



8/2	Security Integrated
8/2	Introduction
8/8	SCALANCE S
8/19	SCALANCE M
8/20	CP 1243-1 and CP 1543-1
8/21	CP 343-1 Advanced and CP 443-1 Advanced
8/23	CP 1628
8/24	SOFTNET Security Client
8/27	Industrial Security Services

Industrial Security

Security Integrated

Introduction

Overview

Industrial security

That is why industrial security is so important

As the use of Ethernet connections all the way down to the field level increases, the associated security issues are becoming a more urgent topic for industry. After all, open communication and 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.

Threat overview

No.	Threat	Explanation
1	Unauthorized use of remote maintenance access	Maintenance access provides deliberate openings to the outside in the ICS network ¹⁾ . However, they 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.
3	Attacks against standard components used in the ICS network	Standard IT components (commercial off-the-shelf, COTS) 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, this 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 of 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 presently 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 acts of God	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.

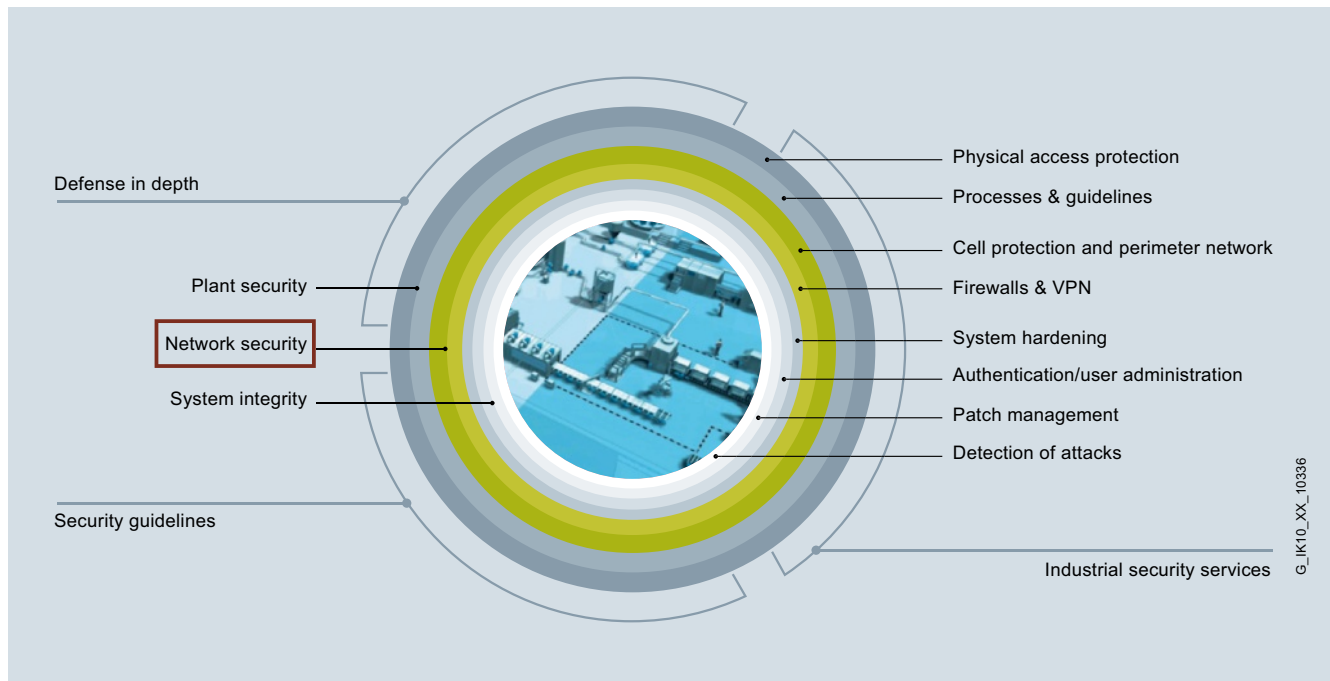
¹⁾ Industrial Control Systems (ICS)

Source: BSI-A-CS 004 | Version 1.00 dated April 12, 2012; page 2 of 2

Note:

The list of threats came about as a result of close cooperation between BSI and business representatives. With its BSI analyses, the Federal Office for Information Security (BSI) publishes statistics and reports on current topics in cyber security. Please send comments and notes to: cs-info@bsi.bund.de

Overview (continued)



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 they 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 constant further 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 protection of system integrity protect against cyber attacks and unauthorized access by operators or external persons.

Factors for success: 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, which can be accomplished by means of firewalls and, if applicable, by establishing a DMZ (demilitarized zone = secure, protected zone). The DMZ is used to provide data for other networks, without granting direct access to the automation network. 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 communication can be secured using "Security Integrated" components such as SCALANCE S Security Modules, SCALANCE M wireless routers, or Security CPs for SIMATIC.

Initial risk assessment and information on the Internet

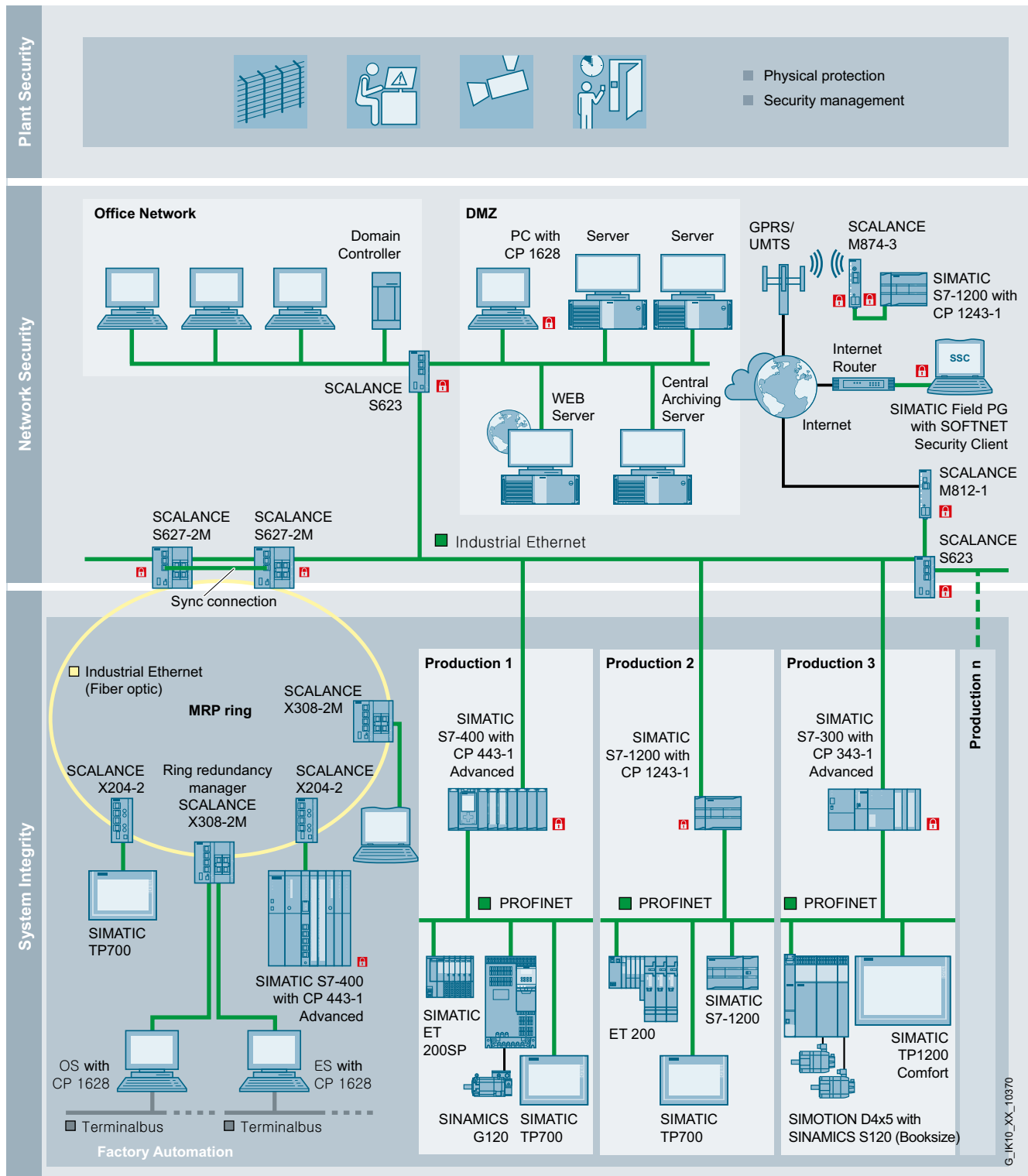
You want to know how good the security of your industrial plant is? We can provide you with detailed information about the special security issues in your industry. Use the opportunity to contact our consulting team about any open issues. Our experts will gladly prepare a security concept that is adapted to 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

Security Integrated

Introduction

Overview (continued)



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

Overview (continued)**Security Integrated****Cell protection concept**

Industrial communication is a key factor for corporate success – as long as the network is protected. As your 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. With the cell protection concept, a plant network is subdivided into 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 implementation.

The following Security Integrated products are available:

SIMATIC S7-1200 / S7-1500:

- Protection of the controller by 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 (firewall and VPN) for S7-1200/S7-1500 with 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.

SCALANCE M router**Mobile radio router**

SCALANCE M industrial router for secure access to plants via mobile radio, e.g. GPRS or UMTS, with integral security functions – firewall for protection against unauthorized access and VPN for protection of the data transmission.

DSL routers








The SCALANCE M DSL routers are ADSL routers (M812-1 and M816-1) for the secure connection of Ethernet-based subnets and automation devices to hard-wired DSL networks or SHDSL routers (M826) for connection via existing wire-pairs or multi-wire cables. They have integral security functions – firewall for protection against unauthorized access and VPN for protection of the data transmission.

Industrial PCs

- Via the **CP 1628** communications processor, the industrial PCs are protected by firewall and VPN – for secure communication without special operating system settings. This means that 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.

	SCALANCE S family	SCALANCE M family	CP 343-1 Adv CP 443-1 Adv	S7-1200 CPU ¹⁾ S7-1500 CPU	CP 1243-1 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 (TIA Portal)

G_IK10_XX_10347

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

Industrial Security

Security Integrated

Introduction

Ordering data

Article No.

Article No.

Security Integrated devices

SCALANCE S Industrial Security Modules

For protecting programmable controllers and automation networks and for securing industrial communication; Security Modules protect network segments against unauthorized access by means of Stateful Inspection Firewall; connection of more than 10/100/1 000 Mbit/s ports; configuring tool and electronic manual on CD ROM; English, German, French, Italian, Spanish;

SCALANCE S602

6GK5602-0BA10-2AA3

SCALANCE S612

up to 128 VPN tunnels simultaneously

6GK5612-0BA10-2AA3

SCALANCE S623

up to 128 VPN tunnels simultaneously; additional RJ45 DMZ port

6GK5623-0BA10-2AA3

SCALANCE S627-2M

up to 128 VPN tunnels simultaneously; additional RJ45 DMZ port; two additional slots for one 2-port media module each

6GK5627-2BA10-2AA3

SOFTNET Security Client V4 HF1

6GK1704-1VW04-0AA0

Software for designing secure IP-based VPN connections from a programming device/PC to network segments which are secured by SCALANCE S, SCALANCE M, CP 343-1 Advanced, CP 443-1 Advanced, or CP 1628; Single License for 1 installation, runtime software (German/English), configuration tool (German/English), and electronic manual on CD-ROM (German/English/French/Spanish/Italian) for Windows 7 Professional, Ultimate, Windows XP Professional (32-bit) + SP3

SCALANCE M industrial modems and routers

SCALANCE M874 mobile radio router

Mobile radio router for wireless IP communication from Industrial Ethernet-based subnets and programmable controllers via UMTS or GSM mobile radio networks; with integrated firewall and VPN with IPsec; 2 x RJ45 ports, 1 x antenna connection

- SCALANCE M874-3¹⁾
- SCALANCE M874-2¹⁾

6GK5874-3AA00-2AA2
6GK5874-2AA00-2AA2

SCALANCE M875 UMTS Router

UMTS router for wireless IP communication from Industrial Ethernet-based programmable controllers via UMTS/GSM mobile radio networks; EGPRS Multislot Class 12; with integrated firewall and VPN with IPsec; 2 x RJ45 ports, 2 x antenna connections

- SCALANCE M875¹⁾
- SCALANCE M875¹⁾ for Japan

6GK5875-0AA10-1AA2
6GK5875-0AA10-1CA2

SCALANCE M81x-1 ADSL router

DSL router for wired IP communication from Industrial Ethernet-based subnets and programmable controllers via telephone or DSL networks; with integrated firewall and VPN with IPsec; 1 x or 4 x RJ45 ports for Industrial Ethernet; 1 x RJ45 port for DSL

- SCALANCE M812-1 (Annex A)
- SCALANCE M812-1 (Annex B)
- SCALANCE M816-1 (Annex A)
- SCALANCE M816-1 (Annex B)

6GK5812-1AA00-2AA2
6GK5812-1BA00-2AA2
6GK5816-1AA00-2AA2
6GK5816-1BA00-2AA2

SCALANCE M826-2 SHDSL router

DSL router for wired IP communication from Industrial Ethernet-based subnets and programmable controllers via telephone or DSL networks; with integrated firewall and VPN with IPsec; 1 x or 4 x RJ45 ports for Industrial Ethernet; 1 x RJ45 port for DSL

- SCALANCE M826-2 (Annex A)

6GK5826-2AB00-2AB2

Ordering data		Article No.	
Communications processors for SIMATIC S7			
CP 1243-1 communication processor; for connection of SIMATIC S7-1200 to Industrial Ethernet via TCP/IP, ISO and UDP, Telecontrol Server Basic and security functions Stateful Inspection Firewall and VPN; 1 x RJ45 interface with 10/100 Mbit/s	6GK7243-1BX30-0XE0	CP 1628 communications processor; PCI Express x1 card for connection to Industrial Ethernet (10/100/1 000 Mbit/s), with 2-port switch (RJ45) and integrated security (firewall, VPN) via HARDNET-IE S7 and S7-REDCONNECT. For operating system support, see SIMATIC NET Software	6GK1162-8AA00
CP 1543-1 communication processor; for connection of SIMATIC S7-1500 to Industrial Ethernet via TCP/IP, ISO and UDP and security functions Stateful Inspection Firewall and VPN; 1 x RJ45 interface with 10/100/1 000 Mbit/s;	6GK7543-1AX00-0XE0	Accessories	
CP 343-1 Advanced communications processor; For connection of SIMATIC S7-300 to Industrial Ethernet over ISO and TCP/IP; PROFINET IO Controller or PROFINET IO Device, MRP, integrated 2-port switch ERTEC; S7 communication, open communication (SEND/RECEIVE), FETCH/WRITE, with and without RFC1006, multicast, DHCP, CPU clock synchronization via SIMATIC procedure and NTP, diagnostics, SNMP, access protection through IP access list, initialization over LAN 10/100 Mbit/s; as well as IT communication (web, e-mail, FTP); PROFINET CBA; security (firewall/VPN); PROFInergy; with electronic manual on DVD	6GK7343-1GX31-0XE0	IE FC TP Standard Cable GP 2 x 2 (Type A) 4-core, shielded TP installation cable for connecting to IE FC RJ45 outlet / IE FC RJ45 plug; PROFINET-compliant; with UL approval; sold by the meter; max. length 1 000 m, minimum order 20 m	6XV1840-2AH10
CP 443-1 Advanced communications processor; For the connection of SIMATIC S7-400 to Industrial Ethernet; PROFINET IO Controller with RT and IRT, MRP, PROFINET CBA, TCP/IP, ISO and UDP; S7 communication, open communication (SEND/RECEIVE) with FETCH/WRITE, with and without RFC1006, diagnostics expansions, multicast, clock synchronization with SIMATIC mode or NTP, access protection by IP access list, FTP client/server, HTTP server, HTML diagnostics, SNMP, DHCP, e-mail, data storage on C-PLUG; PROFINET connector: 4xRJ45 (10/100 Mbit/s) via switch; Gigabit connector: 1xRJ45 (10/100/1 000 Mbit/s); with integrated stateful inspection firewall and VPN appliance	6GK7443-1GX30-0XE0	IE FC RJ45 Plug 180 RJ45 plug-in connector for Industrial Ethernet with a rugged metal enclosure and integrated insulation displacement contacts for connecting Industrial Ethernet FC installation cables; with 180° cable outlet; for network components and CPs/CPUs with Industrial Ethernet interface <ul style="list-style-type: none">• 1 pack = 1 unit• 1 pack = 10 units• 1 pack = 50 units	6GK1901-1BB10-2AA0 6GK1901-1BB10-2AB0 6GK1901-1BB10-2AE0
		IE FC stripping tool Preadjusted stripping tool for fast stripping of Industrial Ethernet FC cables	6GK1901-1GA00
		SITOP compact 24 V/ 0.6 A 1-phase power supply with wide-range input 85 – 264 V AC/110 – 300 V DC, stabilized output voltage 24 V, rated output current value 0.6 A, slim design	6EP1331-5BA00
		C-PLUG Swap medium for simple replacement of devices in the event of a fault; for storing configuration or application data; can be used for SIMATIC NET products with C-PLUG slot	6GK1900-0AB00

¹⁾ Please note national approvals under
<http://www.siemens.com/wireless-approvals>

Note:

Check the current country list:
<http://support.automation.siemens.com/WW/view/en/66627157>

Overview



- Security modules for the protection of automation networks and security during data exchange between automation systems.
- Checking and filtering of data traffic by integrated firewall and thus:
 - Protection against operator mistakes
 - Prevention of unauthorized access
 - Prevention of faults and communications overload
- Authentication of the communication partners and encryption of the transmitted data with VPN and thus protection of communication against espionage and manipulation.
- Rugged, industry-compatible design of the devices
- Easy and clear configuration:
Using the Security Configuration Tool (SCT), all SIMATIC NET security products can be configured and diagnosed from a central position.
- No changes or adaptations necessary in the existing network topology, applications or network stations since SCALANCE S can also be used as a bridge and not just as a router.
- Securing of communication is independent of the protocol (e.g. PROFINET or other Ethernet-based fieldbus solutions)
- Secure remote access via the Internet possible without restrictions and with any providers
- Increased availability is possible by means of redundant protection of automation cells or ring topologies

Product versions:

SCALANCE S602;

- Uses the stateful inspection firewall to protect network segments against unauthorized access.
- "Ghost mode" for protection of individual, even alternating, devices by dynamically taking over the IP address.
- Connection via 10/100/1 000 Mbit/s ports.

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 10/100/1 000 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 10/100/1 000 Mbit/s ports.
- Additional RJ45 DMZ port (DMZ: "demilitarized zone") for secure connection from, for example, remote maintenance modems, laptops, or an additional network. This yellow port 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 linking of the redundant device via the yellow port.

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 10/100/1 000 Mbit/s ports.
- Additional RJ45 DMZ port (DMZ: "demilitarized zone") for secure connection from, for example, remote maintenance modems, laptops, or an additional network. This yellow port 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 of the firewall by means of a synchronization cable between the yellow ports.
- Two additional slots for one 2-port media module each (see 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-wire cables (e.g. PROFIBUS) by deploying MM992-2VD media modules (variable distance).

Benefits

get **Designed for Industry**

- Protection of industrial automation networks against unauthorized access and setup of a DMZ (protected zone) possible for data exchange with other networks without having to grant direct access to the production network.
- Through implementation of the cell protection concept:
 - Protection of any Ethernet-based programmable controllers and automation systems which do not have their own security functions
 - Protecting several devices simultaneously
 - Reduction in risk by means of network segmenting (by generating secure communication islands)
 - Securing of communication to and from the automation cells is possible
- User-specific firewall rules can be used to assign specific access privileges to users and not just to devices.
- System-wide network diagnostics thanks to integration into IT infrastructures and network management systems by means of SNMP
- Securing of remote access via the Internet. Using PPPoE and DynDNS, dynamic IP addresses can also be applied.
- Problem-free 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
- Direct integration in ring structures and FO networks is possible (SCALANCE S627-2M)

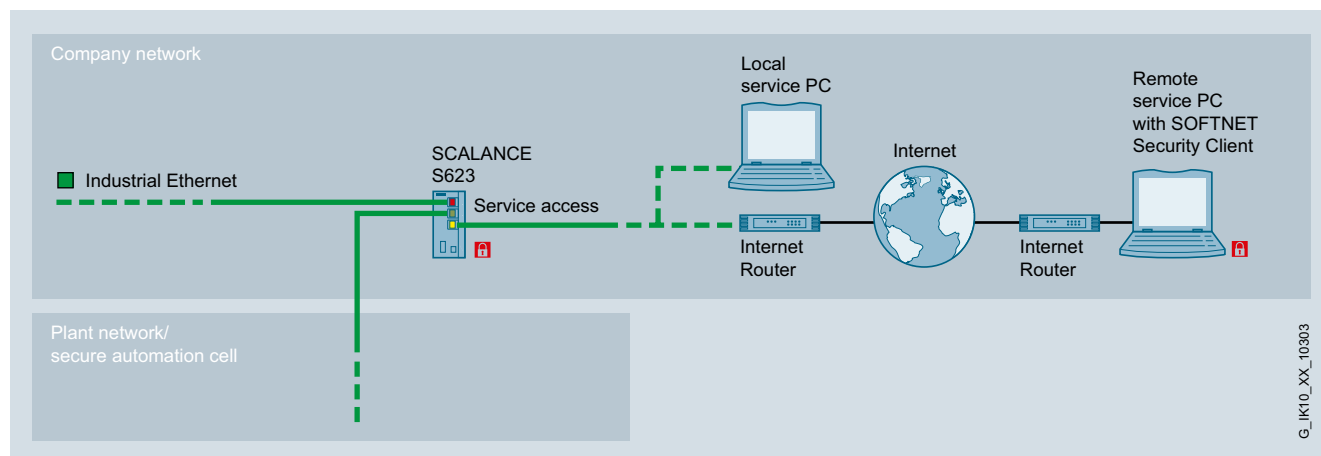
Application

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 S612 or SCALANCE S623 also protect the data transmission between devices or network segments (e.g. automation cells) against data manipulation and espionage; they can also be used for secure remote access over the Internet.

The security modules can be operated not only in bridge mode but also in router mode, and can thus also be used direct at IP subnetwork borders.

Secure remote access over the Internet or GPRS/UMTS is possible with the SCALANCE M875 GPRS/UMTS router.

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 systems, simple installation and minimal downtimes in the event of a fault.



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

Industrial Security

Security Integrated

SCALANCE S

Design

SCALANCE S602

- Checking of data traffic and protection against unauthorized access by means of stateful inspection firewall.
- Simple and fast configuration of the firewall through global firewall rules and symbolic names for IP addresses.
- Specific access privileges for users in accordance with user-specific firewall rules.
- 10/100/1 000 Mbit/s ports for the connection and operation of SCALANCE S in Gigabit networks as well
- In addition to bridge mode, can also be operated in router mode and can therefore also be used directly at IP subnet limits
- Address translation
 - NAT (Network Address Translation) permits the use of private IP addresses in the internal network in that public IP addresses are converted to private ones
 - NAT (Network Address and Port Translation) permits the use of private IP addresses in the internal network in that frames are converted to private IP addresses depending on the communications port used
- Internal network nodes can receive their IP addresses from the integral DHCP server
- Log files can also be evaluated by the Syslog server
- Enhanced integration in IT infrastructures and network management systems by means of SNMP
- Protection of individual, even alternating, devices by dynamically taking over the IP address (ghost mode)

SCALANCE S612

As SCALANCE S602; additionally:

- Encryption of data transmission with VPN (IPSec)
 - Protection against espionage
 - Protection against unauthorized manipulation
- Secure remote access over the Internet, e.g. in conjunction with the SOFTNET Security Client and the SCALANCE M UMTS router (with IPSec VPN function)

SCALANCE S623

As SCALANCE S612; additionally:

- DMZ port with which a protected zone (DMZ = demilitarized) can be set up between two networks. The DMZ is used to provide data for other networks without granting direct access to the automation network, thus increasing security. The DMZ port can also be used to protect remote maintenance access, where, for example, only access to lower-level automation cells is possible and no access to the plant network is required.
- Secure, redundant connection of automation cells through router and firewall redundancy

SCALANCE S627-2M

As SCALANCE S623; additionally:

- Two media module slots for two additional switched red or green ports each.
 - Direct integration in line or ring topologies is possible
 - Integration into redundant rings (MRP, HRP) is possible
 - Secure, redundant connection of automation cells or rings
 - Direct integration in FO networks is possible through the use of FO media modules
 - Bridging of longer cable runs or use of existing 2-wire cables (e.g. PROFIBUS) by deploying the MM992-2VD media modules (variable distance).

Function

Security functions

VPN (Virtual Private Network)

(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. As IP addresses can be falsified (IP spoofing), checking the IP address (of the client access) is not sufficient. In addition, Client PCs may have changing IP addresses. For this reason the 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.

The firewall

can be used as an alternative or to supplement VPN with flexible access control.

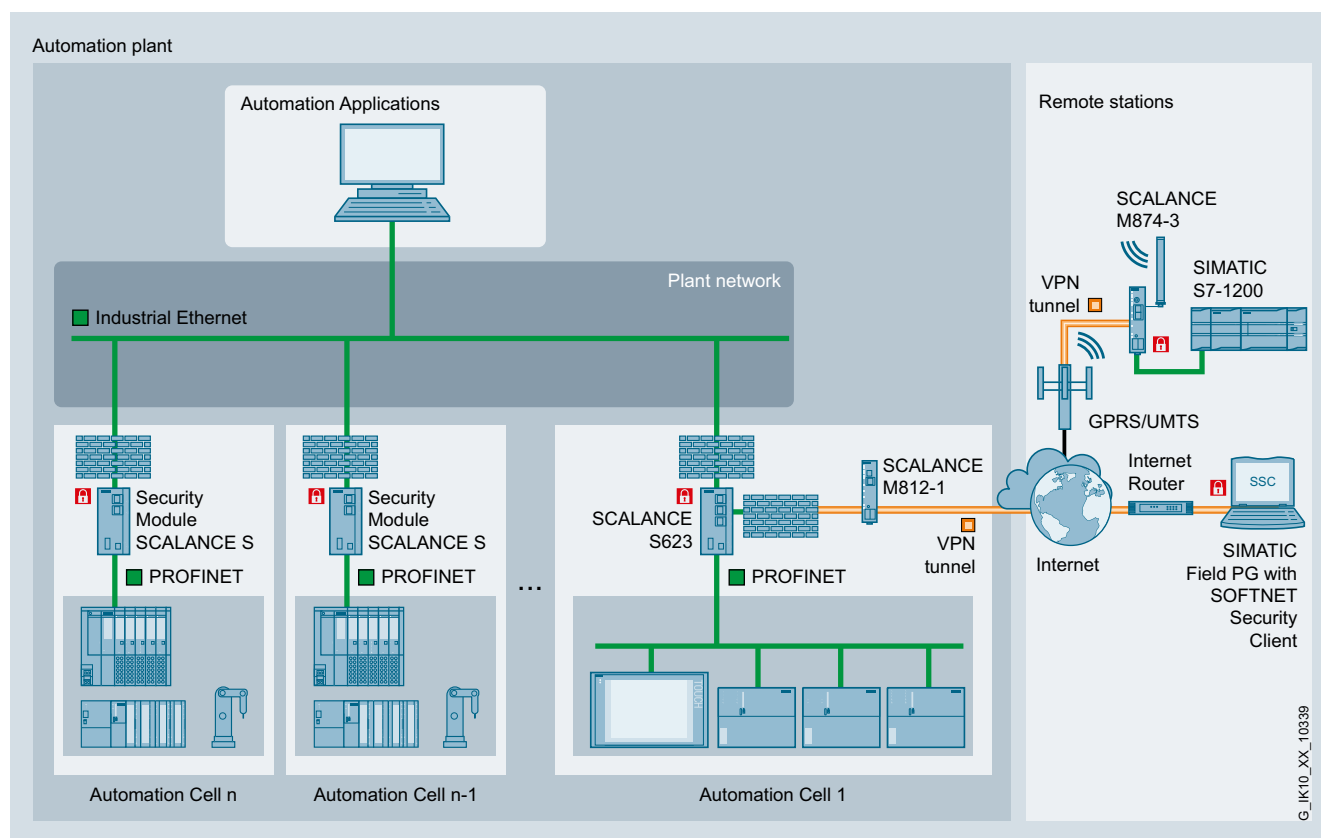
The firewall filters data packets and disables or enables communication links in accordance with the filter list and stateful inspection. Both incoming and outgoing communication can be filtered, either according to IP and MAC addresses as well as communication protocols (ports) or user-specific.

- Logging;

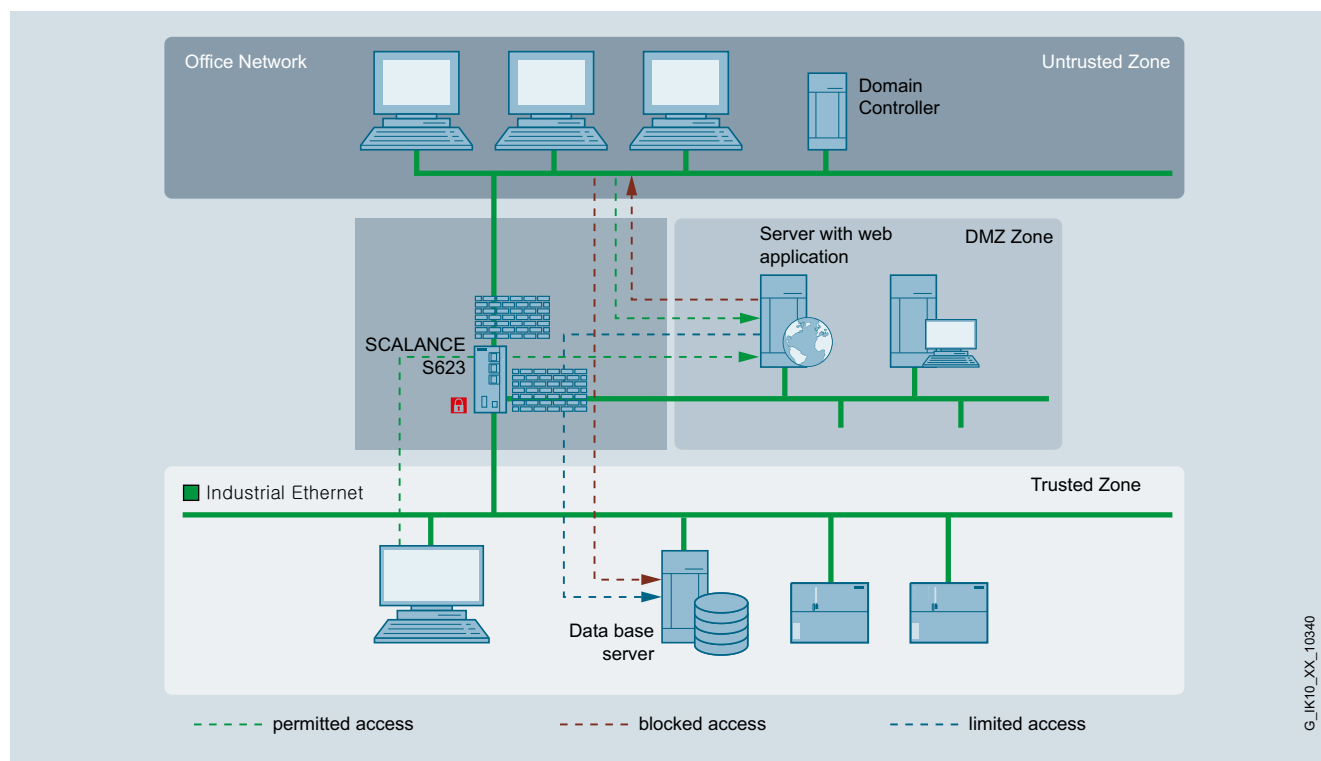
access data are saved by the Security Module in a log file. Detection of how, when and by whom it has been accessed is as important as detecting access attempts, to ensure that appropriate preventative measures can be taken.

Configuration

Configuration is carried out using the Security Configuration Tool (SCT). Therefore all SIMATIC NET security products can 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 and without the need of a programming device.

Function (continued)**Configuration**

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



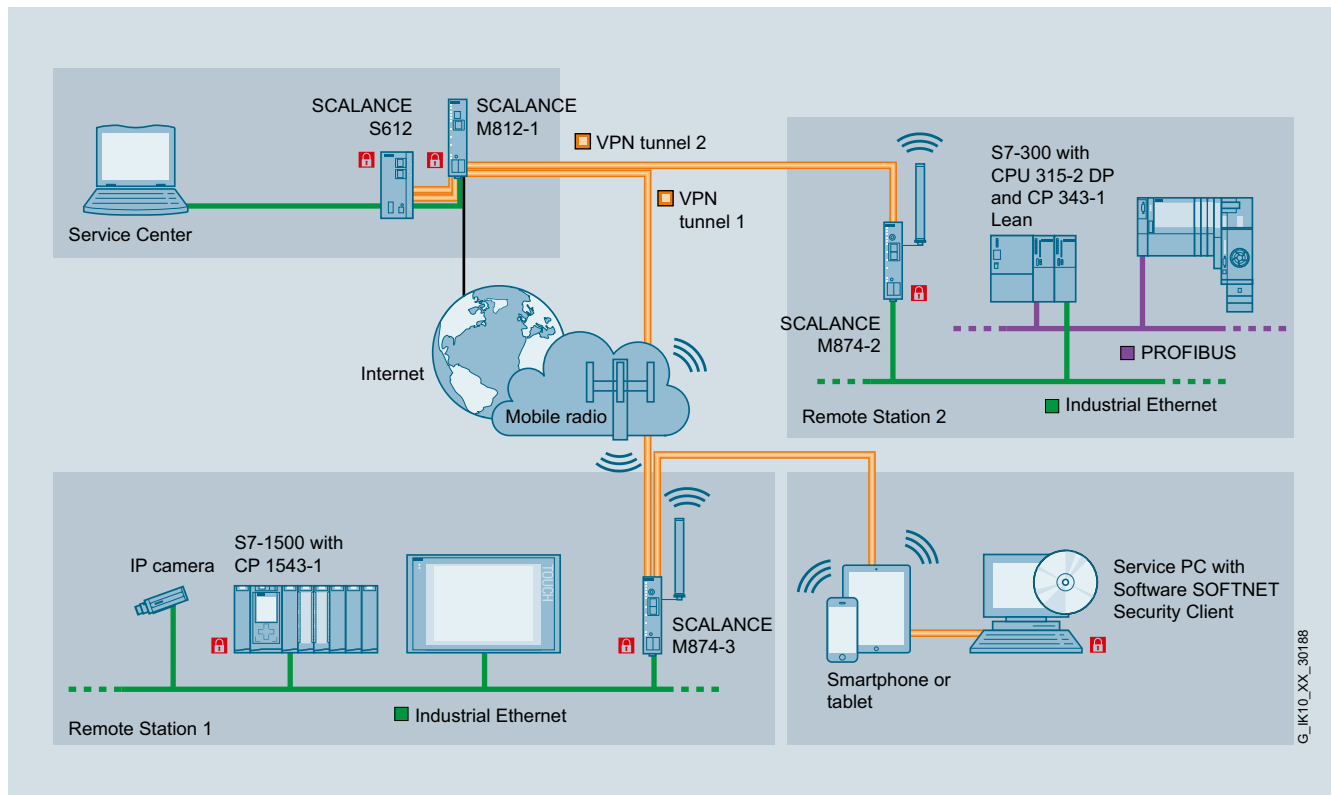
Demilitarized zone (DMZ) for remote maintenance or access to data server with SCALANCE S623

Industrial Security

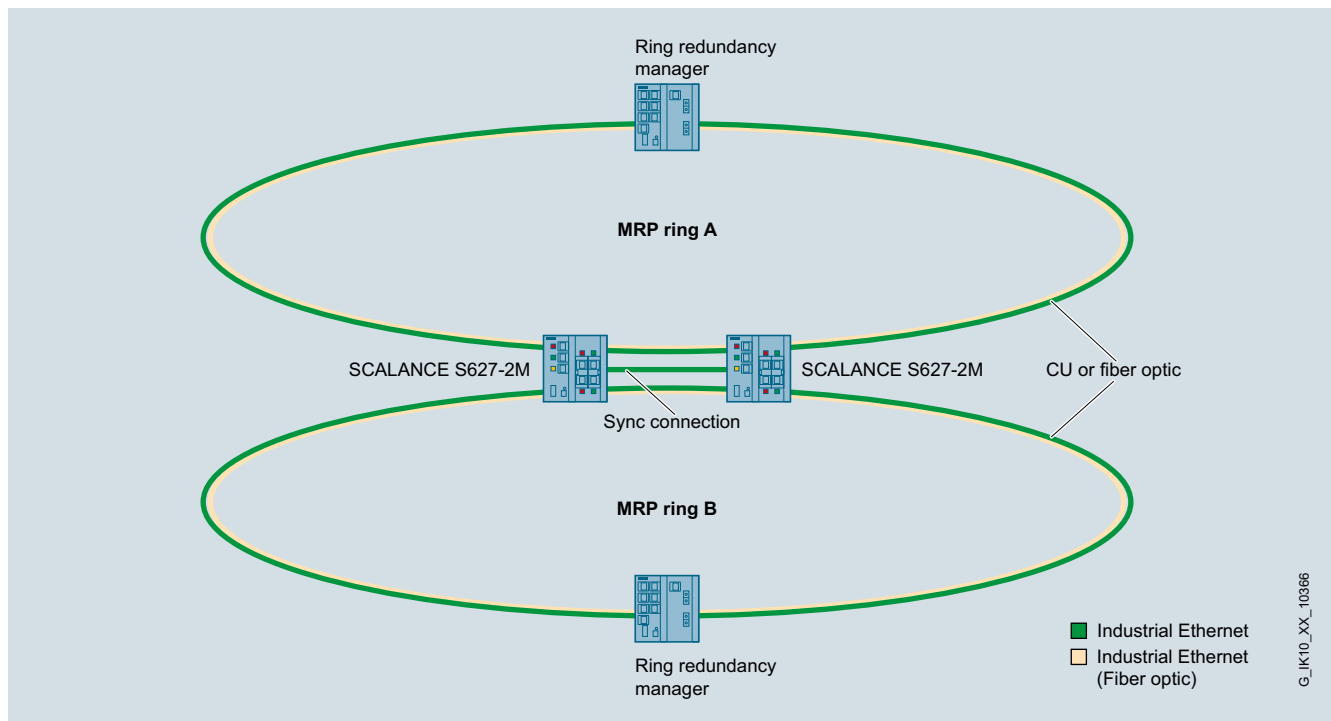
Security Integrated

SCALANCE S

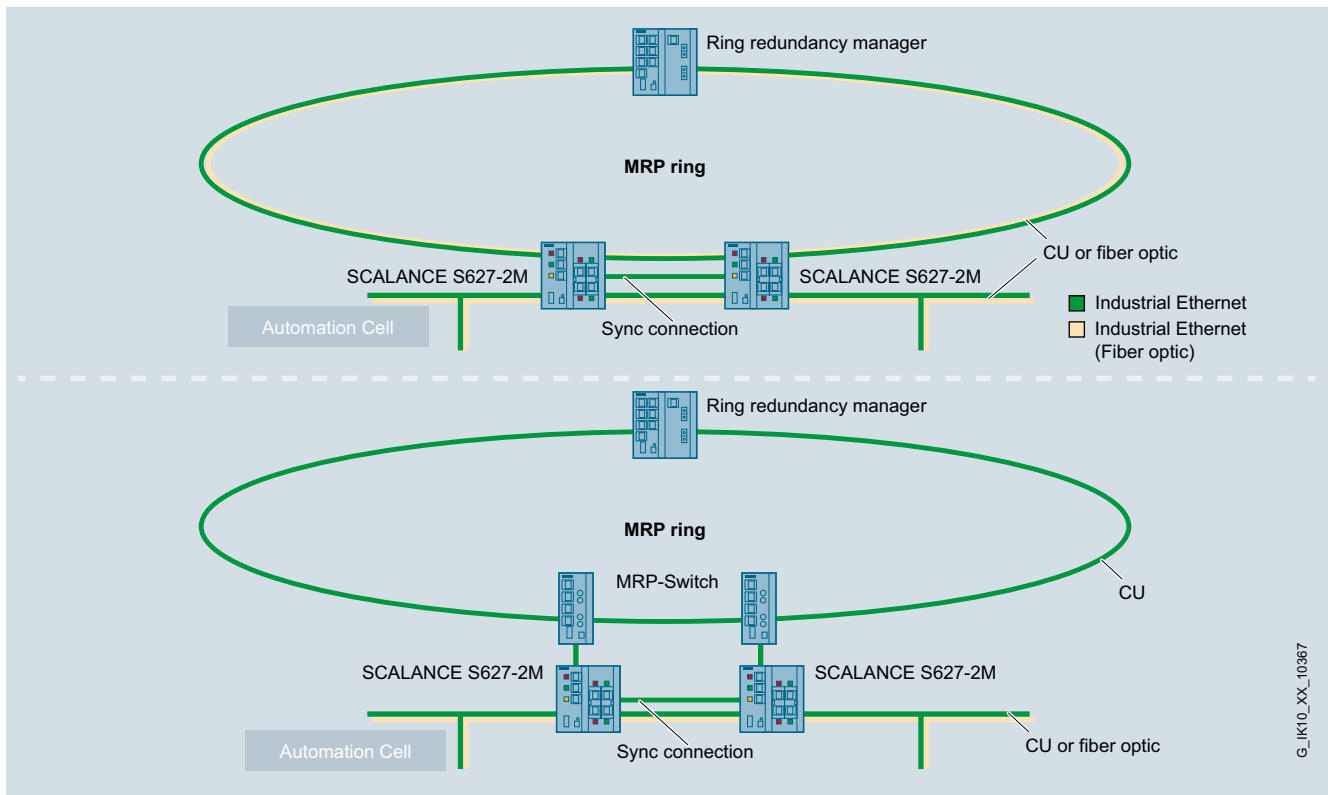
Function (continued)



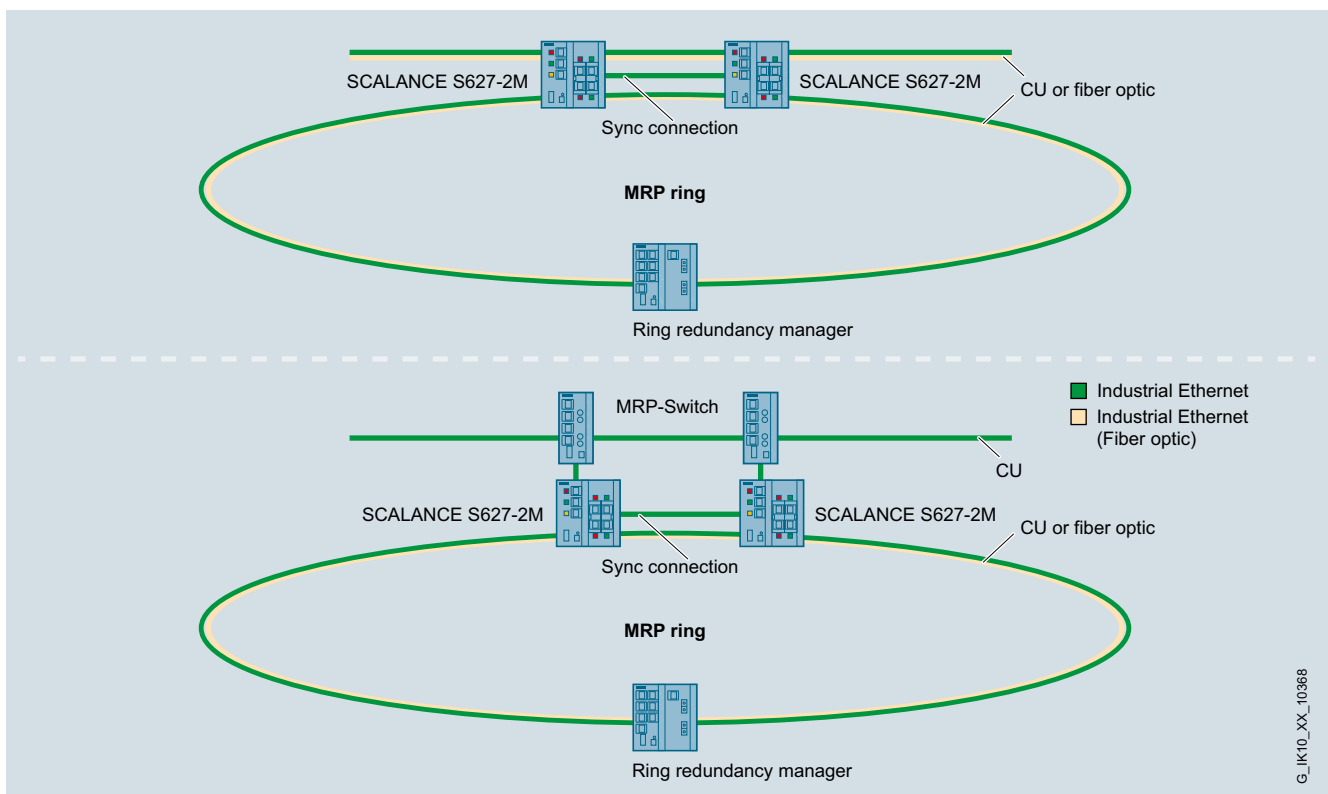
Secure remote access over Internet with SCALANCE S and SCALANCE M



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

Function (continued)

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



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

Industrial Security

Security Integrated

SCALANCE S

Technical specifications

Article No.	6GK5602-0BA10-2AA3	6GK5612-0BA10-2AA3	6GK5623-0BA10-2AA3
Product-type designation	SCALANCE S602	SCALANCE S612	SCALANCE S623
Transmission rate			
Transfer rate 1	10 Mbit/s	10 Mbit/s	10 Mbit/s
Transfer rate 2	100 Mbit/s	100 Mbit/s	100 Mbit/s
Transfer rate 3	1 000 Mbit/s	1 000 Mbit/s	1 000 Mbit/s
Interfaces			
Number of electrical/optical connections for network components or terminal equipment maximum	2	2	3
Number of electrical connections			
• for internal network	1	1	1
• for external network	1	1	1
• for DMZ	0	0	1
• for signaling contact	1	1	1
• for power supply	1	1	1
• for redundant power supply	1	1	1
Design of the electrical connection			
• for internal network	RJ45 port	RJ45 port	RJ45 port
• for external network	RJ45 port	RJ45 port	RJ45 port
• for DMZ	-	-	RJ45 port
• for signaling contact	2-pole terminal block	2-pole terminal block	2-pole terminal block
• for power supply	4-pole terminal block	4-pole terminal block	4-pole terminal block
Design of the removable storage C-PLUG	Yes	Yes	Yes
Signal-Inputs/outputs			
Operating voltage of signaling contacts at DC rated value	24 V	24 V	24 V
Operating current of signaling contacts at DC maximum	0.1 A	0.1 A	0.1 A
Supply voltage, current consumption, power loss			
Type of supply voltage	DC	DC	DC
Supply voltage external	24 V	24 V	24 V
• minimum	19.2 V	19.2 V	19.2 V
• maximum	28.8 V	28.8 V	28.8 V
Consumed current maximum	0.5 A	0.5 A	0.6 A
Product component fusing at power supply input	Yes	Yes	Yes
Type of fusing at input for supply voltage	Non-replaceable melting fuse (F 3 A / 32 V)	Non-replaceable melting fuse (F 3 A / 32 V)	Non-replaceable melting fuse (F 3 A / 32 V)
Active power loss at 24V for DC typical	6.72 W	6.72 W	6.96 W
Permitted ambient conditions			
Ambient temperature			
• during operating	-40 ... +60 °C	-40 ... +60 °C	-40 ... +60 °C
• during storage	-40 ... +80 °C	-40 ... +80 °C	-40 ... +80 °C
• during transport	-40 ... +80 °C	-40 ... +80 °C	-40 ... +80 °C
Relative humidity at 25 °C without condensation during operating maximum	95 %	95 %	95 %
Protection class IP	IP20	IP20	IP20

Technical specifications (continued)

Article No.	6GK5602-0BA10-2AA3	6GK5612-0BA10-2AA3	6GK5623-0BA10-2AA3
Product-type designation	SCALANCE S602	SCALANCE S612	SCALANCE S623
Design, dimensions and weight			
Design	compact	compact	compact
Width	60 mm	60 mm	60 mm
Height	125 mm	125 mm	125 mm
Depth	124 mm	124 mm	124 mm
Net weight	0.8 kg	0.8 kg	0.81 kg
Mounting type			
• 35 mm DIN rail mounting	Yes	Yes	Yes
• S7-300 rail mounting	Yes	Yes	Yes
• wall mounting	Yes	Yes	Yes
Mounting type	Screw mounting on horizontal and vertical surfaces	Screw mounting on horizontal and vertical surfaces	Screw mounting on horizontal and vertical surfaces
Product properties, functions, components general			
Product function DynDNS client	Yes	Yes	Yes
Protocol is supported PPPoE	Yes	Yes	Yes
Product functions management, configuration			
Product function symbolic names for IP addresses	Yes	Yes	Yes
Protocol is supported			
• SNMP v1	Yes	Yes	Yes
• SNMP v3	Yes	Yes	Yes
Type of configuration	SCT: Security Configuration Tool (included in scope of delivery)	SCT: Security Configuration Tool (included in scope of delivery)	SCT: Security Configuration Tool (included in scope of delivery)
Product functions Diagnosis			
Product function			
• SysLog	Yes	Yes	Yes
• Packet Filter Log	Yes	Yes	Yes
• Audit Log	Yes	Yes	Yes
• System Log	Yes	Yes	Yes
Product functions DHCP			
Product function DHCP server - internal network	Yes	Yes	Yes
Product functions Routing			
Product function static IP routing	Yes	Yes	Yes
Product functions Security			
Design of the firewall	Stateful inspection	Stateful inspection	Stateful inspection
Product function with VPN connection	-	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
Type of authentication procedure with VPN connection	-	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
Number of possible connections for VPN connection	0	128	128
Number of network stations			
• maximum	0	128	128
• note	-	Limitation only applies in bridge mode. No limitation in routing mode	Limitation only applies in bridge mode. No limitation in routing mode
Product function			
• Password protection	Yes	Yes	Yes
• bandwidth limiting	Yes	Yes	Yes
• NAT/NAPT	Yes	Yes	Yes

Industrial Security

Security Integrated

SCALANCE S

Technical specifications (continued)

Article No.	6GK5602-0BA10-2AA3	6GK5612-0BA10-2AA3	6GK5623-0BA10-2AA3
Product-type designation	SCALANCE S602	SCALANCE S612	SCALANCE S623
Product functions Time			
Product function pass on time synchronization	Yes	Yes	Yes
Protocol is supported NTP	Yes	Yes	Yes
Product component Hardware real-time clock	Yes	Yes	Yes
Product property battery-backed hardware real-time clock	Yes	Yes	Yes
Standards, specifications, approvals			
Standard	FM 3611	FM 3611	FM 3611
• for EMC from FM	EN 60079-0: 2006, EN60079-15: 2005, II 3 G Ex nA IIT., KEMA 07 ATEX 0145 X	EN 60079-0: 2006, EN60079-15: 2005, II 3 G Ex nA IIT., KEMA 07 ATEX 0145 X	EN 60079-0: 2006, EN60079-15: 2005, II 3 G Ex nA IIT., KEMA 07 ATEX 0145 X
• for hazardous zone	UL 60950 / CSA C22.2 No. 60950-00, UL 508 / CSA C22.2 No. 142	UL 60950 / CSA C22.2 No. 60950-00, UL 508 / CSA C22.2 No. 142	UL 60950 / CSA C22.2 No. 60950-00, UL 508 / CSA C22.2 No. 142
• for security of CSA and UL	EN 61000-6-4 : 2007	EN 61000-6-4 : 2007	EN 61000-6-4 : 2007
• for emitted interference	EN 61000-6-2 : 2005	EN 61000-6-2 : 2005	EN 61000-6-2 : 2005
• for interference immunity	AS/NZS 2064 (Class A), EN 61000-6-2, EN 61000-6-4, marine classification pending	AS/NZS 2064 (Class A), EN 61000-6-2, EN 61000-6-4, marine classification pending	AS/NZS 2064 (Class A), EN 61000-6-2, EN 61000-6-4, marine classification pending
Verification of suitability	Yes	Yes	Yes
• CE mark	Yes	Yes	Yes
• C-Tick	No	No	No
Marine classification association	No	No	No
• American Bureau of Shipping Europe Ltd. (ABS)	No	No	No
• Bureau Veritas (BV)	No	No	No
• Det Norske Veritas (DNV)	No	No	No
• Germanische Lloyd (GL)	No	No	No
• Lloyds Register of Shipping (LRS)	No	No	No
• Nippon Kaiji Kyokai (NK)	No	No	No
• Polski Rejestr Statkow (PRS)	No	No	No
Accessories			
Product expansion optional C-PLUG	Yes	Yes	Yes

8

Article No.	6GK5627-2BA10-2AA3
Product-type designation	SCALANCE S627-2M
Transmission rate	
Transfer rate 1	10 Mbit/s
Transfer rate 2	100 Mbit/s
Transfer rate 3	1 000 Mbit/s
Interfaces	
Number of electrical/optical connections for network components or terminal equipment maximum	7
Number of electrical connections	
• for internal network	3
• for external network	3
• for DMZ	1
• for signaling contact	1
• for power supply	1
• for redundant power supply	1
Design of the electrical connection	
• for internal network	
• for external network	
• for DMZ	RJ45 port
• for signaling contact	2-pole terminal block
• for power supply	4-pole terminal block
Design of the removable storage C-PLUG	Yes

Article No.	6GK5627-2BA10-2AA3
Product-type designation	SCALANCE S627-2M
Signal-Inputs/outputs	
Operating voltage of signaling contacts at DC rated value	24 V
Operating current of signaling contacts at DC maximum	0.1 A
Supply voltage, current consumption, power loss	
Type of supply voltage	DC
Supply voltage external	24 V
• minimum	19.2 V
• maximum	28.8 V
Consumed current maximum	0.7 A
Product component fusing at power supply input	Yes
Type of fusing at input for supply voltage	Non-replaceable melting fuse (F 3 A / 32 V)
Active power loss at 24V for DC typical	12 W

Technical specifications (continued)

Article No.	6GK5627-2BA10-2AA3	Article No.	6GK5627-2BA10-2AA3
Product-type designation	SCALANCE S627-2M	Product-type designation	SCALANCE S627-2M
Permitted ambient conditions		Product functions Security	
Ambient temperature		Design of the firewall	Stateful inspection
• during operating	-40 ... +60 °C	Product function with VPN connection	IPSec
• during storage	-40 ... +70 °C	Type of encryption algorithms with VPN connection	AES-256, AES-192, AES-128, 3DES-168, DES-56
• during transport	-40 ... +70 °C	Type of authentication procedure with VPN connection	Preshared key (PSK), X.509v3 certificates
Relative humidity at 25 °C without condensation during operating maximum	95 %	Type of hashing algorithms with VPN connection	MD5, SHA-1
Protection class IP	IP20	Number of possible connections for VPN connection	128
Design, dimensions and weight		Number of network stations for internal network with VPN connection	
Design	Compact	• maximum	128
Width	120 mm	• note	Limitation only applies in bridge mode. No limitation in routing mode
Height	125 mm	Product function	
Depth	124 mm	• Password protection	Yes
Net weight	1.3 kg	• bandwidth limiting	Yes
Mounting type		• NAT/NAPT	Yes
• 35 mm DIN rail mounting	Yes	Product functions Time	
• S7-300 rail mounting	Yes	Product function pass on time synchronization	Yes
• wall mounting	Yes	Protocol is supported NTP	Yes
Mounting type	Screw mounting on horizontal and vertical surfaces	Product component Hardware real-time clock	Yes
Product properties, functions, components general		Product property battery-backed hardware real-time clock	Yes
Product function DynDNS client	Yes	Standards, specifications, approvals	
Protocol is supported PPPoE	Yes	Standard	
Product functions management, configuration		• for EMC from FM	FM 3611
Product function symbolic names for IP addresses	Yes	• for hazardous zone	EN 60079-0: 2006, EN60079-15: 2005, II 3 G Ex nA IIT., KEMA 07 ATEX 0145 X
Protocol is supported		• for security of CSA and UL	UL 60950 / CSA C22.2 No. 60950-00, UL 508 / CSA C22.2 No. 142
• SNMP v1	Yes	• for emitted interference	EN 61000-6-4 : 2007
• SNMP v3	Yes	• for interference immunity	EN 61000-6-2 : 2005
Type of configuration	SCT: Security Configuration Tool (included in scope of delivery)	Verification of suitability	AS/NZS 2064 (Class A), EN 61000-6-2, EN 61000-6-4, marine classification pending
Product functions Diagnosis		• CE mark	Yes
Product function		• C-Tick	Yes
• SysLog	Yes	Marine classification association	
• Packet Filter Log	Yes	• American Bureau of Shipping Europe Ltd. (ABS)	No
• Audit Log	Yes	• Bureau Veritas (BV)	No
• System Log	Yes	• Det Norske Veritas (DNV)	No
Product functions DHCP		• Germanische Lloyd (GL)	No
Product function DHCP server - internal network	Yes	• Lloyds Register of Shipping (LRS)	No
Product functions Routing		• Nippon Kaiji Kyokai (NK)	No
Product function static IP routing	Yes	• Polski Rejestr Statkow (PRS)	No
		Accessories	
		Product expansion optional C-PLUG	Yes

Industrial Security

Security Integrated

SCALANCE S

Ordering data

Article No.

Article No.

SCALANCE S industrial security modules

For protecting programmable controllers and automation networks and for securing industrial communication; Security Modules protect network segments against unauthorized access by means of stateful inspection firewall; connection of more than 10/100/1 000 Mbit/s ports; configuring tool and electronic manual on CD ROM; English, German, French, Italian, Spanish;

SCALANCE S602

6GK5602-0BA10-2AA3

SCALANCE S612

up to 128 VPN tunnels simultaneously

6GK5612-0BA10-2AA3

SCALANCE S623

up to 128 VPN tunnels simultaneously; additional RJ45 DMZ port

6GK5623-0BA10-2AA3

SCALANCE S627-2M

up to 128 VPN tunnels simultaneously; additional RJ45 DMZ port; two additional slots for one 2-port media module each

6GK5627-2BA10-2AA3

Accessories

IE FC TP Standard Cable GP 2 x 2 (Type A)

4-core, shielded TP installation cable for connecting to IE FC RJ45 outlet / IE FC RJ45 plug; PROFINET-compliant; with UL approval; sold by the meter; max. length 1 000 m, minimum order 20 m

6XV1840-2AH10

IE FC RJ45 Plug 180

RJ45 plug-in connector for Industrial Ethernet with a rugged metal enclosure and integrated insulation displacement contacts for connecting Industrial Ethernet FC installation cables; with 180° cable outlet; for network components and CPs/CPU's with Industrial Ethernet interface

- 1 pack = 1 unit
- 1 pack = 10 units
- 1 pack = 50 units

6GK1901-1BB10-2AA0
6GK1901-1BB10-2AB0
6GK1901-1BB10-2AE0

IE FC stripping tool

Preadjusted stripping tool for fast stripping of Industrial Ethernet FC cables

6GK1901-1GA00

SITOP compact 24 V/ 0.6 A

1-phase power supply with wide-range input 85 – 264 V AC/110 – 300 V DC, stabilized output voltage 24 V, rated output current value 0.6 A, slim design

6EP1331-5BA00

C-PLUG

Swap medium for simple replacement of devices in the event of a fault; for storing configuration or application data; can be used for SIMATIC NET products with C-PLUG slot

6GK1900-0AB00

SOFTNET Security Client

Software for designing secure IP-based VPN connections from a programming device/PC to network segments which are secured by SCALANCE S; single license for 1 installation, runtime software (German/English), configuring tool (German/English) and electronic manual on CD-ROM (German/English/French/Spanish/Italian)

SOFTNET Security Client Edition 2008

For 32-bit Windows, XP Professional + SP1, SP2, SP3

6GK1704-1VW02-0AA0

SOFTNET Security Client V3

For 32-bit Windows 7 Professional, Ultimate, Windows XP Professional + SP3

6GK1704-1VW03-0AA0

SOFTNET Security Client V4

For 32/64-bit Windows 7 Professional/Ultimate

6GK1704-1VW04-0AA0

Note:

Check the current country list:

<http://support.automation.siemens.com/WW/view/en/66627157>

More information

You will find more information on the topic of Industrial Security on the Internet at:

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

Overview



The SCALANCE M874-3 is a mobile wireless router for cost-effectively and securely connecting Ethernet-based subnets and programmable controllers via the 3rd generation mobile wireless network (UMTS) and it supports HSPA+ (High Speed Packet Access). Thus, it 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).

The SCALANCE M874-2 is a mobile wireless router for cost-effectively and securely connecting Ethernet-based subnets and programmable controllers via the 2nd generation mobile wireless network (GSM) and it supports GPRS (General Packet Radio Service) and EDGE (Enhanced Data Rates for GSM Evolution).

The security of access and communication is ensured by the security functions of the integrated firewall and by VPN tunnels (end-to-end connection encryption through IPsec tunneling).

SCALANCE M875 is a UMTS router for wireless IP communication between Industrial Ethernet-based programmable controllers via mobile radio networks of the 3rd generation (UMTS) and the 2nd generation (GSM)

- High data transfer rate thanks to HSDPA
- Integrated security functions with firewall
- Use as VPN end point (IPsec)
- Approved for railway applications



SCALANCE M812-1 and **SCALANCE M816-1** are DSL routers for the low-cost and secure connection of Ethernet-based subnets and automation devices to wired telephone or DSL networks that support ADSL2+ (Asynchronous Digital Subscriber Line). This allows the devices to have high downlink data rates of up to 25 Mbit/s and uplink data rates of up to 3.5 Mbit/s. The security of access and communication is ensured by the security functions of the integrated firewall and by VPN tunnels (end-to-end connection encryption through IPsec tunneling).

The **SCALANCE M826-2** is an SHDSL modem for low-cost, secure connection of Ethernet-based subnets and programmable controllers via existing two-wire or stranded cables and supports the ITU-T standard G.991.2 as well as SHDSL.biz (single-pair high-speed digital subscriber line). This gives the device high symmetrical data rates of up to 15.3 Mbit/s per wire pair.

The security of access and communication is ensured by the security functions of the integrated firewall and by VPN tunnels (end-to-end connection encryption through IPsec tunneling).

Note:

Further information on SCALANCE M can be found in Chapter 7, Industrial Remote Communication, under "Remote networks/ IP-based modems and routers".



Industrial Security

Security Integrated

CP 1243-1 and CP 1543-1

Overview



CP 1243-1

The CP 1243-1 communication 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.



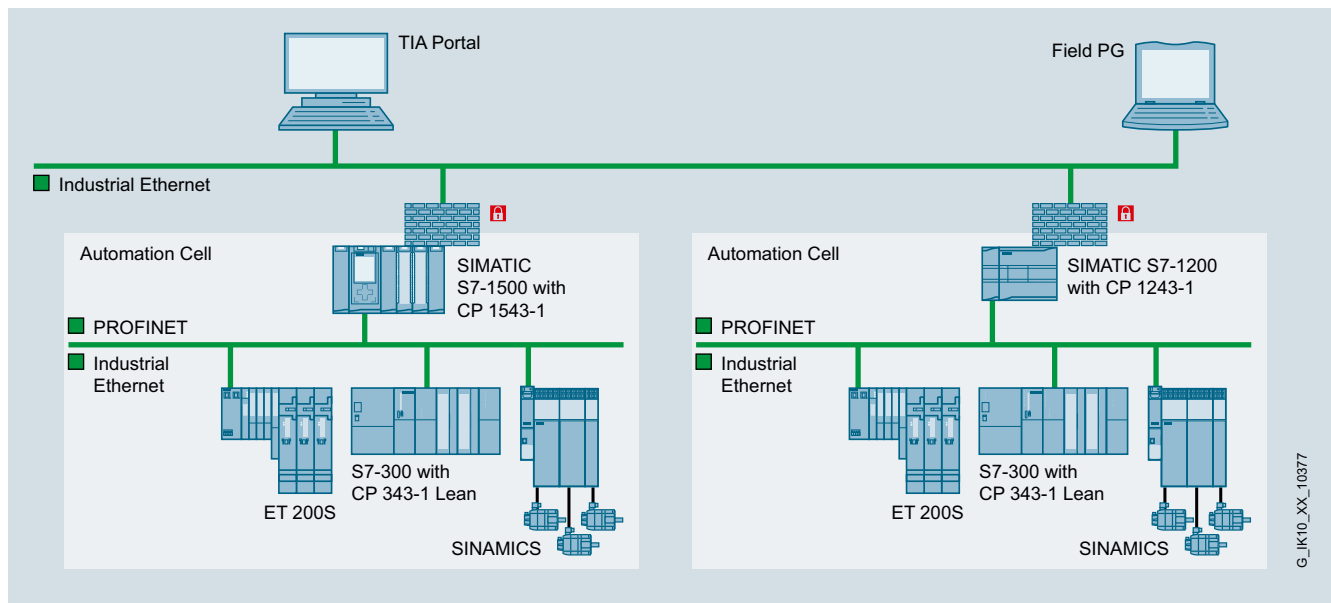
CP 1543-1

The SIMATIC CP 1543-1 communications processor securely connects the new SIMATIC S7-1500 controller to Industrial 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.

Note:

Further information on CP 1243-1 and CP 1543-1 can be found Chapter 2, PROFINET/Industrial Ethernet, under "System connection for SIMATIC S7/communication for SIMATIC S7-1500".

8



Segmentation of networks and protection of the S7-1500 with CP 1543-1 or S7-1200 with CP 1243-1

G_IK10_XX_10377

Overview



CP 343-1 Advanced

Communications processor for connecting the SIMATIC S7-300/ SINUMERIK 840D powerline to Industrial Ethernet networks, also as PROFINET IO controller and IO device.

The CP supports:

- PG/OP communication
- S7 communication
- Open communication (SEND/RECEIVE)
- PROFINET communication
- IT communication
- Security functionality, firewall and VPN



CP 443-1 Advanced

Communications processor for connecting a SIMATIC S7-400 to Industrial Ethernet networks, also as PROFINET IO controller or in SIMATIC H systems.

The CP supports:

- PG/OP communication
- S7 communication
- Open communication (SEND/RECEIVE)
- PROFINET communication
- IT communication
- Security functionality, firewall and VPN

Note:

Further information on the CP 343-1 Advanced and CP 443-1 Advanced can be found in Chapter 2, PROFINET/Industrial Ethernet, under "System connection for SIMATIC S7 communication for SIMATIC S7-300 or S7-400".

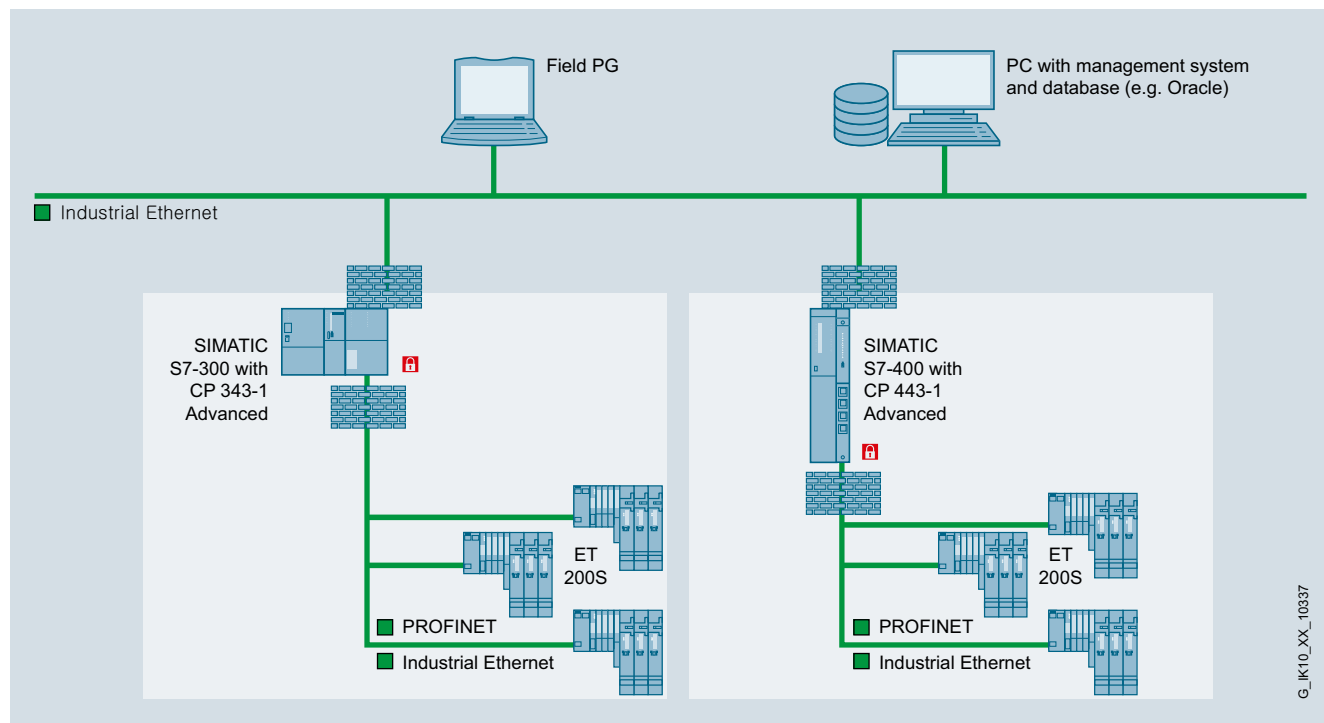
Alongside the familiar communication functions (integrated switch and Layer 3 routing functionality) the CP 343-1 Advanced and CP 443-1 Advanced Industrial Ethernet communications processors also contain the "Security Integrated" function Stateful Inspection Firewall and a VPN gateway to protect the controller and lower-level networks against security risks.

Industrial Security

Security Integrated

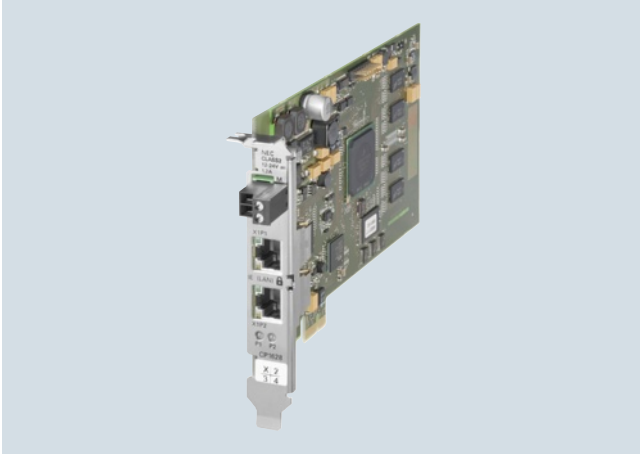
CP 343-1 Advanced and CP 443-1 Advanced

Overview (continued)



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

Overview



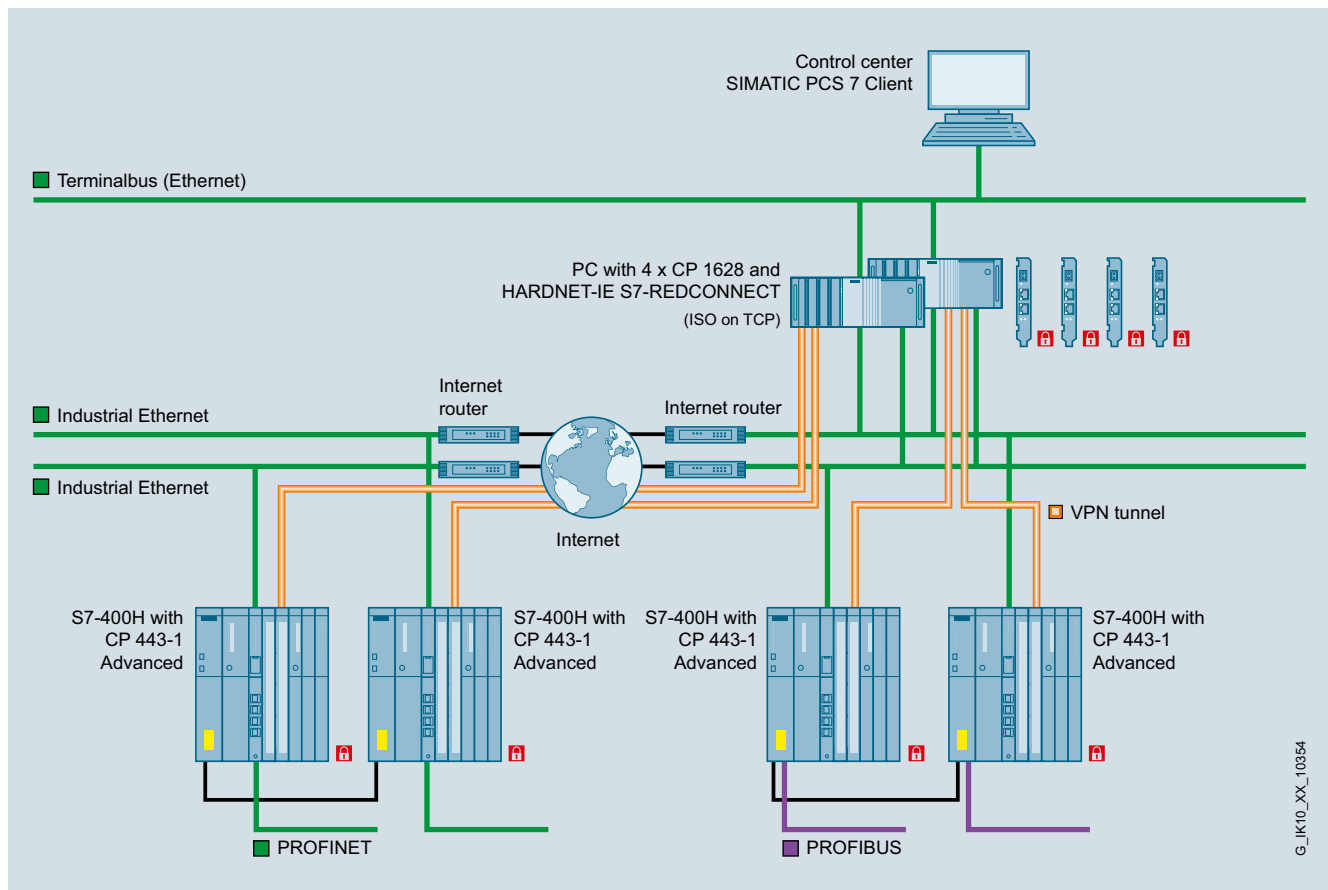
- PCI Express card (PCIe x1) with its own microprocessor and integrated 2-port switch (2 x RJ45 connection, 10/100/1 000 Mbit/s) for the connection of a PG/PC to Industrial Ethernet
- Integrated security mechanisms (e.g. Firewall, VPN)
- ISO and TCP/IP transport protocol on board
- Communications services via
 - Open IE communication (TCP/IP and UDP)
 - ISO transport protocol
 - PG/OP communication
 - S7 communication
 - Open communication (SEND/RECEIVE)
- Integration into network management systems through the support of SNMP (V1/V3)

Note:

Further information on the CP 1628 can be found in Chapter 2, PROFINET/Industrial Ethernet, under "System connection for PG/PC/IPC/communication for PC-based systems".

Industrial PCs are protected by firewall and VPN via the CP 1628 Industrial Ethernet communications processor – for secure communication without special operating system settings. This means that 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 (10/100/1 000 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", i.e. a Stateful Inspection Firewall and a VPN gateway to protect the PG/PC system against security risks.



Secure redundant connection to CP 1628 and CP 443-1 Advanced

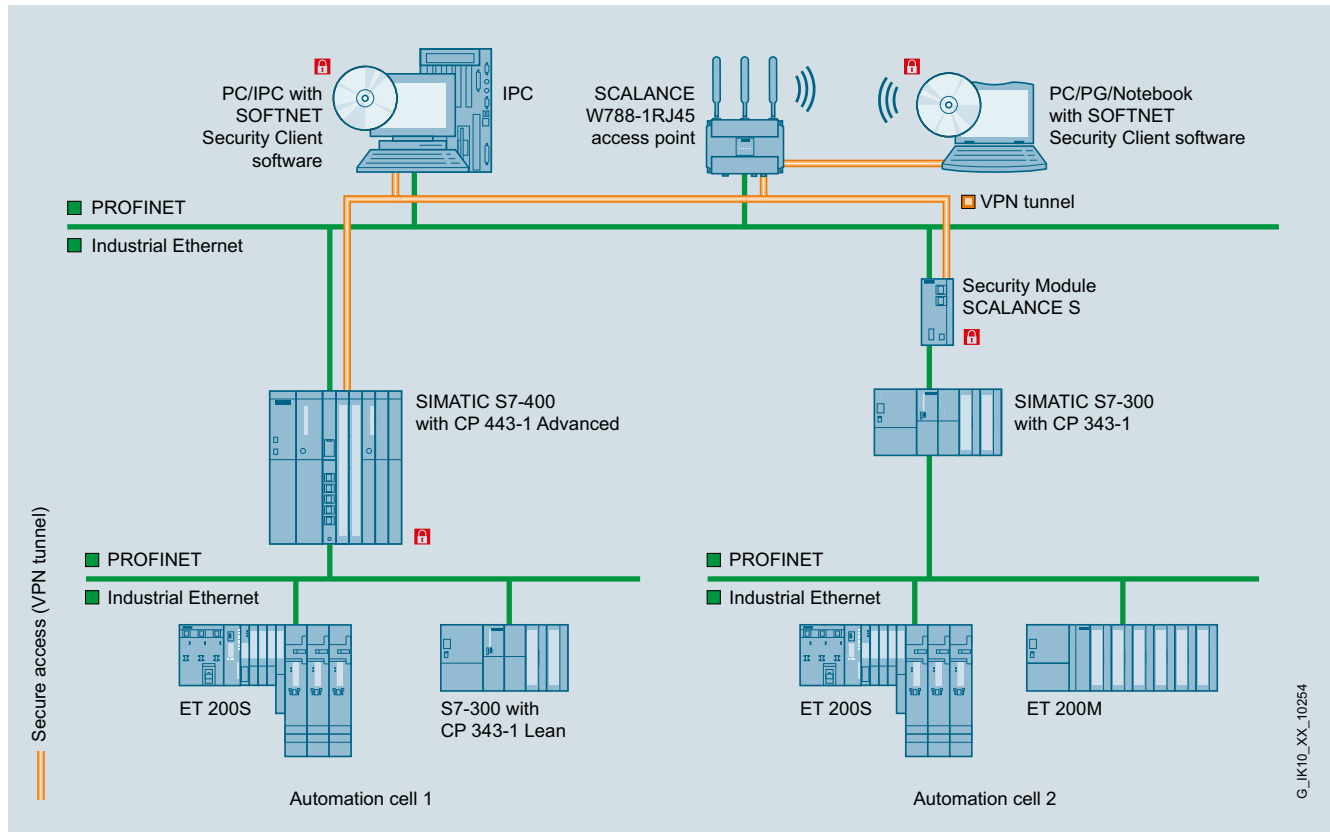
Industrial Security

Security Integrated

SOFTNET Security Client

Overview

- The SOFTNET Security Client is a component of the Industrial Security concept for protecting programmable controllers and for security during data exchange between automation systems.
- It is a VPN client for programming devices, PCs and notebooks in industrial environments and supports secure client access via LAN or even WAN (e.g. for remote maintenance via the Internet) to automation systems protected by Security Integrated devices with VPN functionality.
- Data transmission is protected against operator error, eavesdropping/espionage and manipulation; communication can only take place between authenticated and authorized devices.
- Use of field-proven IPsec mechanisms for setting up and operating VPNs.



Secure access to automation cells protected by Security Integrated devices with VPN functionality with the SOFTNET Security Client

Benefits

- Avoidance of system disruptions through exclusive access to programmable controllers or complete automation cells using approved programming devices or notebooks
- High flexibility when used on mobile PCs as no hardware is required for securing the communication
- Uniform configuration and integrated security concept for automation engineering with SCALANCE S, the security S7-CPs (CP 1243-1, CP 1543-1, CP 343-1 Adv., CP 443-1 Adv.), the PC-CP 1628, the CP 1543-1, the CP 1243-1 and the SOFTNET Security Client without special IT know-how
- Protection of data transmission against espionage and manipulation based on certified standards
- Considerable savings when used as a remote maintenance solution together with SCALANCE S and SCALANCE M compared to expensive service callouts

Application

The security modules of the SCALANCE S family are provided specially for use in automation, yet connect seamlessly with the security structures of the office and IT world. They provide security and meet the specific requirements of automation technology, such as simple upgrades of existing systems, simple installation and minimum downtimes if a fault occurs.

Depending on the particular security needs, various different security measures can be combined. The SOFTNET Security Client allows programming devices, PCs, and notebooks access to devices with IPsec VPN functionality (e.g. SCALANCE S, SCALANCE M, CP 1243-1, CP 1543-1, CP 343-1/CP 443-1 Advanced, CP 1628), protected network stations or automation systems.

get Designed for Industry

Function**Authentication**

Since IP addresses can be falsified (IP spoofing), checking the IP address (of the client access) is not sufficient for reliable authentication. In addition to this, Client PCs may have changing IP addresses. For this reason, the authentication is performed using tried and tested VPN mechanisms.

Data encryption

Secure encryption is necessary to protect data traffic from espionage and manipulation. This means that the data traffic remains incomprehensible to any eavesdropper in the network. To achieve this, the SOFTNET Security Client establishes connections on IPSec based VPN tunnels to other SCALANCE S, SCALANCE M, the S7 Security CPs or the PC-CP 1628.

Performance data

System requirements (please note the descriptions under "Ordering data"):

Windows 7 Professional or Ultimate 32/64-bit
Windows XP Professional (32-bit) + SP3

Configuration

Using the associated configuration tool it is possible to create and manage security rules even without special security knowledge. In the simplest case, only the SCALANCE S modules or SOFTNET Security Clients that will communicate with each other are created and configured. As soon as SOFTNET Security Client knows the programmable controllers to be accessed, communication can be established.

Ordering data**SOFTNET Security Client V4 HF1****6GK1704-1VW04-0AA0**

Software for designing secure IP-based VPN connections from a programming device/PC to network segments which are secured by SCALANCE S, SCALANCE M, CP 1243-1, CP 1543-1, CP 343-1 Advanced, CP 443-1 Advanced, CP 1628, CP 1543-1 or CP 1243-1; single license for 1 installation, runtime software (German/English), configuration tool (German/English), and electronic manual on CD-ROM (German/English/French/Spanish/Italian) for Windows 7 Professional, Ultimate, Windows XP Professional (32 bit) + SP3

SCALANCE S Industrial Security Modules

For protection of programmable controllers and automation networks, and for securing of industrial communication; configuration tool and electronic manual on CD-ROM
German, English, French, Italian, Spanish

SCALANCE S612**6GK5612-0BA10-2AA3**

Up to 128 VPN tunnels
simultaneously

SCALANCE S623**6GK5623-0BA10-2AA3**

up to 128 VPN tunnels
simultaneously;
additional RJ45 DMZ port

SCALANCE S627-2M**6GK5627-2BA10-2AA3**

up to 128 VPN tunnels
simultaneously;
additional RJ45 DMZ port;
two additional slots for one 2-port
media module each

SCALANCE M industrial modems and routers**SCALANCE M874
mobile radio router**

Mobile radio router for wireless IP communication from Industrial Ethernet-based subnets and programmable controllers via UMTS or GSM mobile radio networks; with integrated firewall and VPN with IPsec;
2 x RJ45 ports,
1 x antenna connection
• **SCALANCE M874-3¹⁾**
• **SCALANCE M874-2¹⁾**

**6GK5874-3AA00-2AA2
6GK5874-2AA00-2AA2****SCALANCE M875 UMTS router**

UMTS router for wireless IP communication from Industrial Ethernet-based programmable controllers via UMTS/GSM mobile radio networks;
EGPRS Multislot Class 12;
with integrated firewall and VPN with IPsec;
2 x RJ45 ports,
2 x antenna connections
• **SCALANCE M875¹⁾**
• **SCALANCE M875¹⁾**
for Japan

**6GK5875-0AA10-1AA2
6GK5875-0AA10-1CA2**

Industrial Security

Security Integrated

SOFTNET Security Client

Ordering data

Article No.

Article No.

SCALANCE M industrial modems and routers (continued)

SCALANCE M81x-1 ADSL router

DSL router for wired IP communication from Industrial Ethernet-based subnets and programmable controllers via telephone or DSL networks; with integrated firewall and VPN with IPsec; 1 x or 4 x RJ45 ports for Industrial Ethernet; 1 x RJ45 port for DSL

- **SCALANCE M812-1 (Annex A)** **6GK5812-1AA00-2AA2**
- **SCALANCE M812-1 (Annex B)** **6GK5812-1BA00-2AA2**
- **SCALANCE M816-1 (Annex A)** **6GK5816-1AA00-2AA2**
- **SCALANCE M816-1 (Annex B)** **6GK5816-1BA00-2AA2**

SCALANCE M826-2 SHDSL router

DSL router for wired IP communication from Industrial Ethernet-based subnets and programmable controllers via telephone or DSL networks; with integrated firewall and VPN with IPsec; 1 x or 4 x RJ45 ports for Industrial Ethernet; 1 x RJ45 port for DSL

- **SCALANCE M826-2 (Annex A)** **6GK5826-2AB00-2AB2**

Communications processors for SIMATIC S7

CP 1243-1

communication processor; for connection of SIMATIC S7-1200 to Industrial Ethernet via TCP/IP, ISO and UDP, Telecontrol Server Basic and security functions Stateful Inspection Firewall and VPN; 1 x RJ45 interface with 10/100 Mbit/s

6GK7243-1BX30-0XE0

CP 1543-1

communication processor; for connection of SIMATIC S7-1500 to Industrial Ethernet via TCP/IP, ISO and UDP and security functions Stateful Inspection Firewall and VPN; 1 x RJ45 interface with 10/100/1 000 Mbit/s;

6GK7543-1AX00-0XE0

CP 343-1 Advanced

communications processor;

For connection of SIMATIC S7-300 to Industrial Ethernet over ISO and TCP/IP; PROFINET IO Controller or PROFINET IO Device, MRP, integrated 2-port switch ERTEC; S7 communication, open communication (SEND/RECEIVE), FETCH/WRITE, with and without RFC1006, multicast, DHCP, CPU clock synchronization via SIMATIC procedure and NTP, diagnostics, SNMP, access protection through IP access list, initialization over LAN 10/100 Mbit/s; as well as IT communication (web, e-mail, FTP); PROFINET CBA; security (firewall/VPN); PROFinergy; with electronic manual on DVD

6GK7343-1GX31-0XE0

Communications processors for SIMATIC S7 (continued)

CP 443-1 Advanced communications processor;

For the connection of SIMATIC S7-400 to Industrial Ethernet; PROFINET IO Controller with RT and IRT, MRP, PROFINET CBA, TCP/IP, ISO and UDP; S7 communication, open communication (SEND/RECEIVE) with FETCH/WRITE, with and without RFC1006, diagnostics expansions, multicast, clock synchronization with SIMATIC mode or NTP, access protection by IP access list, FTP client/server, HTTP server, HTML diagnostics, SNMP, DHCP, e-mail, data storage on C-PLUG; PROFINET connector: 4xRJ45 (10/100 Mbit/s) via switch; Gigabit connector: 1xRJ45 (10/100/1 000 Mbit/s); with integrated stateful inspection firewall and VPN appliance

6GK7443-1GX30-0XE0

Communications processors for PG/PC/IPC

CP 1628

communications processor;

PCI Express x1 card for connection to Industrial Ethernet (10/100/1 000 Mbit/s), with 2-port switch (RJ45) and integrated security (firewall, VPN) via HARDNET-IE S7 and S7-REDCONNECT. For operating system support, see SIMATIC NET Software

6GK1162-8AA00

Accessories

IE FC RJ45 Plug 180

RJ45 plug connector for Industrial Ethernet with a rugged metal enclosure and integrated insulation displacement contacts for connecting Industrial Ethernet FC installation cables; with 180° cable outlet; for network components and CPs/CPUs with Industrial Ethernet interface

- 1 pack = 1 unit
- 1 pack = 10 units
- 1 pack = 50 units

6GK1901-1BB10-2AA0
6GK1901-1BB10-2AB0
6GK1901-1BB10-2AE0

ANT794-4MR antenna

Omnidirectional antenna for GSM (2G) and UMTS (3G) networks; weather-resistant for indoor and outdoor use; 5 m cable with fixed connection to antenna; SMA connector; including mounting bracket, screws, wall plugs

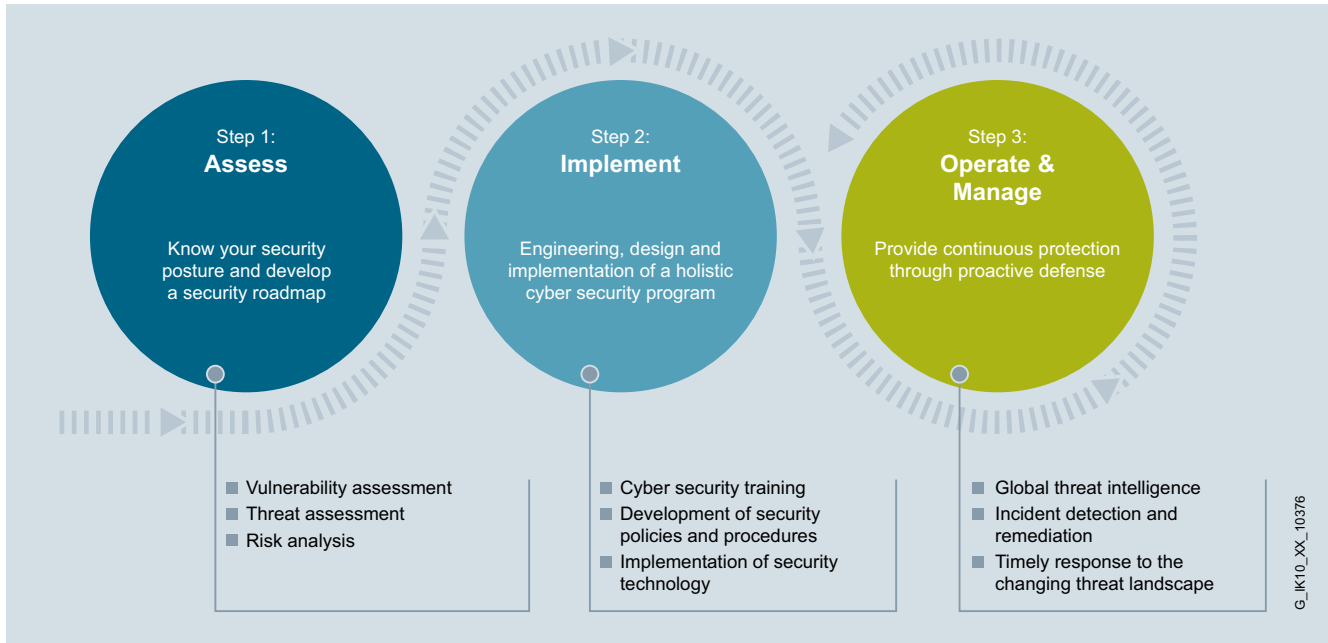
6NH9860-1AA00

Note:

Check the current country list:

<http://support.automation.siemens.com/WW/view/en/66627157>

Overview



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. These developments, however, have also increased the security risk.

Today it is no longer just the office environment that is under threat from viruses, trojans and hackers - 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 "implementation" stage - 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, long-term 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, 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.

Industrial Security

Security Integrated

Industrial Security Services

Benefits

Customer benefits

- 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
- Increasing plant security through tailored 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 the threat
- Keeping the system up to date (pattern, patches, signatures).

Ordering data

Article No.

**Security assessment
for complete plants**

9AS1411-1AA11-1AA1

**Risk and Vulnerability
Assessment**

On request

**Customized analyses, projects
and advice**

On request

More information

Further information can be found at:
www.siemens.com/industrialsecurity