scalance-s

Application example

Secured remote maintenance with SCALANCE S



Secured remote access without direct connection to the automation network with SCALANCE S Industrial Security Appliances

Task

A system integrator requires secured Internet access to his machine, or part of an end user's plant, for servicing purposes. But the integrator is to be given access only to specific devices and not the plant network. In addition, a secured connection from the plant to a remote station via mobile networks (e.g. UMTS or LTE) is to be established.

Solution

Starting points are, for example, system integrator with VPN client (SOFTNET Security Client, CP 1628, SCALANCE M874-3)

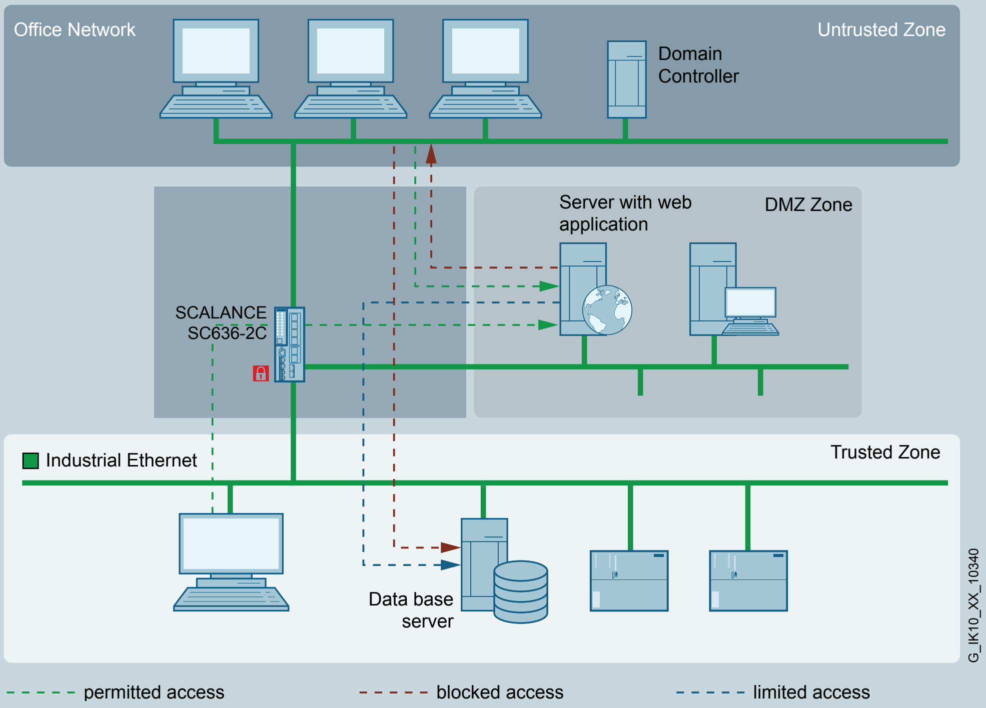
End point (automation system):
SCALANCE SC646-2C as VPN server

Advantages at a glance

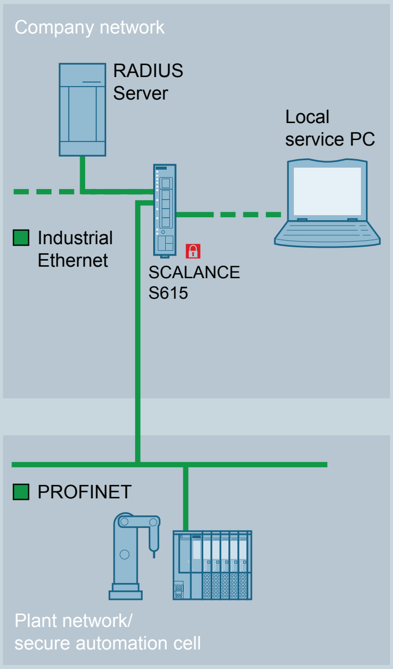
- Secured remote access via the Internet or mobile networks such as UMTS or LTE by safeguarding the data transmission with VPN (IPsec)
- Restriction of access possibilities with integrated firewall function
- Secured remote access to plant units without direct access to the plant network with SCALANCE SC646-2C firewall

Application example

Network access protection with DMZ



Network security as a central component of the Siemens Industrial Security concept



Connection of a local service PC
via the DMZ port of the SCALANCE S615

Task

Network nodes or servers (e.g. MES servers) are to be accessible from both the secured network and the insecure network without a direct connection between the networks.

Solution

A DMZ can be set up with the help of a SCALANCE SC636-2C. The servers can be positioned in this DMZ.

Advantages at a glance

- Increased security through data exchange via DMZ and prevention of direct access to the automation network
- Protection of automation networks against unauthorized access starting at the network boundaries

Task

The local network is to be protected against unauthorized access and authorized individuals are to receive only the access rights for their role.

Solution

The DMZ port of a SCALANCE S615 is the single locally accessible port.
The Industrial Security Appliance is connected to the plant network and a lower-level automation cell. User-specific firewall rules are created for each user. To receive access to the network, the user must be logged into the SCALANCE S with user name and password.

Advantages at a glance

- Securing the local network access
- Flexible and user-specific access rights
- Central authentication using RADIUS is possible

SCALANCE M routers and modems

The SCALANCE M portfolio consists of modems and routers for the areas telecontrol, teleservice and any additional application for Industrial Remote Communication.
The integrated firewall and VPN (IPsec; OpenVPN as client and for connection to SINEMA Remote Connection) security functions protect against unauthorized access and secured the data transmission.

Wireless connection to remote networks

The wireless SCALANCE M routers use the globally available, public cellular telephone networks (2G, 3G, 4G) for data transmission.

SCALANCE M874-2 supports the GSM data services GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for GSM Evolution).

SCALANCE M874-3 supports the UMTS data service HSPA+ (High Speed Packet Access) and therefore enables high transmission rates of up to 14.4 Mbit/s in the downlink and up to 5.76 Mbit/s in the uplink.

SCALANCE M876-3 supports Dual Band CDMA2000 and the UMTS data service HSPA+. Thus, it enables high transmission rates of up to 14.4 Mbit/s in the downlink and up to 5.76 Mbit/s in the uplink.

SCALANCE M876-4 supports LTE (Long Term Evolution). Thus, it enables high transmission rates of up to 100 Mbit/s in the downlink and up to 50 Mbit/s in the uplink.

Wired connection to remote networks

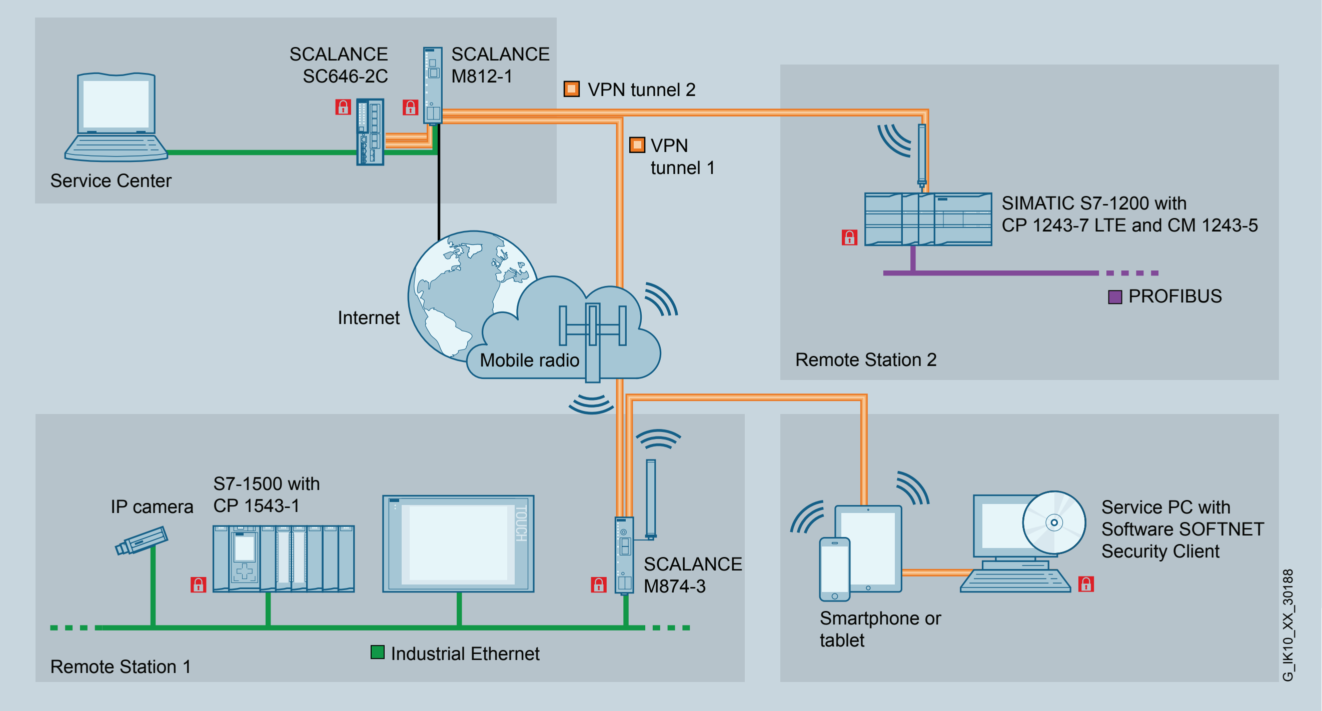
The SHDSL and ADSL2 routers of the SCALANCE M product family support the cost-effective and secured connection of Ethernet-based subnets and automation devices. The connection can be made over existing two-wire or stranded cables or wired telephone or DSL networks.

SCALANCE M812-1 and SCALANCE M816-1 are DSL routers for connection to wired telephone or DSL networks that support ASDL2+ (Asynchronous Digital Subscriber Line). Thus, the devices enable high transmission rates of up to 25 Mbit/s in the downlink and up to
1.4 Mbit/s in the uplink.

SCALANCE M826-2 is an SHDSL modem for connection via existing two-wire or stranded cables and supports the ITU-T standard G.991.2, or SHDSL.biz (Single-pair Highspeed Digital Subscriber Line). Thus, the device enables high symmetrical transmission rates of up to 15.3 Mbit/s per wire pair.

Application example

Secured access to plant sections via mobile wireless networks



VPN for secured remote maintenance with SCALANCE M874-3

Task

A service center is to be connected via the Internet, and typical applications such as remote programming, parameter assignment and diagnostics, but also monitoring of machines and plants installed worldwide are to possible.

Solution

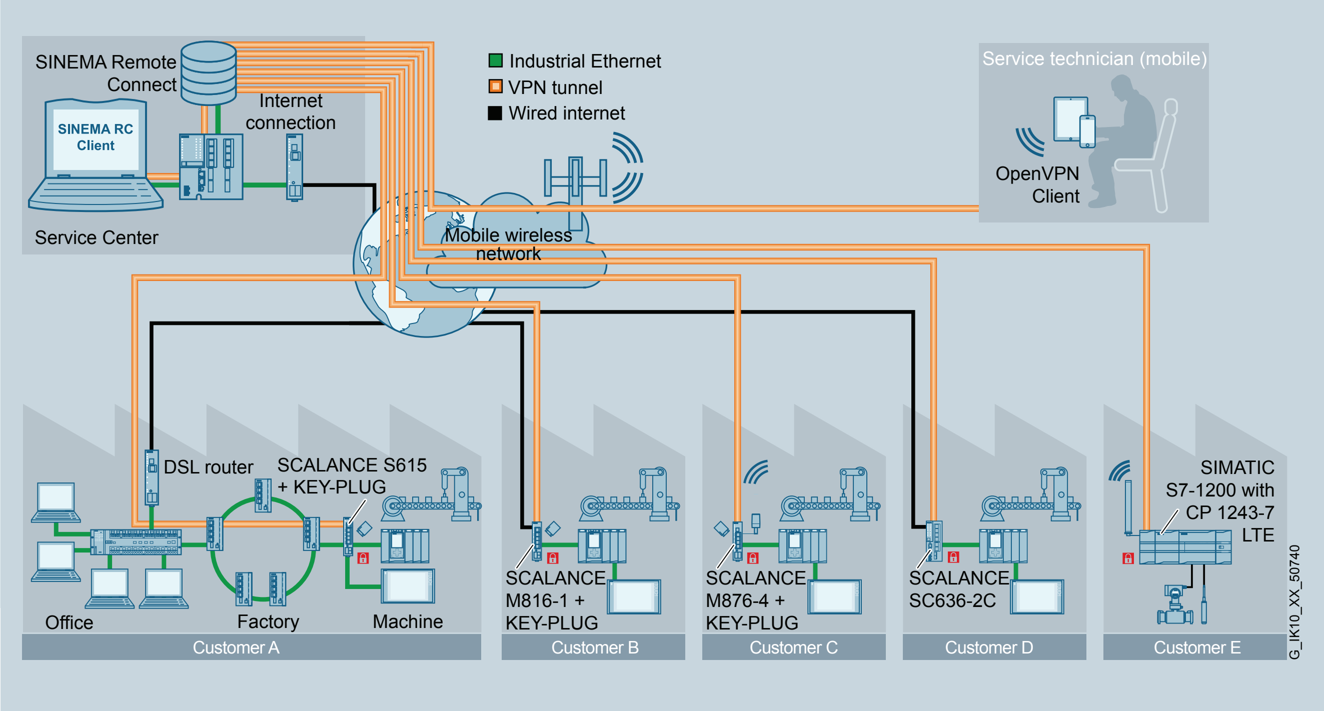
All IP-based devices and, in particular, automation devices in the local network behind the SCALANCE mobile wireless router (e.g. SCALANCE M874-3) can be accessed. Multimedia applications such as video streaming can also be implemented due to the increased bandwidth in the uplink. The VPN functionality allows secured data transmission around the world.

Advantages at a glance

- Low investment and operating costs for secured remote access to machines and equipment
- Lower travel costs and telephone charges thanks to remote programming and remote diagnostics via 3G/UMTS or 4G/LTE networks
- User-friendly diagnostics via Web interface
- Short transmission times due to high transmission rate with HSPA+
- Protection by integrated firewall and VPN
- Utilization of the existing UMTS or LTE infrastructure of the mobile wireless providers
- Can be used worldwide thanks to UMTS/GSM (quad band) technology; note country-specific approvals

Application example

Secured access to plant sections with SINEMA Remote Connect



Configuration example for SINEMA Remote Connect – General overview

Task

- Remote maintenance for series machines and larger plants with identical subnets
- Remote access to special-purpose machines and sensitive areas. Central management of the connections needed to acquire status/maintenance data
- Easy creation of devices with routing/NAT information

Solution

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

Typical areas of application

- Plant and machine builders
- Energy distribution / substations (municipal authorities)
- Logistics / port logistics
- Intelligent Traffic Systems (ITS) / transportation companies
- Water & wastewater (municipal authorities, etc.)

Advantages at a glance

- High transparency and security
- Logging of accesses
- Secured and easy access to plant sections from anywhere in the world (with OpenVPN and IPsec)
- Current encryption method TLS 1.2
- Optimum connection of identical machines with identical local subnets (NAT)
- Convenient management of different users (service technicians) through group management
- Quick and effortless connection setup thanks to address book function
- Easy integration into industrial facilities
- No special IT know-how required thanks to simple user interface with auto-configuration for terminal devices and SINAMA RC Client
- Secured and convenient multifactor authentication with user name / password and PKI Smartcard
- Operation in virtual environment is possible

Security communications processors for SIMATIC S7-1200, S7-1500 and ET 200SP CPU

Security communications processors protect controllers with integrated firewall (control of data flow) and VPN for protection against data manipulation and espionage.

CP 1243-1 and CP 1243-7 LTE

The CP 1243-1 and CP 1243-7 LTE communications processors connect the SIMATIC S7-1200 controller to Ethernet networks (CP 1243-1) or mobile wireless networks (CP 1243-7 LTE). With its integrated firewall (Stateful Inspection) and VPN (IPsec) security functions, the communications processor protects S7-1200 stations and lower-level networks against unauthorized access and protects data transmission against manipulation and espionage by encrypting it. Furthermore, the CPs can also be used for integrating the S7-1200 station into the TeleControl Server Basic control center software via IP-based remote networks.

Advantages at a glance

A special advantage of the security communications processors for SIMATIC controllers is the automatic creation of firewall rules during configuration with the TIA Portal. Configured communication connections are automatically enabled in the firewall so that the configuration effort and the error rate are drastically reduced.

CP 1543SP-1

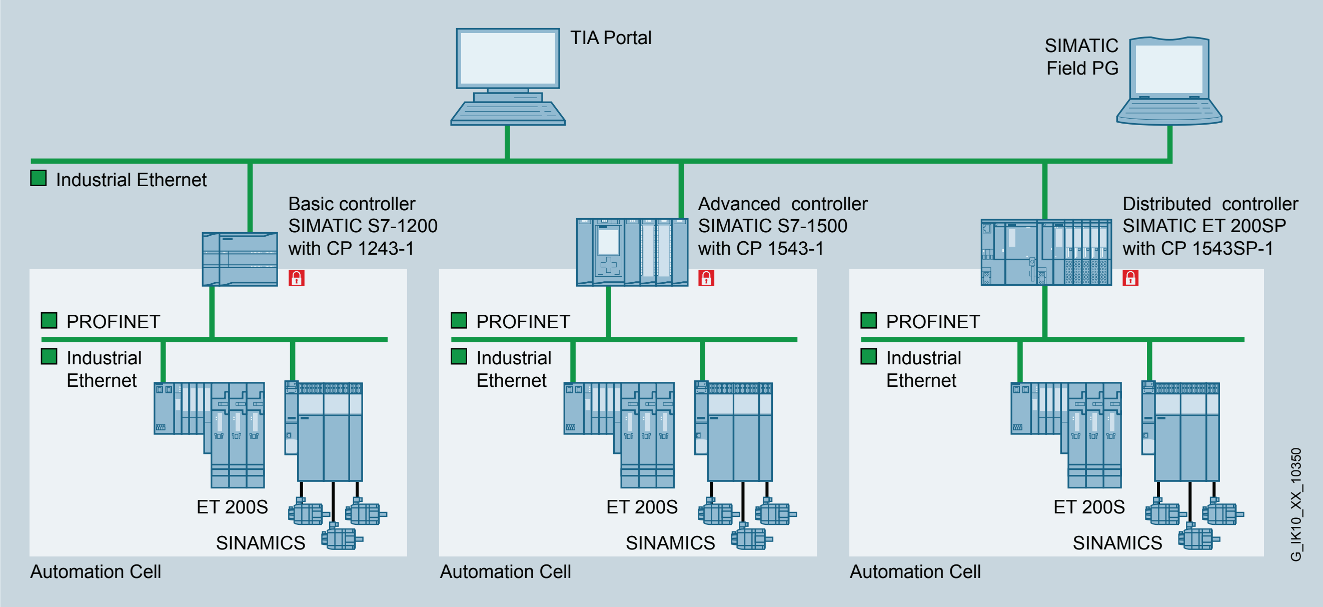
The CP 1543SP-1 communications processor allows the SIMATIC ET 200SP System to be flexibly expanded to include an Industrial Ethernet interface. This enables the setup of identical machines with the same IP addresses through network segmentation.

It also offers extended security functions, such as encryption of all transmitted data using VPN with IPsec or the Stateful Inspection Firewall for secure access to the SIMATIC ET 200SP.

CP 1543-1

The CP 1543-1 communications processor securely connects the SIMATIC S7-1500 controller to Ethernet networks. With its integrated firewall (Stateful Inspection) and VPN (IPsec) security functions and protocols for data encryption such as FTPS and SNMPv3, the communications processor protects S7-1500 stations and lower-level networks against unauthorized access and protects data transmission against manipulation and espionage by encrypting it. The CP also has encrypted e-mail communication via SMTPS (Ports 587 and 25) and secured open communication via TCP/IP.

Application example
Network segmentation with security communications processors



Segmentation of networks and protection of the SIMATIC controllers S7-1200 with CP 1243-1, S7-1500 with CP 1543-1 or SIMATIC ET 200SP CPU with CP 1543SP-1

Task
Communication between the automation network and lower-level networks on SIMATIC controllers is to be secured by means of access control.

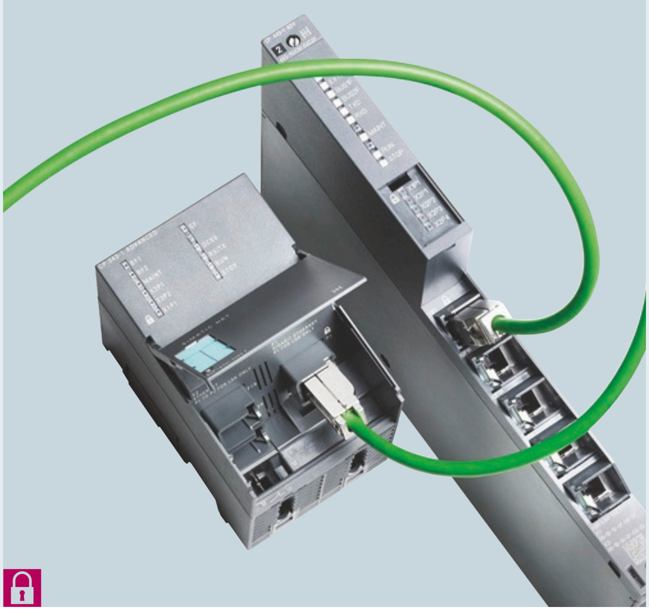
Solution
The communications processors are placed in the rack of the respective target system (S7-1200, S7-1500, ET 200SP) upstream of the automation cells to be protected. In this way, the communication to and from the SIMATIC CPU and lower-level automation cell is restricted to the permitted connections with the aid of firewall rules and, if necessary, protected against manipulation or espionage by setting up VPN tunnels.

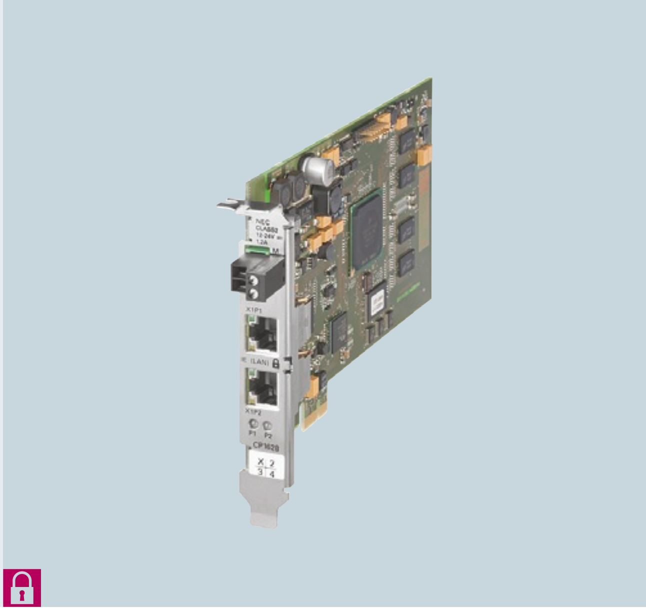
Advantages at a glance

- Secured connection of the SIMATIC S7-1200, S7-1500 and ET 200SP CPU to Industrial Ethernet by means of integrated Stateful Inspection Firewall and VPN
- Additional secured communication possibilities: File transfer and email
- Use in an IPv6-based infrastructure [1]

[1] Applies to CP 1543-1, CP 1543SP-1

Security communications processors for SIMATIC S7-300, S7-400 and PG/PC





CP 343-1 Advanced and CP 443-1 Advanced

Alongside the familiar communication functions, an integrated switch and Layer 3 routing functionality, the Industrial Ethernet communications processors CP 343-1 Advanced and CP 443-1 Advanced for SIMATIC S7-300 and S7-400 contain Security Integrated, i.e. a Stateful Inspection Firewall and a VPN gateway for protection of the controller and lower-level devices against security risks.

CP 1628

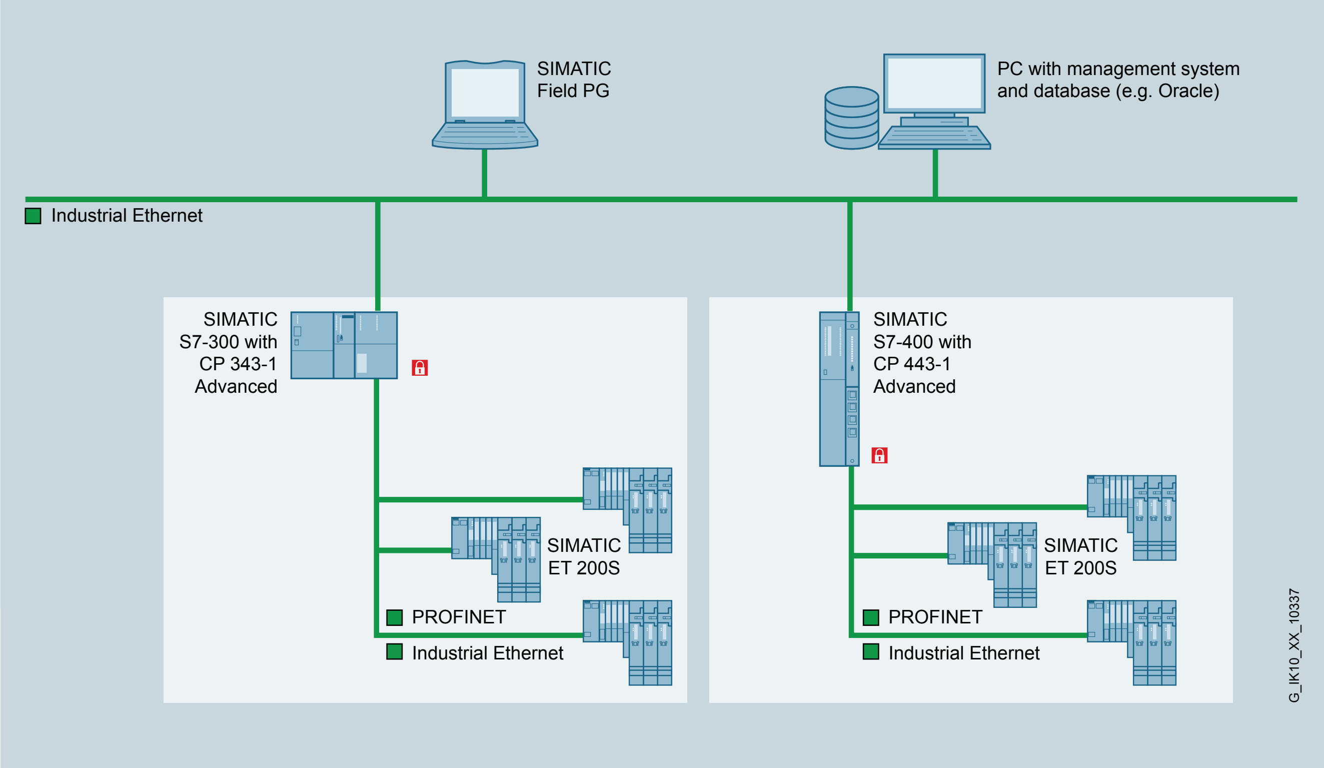
The CP 1628 Industrial Ethernet communications processor protects Industrial PCs through a firewall and VPN – for secured communication without special operating system settings. In this manner, computers equipped with the module can be connected to protected cells. The CP 1628 makes it possible to connect a SIMATIC PG/PC and PCs with PCI Express slot to Industrial Ethernet (10/100/1000 Mbit/s). Additional field devices can be flexibly connected to Industrial Ethernet via the integrated switch. Along with the automation functions familiar from CP 1623, the communications processor also has Security Integrated, i.e. a Stateful Inspection Firewall and a VPN gateway for protection of the PG/PC system against security risks.

Advantages at a glance

A special advantage of the security communications processors for SIMATIC controllers is the automatic creation of firewall rules during configuration with the TIA Portal. Configured communication connections are automatically enabled in the firewall so that the configuration effort and the error rate are drastically reduced.

Application example

Network segmentation with security communications processors



Segmentation of networks and protection of the SIMATIC S7-300 and S7-400 controllers with CP 343-1 Advanced or CP 443-1 Advanced

Task

Communication between the administration system on the office level and lower-level networks of the automation level is to be secured by means of access control.

Solution

CP 343-1 Advanced and
CP 443-1 Advanced are placed upstream of the automation cells to be protected. As a result, communication is limited to the permitted connections with the aid of firewall rules.

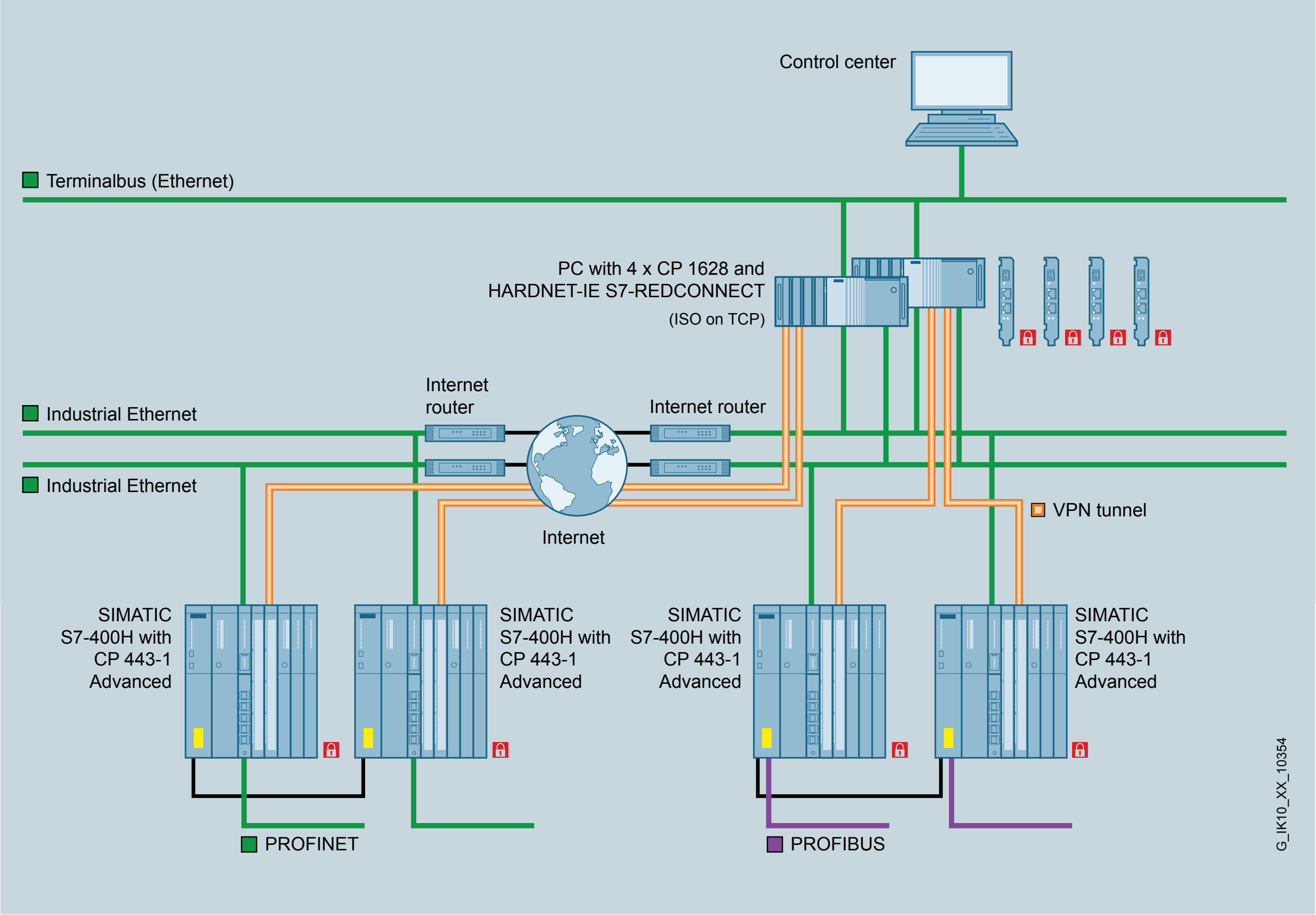
Advantages at a glance

- Firewall, VPN gateway and CP in one device:
  Advanced CPs come with integrated firewall and VPN security functions for implementing a protected automation cell and for protecting data transmission
- Secure communication integration: CPs are easily configured with STEP 7;
  VPN tunnels can be set up between the CPs or to the SCALANCE S Industrial Security Appliance, the SOFTNET Security Client VPN software, the CP 1628 PC module and the SCALANCE M Internet and mobile wireless routers.

All CP 343-1 Advanced and CP 443-1 Advanced users get Security Integrated and do not need separate hardware or special tools besides SIMATIC S7 to configure the security of industrial plants.

Application example

Secured redundant coupling with security communications processors



Secured redundant coupling with CP 1628 and CP 443-1 Advanced

Task

Protection for the redundant connections between a PC system and the S7-400H controllers in a high-availability plant.

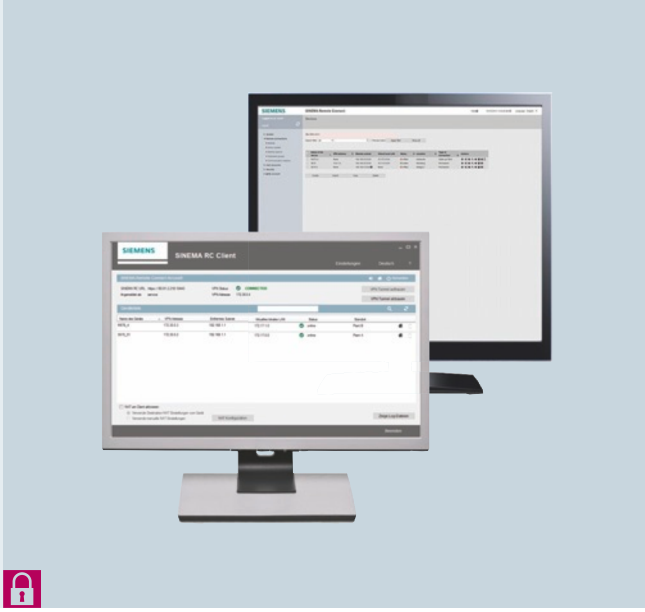
Solution

VPN tunnels are set up between the security communications processors CP 1628 and CP 443-1 Advanced, which allow the secured transmission of the H communication. In addition, the CP 1628 protects the PC system from unauthorized access by means of its integrated firewall.

Advantages at a glance

- Firewall, VPN gateway and CP in one device: with this product variant, the user has an integrated, fully-fledged security module and thus protects the PC from manipulation and unauthorized access.
- Secured communication integration: CP is easily configured with STEP 7/NCM PC (V5.5 SP3 or higher) or with STEP 7 (TIA Portal) V12 SP1 or higher.

SOFTNET Security Client and SINEMA Remote Connect



SOFTNET Security Client

The SOFTNET Security Client enables programming devices, PCs and notebooks to set up a VPN connection to other VPN appliances, such as SCALANCE S, SCALANCE M or security communications processors. Secured client access to automation systems via LAN or via WAN (e.g. for remote maintenance via the Internet) is thus possible. Plant disturbances can be prevented because only authorized programming devices or notebooks are permitted to access automation devices or automation cells.

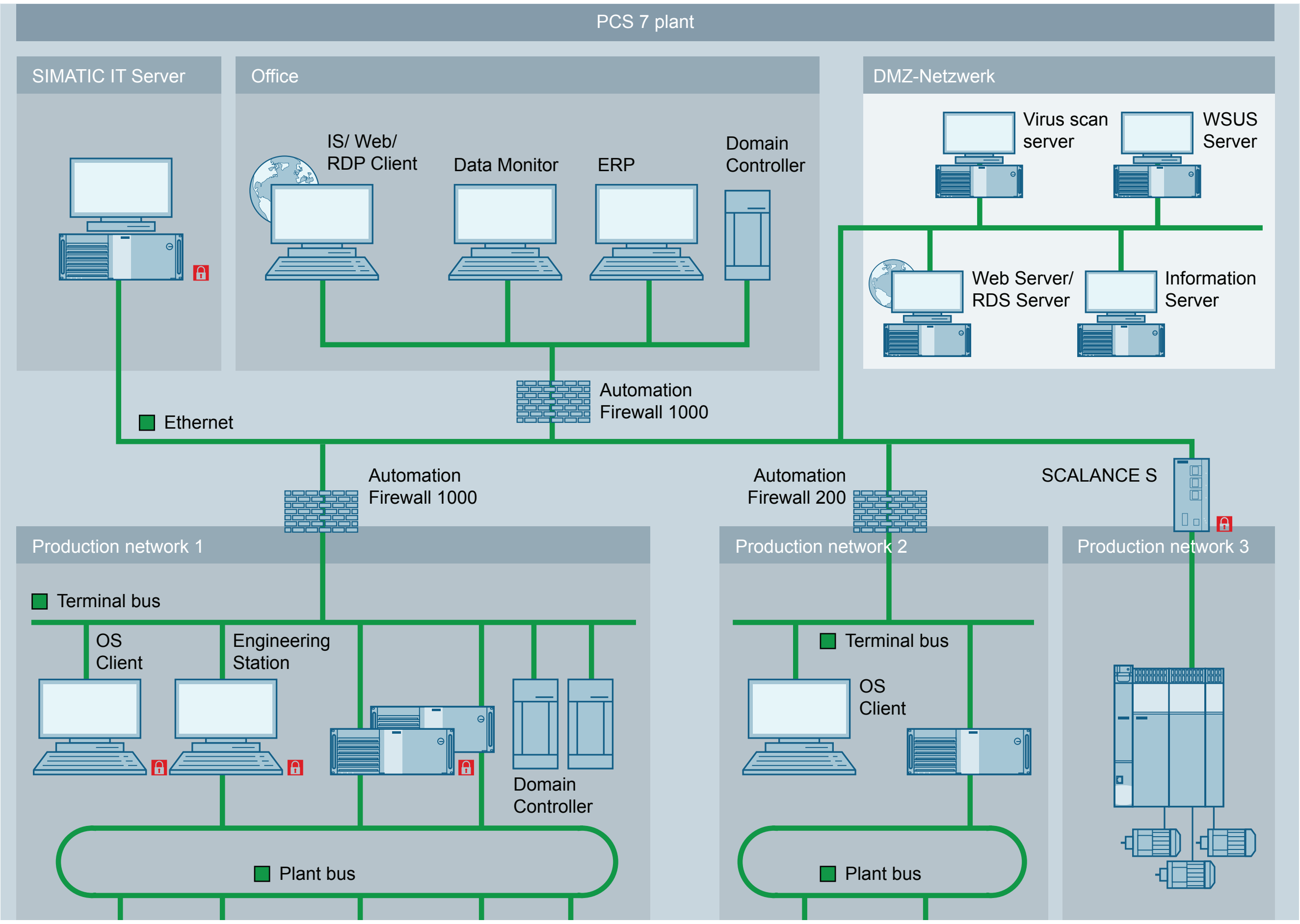
The use of software on mobile PCs provides greater flexibility because additional hardware is not needed to secure the communication.

SINEMA Remote Connect

The management platform for remote networks that facilitates remote access to machines and equipment around the world. SINEMA Remote Connect ensures the secured administration of tunnel connections (VPN) between the service center, the service engineers and the installed equipment. Direct access to the corporate network, in which the equipment or machine is integrated, is prevente initially. The service technician and the machine undergoing maintenance separately establish a connection to the SINEMA Remote Connect server. This then verifies the identity of the individual stations by an exchange of certificates, before any access to the machine is granted.

The connection to SINEMA Remote Connect can be established using a variety of media, such as cellular phone networks, DSL or existing private network infrastructures.

SIMATIC PCS 7 Security



SIMATIC PCS 7 Security – Example system

A top priority in PCS 7 is that operating personnel always retain control over production and processes, even when security threats occur. Full operator control and monitoring capabilities are to be retained when actions are being taken to prevent or contain security threats in plants and networks. A security concept for PCS 7 is to ensure that only authenticated users can perform authorized operator inputs on authenticated devices using the possible operator inputs assigned to them. These operator inputs are to be performed using only clearly-defined and planned access paths in order to ensure reliable production or coordination of an order without endangering people, the environment, the product, the goods to be coordinated, or the company's business.

The PCS 7 Security concept follows the defense-in-depth strategy. That is, multiple protection levels are created in order to minimize risks and to increase the security of plants with the following functions:

- Assignment of access rights only to certain users, with SIMATIC LOGON
- Firewalls: segmentation of your networks, use of security cells, firewalls and so-called demilitarized zones (DMZ), which allow certain network areas to be segmented for security purposes
- VPN: secured communication over insecure networks
- Use of up-to-date virus scanners and adoption of a patch management strategy in order to reduce the risk of harm to your system
- Specification of the programs that are permitted to be run on your system – through the use of so-called whitelisting

Elements of the PCS 7 Security concept

- System hardening
- User administration (SIMATIC Logon)
- Patch management
- Malware detection and prevention
- Firewalls and cell protection
- Training and processes

Technical specifications

SCALANCE S Industrial Security Appliances

	Industrial Firewall Appliances		Industrial VPN Appliances		
Product type designation	**SCALANCE SC632-2C**	**SCALANCE SC636-2C**	**SCALANCE S615**	**SCALANCE SC642-2C**	**SCALANCE SC646-2C**
Article number	**6GK5632-2GS00-2AC2**	**6GK5636-2GS00-2AC2**	**6GK5615-0AA00-2AA2**	**6GK5642-2GS00-2AC2**	**6GK5646-2GS00-2AC2**
Transmission rate					
Transmission rate	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s	10 / 100 Mbit/s	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s
Interfaces					
Electrical connection	2x RJ45 port	6x RJ45 port	5x RJ45 port	2x RJ45 port	6x RJ45 port
Optical connection	2x combo port with SFP	2x combo port with SFP	–	2x combo port with SFP	2x combo port with SFP
for signaling contact	1x 2-pin terminal block	1x 2-pin terminal block	–	1x 2-pin terminal block	1x 2-pin terminal block
for power supply	1x 4-pin terminal block	1x 4-pin terminal block	1x 5-pin terminal block	1x 4-pin terminal block	1x 4-pin terminal block
C-PLUG swap medium	Yes	Yes	Yes	Yes	Yes
Supply voltage, current consumption, power loss					
Supply voltage, external	24 V DC	24 V DC	24 V DC	24 V DC	24 V DC
Range	9.6 V ... 31.2 V DC	9.6 V ... 31.2 V DC	10.8 V ... 28.2 V DC	9.6 V ... 31.2 V DC	9.6 V ... 31.2 V DC
Permissible ambient conditions					
Ambient temperature					
during operation	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C
during storage	-40 °C ... +85 °C	-40 °C ... +85 °C	-40 °C ... +80 °C	-40 °C ... +85 °C	-40 °C ... +85 °C
during transport	-40 °C ... +85 °C	-40 °C ... +85 °C	-40 °C ... +80 °C	-40 °C ... +85 °C	-40 °C ... +85 °C
Degree of protection	IP20	IP20	IP20	IP20	IP20
Design, dimensions and weight					
Design	Compact	Compact	Compact	Compact	Compact
Width / height / depth	60 mm / 145 mm / 125 mm	60 mm / 145 mm / 125 mm	35 mm / 147 mm / 127 mm	60 mm / 145 mm / 125 mm	60 mm / 145 mm / 125 mm
Net weight	0.58 kg	0.58 kg	0.4 kg	0.58 kg	0.58 kg
Product function: Security					
Firewall type	Stateful Inspection	Stateful Inspection	Stateful Inspection	Stateful Inspection	Stateful Inspection
Password protection	Yes	Yes	Yes	Yes	Yes
Product function with VPN connection	OpenVPN (as client for SINEMA RC)	OpenVPN (as client for SINEMA RC)	IPsec, OpenVPN (as client for SINEMA RC)	IPsec, OpenVPN (as client for SINEMA RC)	IPsec, OpenVPN (as Client for SINEMA RC)
IPsec VPN data throughput	_	_	35 Mbit/s	120 Mbit/s	120 Mbit/s
Number of possible connections with VPN connection	0	0	20	200	200
Firewall data throughput	600 Mbit/s	600 Mbit/s	100 Mbit/s	600 Mbit/s	600 Mbit/s
NAT/NAPT	Yes	Yes	Yes	Yes	Yes
Encryption algorithms	–	–	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Authentication procedure	–	–	Preshared Key, X.509v3 certificates	Preshared Key, X.509v3 certificates	Preshared Key, X.509v3 certificates
Hashing algorithms	–	–	MD5, SHA-1, SHA-256, SHA-384, SHA-512	MD5, SHA-1	MD5, SHA-1

SCALANCE M mobile wireless and DSL routers

Product type designation	SCALANCE M wireless		SCALANCE M wired		
	M874-2, M874-3	M876-3, M876-4	M812/M816		M826
Article number	6GK5874-2AA00-2AA2 6GK5874-3AA00-2AA2	6GK5876-3AA02-2BA2 6GK5876-4AA00-2BA2	6GK5812-1BA00-2AA2 6GK5816-1BA00-2AA2		6GK5826-2AB00-2AB2
Transmission rate					
1 with Industrial Ethernet / 2 with Industrial Ethernet	10 Mbit/s / 100 Mbit/s		10 Mbit/s / 100 Mbit/s		
GPRS transmission uplink / downlink, max.	85.6 Kbit/s	85.6 Kbit/s	–		–
EDGE transmission uplink / downlink, max.	237 Kbit/s	237 Kbit/s	–		–
HSPA+ transmission uplink / downlink, max.	5.76 Mbit/s	14.4 Mbit/s	–		–
EV-DO transmission forward link / reverse link	–	3.1 Mbit/s / 1.8 Mbit/s (M876-3 only)	–		–
LTE transmission uplink / downlink, max.	–	50 Mbit/s / 100 Mbit/s (M876-4 only)	–		–
ADSL2+ transmission uplink / downlink, max.	–	–	1.4 Mbit/s / 25 Mbit/s		–
SHDSL transmission, max	–	–	–		15.3 Mbit/s
Interfaces					
Number of electrical connections					
- for internal network	2	4	1	4	4
- for external network	1	2	1	1	2
- for power supply	2	2	2	2	2
Electrical connection					
- for internal network	RJ45 port (10/100 Mbit/s, TP, autocrossover)		RJ45 port (10/100 Mbit/s, TP, autocrossover)		
- for external network	SMA antenna sockets (50 ohms)		RJ45 DSL port	–	Terminal strip
- for power supply	Terminal strip			–	–
Supply voltage, current consumption, power loss					
Supply voltage / range	10.8 V ... 28.8 V		10.8 V ... 28.8 V		
Permissible ambient conditions					
Ambient temperature during operation [°C]	-20 ... +60		-0 °... +60	0 ... +60	-40 ... +70
Ambient temperature during storage [°C]	-40 ... +85		-40 ... +70	-40 ... +70	-40 ... +80
Degree of protection	IP20		IP20		
Design, dimensions and weight					
Module format	Compact		Compact		
Width / height / depth	35 mm / 147 mm / 127 mm		35 mm / 147 mm / 127 mm		
Net weight	0.4 kg		0.4 kg		
Product function: Security					
Firewall type	Stateful Inspection		Stateful Inspection		
Password protection	Yes		Yes		
Packet filter	Yes		Yes		
Product function with VPN connection	IPsec, OpenVPN (as client)		IPsec, OpenVPN (as client)		
Number of possible connections with VPN connection	20		20		
PSK type of authentication for VPN	Yes		Yes		
Key length					
1 | 2 | 3 with IPsec AES for VPN	128 bit | 192 bit | 256 bit		128 bit | 192 bit | 256 bit		
with IPsec 3DES / with virtual private network	168 bit		168 bit		
Main mode Internet Key Exchange in VPN	Yes		Yes		
Quick mode Internet Key Exchange in VPN	Yes		Yes		
Type of packet authentication for VPN	MD5, SHA-1, SHA-256, SHA-384, SHA-512		MD5, SHA-1, SHA-256, SHA-384, SHA-512		

Communications processors CP 1243-1, CP 1243-7, CP 1543-1 and CP 1543SP-1

Product type designation	CP 1243-1	CP 1243-7	CP 1543-1	CP 1543SP-1
Article number	6GK7243-1BX30-0XE0	6GK7243-7KX30-0XE0	6GK7543-1AX00-0XE0	6GK7543-6WX00-0XE0
Transmission rate				
at interface 1 / 2	10/100 Mbit/s / –	–	10/100/1 000 Mbit/s / –	10 ... 100 Mbit/s
Interfaces				
Electrical connection				
to interface 1 according to IE	1x RJ45 port	–	1x RJ45 port	2 x RJ45 port (using BusAdapter)
to interface 2 according to IE	–	–	–	–
for power supply	–	1	–	–
C-PLUG swap medium	–		–	–
Supply voltage, current consumption, power loss				
Supply voltage				
1 from backplane bus	5 V DC	–	15 V DC	–
external	–	24 V DC	–	24 V DC
Permissible ambient conditions				
Ambient temperature				
during operation				
- when installed vertically	-20 °C ... +60 °C	-20 °C ... +60 °C	0 °C ... +40 °C	0 °C ... +50 °C
- when installed horizontally	-20 °C ... +70 °C	-20 °C ... +70 °C	0 °C ... +60 °C	0 °C ... +60 °C
during storage	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C
during transport	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C	-40 °C ... +70 °C
Degree of protection	IP20	IP20	IP20	IP20
Design, dimensions and weight				
Module format	Compact S7-1200, single width	Compact S7-1200, single width	Compact S7-1500, single width	Compact module for ET 200SP
Width / height / depth	30 mm / 110 mm / 75 mm	30 mm / 100 mm / 75 mm	35 mm / 142 mm / 129 mm	60 mm / 117 mm / 74 mm
Net weight	0.122 kg	0.133 kg	0.35 kg	0.18 kg
Product function: Security				
Firewall type	Stateful Inspection	Stateful Inspection	Stateful Inspection	Stateful Inspection
Product function with VPN connection	IPsec	IPsec	IPsec	IPsec
Type of encryption algorithms with VPN connection	AES-256, AES-192, AES-128, 3DES-168	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Type of authentication methods with VPN connection	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates
Type of hashing algorithms with VPN connection	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1
Number of possible connections with VPN connection	8	1	16	4
Product function				
Password protection for Web applications	No	–	No	–
ACL – IP-based	No	–	No	–
ACL – IP-based for PLC/routing	No	–	No	–
Deactivation of services that are not needed	Yes	–	Yes	Yes
Blocking of communication via physical ports	No	–	No	Yes
Log file for unauthorized access	No	–	Yes	Yes

Communications processors
CP 343-1 Advanced, CP 443-1 Advanced and CP 1628

Product type designation	CP 343-1 Advanced	CP 443-1 Advanced	CP 1628
Article number	6GK7343-1GX31-0XE0	6GK7443-1GX30-0XE0	6GK1162-8AA00
Transmission rate			
at interface 1 / 2	10 /1000 Mbit/s / 10/100 Mbit/s	10/1000 Mbit/s / 10/100 Mbit/s	10/1 000 Mbit/s / –
Interfaces			
Electrical connection			
to interface 1 according to IE	1x RJ45 port	1x RJ45 port	2x RJ45 port
to interface 2 according to IE	2x RJ45 port	4x RJ45 port	–
of the backplane bus			PCI Express x1
for power supply	2-pin plug-in terminal strip	–	1x 2-pin terminal block
C-PLUG swap medium	Yes	Yes	
Supply voltage, current consumption, power loss			
Type of power supply voltage	–	–	DC
Supply voltage			
1 from backplane bus	5 V DC	5 V DC	
2 from backplane bus			3.3 V
external	24 V DC	–	12 V
Range	–	–	24 V 10.5 V ... 32 V
Permissible ambient conditions			
Ambient temperature			
during operation		0 °C ... +60 °C	+5 °C ... +55 °C
- when installed vertically	0 °C ... +40 °C	–	–
- when installed horizontally	0 °C ... +60 °C	–	–
during storage	-40 °C ... +70 °C	-40 °C ... +70 °C	-20 °C ... +60 °C
during transport	-40 °C ... +70 °C	-40 °C ... +70 °C	-20 °C ... +60 °C
Degree of protection	IP20	IP20	–
Design, dimensions and weight			
Module format	Compact	Compact S7-400 single width	PCI Express x1 (half length)
Width / height / depth	80 mm / 125 mm / 120 mm	25 mm / 290 mm / 210 mm	18 mm / 111 mm / 167 mm
Net weight	0.8 kg	0.7 kg	0.124 kg
Product function: Security			
Firewall type	Stateful Inspection	Stateful Inspection	Stateful Inspection
Product function with VPN connection	IPsec	IPsec	IPsec
Type of encryption algorithms with VPN connection	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Type of authentication methods with VPN connection	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates
Type of hashing algorithms with VPN connection	MD5, SHA-1	MD5, SHA-1	MD5, SHA-1
Number of possible connections with VPN connection	32	32	64
Product function			
Password protection for Web applications	Yes	Yes	–
ACL – IP-based	Yes	Yes	–
ACL – IP-based for PLC/routing	Yes	Yes	–
Deactivation of services that are not needed	Yes	Yes	–
Blocking of communication via physical ports	Yes	Yes	–
Log file for unauthorized access	No	No	–

SOFTNET Security Client and SINEMA Remote Connect

Product type designation	SOFTNET Security Client	SINEMA Remote Connect	SINEMA RC Client
Article number	6GK1704-1VW04-0AA0	6GK1720-1AH01-0BV0	6GK1721-1XG01-0AA0
Transmission rate			
at interface 1 / 2	dependent on the PC system		
Product function: Security			
Firewall type	–	–	–
Product function with VPN connection	IPsec	IPsec/OpenVPN	OpenVPN
Type of encryption algorithms with VPN connection	AES-256, AES-192, AES-128, 3DES, DES	AES-128, 192, 256: Advanced Encryption Standard (128-, 192- or 256-bit key length, mode CBC) DES-EDE, DES-EDE3: Data Encryption Standard (128- or 192-bit key length, mode CBC)	
Type of authentication methods with VPN connection	Preshared key (PSK), X.509v3 certificates	Certificate	Certificate
Type of hashing algorithms with VPN connection	MD5, SHA-1	IPsec: SHA 1, 256, 384, 512 OpenVPN: SHA-1, 256, 512	OpenVPN: SHA-1, 256, 512
Number of possible VPN connections	Unlimited or dependent on the computer configuration	Unlimited or dependent on the target system, network	1:1 relationship with SINEMA Remote Connect server

Industrial Security

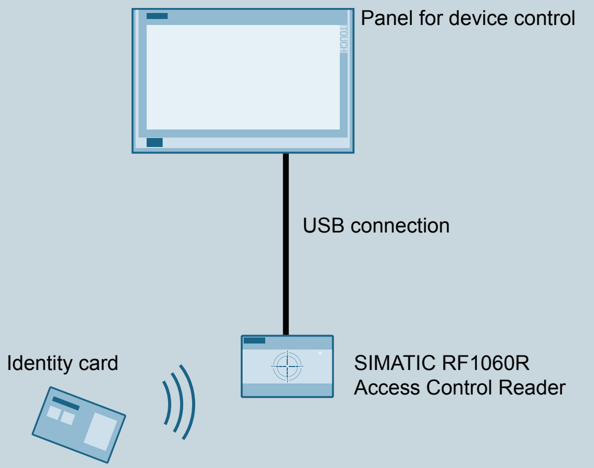
IE RJ45 Port Lock

IE RJ45 Port Lock

Physical network access protection with IE RJ45 Port Lock

A well-balanced and holistic security concept also includes physical protection measures. A known problem is the presence of open unused RJ45 ports that can be used by unauthorized persons to gain access to the network. The IE RJ45 Port Lock has been developed to reduce this risk. The IE RJ45 Port Lock enables mechanical locking of RJ45 ports at terminal devices or network components. The rugged design of the port lock in the form of a plug-in connector completely occupies the RJ45 port. In this way, the insertion of RJ45 cables can be prevented and undesired use of unused RJ45 ports on unconfigurable network components can also be avoided. The detent lug of the RJ45 Port Lock is blocked by the integrated lock, which can only be unlocked with a mechanical key. Additional advantages of the port lock are its rugged, industry-compatible mounting technology and its ease of installation without additional tools thanks to the RJ45-compatible design.

SIMATIC RF1060R Access Control Reader



Access to machines with existing RFID-based identification card system

SIMATIC RF1060R

The growing demands for security and increasing requirements for documentation call for solutions that can control access to machines and equipment on a user-specific basis. With its new SIMATIC RF1060R Reader, Siemens is providing a simple way to use existing employee IDs for operation of machines. This allows finely graduated access concepts to be implemented or user-specific instructions to be stored – all with one card. Use of existing employee IDs (ISO 14443A/B and ISO 15693) allows individual control of access rights. The identification of operating personnel at machines and equipment is also used for retracing purposes and prevents maloperations. With its compact design and small overall depth, the SIMATIC RF1060 Reader can be combined with existing hardware (HMI devices and PC-based panels), thereby making it easier to use. The high degree of protection (IP65 at the front) and temperature range from -25 to +55 °C enables use directly on machines and equipment in harsh industrial environments.

Security with SCALANCE X and SCALANCE W

SCALANCE X-200 product line

SCALANCE W product family

SCALANCE X

The managed switches of the SCALANCE X product family are well suited for setup of line, star and ring structures.

The SCALANCE X-200, X-300, X-400 and X-500 modules can control network access and have the following security functions:

- ACL port/MAC and IP-based
- IEEE 802.1X (RADIUS)
- 802.1Q-VLAN – enables logical separation of the data traffic between pre-defined ports on the switches
- Broadcast/Multicast/Unicast Limiter
- Broadcast blocking

In addition, the following secured protocols are supported:

- SSH (instead of Telnet)
- HTTPS (instead of HTTP)
- SNMP v3 (instead of SNMP v1/v2)

SCALANCE W

Reliable wireless communication solution on different automation levels according to WLAN standard IEEE 802.11n – the SCALANCE W IWLAN products enable scalable applications.

SCALANCE W access points and client modules have the following security functions:

- Management protection with IP- and MAC-based access control list (ZSL/ACL)
- IEEE 802.1X (RADIUS)
- Access protection according to IEEE 802.11i
- WPA2(RADIUS)/ WPA2-PSK with AES

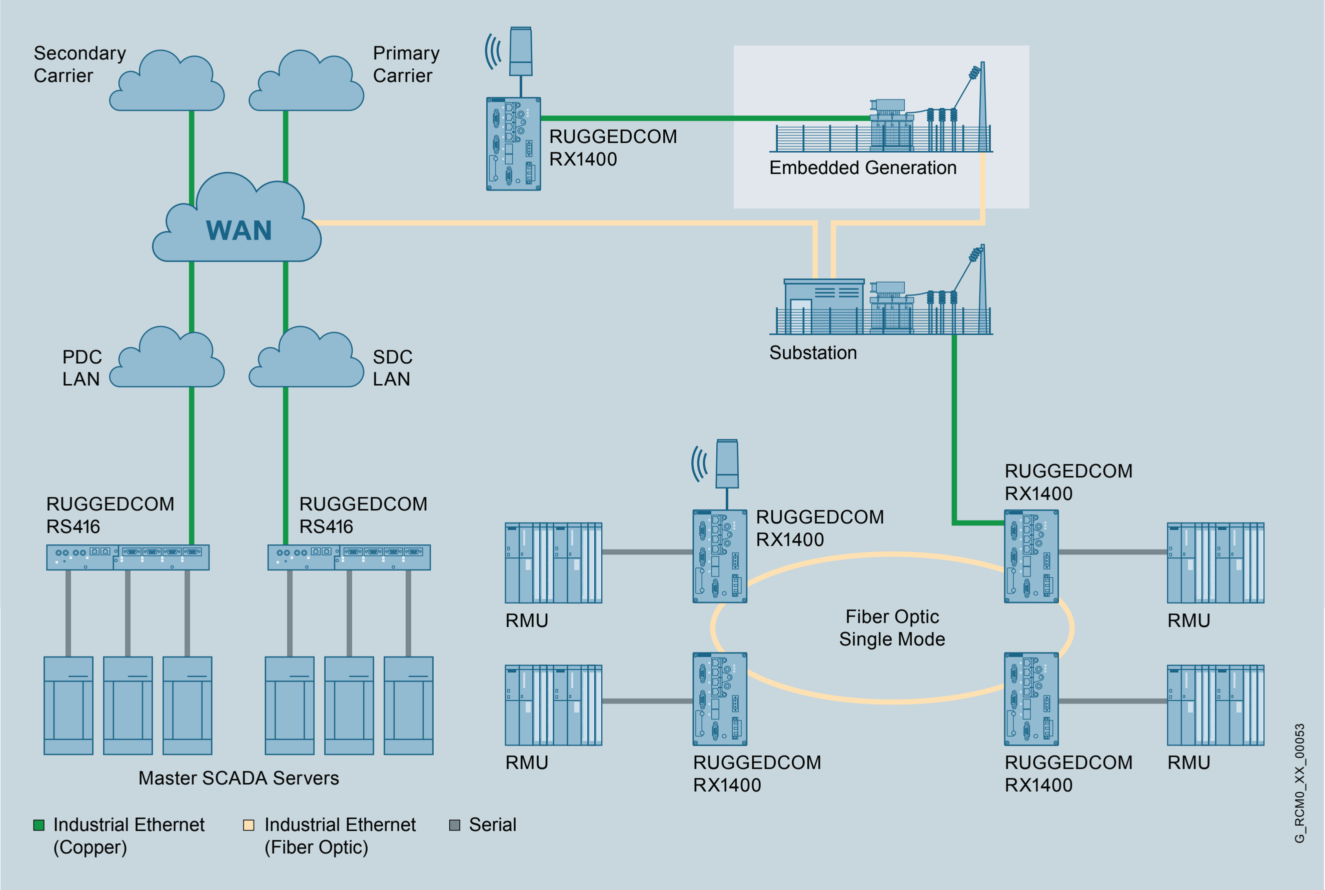
In addition, the following secured protocols are supported:

- SSH
- HTTPS
- SNMP v3

Inter AP Blocking

Available in firmware version 4.2 and higher.
This increases the security in a network environment with multiple SCALANCE W access points. WLAN clients that are connected via a layer 2 network (switches) using different access points can communicate directly with one other. This could pose a security risk depending on the application. "Inter AP Blocking" is used to specify those communication partners or gateways that WLAN clients are permitted to communicate with, thereby minimizing the security risk. Communication with other devices in the network is prevented using KEY-PLUG W700 Security (6GK5907-0PA00). It can be used with all SCALANCE W access points with a KEY-PLUG slot.

Security with RUGGEDCOM

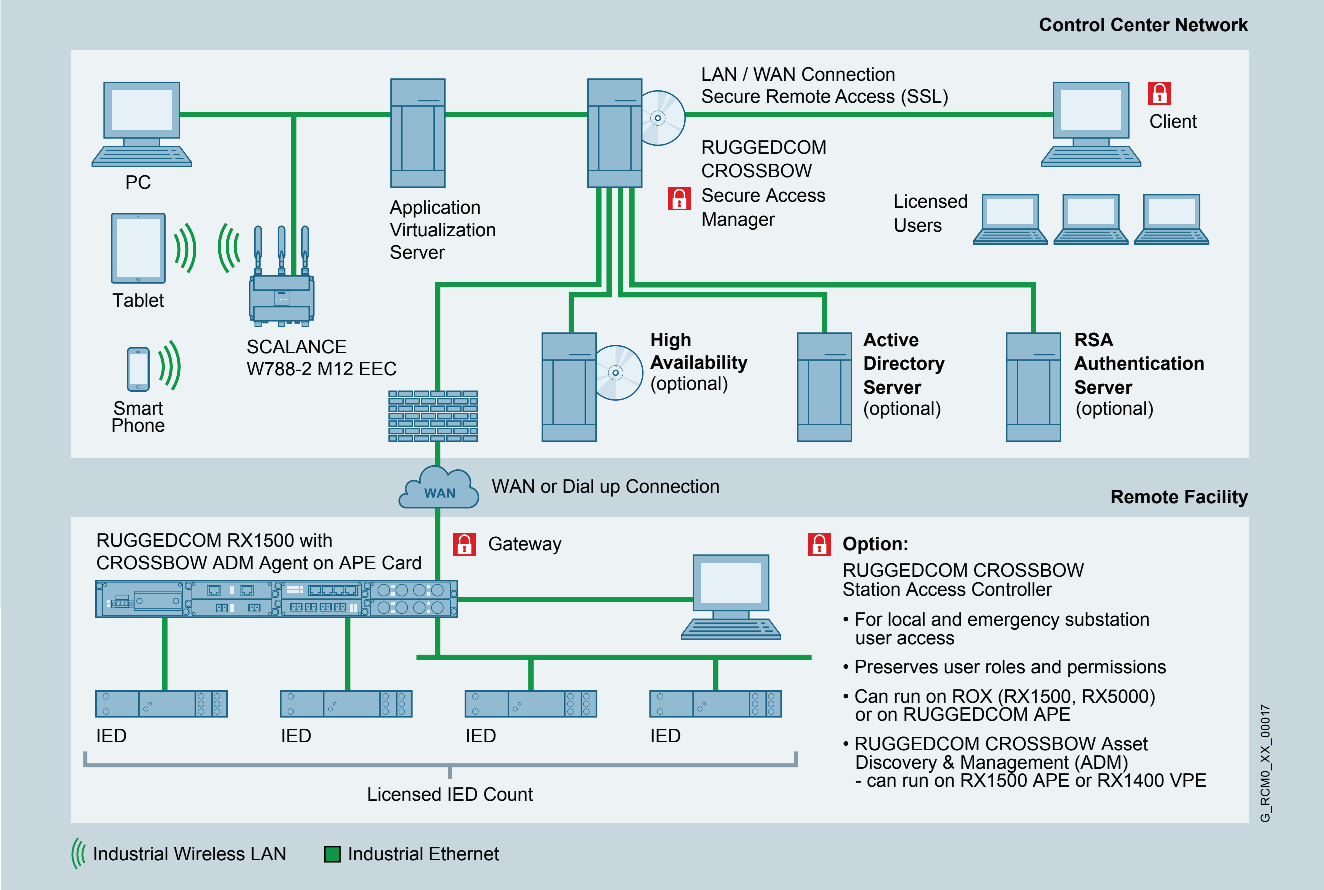


The RUGGEDCOM RX1400 is suitable for reliable connection of low-voltage transformer substations and distributed power generation plants over public mobile wireless networks.

Security

Security is especially important in the energy sector. Automation and communication networks also play a key role here for task-critical applications, and high reliability is of utmost importance. The following features of the RUGGEDCOM RX1400 address security threats at the network level:

- VPN (IPsec) – the integrated hardware encryption engine enables highly efficient IPsec data communication without use of the main processor
- Passwords – satisfy the NERC guidelines including the option for RADIUS-based authentication
- SSH / SSL – enhanced password protection with the option of encrypting passwords and data for transmission within the network
- Unblocking/blocking of ports – ability to block ports so that unauthorized devices cannot establish a connection to unused ports
- 802.1Q-VLAN – enables logical separation of the data traffic between pre-defined ports on the switches
- SNMPv3 – encrypted authentication and access protection
- HTTPS – for secured access to the web interface
- 802.1X – ensures that only permissible field devices can be connected to the device
- MAC address list – access control for devices that do not support RADIUS


Control Center Network
PC
Tablet
Smart Phone
SCALANCE W788-2 M12 EEC
Application Virtualization Server
LAN / WAN Connection Secure Remote Access (SSL)
RUGGEDCOM CROSSBOW Secure Access Manager
Client
Licensed Users
High Availability (optional)
Active Directory Server (optional)
RSA Authentication Server (optional)
WAN
WAN or Dial up Connection
Remote Facility
RUGGEDCOM RX1500 with CROSSBOW ADM Agent on APE Card
Gateway
Option:
RUGGEDCOM CROSSBOW Station Access Controller
• For local and emergency substation user access
• Preserves user roles and permissions
• Can run on ROX (RX1500, RX5000) or on RUGGEDCOM APE
• RUGGEDCOM CROSSBOW Asset Discovery & Management (ADM) - can run on RX1500 APE or RX1400 VPE
IED
IED
IED
IED
Licensed IED Count
G_RCM0_XX_00017
Industrial Wireless LAN
🟩 Industrial Ethernet

RUGGEDCOM CROSSBOW: Application overview

System architecture

The figure illustrates the typical system architecture of a utility using RUGGEDCOM CROSSBOW. The CROSSBOW Secure Access Manager (SAM) is the central enterprise server via which all remote access connections are established. It represents the sole trustworthy data source for clients from the perspective of intelligent electronic devices (IED). It forms the heart of the system and provides role-based access control and management of website and IED access.

For user access to remote IEDs, the CROSSBOW clients establish secured SSL connections to the SAM. The SAM is connected via a secure WAN to gateway devices on the transformer substation, such as RUGGEDCOM RX1500 or another supported device. The gateway establishes the connection to IEDs either directly or through lower-level remote terminal units (RTU).

CROSSBOW SAM also enables access to IEDs via their own direct modem access, e.g. for applications on the lattice tower, counter or process control, IEDs for status monitoring or other host computers/servers. Based on its ability to provide secured RBAC remote access to any IED, CROSSBOW is an indispensable tool for any application with IEDs in the following sectors:

- Utilities (power, gas, water)
- Transport control systems
- Industry and mining applications
- Building management systems

Industrial Security Services

The increasing internetworking of production and office has made many processes faster and easier. Uniform use of the same data and information creates synergies. This trend, however, also poses increased risks.

Today it is no longer just the office environment that is under threat from viruses, hacker attacks, etc. There is also a risk of intrusions, influencing of integrity and loss of know-how in production facilities Many weak spots in security are not obvious at first glance. For this reason, it is advisable to review and optimize the security of existing automation environments in order to maintain a high level of plant availability.

The Industrial Security Services portfolio provides a comprehensive product range for developing, implementing and maintaining a strategy conforming to the defense-in-depth concept. The scalable offer includes comprehensive advice (Access Security), technical implementation (Implement Security) and continuous service (Manage Security).

Assess Security

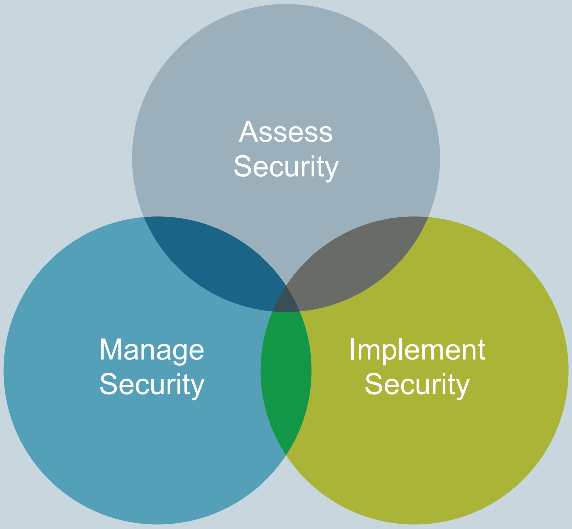
Assess Security consists of multiple assessments that ensure evaluation-based transparency within an automation system. For this, the system is analyzed together with the customer for the purpose of identification of vulnerabilities for critical components and careful examination of processes.

Implement Security

Implement Security means the implementation of security measures to increase the security level of production facilities. Systems that can detect and defend against concrete attacks are installed for this. Measures are also integrated that make it difficult for unauthorized persons to infiltrate the system with unnoticed viruses or malware.

Manage Security

Manage Security enables continuous monitoring and regular tuning and update of existing security measures, patch and vulnerability management and incident handling in automation systems. Manage Security is combining Siemens expertise in automation with the best practices from the IEC 62443 and NERC-CIP standards.



Assess Security for a risk-based security roadmap

Assess Security includes comprehensive analysis of threats, identification of risks and concrete recommendation of security measures.

- You benefit from: a plant-specific and risk-based security roadmap for a consistently optimal security level.

Implement Security for risk reduction measures

Implement Security means the implementation of security measures to increase the security level of plants and production facilities.

- You benefit from: prevention of security gaps and better protection against cyber threats thanks to technical and organizational measures.

Manage Security for a comprehensive, continuous protection

Manage Security means continuous monitoring, regular tuning and update of existing security measures, through use of our security tools.

- You benefit from: maximum transparency with regard to the security status of your plant and proactive prevention of potential threat scenarios thanks to our line of security tools optimized for use in your sensitive industrial equipment.

Terms, definitions

Cybersecurity
Cybersecurity, also referred to as computer security or IT security, is the protection of hardware, software, information and offered services of computer-based systems from theft, sabotage or misuse.

Demilitarized zone (DMZ)
A demilitarized zone or DMZ denotes a computer network with security-related control of the ability to access the connected servers. The systems in the DMZ are shielded from other networks (such as Internet, LAN) by one or more firewalls. This separation can allow access to publicly accessible services (e.g. email) while allowing the internal network (LAN) to be protected against unauthorized access. The point is to make computer network services available to both the WAN (Internet) and the LAN (intranet) on the most secure basis possible. A DMZ's protective action works by isolating a system from two or more networks.

Firewall
Security components that allow or block data communication between interconnected networks according to specified security restrictions. Firewall rules can be configured for this. It is thus possible to specify that only a particular PC may access a given controller, for example.

Industrial Security
Industrial security comprises the protection of information, data and intellectual property during processing, transmission and storage in the industrial environment. Availability, integrity and confidentiality are to be safeguarded. The purpose is to defend against attacks, threats, dangers and economic losses and to minimize risks. Guidance is provided by various national and international standards such as IEC 62443, ISO/IEC 27000, ISO/IEC 15408 and the national laws in effect, e.g. Federal Data Protection Act in Germany.

Port security
The access control function allows individual ports to be blocked for unknown nodes. If the access control function is enabled on a port, packets arriving from unknown MAC addresses are discarded immediately. Only packets arriving from known nodes are accepted.

RADIUS (IEEE 802.1X): Authentication via an external server
The concept of RADIUS is based on a central authentication server. A terminal device can only access the network or a network resource after the logon data of the device has been verified by the authentication server. Both the terminal device and the authentication server must support the Extensive Authentication Protocol (EAP).

System hardening
System hardening involves the disabling of unneeded interfaces and ports, thereby reducing the vulnerability of the network to external and internal attacks. Every level of an automation system is considered: the control system, network components, PC-based systems and programmable logic controllers.

Virtual Private Network (VPN)
A VPN tunnel connects two or more network nodes (e.g. security components) and the network segments behind them. Encrypting the data within this tunnel makes it impossible for third parties to listen in on or falsify the data when it is transmitted over an insecure network (e.g. the Internet).

Virtual LAN (VLAN)
VLANs (IEEE 802.1Q) enable logical separation of the data traffic between pre-defined ports on the switches. The result is several "virtual" networks on the same physical network. Data communication takes place only within a VLAN.

Whitelisting
Whether it's for individuals, companies, or programs: a whitelist – or positive list – refers to a collection of like elements that are classified as trustworthy. Whitelisting for PCs ensures that only those programs that are actually required can be executed.

Learn everything about industrial security:

- An overview of our security products and services
- The latest innovations from the field of industrial security

www.siemens.com/industrial-security

SIEMENS
Ingenuity for life
Products & Services
Market-specific Solutions
Company
Company › Topic Areas › Future of Manufacturing › Industrial Security
You are here: Overview

Thinking security to ensure productivity

Continuously monitored and integrated security is an important basis for industrial automation

Industrial Security – take a look!

Follow us on:

twitter.com/siemensindustry

youtube.com/siemens

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

© Siemens AG 2018
Subject to change without prior notice
Article No. 6ZB5530-1AP02-0BA7
W-FPN8Z-PD-PA265 / Dispo 26000
BR 0418 1. ROT 36 En
Printed in Germany

The information provided in this brochure contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

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 **http://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 **http://www.siemens.com/industrialsecurity.**

siemens.com/networksecurity