

SIEMENS



Network security

Industrial Security

Brochure

Edition
February
2014

Answers for industry.

Industrial Security

That is why industrial security is so important

As the use of Ethernet connections increases all the way down to the field level, the associated security issues are becoming a more urgent topic for industry. 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 can support you here in selectively implementing these measures – within the scope of an integrated range for industrial security.

No.	Threat	Explanation
1	Unauthorized use of remote maintenance access	Maintenance access provides deliberate openings to the outside in the ICS network ¹⁾ which, however, are often inadequately protected.
2	Online attacks via office/enterprise networks	In general, office IT equipment is connected with the Internet in many ways. Usually, there are also network connections from the office network to the ICS network, allowing attackers to use this route, too.
3	Attacks against standard components used in the ICS network	Commercial off-the-shelf (COTS) standard IT components such as operating systems, application servers, or databases generally contain flaws and weak points which can be exploited by attackers. If these standard components are also used in the ICS network, it increases the risk of a successful attack on the ICS systems.
4	(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.
5	Human error and sabotage	Deliberate actions – regardless of whether by internal or external agents – are a massive threat for all security goals. In addition, negligence and human error are a great danger, especially when it comes to protecting confidentiality and availability.
6	Introduction of harmful code via removable media and external hardware	The use of removable media and mobile IT components by external employees always presents a great risk of malware infections. The importance of this aspect was demonstrated by Stuxnet, for example.
7	Reading and writing messages in the ICS network	Because most control components at present communicate via plain-text protocols, and are thus unprotected, it is often possible to read and insert commands without great difficulty.
8	Unauthorized access to resources	In particular, insiders or follow-up attacks after intrusion from the outside have an easy time if authentication and authorization for services and components in the process network are non-existent or insecure.
9	Attacks on network components	Network components can be manipulated by attackers, for example to carry out man-in-the-middle attacks or to make sniffing easier.
10	Technical faults and force majeure	Failures are always possible as a result of extreme environmental influences or technical defects – the risk and the potential for damage can only be minimized here.

Threat overview

¹⁾ Industrial Control Systems (ICS)

Source:

[BSI-A-CS 004 | Version 1.00 dated April 12, 2012; page 2 of 2](#)

Note:

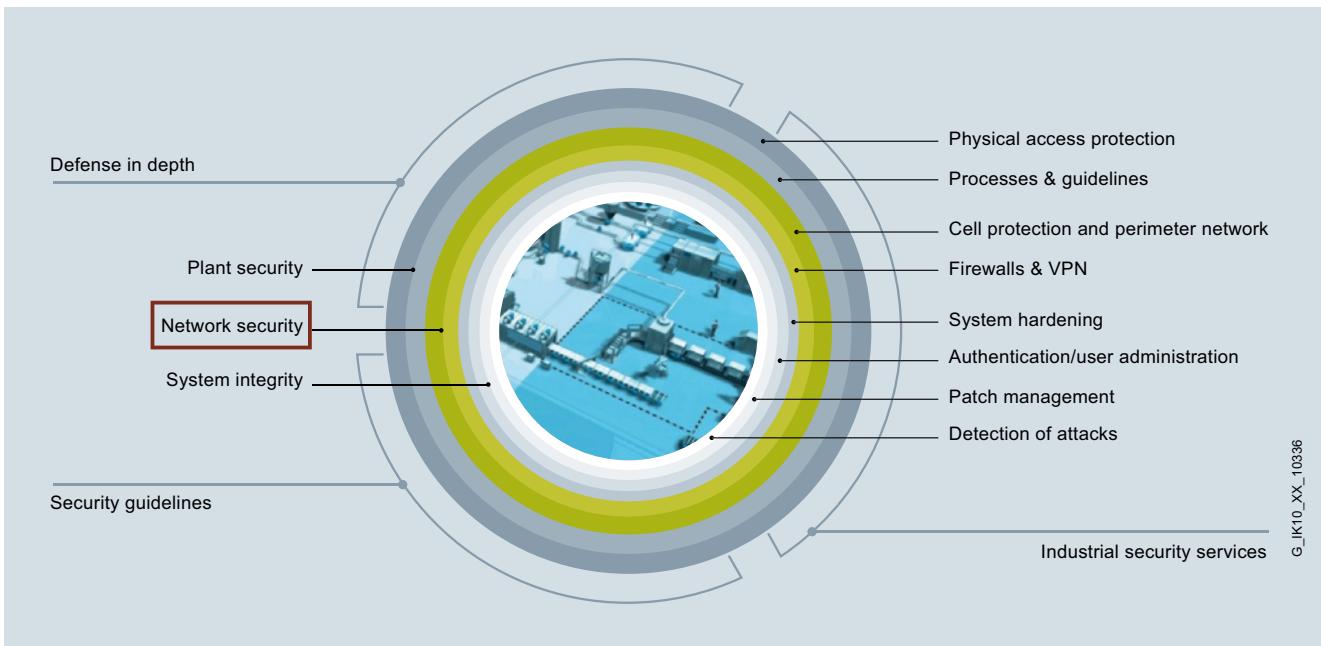
This list of threats was compiled in close cooperation between BSI and representatives of the industry.

Using BSI analyses, the Federal Office for Information Security (BSI) publishes statistics and reports on current topics dealing with cyber-security.

Please direct all comments and notes to:

cs-info@bsi.bund.de





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

Siemens Industrial Security – continuous protection for your plant

An optimum industrial security solution can only be implemented if new approaches are taken because it must be continuously adapted to new threats. There is no such thing as absolute security. To ensure a comprehensive and permanent solution, we provide in-depth advice, partner-like cooperation, and continuous development of our security measures and products.

All-round, but also in-depth protection

With Defense in Depth, Siemens provides a multi-level concept that offers your plant both all-round and in-depth protection. The concept is based on the components plant security, network security, and system integrity, as recommended by ISA 99 / IEC 62443 – the leading standard for security in industrial automation. While conventional plant security defends the plant against physical attacks, network protection and the protection of system integrity offer protection against cyber attacks and unauthorized access by operators or external persons.

Success factor: 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 secure 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 secure segmenting 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 is encrypted by means of a VPN and is thus protected from data espionage and manipulation. The communication stations are securely authenticated. The cell protection concept can be implemented and communications can be secured using "Security Integrated" components such as SCALANCE S security modules or security CPs for SIMATIC.

Initial risk assessment and information on the Internet

You want to know right now how good the security of your industrial plant is? We can provide you with detailed information about the special security issues in your industry in a customer consultation meeting. Use this opportunity to talk to our consulting team about any open issues. Our experts will gladly prepare a security strategy that is adapted to suit the needs of your production plant or process infrastructure. You can download the additional "Operational Guidelines" with many recommendations for protecting your production plant from our Internet site.

Industrial Security

Network security as a factor for success

Plant Security



Network Security

Office Network



SCALANCE S627-2M

SCALANCE S627-2M

SCALANCE S623

Industrial Ethernet

System Integrity

Industrial Ethernet
(Fiber optic)

MRP ring

SCALANCE X308-2M



Production 1

SCALANCE X204-2

SCALANCE X204-2

SCALANCE X308-2M

SIMATIC
TP700

OS with
CP 1628

Ring redundancy
manager
SCALANCE
X308-2M

SIMATIC
S7-400 with
CP 443-1
Advanced

PROFINET

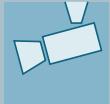
Terminalbus

Terminalbus

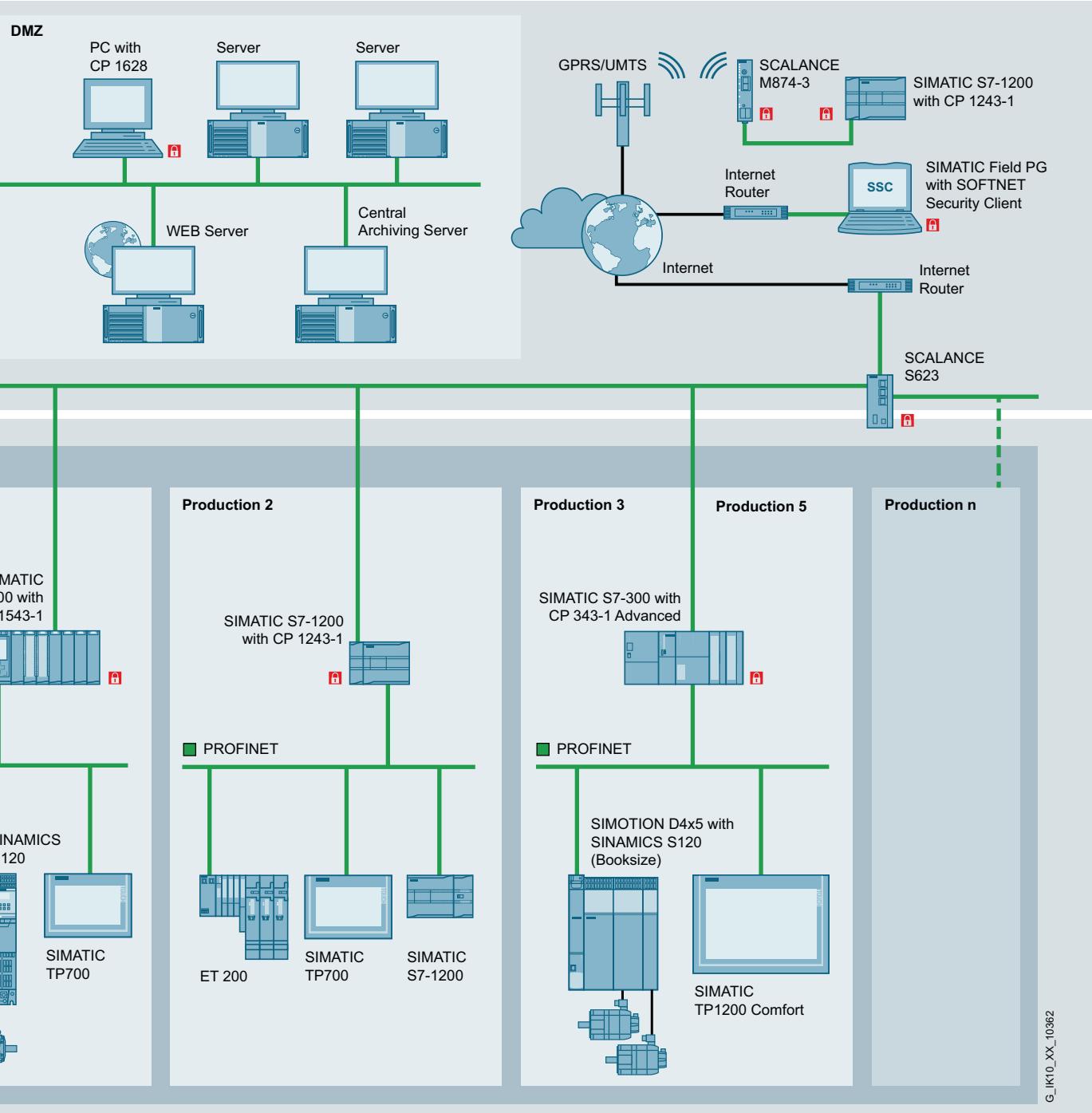
SIMATIC
ET 200SP

Factory Automation

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



- Physical protection
- Security management



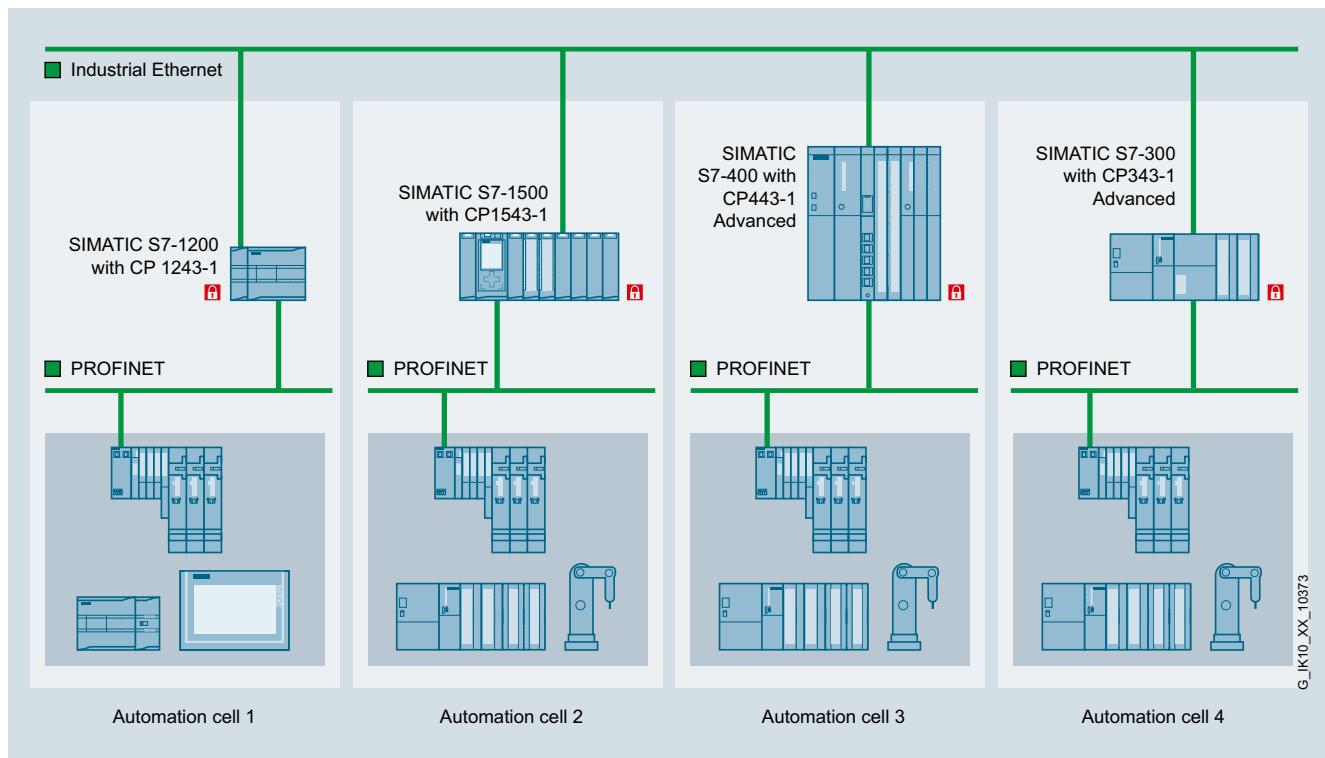
G_IK10_XX_10362

Security Integrated

Cell protection concept

Industrial communication is a key factor for corporate success – as long as the network is protected.

As a partner, Siemens provides its customers with Security Integrated components which not only have communication functions, but also include special security functions such as firewall and VPN functionality, in order to implement the cell protection concept.



Secure communication between components with Security Integrated in separate automation cells

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 communicate with each other securely. The individual cells are connected to the plant network protected by a 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, SCALANCE M and SIMATIC S7/PC communications processors can be used for implementing this concept.



The following Security Integrated products are available:

SIMATIC S7-1200 / S7-1500:

- Protection of the controller by means of access protection (authentication) via the **S7-1200/S7-1500 CPU**:
 - Know-how protection
 - Manipulation protection
 - Copy protection
 - Graded security concept for HMI connection
- Expandable access protection for S7-1200/S7-1500 (firewall) via Security **CP 1243-1/CP 1543-1** by means of
 - Integrated firewall (monitoring of the data flow)
 - Protection against data manipulation and espionage by means of a VPN

SIMATIC S7-300 and S7-400

- Protection of controllers by **CP 343-1 Advanced** and **CP 443-1 Advanced** communications processors, which contain both firewall and VPN (virtual private network) functionality.

SCALANCE S security modules

- **SCALANCE S** modules protect industrial networks and automation systems by means of security-related segmentation (cell protection) with a firewall against authorized access and protect data transmission with VPN against manipulation and espionage.

Industrial PCs

- Via the **CP 1628** communications processor, industrial PCs are protected by firewall and VPN – for secure communication without the need for special operating system settings. In this manner, computers equipped with the module can be connected to protected cells.

Software

- The **SOFTNET Security Client** software enables VPN access via the Internet or a company intranet to automation cells or PCs protected by SCALANCE S or another Security component with VPN functionality.

Remote access

- SCALANCE M industrial routers for secure remote access to plants via mobile networks, e.g. **M874-3** via UMTS.

SCALANCE S family	SCALANCE M family	CP 343-1 Adv CP 443-1 Adv	S7-1200 CPU ¹⁾ S7-1500 CPU	CP 1243-1 CP 1543-1	CP 1628	SOFTNET Security Client
Configurable copy protection				•		
Access protection (authentication)				•		
Extended access protection (Firewall)	•	•	•	•	•	
Virtual Private Network with IPSec	•	•	•	•	•	•
Manipulation protection (communication, configuration)	•	•	•	•	•	•

● applies 1) from CPU firmware V4.0
from STEP 7 Professional V13

G_IK10_XX_10347

Security Integrated products for industrial use with special security functions to improve the security standard

Security Integrated

Protection of automation cells with SCALANCE S modules

The security modules of the SCALANCE S range can be used to protect all devices of an Ethernet network against unauthorized access. In addition, SCALANCE S modules also protect the data transmission between devices or network segments (such as automation cells) against data manipulation and espionage by setting up VPN tunnels; they can also be used for secure remote access over the Internet.

The SCALANCE S security modules can be operated not only in bridge mode, i.e. within an IP subnetwork, but also in router mode, i.e. operated at the IP subnetwork borders.

SCALANCE S is optimized for use in automation and industrial environments, and meets the specific requirements of automation systems such as easy upgrades of existing plants, simple installation, and minimal downtimes in the event of a fault.



Product versions

SCALANCE S602

- Uses the Stateful Inspection Firewall to protect network segments against unauthorized access
- Connection via 10/100/1000 Mbit/s ports
- "Ghost mode" for protection of individual, even alternating, devices by dynamically taking over the IP address

SCALANCE S612

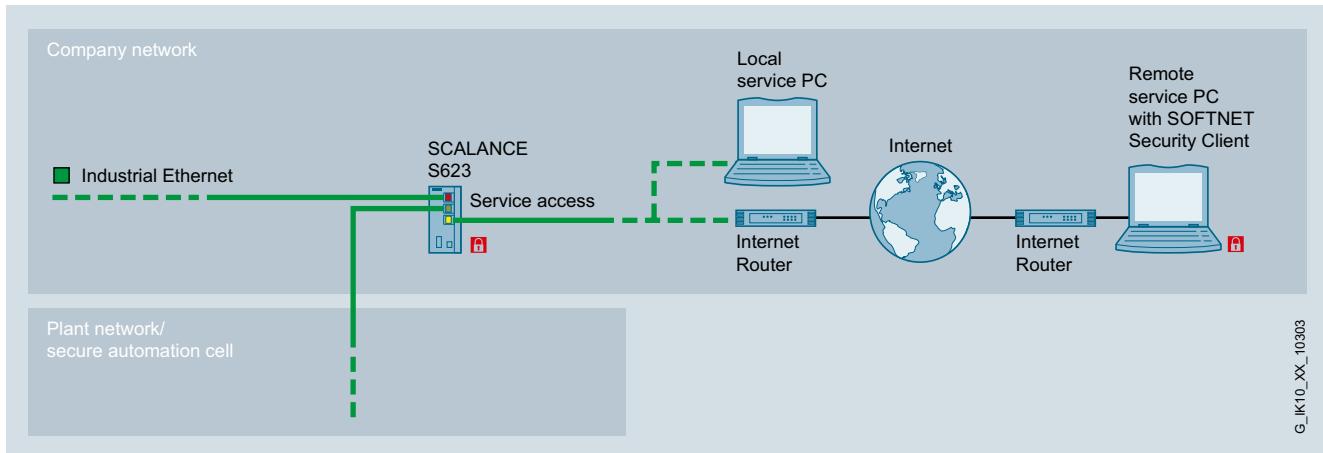
- Uses the Stateful Inspection Firewall to protect network segments against unauthorized access
- Up to 128 VPN tunnels can be operated simultaneously
- Connection via 10/100/1000 Mbit/s ports

SCALANCE S623

- Uses the Stateful Inspection Firewall to protect network segments against unauthorized access
- Up to 128 VPN tunnels can be operated simultaneously
- Connection via 10/100/1000 Mbit/s ports
- Additional RJ45 DMZ (demilitarized zone) port for secure connection, for example, of remote maintenance modems, laptops, or an additional network. The yellow port is protected by firewalls from the red and green ports and can also terminate VPNs
- Redundant protection of automation cells by means of router and firewall redundancy and stand-by mode of the redundant device; status matching by means of synchronization cable between the yellow ports

SCALANCE S627-2M

- Uses the Stateful Inspection Firewall to protect network segments against unauthorized access
- Up to 128 VPN tunnels can be operated simultaneously
- Connection via 10/100/1000 Mbit/s ports
- Additional RJ45 DMZ (demilitarized zone) port for secure connection, for example, of remote maintenance modems, laptops, or an additional network. The yellow port is protected by firewalls from the red and green ports and can also terminate VPNs
- Redundant protection of automation cells by means of router and firewall redundancy and stand-by mode of the redundant device; status matching by means of synchronization cable between the yellow ports
- Two additional slots for 2-port media modules (of SCALANCE X-300) for direct integration in ring structures and FO networks with two additional switched red or green ports per module
- Bridging of longer cable runs or use of existing 2-core cables (e.g. PROFIBUS) by deploying the MM992-2VD media modules (variable distance)



G_IK10_XX_10303

Connection of a local or remote service PC (by means of Internet access) via the DMZ port of the SCALANCE S623

SCALANCE S security functions

VPN (Virtual Private Networks)

(only for SCALANCE S612, S623 and SCALANCE S627-2M); for reliable authentication (identification) of the network stations, for encrypting data and checking data integrity.

- Authentication
All incoming data traffic is monitored and checked. Since IP addresses can be falsified (IP spoofing), checking the IP address (of the client access) alone is not sufficient. In addition, client PCs may have changing IP addresses. For this reason, authentication is performed by means of tried and tested VPN mechanisms.
- Data encryption
Secure encryption is necessary in order to protect data communication from espionage and unauthorized manipulation. This means that the data traffic remains incomprehensible to any eavesdropper in the network. The SCALANCE Security Module establishes VPN tunnels to other security modules for this purpose.

Firewalls

Can be used as an alternative or to supplement VPN with flexible access control. Firewalls filter data packets and disable or enable communication links in accordance with the filter list and stateful inspection.

Both incoming and outgoing communication can be filtered, either according to IP and MAC addresses as well as communication protocols (ports), or user-specifically.

- Logging
Access data is stored by the Security Module in a log file. This ensures both identification of how, when and by whom data has been accessed as well as facilitating identification of access attempts, thus ensuring that appropriate preventative measures can be taken.

Configuration

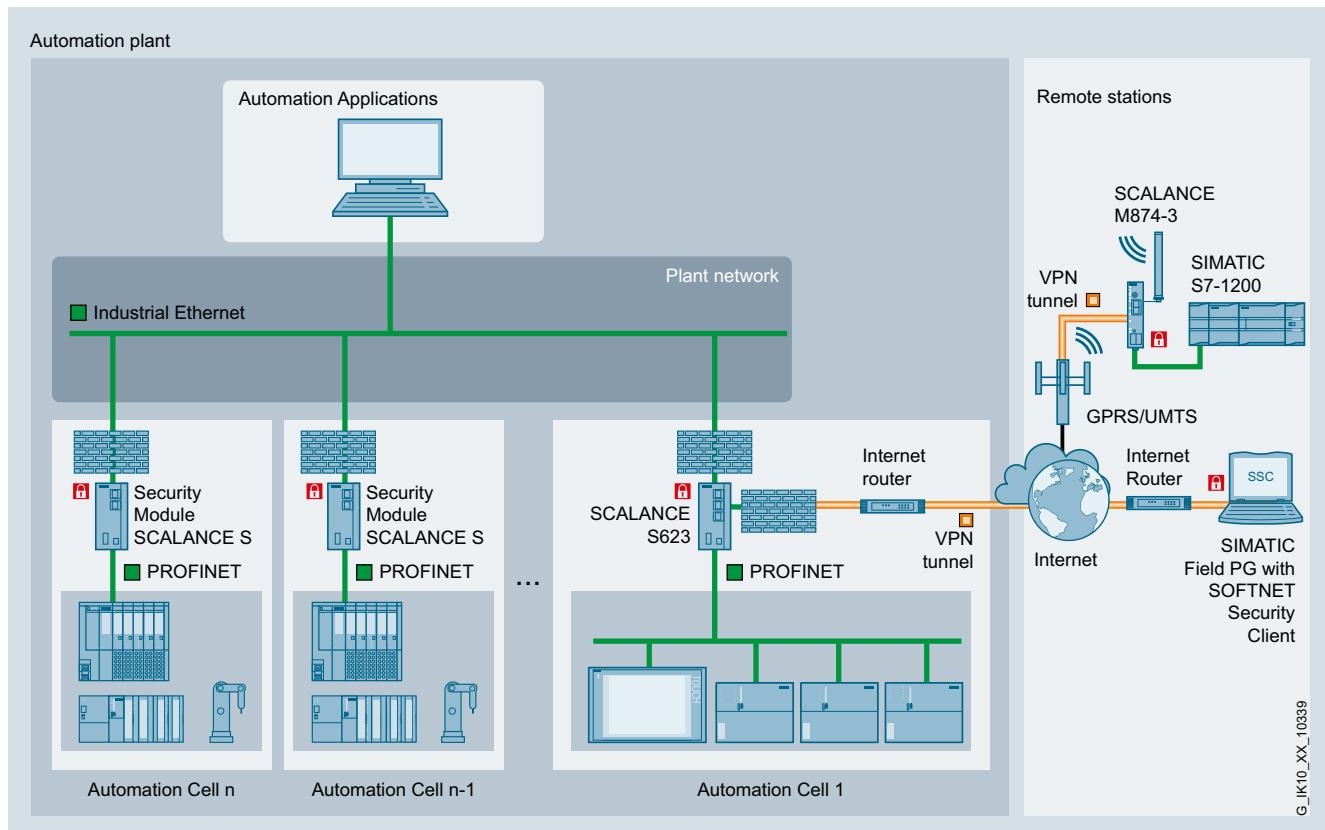
Configuration is carried out using the Security Configuration Tool (SCT), which enables all SIMATIC NET security products to be configured and diagnosed from a central position. All the configuration data can be saved on the optional C-PLUG swap media (not included in scope of supply) so that the Security Module can be replaced quickly in the event of a fault, without the need for a programming device.

Advantages at a glance

- High level of IT security for machines and plants thanks to implementation of the cell protection concept
- System-wide network diagnostics thanks to integration into IT infrastructures and network management systems by means of SNMP
- Simple remote maintenance via the Internet by means of PPPoE and DNS using dynamic IP addresses
- Easy integration into existing networks without reconfiguring terminal nodes or setting up new IP subnetworks
- Module replacement without the need for a programming device, using the C-PLUG swap media for backing up the configuration data

Security Integrated

Application examples with SCALANCE S modules



Secure remote access without direct connection to the automation network with SCALANCE S623

Task

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

Solution

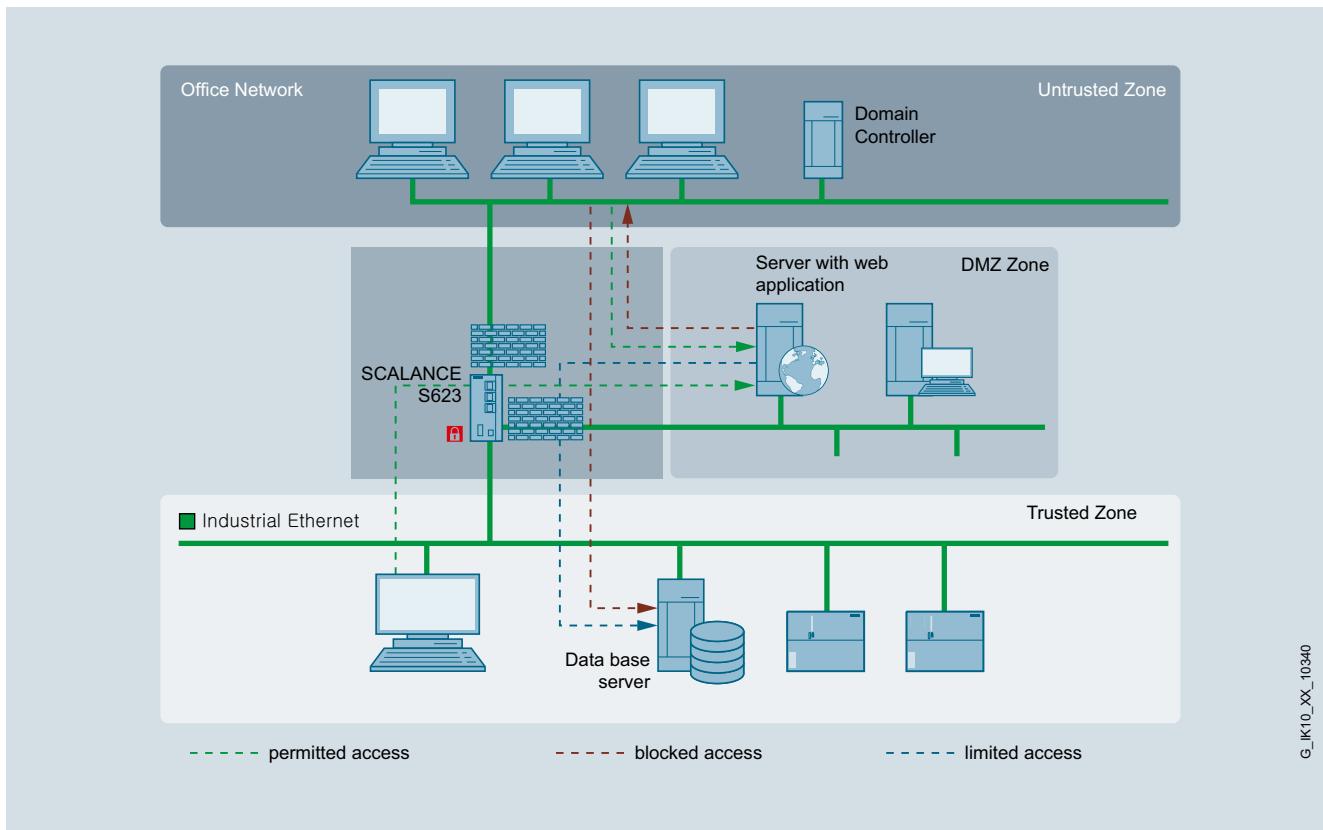
Starting points are, for example, system integrator with VPN client (SOFTNET Security Client, CP 1628, SCALANCE M874-3)

End point (automation system):
SCALANCE S623 as VPN server

- Red port: connection to plant network
- Yellow port: connection of Internet modem/router
- Green port: connection to protected cell

Advantages at a glance

- Secure remote access via Internet or mobile networks such as UMTS by safeguarding the data transmission with VPN (IPSec)
- Restriction of access possibilities with integrated firewall function
- Secure remote access to plant units without direct access to the plant network with SCALANCE S623 3-port firewall



G_IK10_XX_10340

Setup of a demilitarized zone (DMZ) using SCALANCE S623

Task

Network participants or servers (e.g. MES servers) should be accessible both from the secure and non-secure network without a direct connection between the networks.

Solution

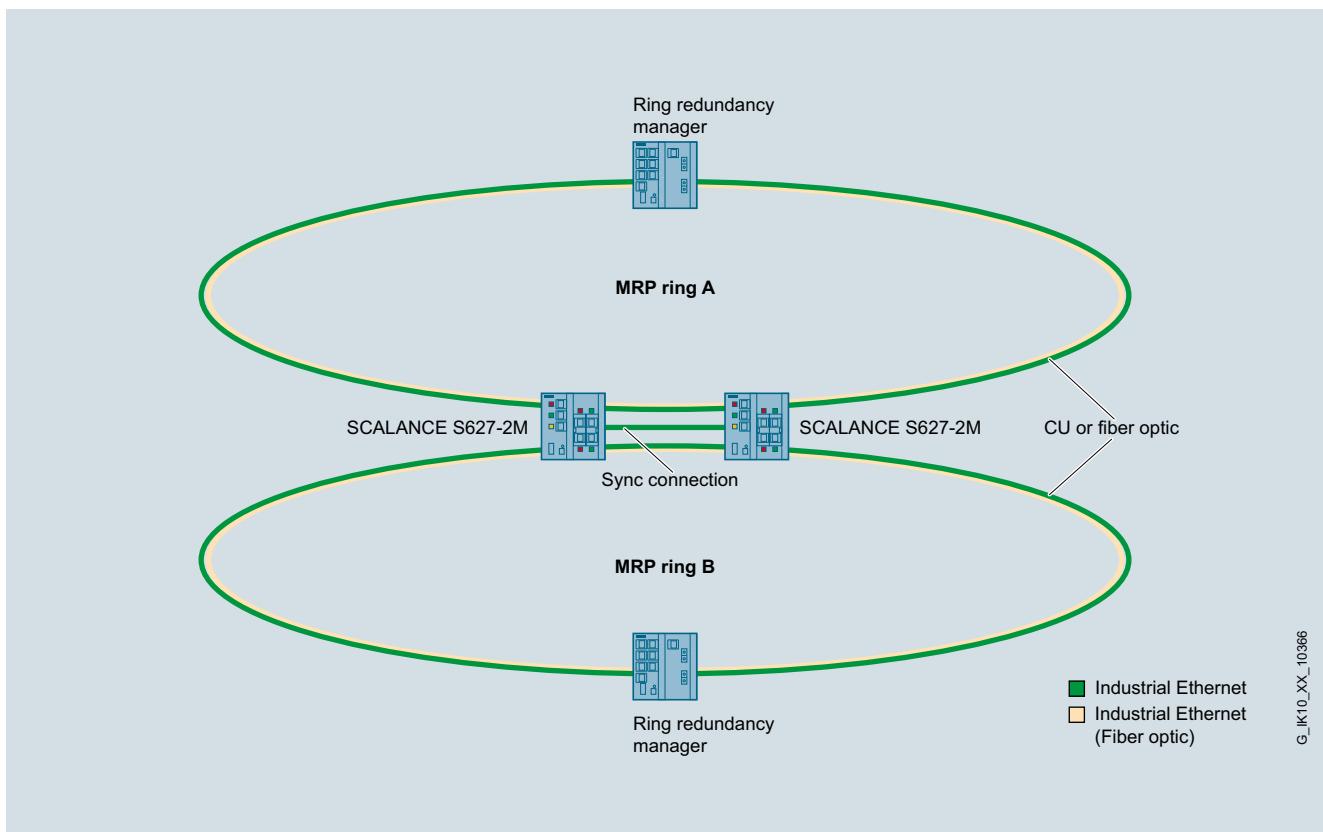
A DMZ can be set up at the yellow port by means of a SCALANCE S623. The servers can be positioned in this DMZ.

Advantages at a glance

- Secure data exchange through the use of a "demilitarized zone" for the exchange of data between corporate and plant network using a SCALANCE S623 3-port firewall
- Protection of automation networks against unauthorized access at the network boundaries

Security Integrated

Application examples with SCALANCE S modules



Secure, redundant connection between two MRP rings with SCALANCE S627-2M

Task

Two rings should be securely and redundantly connected to one another.

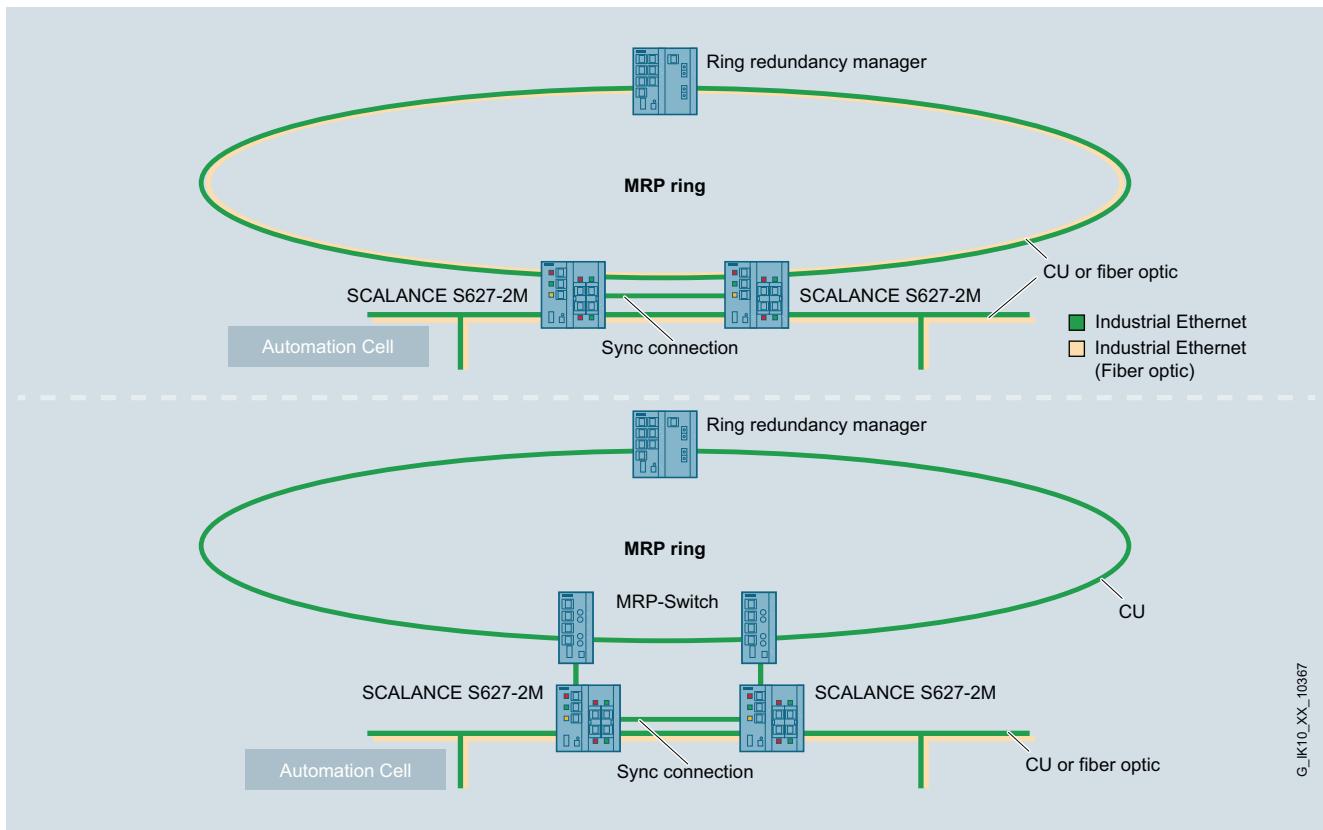
Solution

Ring A is connected to the ports of the first media module (red ports) and Ring B with the ports of the second media module (green ports) using SCALANCE S627-2M.

S627-2M functions as a router and firewall. A second SCALANCE S627-2M is likewise connected and operates in stand-by mode. In order to match the firewall status between the two SCALANCE S modules, the yellow ports are coupled by means of a synchronization cable.

Advantages at a glance

- Secure redundant coupling of redundant rings
- Control of data communication between redundant rings
- High availability due to redundant design of the SCALANCE S627-2M



G_IK10_XX_10367

Secure, redundant connection of an automation cell to a redundant ring with SCALANCE S627-2M

Task

An automation cell is to be connected securely and redundantly to a higher-level ring.

Solution

The ring is connected to the ports of the first media module (red ports) and the lower-level cell with the ports of the second media module (green ports) using SCALANCE S627-2M. A second SCALANCE S627-2M is likewise connected and operates in stand-by mode. In order to match the firewall status between the two SCALANCE S modules, the yellow ports are coupled by means of a synchronization cable.

Alternative:

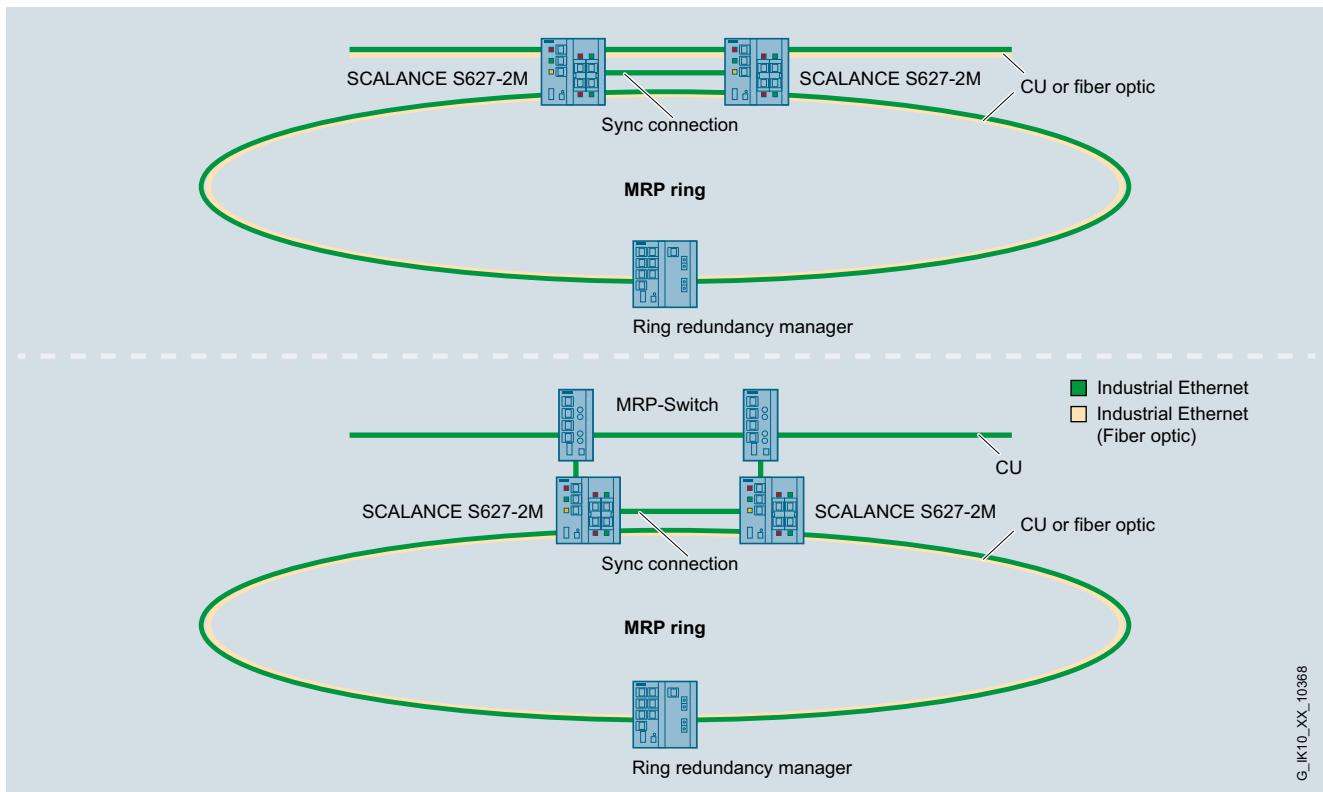
The ring is coupled with the red RJ45 port and the lower-level automation cell is connected to the ports of the second media module (green ports) using SCALANCE S627-2M. A second SCALANCE S627-2M is likewise connected and operates in stand-by mode. In order to match the firewall status between the two SCALANCE S modules, the yellow ports are coupled by means of a synchronization cable.

Advantages at a glance

- Secure redundant connection of an automation cell to a higher-level ring
- Control of the data communication between a redundant ring and a lower-level automation cell
- High availability due to redundant design of the SCALANCE S627-2M

Security Integrated

Application examples with SCALANCE S modules



G_IK10_XX_10368

Secure, redundant connection of a redundant ring to a plant network with SCALANCE S627-2M

Task

The ring is to be securely and redundantly connected to the plant network.

Solution

The ring is connected to the ports of the second media module (green ports) and the production network with the ports of the first media module (red ports) using SCALANCE S627-2M. A second SCALANCE S627-2M is likewise connected and operates in stand-by mode. In order to match the firewall status between the two SCALANCE S modules, the yellow ports are coupled by means of a synchronization cable.

Alternative:

The ring is connected to the ports of the second media module (green ports) and the production network with the red RJ45 port using SCALANCE S627-2M. A second SCALANCE S627-2M is likewise connected and operates in stand-by mode. In order to match the firewall status between the two SCALANCE S modules, the yellow ports are coupled by means of a synchronization cable.

Advantages at a glance

- Secure redundant connection of a redundant ring to the plant network
- Control of data communication between plant network and redundant ring
- High availability due to redundant design of the SCALANCE S627-2M

Secure access to plant sections via mobile networks



SCALANCE M874

SCALANCE M874-3 and SCALANCE M874-2 are mobile wireless routers for cost-effective and secure connection of Ethernet-based subnets and programmable controllers via UMTS (3rd generation mobile network) or GSM (2nd generation mobile network).

SCALANCE M874-3

Supports HSPA+ (High Speed Packet Access) and allows high transfer rates of up to 14.4 Mbit/s in the downlink and up to 5.76 Mbit/s in the uplink (depending on the infrastructure of the mobile wireless provider).

SCALANCE M874-2

Supports GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for GSM Evolution).

Protects against unauthorized access and offers data transmission via the Integrated Security functions Firewall and VPN (IPSec).

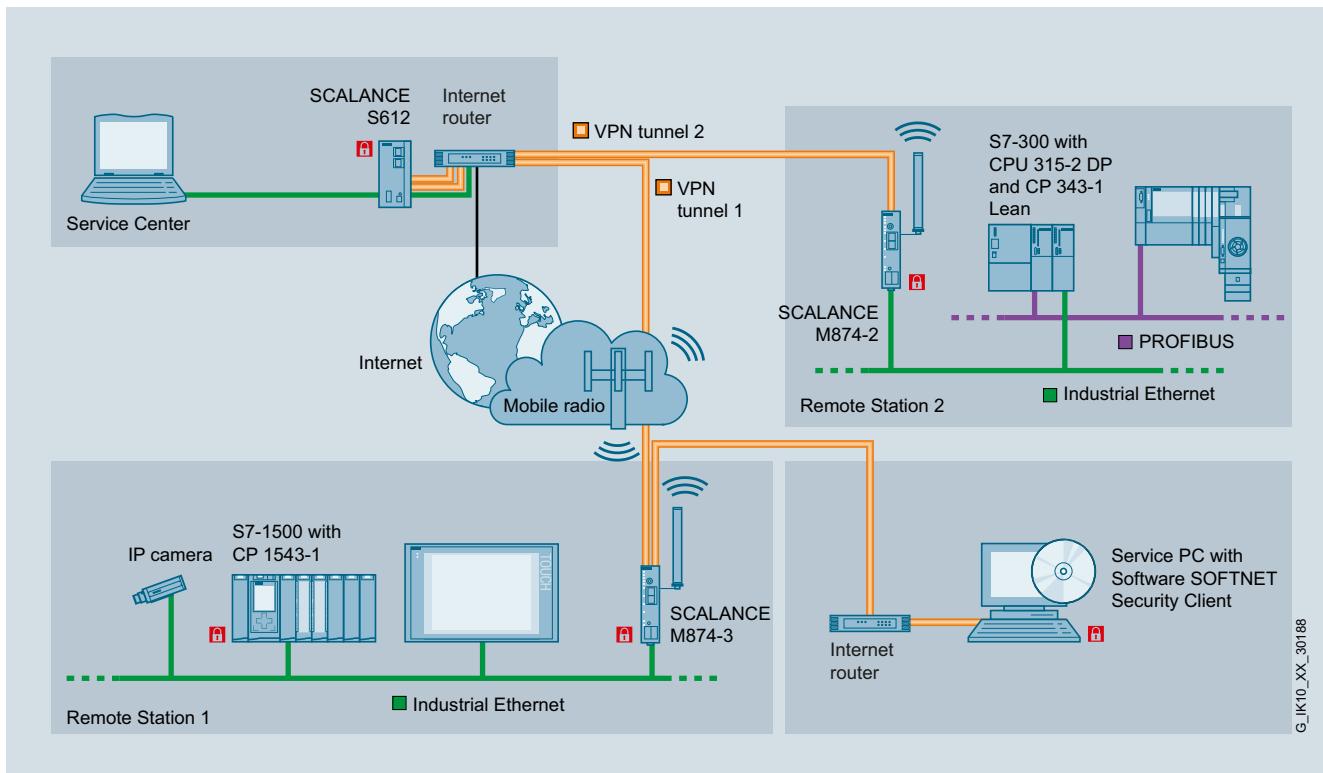
SCALANCE M875

The SCALANCE M875 UMTS router offers IP routing, stateful inspection firewall, and a VPN gateway to protect lower-level devices from security risks such as manipulation or espionage.

SCALANCE M875 has obtained type approval as a vehicle component in accordance with directive 72/245/EEC in its 2009/19/EC version and type approval for use on rail vehicles in accordance with EN 50155.

Security Integrated

Secure access to plant sections via mobile networks



VPN for secure remote maintenance with SCALANCE M874

Task

Conventional applications such as remote programming, parameterization and diagnostics, but also monitoring of machines and plants installed worldwide, should be performed by a service center that is connected over the Internet.

Solution

Any IP-based devices and particularly automation devices that are downstream of the SCALANCE M875 or SCALANCE M874 in the local network 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 the secure transfer of data around the world.

Advantages at a glance

- Low investment and operating costs for secure remote access to machines and plants
- Reduced travel costs and telephone charges thanks to remote programming and remote diagnostics via 3G/UMTS
- User-friendly diagnostics via Web interface
- Short transmission times thanks to high transmission rates with HSDPA and HSUPA
- Protection by integrated firewall and VPN
- Utilization of existing (3G)UMTS infrastructure of mobile network providers
- Simple planning and commissioning of telecontrol substations without the need for special radio expertise
- Worldwide availability thanks to UMTS/GSM (quad band) technology; observe national regulations

Protection of controllers through communications processors



CP 1243-1

The CP 1243-1 communications processor securely connects the SIMATIC S7-1200 controller to Ethernet networks.

With its integrated security functions of firewall (Stateful Inspection) and VPN protocol (IPSec), the communications processor protects S7-1200 stations and lower-level networks against unauthorized access, and protects the data transmission against manipulation and espionage by means of encryption.

Furthermore, the CP can also be used for integrating the S7-1200 station into the TeleControl Server Basic control center software via IP-based remote networks.

Task

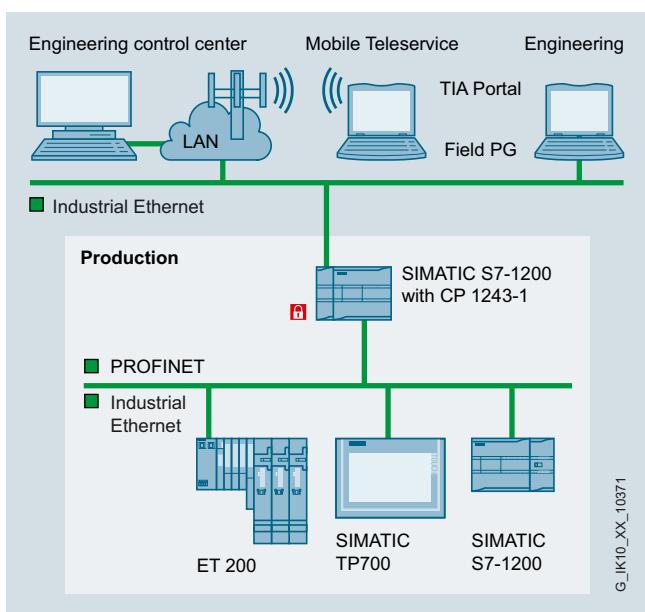
Communication between the automation network and lower-level networks with S7-1200 is to be secured by means of access control.

Solution

The CP 1243-1 is placed upstream of the automation cells to be protected in the rack of the S7-1200. In this way, the communication to and from the S7-1200 and the 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

- Secure connection of the SIMATIC S7-1200 to Industrial Ethernet by means of integrated Stateful Inspection Firewall and VPN
- Can be used in an IPv6-based infrastructure
- Connection to control centers with TeleControl Server Basic



Protection of an S7-1200 and lower-level automation cell with CP1243-1

Security Integrated

Protection of controllers through communications processors



CP 1543-1

The CP 1543-1 communication processor securely connects the SIMATIC S7-1500 controller to Ethernet networks.

With its integrated security functions of firewall (Stateful Inspection), VPN protocol (IPSec) and protocols for data encryption such as FTPS and SNMPv3, the communications processor protects S7-1500 stations and lower-level networks against unauthorized access, as well as protecting data transmission against manipulation and espionage by means of encryption.

Task

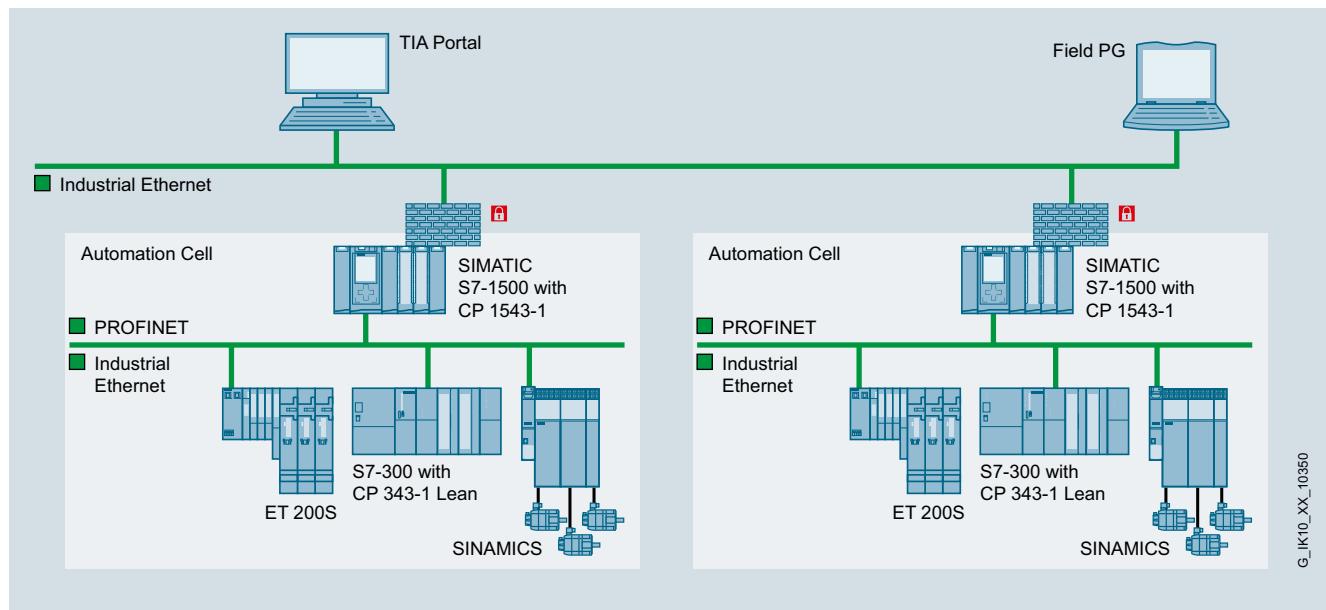
Communication between the automation network and lower-level networks with S7-1500 is to be secured by means of access control.

Solution

The CP 1543-1 is placed in the rack of the S7-1500, upstream of the automation cells to be protected. In this way, the communication to and from the S7-1500 and the 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.

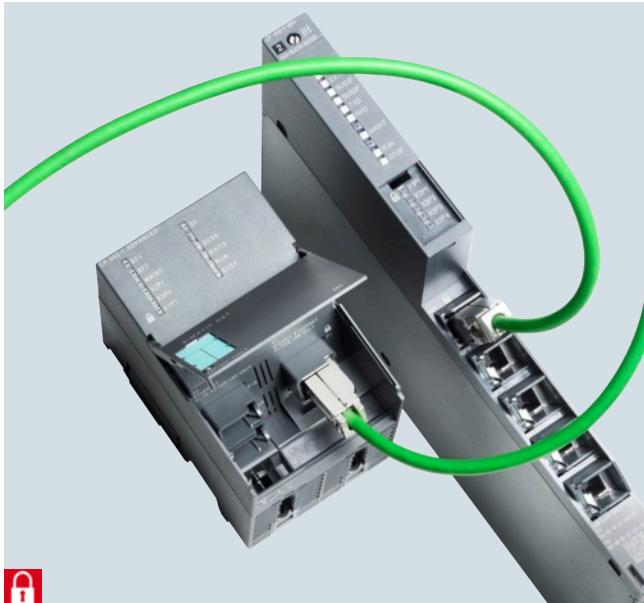
Advantages at a glance

- Secure connection of the SIMATIC S7-1500 to Industrial Ethernet by means of integrated Stateful Inspection Firewall and VPN
- Additional communication options: File transfer and e-mail
- Can be used in an IPv6-based infrastructure



Segmentation of networks and protection of the S7-1500 with CP1543-1

G_IK10_XX_10350



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 or S7-400, contain Security Integrated with a Stateful Inspection Firewall and a VPN gateway to protect the controller and lower-level devices against security risks.

Task

Communication between the office level administration system 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. This limits communication to the permitted connections with the aid of firewall rules.

Advantages at a glance

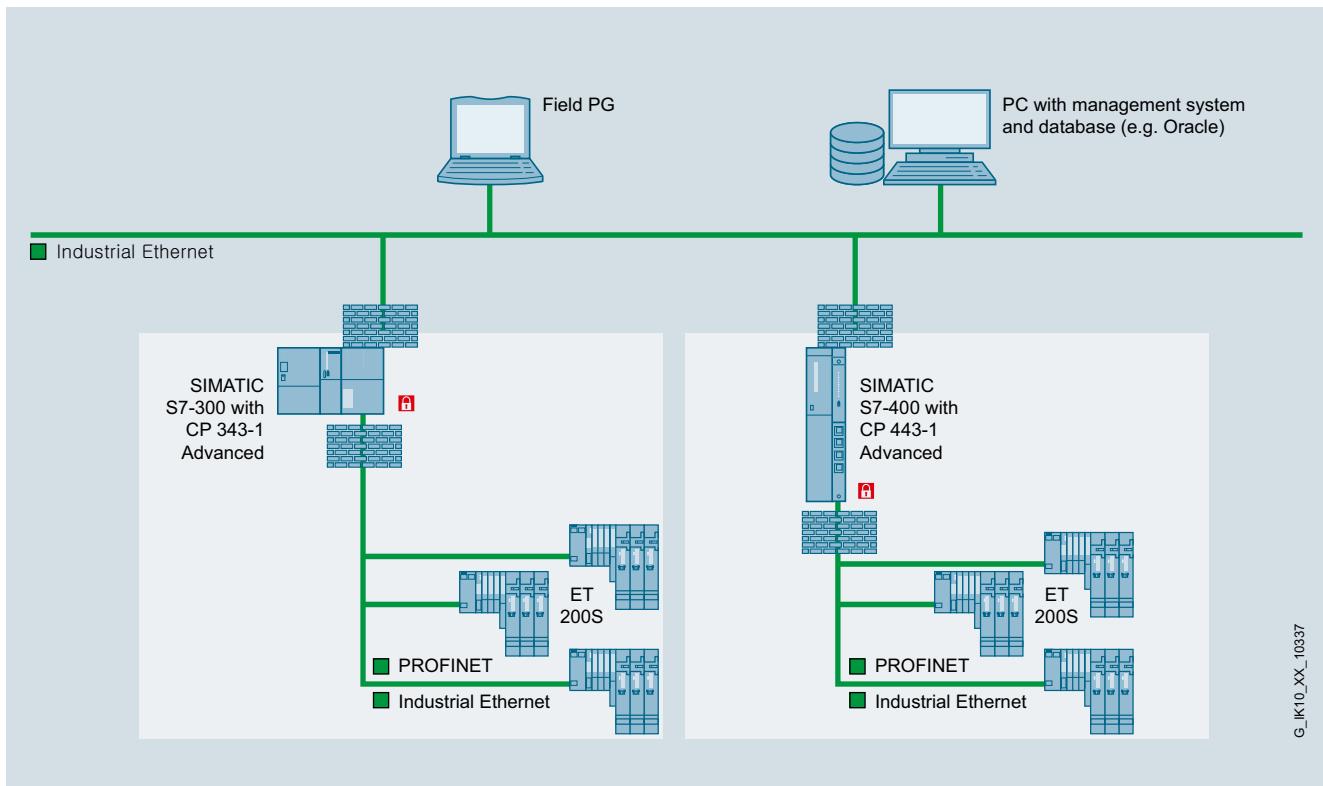
- Firewall, VPN gateway, and CP in one device:
With the latest generation of Advanced CPs and for the same price as the predecessor version, the user gets the integrated security functions of firewall and VPN for implementing a protected automation cell and for protecting data transmission.
- Secure communication integration: The CP is easily configured with STEP 7; VPN tunnels can be set up between the CPs themselves or to the SCALANCE S security appliance, the SOFTNET Security Client VPN software, the secure CP 1628 PC module, and the SCALANCE M mobile wireless router.

Particularly users already employing Advanced CPs will find it simple to set up secure networks. All CP 343-1 Advanced and CP 443-1 Advanced users get Security Integrated and do not need any separate hardware or special tools besides SIMATIC S7 to configure the security of industrial plants.



Security Integrated

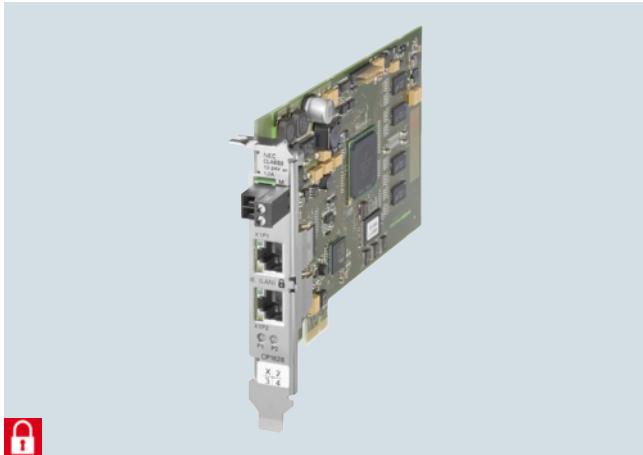
Protection of controllers through communications processors



G_IK10_XX_10337

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





CP 1628

Via the CP 1628 Industrial Ethernet communications processor, industrial PCs are protected by firewall and VPN – for secure 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 SIMATIC PG/PC and PCs with PCI Express slots 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 contains Security Integrated, comprising a Stateful Inspection Firewall and a VPN gateway to protect the PG/PC systems against security risks.

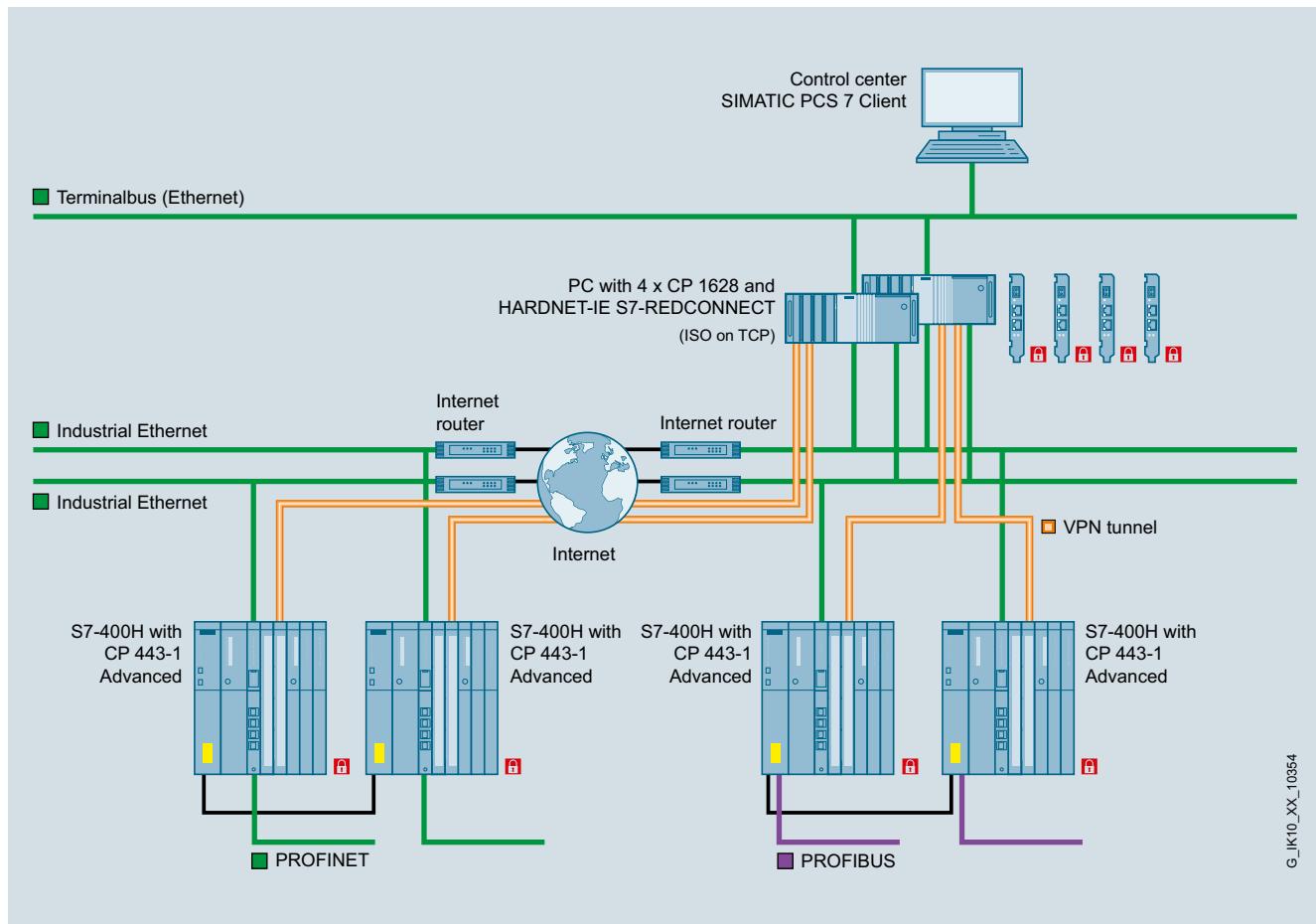
Advantages at a glance

- Firewall, VPN gateway, and CP in one device: This new product version offers users an integrated, fully-fledged security module that protects the PC from manipulation and unauthorized access.
- Secure communication integration: The CP is easily configured using STEP 7/NCM PC (V5.5 SP3 or higher) or TIA Portal (V12 SP1 or higher).



Security Integrated

Protection of controllers through communications processors



G_IK10_XX_10354

Secure redundant connection to 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 secure transmission of the H communication. In addition, the CP 1628 protects the PC system from unauthorized access by means of its integrated firewall.

Technical data at a glance

Product type designation	SCALANCE S602	SCALANCE S612	SCALANCE S623	SCALANCE S627-2M
Article No.	6GK5602-0BA10-2AA3	6GK5612-0BA10-2AA3	6GK5623-0BA10-2AA3	6GK5627-2BA10-2AA3
Transmission rate				
Transfer rate 1 / 2 / 3	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s	10 / 100 / 1000 Mbit/s
Ports				
Electrical connection				
■ for internal network	1 x RJ45 port	1 x RJ45 port	1 x RJ45 port	3 x RJ45 ports + media module
■ for external network	1 x RJ45 port	1 x RJ45 port	1 x RJ45 port	3 x RJ45 ports + media module
■ for DMZ	–	–	1 x RJ45 port	1 x RJ45 port
■ for signaling contact	1 x 2-pole terminal block	1 x 2-pole terminal block	1 x 2-pole terminal block	1 x 2-pole terminal block
■ for power supply	1 x 4-pole terminal block	1 x 4-pole terminal block	1 x 4-pole terminal block	1 x 4-pole terminal block
C-PLUG swap media	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
Range	19.2 V ... 28.8 V DC	19.2 V ... 28.8 V DC	19.2 V ... 28.8 V DC	19.2 V ... 28.8 V DC
Permissible ambient conditions				
Ambient temperature				
■ during operation	-40 °C ... +60 °C	-40 °C ... +60 °C	-40 °C ... +60 °C	-40 °C ... +60 °C
■ during storage	-40 °C ... +80 °C	-40 °C ... +80 °C	-40 °C ... +80 °C	-40 °C ... +70 °C
■ during transportation	-40 °C ... +80 °C	-40 °C ... +80 °C	-40 °C ... +80 °C	-40 °C ... +70 °C
Degree of protection	IP20	IP20	IP20	IP20
Design, dimensions, and weight				
Design	Compact	Compact	Compact	Compact
Width / height / depth	60 mm / 125 mm / 124 mm	60 mm / 125 mm / 124 mm	60 mm / 125 mm / 124 mm	120 mm / 125 mm / 124 mm
Net weight	0.8 kg	0.8 kg	0.81 kg	1.3 kg
Product function: Security				
Firewall configuration	Stateful inspection	Stateful Inspection	Stateful inspection	Stateful Inspection
Product function in VPN connection	–	IPSec	IPSec	IPSec
Product function				
■ Password protection	Yes	Yes	Yes	Yes
■ Restricted bandwidth	Yes	Yes	Yes	Yes
■ NAT/NAPT	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	MD5, SHA-1	MD5, SHA-1

Security Integrated

Technical data at a glance

Product type designation	SCALANCE M874-2/M874-3	SCALANCE M875
Article No.	6GK5874-2AA00-2AA2 6GK5874-3AA00-2AA2	6GK5875-0AA10-1AA2
Transmission rate		
1 for Industrial Ethernet / 2 for Industrial Ethernet for GSM transmission for GPRS transmission for eGPRS transmission for UMTS transmission	10 Mbit/s / 100 Mbit/s – max. 42.8/85.6 kbit/s uplink/downlink max. 118/236.8 kbit/s uplink/downlink max. 5.76/14.4 Mbit/s uplink/downlink (for M874-3 only)	10 Mbit/s / 100 Mbit/s 9 600 bit/s max. 42.8/85.6 kbit/s uplink/downlink max. 118/236.8 kbit/s uplink/downlink max. 5.76/14.4 Mbit/s uplink/downlink
Ports		
Electrical connection ■ for network components/terminal equipment ■ for external antenna(s) ■ for power supply	RJ45 port (10/100 Mbit/s, TP, autocrossover) SMA antenna sockets (50 ohms)	RJ45 port (10/100 Mbit/s, TP, autocrossover) SMA antenna sockets (50 ohms) Terminal strip
Supply voltage, current consumption, power loss		
Supply voltage Range	12 V ... 28.8 V DC	12 V ... 30 V DC
Permissible ambient conditions		
Ambient temperature ■ during operation ■ during storage Degree of protection	-20 °C ... +60 °C -40 °C ... +85 °C IP20	-40 °C ... +75 °C -40 °C ... +85 °C IP20
Design, dimensions, and weight		
Design Width / height / depth Net weight	Compact 35 mm / 147 mm / 127 mm –	Compact 45 mm / 99 mm / 114 mm 280 g
Product function: Security		
Firewall configuration Product function ■ Password protection ■ Packet filter Suitability for VPN use Product function in VPN connection Number of possible connections in the case of VPN connection Type of authentication for VPN PSK Protocol is supported, IPsec tunnel and transport mode Key length ■ for IPsec DES for VPN ■ 1 for IPsec AES for VPN ■ 2 for IPsec AES for VPN ■ 3 for IPsec AES for VPN Type of Internet key exchange for VPN main mode Key length for IPsec 3DES for VPN Type of Internet key exchange for VPN quick mode Type of packet authentication for VPN	Stateful Inspection Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes MD5, SHA-1	Stateful Inspection Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes Yes

Product type designation	CP 1243-1	CP 1543-1
Article No.	6GK7243-1BX30-0XE0	6GK7543-1AX00-0XE0
Transmission rate		
■ at interface 1 / 2	10 ... 100 Mbit/s / –	10 ... 1 000 Mbit/s / –
Ports		
Electrical connection		
■ to interface 1 according to IE	1 x RJ45 port	1 x RJ45 port
■ to interface 2 according to IE	–	–
■ for power supply	–	–
C-PLUG swap media	–	–
Supply voltage, current consumption, power loss		
Supply voltage		
■ 1 from backplane bus	5 V DC	15 V DC
■ External	–	–
Permissible ambient conditions		
Ambient temperature		
■ during operation		
- when installed vertically	-20 °C ... +60 °C	0 °C ... +40 °C
- when installed horizontally	-20 °C ... +70 °C	0 °C ... +60 °C
■ during storage	-40 °C ... +70 °C	-40 °C ... +70 °C
■ during transportation	-40 °C ... +70 °C	-40 °C ... +70 °C
Degree of protection	IP20	IP20
Design, dimensions, and weight		
Module format	Compact S7-1200, single width	Compact S7-1500, single width
Width / height / depth	30 mm / 110 mm / 75 mm	35 mm / 142 mm / 129 mm
Net weight	0.122 kg	0.35 kg
Product function: Security		
Firewall configuration	Stateful Inspection	Stateful Inspection
Product function in VPN connection	IPSec	IPSec
Type of encryption algorithms for VPN connection	AES-256, AES-192, AES-128, 3DES-168	AES-256, AES-192, AES-128, 3DES-168, DES-5
Type of authentication algorithms for VPN connection	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 Certificates
Type of hashing algorithms for VPN connection	MD5, SHA-1	MD5, SHA-1
Number of possible connections in the case of VPN connection	8	16
Product function		
■ Password protection for Web applications	No	No
■ ACL – IP-based	No	No
■ ACL – IP-based for PLC/routing	No	No
■ Deactivation of non-required services	Yes	Yes
■ Blocking of communication via physical ports	No	No
■ Log file for unauthorized access	No	Yes

Security Integrated

Technical data at a glance

Product type designation	CP 343-1 Advanced	CP 443-1 Advanced
Article No.	6GK7343-1GX31-0XE0	6GK7443-1GX30-0XE0
Transmission rate		
■ at interface 1 / 2	10 ... 1000 Mbit/s / 10 ... 100 Mbit/s	10 ... 1000 Mbit/s / 10 ... 100 Mbit/s
Ports		
Electrical connection		
■ to interface 1 according to IE	1 x RJ45 port	1 x RJ45 port
■ to interface 2 according to IE	2 x RJ45 ports	4 x RJ45 ports
■ for power supply	2-pole plug-in terminal strip	–
C-PLUG swap media	Yes	Yes
Supply voltage, current consumption, power loss		
Supply voltage		
■ 1 from backplane bus	5 V DC	5 V DC
■ External	24 V DC	–
Permissible ambient conditions		
Ambient temperature		
■ during operation	0 °C ... +40 °C	0 °C ... +60 °C
- when installed vertically	0 °C ... +60 °C	–
- when installed horizontally	-40 °C ... +70 °C	–
■ during storage	-40 °C ... +70 °C	-40 °C ... +70 °C
■ during transportation	-40 °C ... +70 °C	-40 °C ... +70 °C
Degree of protection	IP20	IP20
Design, dimensions, and weight		
Module format	Compact	Compact S7-400, single width
Width / height / depth	80 mm / 125 mm / 120 mm	25 mm / 290 mm / 210 mm
Net weight	0.8 kg	0.7 kg
Product function: Security		
Firewall configuration	Stateful Inspection	Stateful Inspection
Product function in VPN connection	IPSec	IPSec
Type of encryption algorithms for VPN connection	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Type of authentication algorithms for VPN connection	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates
Type of hashing algorithms for VPN connection	MD5, SHA-1	MD5, SHA-1
Number of possible connections in the case of VPN connection	32	32
Product function		
■ Password protection for Web applications	Yes	Yes
■ ACL – IP-based	Yes	Yes
■ ACL – IP-based for PLC/routing	Yes	Yes
■ Deactivation of non-required services	Yes	Yes
■ Blocking of communication via physical ports	Yes	Yes
■ Log file for unauthorized access	No	No

Product type designation	CP 1628	SOFTNET Security Client
Article No.	6GK1162-8AA00	6GK1704-1VW04-0AA0
Ports		
Electrical connection		
<ul style="list-style-type: none"> ■ to interface 1 according to IE ■ of the backplane bus ■ for power supply 	2 x RJ45 port PCI Express x1 1 x 2-pole terminal block	
Supply voltage, current consumption, power loss		
Type of power supply voltage	DC	
Optional external supply	Yes	
Supply voltage		
<ul style="list-style-type: none"> ■ 1 from backplane bus ■ 2 from backplane bus ■ external ■ range 	3.3 V 12 V 24 V 10.5 V ... 32 V	
Permissible ambient conditions		
Ambient temperature		
<ul style="list-style-type: none"> ■ during operation ■ during storage ■ during transportation 	+5 °C ... +55 °C -20 °C ... +60 °C -20 °C ... +60 °C	
Design, dimensions, and weight		
Module format	PCI Express x1 (half length)	
Width / height / depth	18 mm / 111 mm / 167 mm	
Net weight	0.124 kg	
Product function: Security		
Firewall configuration	Stateful Inspection	–
Product function in VPN connection	IPSec	IPSec
Type of encryption algorithms for VPN connection	AES-256, AES-192, AES-128, 3DES-168, DES-56	AES-256, AES-192, AES-128, 3DES-168, DES-56
Type of authentication algorithms for VPN connection	Preshared key (PSK), X.509v3 certificates	Preshared key (PSK), X.509v3 certificates
Type of hashing algorithms for VPN connection	MD5, SHA-1	MD5, SHA-1
Number of possible connections in the case of VPN connection	64	Unlimited or depending on computer configuration
Maximum number of usable IP addresses on VPN connection	16	Depends on computer configuration

Industrial Security

Industrial security services



The merge of data systems in the production and office environments has made many processes faster and easier, while the use of the same data processing programs creates synergies. This development, however, also increases risks to security.

Today it is no longer just the office environment that is under threat from viruses, trojans, hackers, etc., but production plants are also at risk of malfunctions and data loss. Many weak spots in security are not obvious at first glance. For this reason, it is advisable to check existing plants in regard to security and to optimize them in order to maintain a higher level of plant availability. To enhance the security of a plant against cyber attacks, a multi-level service concept for Industrial Security is available from Siemens Industry.

The first step involves "assessment" – the initial examination of the existing plant. This identifies weak spots or deviations from standards. The result of this examination is a detailed report about the actual status of the plant with a description of the weak points and an assessment of the risks. The report also contains suggested actions for improving the level of security.

In the second stage of "implementation", the measures defined in the assessment are implemented, i.e.:

- **Training:**

Personnel are given specific training so that they understand what IT and infrastructure security means in the industrial environment.

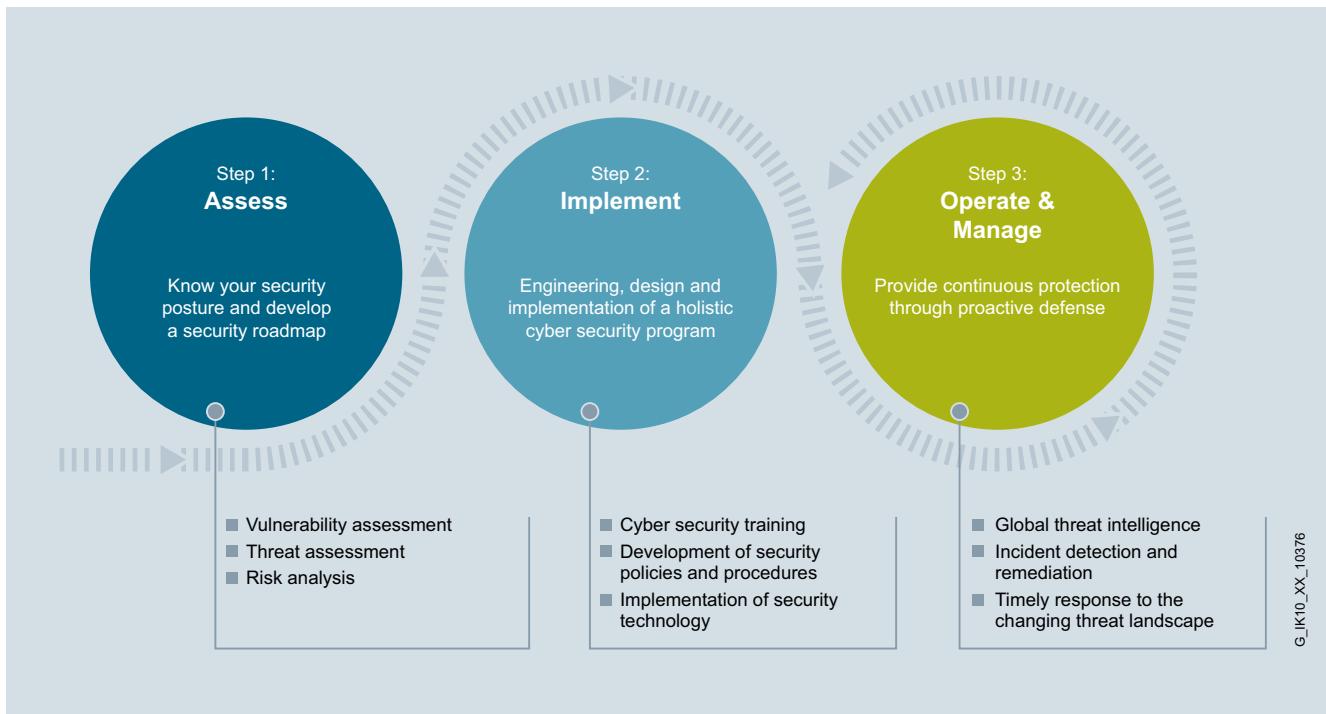
- **Process improvement:**

Security-relevant regulations and guidelines relating to the existing plant requirements are drawn up and implemented.

- **Security technologies:**

Protective measures are implemented for hardware and software, as well as in the plant network, in addition longterm protection through monitoring is available.

The measures defined and implemented in the first two phases are continuously developed in the third phase of "**operation and management**", i.e. monitoring the security status of the plant, checking the security level, redefining and optimizing actions, as well as regular reports and functions such as updates, backup and restore. Even if changes are made to the plant network, the software environment or the administration of access rights for users and administrators, the services increase the security level so that the corresponding data remains in the plant and attackers are given minimal opportunities to compromise the plant. The phases of implementation, operation and management are tailored precisely to meet the existing needs.



Advantages at a glance

- Determination of the security level and, based on this, drawing up a plan of action for reducing the risks
- Specific training for building up technical knowledge
- Tightened plant security through coordinated processes and specifications
- Implementation of a comprehensive security solution for protecting the automation system

- Connection to a Managed Service Center for continuous monitoring of the security status of the plant
- Continuous monitoring of the security status of the plant
- Detection of incidents and adaptation of the environment to deal with threat situations
- Plant kept state-of-the-art by means of updates (patterns, patches, signatures).

Industrial Security

Terms, definitions

DDNS

The Dynamic Domain Name System is an IT system that can update domain name entries.

Demilitarized Zone (DMZ)

A demilitarized zone or DMZ denotes a computer network with security monitoring of the ability to access the connected servers.

The systems in the DMZ are shielded by one or more firewalls against other networks (such as Internet, LAN). This separation can allow access to publicly available 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.

Firewalls

Security modules 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.

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: External authentication server

The concept of RADIUS is based on an external authentication server. An end device can only access the network after the Industrial Ethernet switch has verified the logon data of the device with the authentication server. Both the end device and the authentication server must support the Extensive Authentication Protocol (EAP).

System hardening

The system hardening package closes interfaces and ports that are not required, 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 networks (VPN)

A "VPN tunnel" connects two or more network stations (e.g. security modules) 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 LANs (VLAN)

The special feature of a VLAN: Devices can be assigned by configuration to a device group, irrespective of their physical location. In doing so, several of these device groups share a single physical network infrastructure. The result is several "virtual networks" on the same physical network. Data communication takes place only within a VLAN.

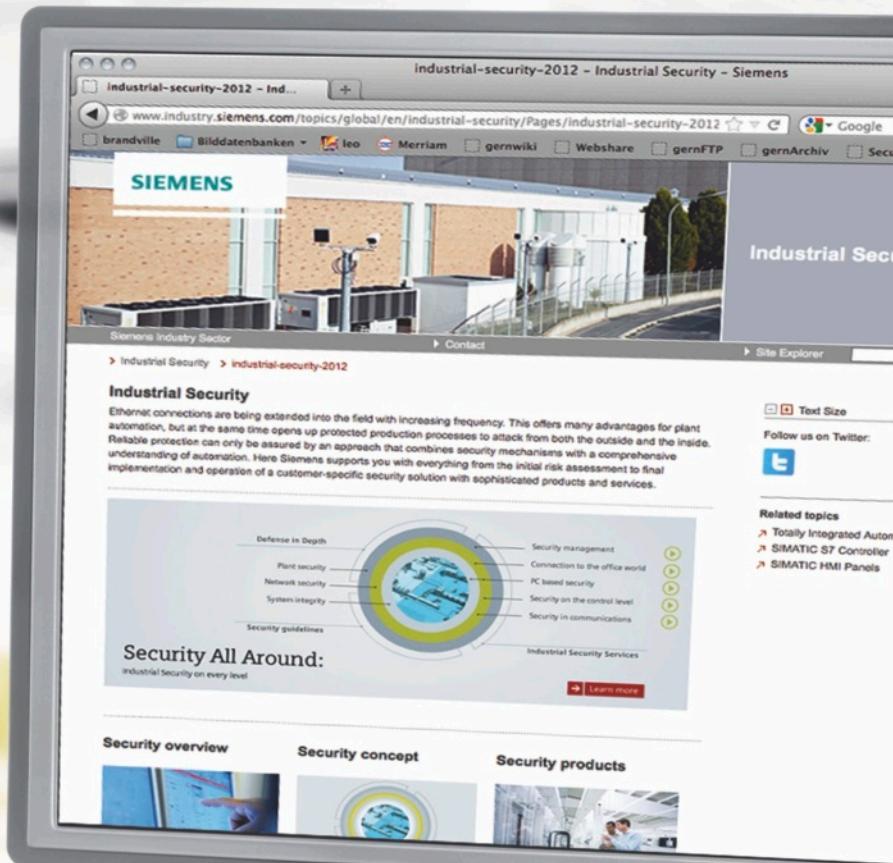
Whitelisting

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



Get the full Industrial Security experience:

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



Industrial
Security –
take a look!



Follow us on:

twitter.com/siemensindustry

youtube.com/siemens

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit:

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

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit:

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

Get more information

Information material available for downloading:
www.siemens.com/automation/infocenter

Service & Support:
www.siemens.com/automation/service&support

SIMATIC NET contacts:
www.siemens.com/automation/partner

Industry Mall for electronic ordering:
www.siemens.com/industrymall

Siemens AG
Industry Sector
Industrial Automation Systems
Postfach 48 48
90026 NÜRNBERG
GERMANY

Subject to change without notice
Article No.: 6ZB5530-1AP02-0BA3
DR.PN.SC.14.XXBR.95.31 / Dispo 26000
BR 0314 2. PES 32 En
Printed in Germany
© Siemens AG 2014

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.