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

Moreover, security is now also regulated by laws addressing critical infrastructures in particular in order to accommodate increased security requirements. Examples include the IT Security Act in Germany, the ANSSI Certification in France and NERC CIP in USA. 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.
Content

INDUSTRIAL SECURITY

Why industrial security is so important 04
Defense in depth 05
Industrial security at a glance 06
Industrial security as part of Totally Integrated Automation 08

NETWORK SECURITY

Cell protection concept 09
SCALANCE S security modules 10
Application examples 12
Secure remote maintenance with SCALANCE S 12
Network access protection with DMZ 13
Secure redundant ring coupling 14
Secure redundant coupling of a ring on plant network 15
SCALANCE M Internet and mobile wireless routers 16
Application examples 18
Secure access to plant sections via mobile wireless networks 18
Secure access to plant sections with SINEMA Remote Connect 19
Security communications processors for SIMATIC S7 20
SIMATIC S7-1200 20
SIMATIC S7-1500 21
SIMATIC S7-300 and S7-400 22
Application example 23
Security communications processors for PCs 24
Application example 25
SIMATIC PCS 7 Security 26

TECHNICAL SPECIFICATIONS

SCALANCE S 28
SCALANCE M 29
CP 1243-1 and CP 1543-1 30
CP 343-1 Advanced and CP 443-1 Advanced 31
CP 1628 and SOFTNET Security Client 32

MORE ON INDUSTRIAL SECURITY

Security with SCALANCE X and SCALANCE W 33
Security with RUGGEDCOM 34
Plant Security Services 36

GLOSSARY

Terms, definitions 38
## Industrial Security

**Why industrial security is so important**

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

**Threat overview**

Source:
Industrial Control System Security: Top 10 Threats and Countermeasures v1.1
Publication date: March 26, 2014

**Note:**
This list of threats was compiled in close cooperation between BSI (German Federal Office for Information Security) and representatives of industry.
Using BSI analyses, the Federal Office for Information Security (BSI) publishes statistics and reports on current topics dealing with cyber-security. Please direct all comments and notes to: cs-info@bsi.bund.de
With defense in depth, Siemens provides a multi-faceted concept that gives your system both all-round and in-depth protection. The concept is based on plant security, network security and system integrity – according to the recommendations of ISA 99 / IEC 62443, the leading standard for security in industrial automation.

**Plant security**
Plant security uses a number of different methods to prevent unauthorized persons from gaining physical access to critical components. This starts with conventional building access and extends to securing sensitive areas by means of key cards. The customized Plant Security Services include consulting services, implementation packages and managed security services for comprehensive, long-term plant protection. Production facilities are at the mercy of constant threats. Infected devices, unauthorized personnel, unauthorized access via networks and the Internet call for measures. A security assessment analyzes and assesses the security status of a plant with respect to technology, network architecture, and personnel. Implementation packages range from support for network planning and installation of attack detection systems to integration of system hardening measures. With continuous updates and comprehensive monitoring, managed security services ensure rapid adjustments to changing threats and transparency of a plant’s security status thanks to worldwide monitoring and real-time warnings.

**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 can be encrypted using VPN and is thus protected from data espionage and manipulation. The communication stations are securely authenticated. Automation networks, automation systems and industrial communication can be made secure with “Security Integrated” components such as SCALANCE S security modules, SCALANCE M Internet and mobile wireless routers and Security CPs for SIMATIC.

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

Plant Security

Network Security

System Integrity

Factory Automation

Secure communication, network access protection and network segmentation with Security Integrated components
Physical protection
Security management
Cyber security operation center

DMZ
- PC with CP 1628
- Server
- Server
- GPRS/UMTS/LTE
- SIMATIC S7-1500 with SCALANCE M874
- SIMATIC S7-1200 with CP 1243-7
- SIMATIC Field PG with SOFTNET Security Client
- Internet Router
- SCALANCE M812-1
- SCALANCE S623

Production 2
- SIMATIC S7-1200 with CP 1243-1
- PROFINET
- ET 200
- SIMATIC TP700
- SIMATIC S7-1200

Production 3
- SIMATIC S7-300 with CP 343-1 Advanced
- PROFINET
- SIMOTION D4x5 with SINAMICS S120 (Booksize)

Production 4
- SCALANCE S615
- Cell 1
- Cell 2
- Cell 3

Production n
- SIMATIC S7-1200 with CP 1243-7
- SCALANCE S615
- Cell 1
- Cell 2
- Cell 3

© Siemens AG 2015
Industrial security products as part of Totally Integrated Automation

<table>
<thead>
<tr>
<th>SCALANCE S</th>
<th>SCALANCE M</th>
<th>CP 343-1 Adv</th>
<th>CP 443-1 Adv</th>
<th>S7-1200 CPU</th>
<th>S7-1500 CPU</th>
<th>CP 1243-1</th>
<th>CP 1243-7 LTE</th>
<th>CP 1543-1</th>
<th>CP 1628</th>
<th>SOFTNET Security Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

- Configurable copy protection
- Access protection (authentication)
- Enhanced access protection (firewall)
- Virtual Private Network with IPsec
- Manipulation protection (communication, configuration)

* Applies 1) as of CPU Firmware V4.0 and STEP 7 Professional V13 (TIA Portal)

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

Totally Integrated Automation: Efficient interaction between all automation components

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

Cell protection concept

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

For realization of the cell protection concept, Siemens partners with its customers to provide them Security Integrated components, which not only have integrated communication functions but also special security functions such as firewall and VPN functionality.

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 implementation.
SCALANCE S security 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 protect the data transmission between devices or network segments (such as automation cells) against data manipulation and espionage by setting up VPN tunnels and can also be used for secure remote access over the Internet. The SCALANCE S security modules can be operated in bridge mode, i.e. within an IP subnet, or in router mode, i.e. at the IP subnet boundaries. SCALANCE S is optimized for use in automation and industrial environments and meets the special requirements of automation systems, such as easy upgrades of existing systems, simple installation and minimal downtimes in the event of a fault.

Product variants

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, including changeable, devices through dynamic adoption of 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 S615
- Uses a firewall and Virtual Private Network VPN to protect data traffic against unauthorized access (IPsec and OpenVPN for connection to SINEMA Remote Connect)
- Up to five variable security zones per port-based VLAN (Virtual Local Area Network) allow configuration of security zones and any firewall rules between security zones
- A variety of configuration, management and diagnostic capabilities with WBM (Web-based Management), CLI (Command Line Interface) and SNMP (Simple Network Management Protocol)
- Digital input (DI) for connection of a key-operated switch for controlled setup of a tunnel connection
- Autoconfiguration interface for easy configuration of a connection to SINEMA Remote Connect
- Connection via 10/100 Mbit/s ports

You will find more information on security modules at: siemens.com/scalance-s
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. This 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, stand-by mode of the redundant device and status matching via 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. This 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, stand-by mode of the redundant device and status synchronization via the yellow ports
- Two additional slots for 2-port media modules (same as for 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 lengths or use of existing 2-wire cables (e.g. PROFIBUS) through the use of MM992-2VD media modules (variable distance)
Task
A system integrator requires secure Internet access to their machine, or part of an end user’s plant, for servicing purposes. But the integrator is to be given access only to specific devices and not the plant network. In addition, a secured connection is to be set up from the system to a remote station using mobile networks (e.g. UMTS or LTE).

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

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

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

Solution
The DMZ port of a SCALANCE S623 is the single locally accessible port. The security module is connected to the plant network (red port) and a lower-level automation cell (green port). User-specific firewalls are created for each user. To receive access to the network, the user must be logged in to the SCALANCE S with user name and password.

Advantages at a glance
- Securing of local network access
- Flexible and user-specific access rights
- Central authentication possible with RADIUS
Application examples

Secure redundant ring coupling

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 to the ports of the second media module (green ports) using SCALANCE S627-2M. SCALANCE S627-2M functions as a router and firewall. A second SCALANCE S627-2M is similarly connected and operates in stand-by mode. The coupling for synchronization of the firewall status between the two SCALANCE S modules is by means of the yellow ports, which are connected with a synchronization cable.

Note
As an alternative to MRP, Ring A or Ring B can be an HRP ring.

Advantages at a glance

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

Task
1. A ring is to be securely and redundantly connected to the plant network or
2. Lower-level cell is to be similarly connected to the ring.

Solution
1. The ring is connected to the ports of the second media module (green ports) and the production network to the ports of the first media module (red ports) using SCALANCE S627-2M.
2. For the connection of lower-level cells to the ring, the ring is connected to the ports of the first media module (red ports) and the lower-level cell to the ports of the second media module (green ports).

A second SCALANCE S627-2M is similarly connected in each case 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.

Note
As an alternative to MRP, Ring A or Ring B can be an HRP ring.

Advantages at a glance
- Secure redundant connection of an MRP ring to the plant network or secure redundant connection of an automation cell to a higher-level ring
- Control of the data communication between an MRP ring and a lower-level automation cell
- High availability due to redundant design of the SCALANCE S627-2M
SCALANCE M Internet and mobile wireless routers

SCALANCE M874-3 and SCALANCE M874-2 are mobile wireless routers for cost-effective and secure connection of Ethernet-based subnets and automation devices via mobile networks of the 3rd generation (UMTS) or 2nd generation (GSM). The integrated firewall and VPN (OpenVPN and IPsec) security functions protect against unauthorized access and secure the data transmission.

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

SCALANCE M874-3
The SCALANCE M874-3 supports HSPA+ (High Speed Packet Access) and therefore enables high transmission rates of up to 14.4 Mbit/s in the downlink and up to 5.76 Mbit/s in the uplink (depending on the infrastructure of the mobile wireless provider).

SCALANCE M876-3 and SCALANCE M876-4 are mobile wireless routers for cost-effective and secure connection of Ethernet-based subnets and automation devices via mobile networks of the 4th generation (LTE), 3rd generation (UMTS) or 2nd generation (GSM).

The integrated firewall and VPN (IPsec) security functions protect against unauthorized access and secure the data transmission.

SCALANCE M876-3
The SCALANCE M876-3 supports dual-band CDMA2000 and HSPA+ (High Speed Packet Access). Thus, it enables high transmission rates of up to 14.4 Mbit/s in the downlink and up to 5.76 Mbit/s in the uplink (depending on the infrastructure of the mobile wireless provider).

SCALANCE M876-4
The SCALANCE M876-4 supports EDGE (Enhanced Data Rates for GSM Evolution) and LTE (Long Term Evolution). Thus, the device enables allows high transmission rates of up to 100 Mbit/s in the downlink and up to 50 Mbit/s in the uplink (depending on the infrastructure of the mobile wireless provider).
SCALANCE M812-1 and SCALANCE M816-1
SCALANCE M812-1 and SCALANCE M816-1 are DSL routers for cost-effective and secure connection of Ethernet-based subnets and automation devices to wired telephone or DSL networks that support ASDL2+ (Asynchronous Digital Subscriber Line). Thus, the devices enable high transmission rates of up to 25 Mbit/s in the downlink and up to 3.5 Mbit/s in the uplink.

Secure access and communication is achieved through the security functions of the integrated firewall and through VPN tunnels.

SCALANCE M826-2
The SCALANCE M826-2 is an SHDSL modem for cost-effective and secure connection of Ethernet-based subnets and automation devices via existing two-wire or stranded cables and supports the ITU-T standard G.991.2 and SHDSL.biz (single-pair high-speed digital subscriber line). Thus, the device enables high symmetrical transmission rates of up to 15.3 Mbit/s per wire pair.

Secure access and communication is achieved through the security functions of the integrated firewall and through VPN tunnels.
VPN for secure remote maintenance with SCALANCE M874

**Task**
Typical 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 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 the existing UMTS and LTE infrastructure of the mobile wireless provider
- Simple planning and commissioning of telecontrol substations without the need for special radio expertise
- Worldwide availability thanks to UMTS/GSM (quad band) technology; note country-specific approvals

---

**Application examples**
Secure access to plant sections via mobile wireless networks
Secure access to plant sections with SINEMA Remote Connect

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

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

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

**Advantages at a glance**
- High transparency and security
- Error prevention through explicit assignment of know-how owners to the respective plant sections
- Transparent IP communication
- Logging of accesses

Secure connection of SIMATIC RTU3030C via OpenVPN with SINEMA RC
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 CP 1243-1
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 secure communication possibilities: File transfer and e-mail
- Can be used in an IPv6-based infrastructure

Segmentation of networks and protection of the S7-1500 with CP 1543-1
Security communications processors for SIMATIC S7-300 and S7-400

Alongside the familiar communication functions, an integrated switch, and Layer 3 routing functionality, the Industrial Ethernet communications processors CP 343-1 Advanced and CP 443-1 Advanced for SIMATIC S7-300 and S7-400 contain Security Integrated, i.e. a Stateful Inspection Firewall and a VPN gateway for protection of the controller and lower-level devices against security risks.
**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: The latest generation of Advanced CPs comes with integrated firewall and VPN security functions for implementing a protected automation cell and for protecting data transmission – and for the same price as the predecessor version.
- Secure communication integration: The CPs are easily configured with STEP 7; VPN tunnels can be set up among the CPs or to the SCALANCE S security appliance, the SOFTNET Security Client VPN software, the secure CP 1628 PC module and the SCALANCE M Internet and mobile wireless routers.

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 communications processor
CP 1628 for PCs

CP 1628
The CP 1628 Industrial Ethernet communications processor protects Industrial PCs through a 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 a 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 has Security Integrated, i.e. a Stateful Inspection Firewall and a VPN gateway for protection of the PG/PC system against security risks.
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.

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 with STEP 7/NCM PC (V5.5 SP3 or higher) or with STEP 7 (TIA Portal) V12 SP1 or higher.
SIMATIC PCS 7 Security

Network Security

PCS 7 plant

SIMATIC IT Server

Office

DMZ network

- CAS Web Client
- Data Monitor
- ERP
- Domain Controller
- Automation Firewall 1000
- Automation Firewall 200
- SCALANCE S

Production network 1

- OS Client
- Engineering Station
- Domain Controller
- Plant bus
- S7-300 with CP 343-1 Advanced
- S7-400 with CP 443-1 Advanced

Production network 2

- OS Client
- Plant bus
- SCALANCE S

Production network 3

- Terminal bus
- Plant bus
- SCALANCE S

Internet

Ethernet, Office LAN

© Siemens AG 2015
The PCS 7 Security concept follows the defense-in-depth strategy. That is, multiple protection levels are created in order to minimize risks and to increase the security of plants with the following functions:

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

Elements of the PCS 7 Security concept

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

### SCALANCE S security modules

<table>
<thead>
<tr>
<th>Product type designation</th>
<th>SCALANCE S602</th>
<th>SCALANCE S612</th>
<th>SCALANCE S615</th>
<th>SCALANCE S623</th>
<th>SCALANCE S627-2M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article No.</td>
<td>6GK5602-0BA10-2AA3</td>
<td>6GK5612-0BA10-2AA3</td>
<td>6GK5615-0AA00-2AA2</td>
<td>6GK5623-0BA10-2AA3</td>
<td>6GK5627-2BA10-2AA3</td>
</tr>
<tr>
<td><strong>Transmission rate</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transmission rate</td>
<td>10 / 100 / 1000 Mbit/s</td>
<td>10 / 100 / 1000 Mbit/s</td>
<td>10 / 100 Mbit/s</td>
<td>10 / 100 / 1000 Mbit/s</td>
<td>10 / 100 / 1000 Mbit/s</td>
</tr>
<tr>
<td><strong>Interfaces</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>for internal network</td>
<td>1x RJ45 port</td>
<td>1x RJ45 port</td>
<td>1 ... 4 x RJ45 port</td>
<td>1x RJ45 port</td>
<td>3x RJ45 port+media module</td>
</tr>
<tr>
<td>for external network</td>
<td>1x RJ45 port</td>
<td>1x RJ45 port</td>
<td>1 ... 4 x RJ45 port</td>
<td>1x RJ45 port</td>
<td>3x RJ45 port+media module</td>
</tr>
<tr>
<td>for DMZ</td>
<td>–</td>
<td>–</td>
<td>1 ... 4 x RJ45 port</td>
<td>1x RJ45 port</td>
<td>1x RJ45 port</td>
</tr>
<tr>
<td>for signaling contact</td>
<td>1x 2-pin terminal block</td>
<td>1x 2-pin terminal block</td>
<td>–</td>
<td>1x 2-pin terminal block</td>
<td>1x 2-pin terminal block</td>
</tr>
<tr>
<td>for power supply</td>
<td>1x 4-pin terminal block</td>
<td>1x 4-pin terminal block</td>
<td>1x 5-pin terminal block</td>
<td>1x 4-pin terminal block</td>
<td>1x 4-pin terminal block</td>
</tr>
<tr>
<td>C-PLUG swap media</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Supply voltage, current consumption, power loss</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply voltage, external</td>
<td>24 V DC</td>
<td>24 V DC</td>
<td>24 V DC</td>
<td>24 V DC</td>
<td>24 V DC</td>
</tr>
<tr>
<td>Range</td>
<td>19.2 V ... 28.8 V DC</td>
<td>19.2 V ... 28.8 V DC</td>
<td>10.8 V ... 28.2 V DC</td>
<td>19.2 V ... 28.8 V DC</td>
<td>19.2 V ... 28.8 V DC</td>
</tr>
<tr>
<td><strong>Permissible ambient conditions</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ambient temperature</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>during operation</td>
<td>-40 °C ... +60 °C</td>
<td>-40 °C ... +60 °C</td>
<td>-40 °C ... +70 °C</td>
<td>-40 °C ... +60 °C</td>
<td>-40 °C ... +60 °C</td>
</tr>
<tr>
<td>during storage</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +70 °C</td>
</tr>
<tr>
<td>during transportation</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +80 °C</td>
<td>-40 °C ... +70 °C</td>
</tr>
<tr>
<td>Degree of protection</td>
<td>IP20</td>
<td>IP20</td>
<td>IP20</td>
<td>IP20</td>
<td>IP20</td>
</tr>
<tr>
<td><strong>Design, dimensions and weight</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design</td>
<td>Compact</td>
<td>Compact</td>
<td>Compact</td>
<td>Compact</td>
<td>Compact</td>
</tr>
<tr>
<td>Width / height / depth</td>
<td>60 mm / 125 mm / 124 mm</td>
<td>60 mm / 125 mm / 124 mm</td>
<td>35 mm / 147 mm / 127 mm</td>
<td>60 mm / 125 mm / 124 mm</td>
<td>120 mm / 125 mm / 124 mm</td>
</tr>
<tr>
<td>Net weight</td>
<td>0.8 kg</td>
<td>0.8 kg</td>
<td>0.4 kg</td>
<td>0.81 kg</td>
<td>1.3 kg</td>
</tr>
<tr>
<td><strong>Product function: Security</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall configuration</td>
<td>Stateful Inspection</td>
<td>Stateful Inspection</td>
<td>Stateful Inspection</td>
<td>Stateful Inspection</td>
<td>Stateful Inspection</td>
</tr>
<tr>
<td>Password protection</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Product function with VPN connection</td>
<td>–</td>
<td>IPsec</td>
<td>IPsec, OpenVPN (as Client for SINEMA RC)</td>
<td>IPsec</td>
<td>IPsec</td>
</tr>
<tr>
<td>Number of possible connections with VPN connection</td>
<td>128</td>
<td>128</td>
<td>20</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Restricted bandwidth</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NAT/NAPT</td>
<td>Yes</td>
<td>Yes</td>
<td>–</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication procedure</td>
<td>–</td>
<td>Preshared Key, X.509v3 certificates</td>
<td>Preshared Key, X.509v3 certificates</td>
<td>Preshared Key, X.509v3 certificates</td>
<td>Preshared Key, X.509v3 certificates</td>
</tr>
<tr>
<td>Hashing algorithms</td>
<td>–</td>
<td>MD5, SHA-1</td>
<td>MD5, SHA-1</td>
<td>MD5, SHA-1</td>
<td>MD5, SHA-1</td>
</tr>
</tbody>
</table>
# SCALANCE M Internet and mobile wireless routers

<table>
<thead>
<tr>
<th>Product type designation</th>
<th>SCALANCE M wireless</th>
<th>SCALANCE M wired</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article No.</td>
<td>6GK5874-2AA00-2AA2</td>
<td>6GK5812-1BA00-2AA2</td>
</tr>
<tr>
<td></td>
<td>6GK5874-3AA00-2AA2</td>
<td>6GK5816-1BA00-2AA2</td>
</tr>
<tr>
<td></td>
<td>6GK5876-3AA00-2BA2</td>
<td>6GK5826-2AB00-2AB2</td>
</tr>
</tbody>
</table>

| Transmission rate         | 1 with Industrial Ethernet / 2 with Industrial Ethernet |
|                         | GPRS transmission uplink / downlink, max. |
|                         | eGPRS transmission uplink / downlink, max. |
|                         | UMTS transmission uplink / downlink, max. |
|                         | EV-DO transmission forward link / reverse link |
|                         | LTE transmission uplink / downlink, max. |
|                         | ADSL2+ transmission uplink / downlink, max. |
|                         | SHDSL transmission, max |
|                         | 10 Mbit/s / 100 Mbit/s |
|                         | 85.6 kbit/s / 85.6 kbit/s |
|                         | 236.8 kbit/s / 236.8 kbit/s |
|                         | 5.76 Mbit/s / 14.4 Mbit/s |
|                         | 3.1 Mbit/s / 1.8 Mbit/s (M874-3 and M876-3 only) |
|                         | 50 Mbit/s / 100 Mbit/s (M876-4 only) |

<table>
<thead>
<tr>
<th>Interfaces</th>
<th>Electrical connection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>for internal network</td>
</tr>
<tr>
<td></td>
<td>RJ45 port (10/100 Mbit/s, TP, autocrossover)</td>
</tr>
<tr>
<td></td>
<td>for external network</td>
</tr>
<tr>
<td></td>
<td>SMA antenna sockets (50 ohms)</td>
</tr>
<tr>
<td></td>
<td>for power supply</td>
</tr>
<tr>
<td></td>
<td>Terminal strip</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supply voltage, current consumption, power loss</th>
<th>Supply voltage / range</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10.8 V ... 28.8 V</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Permissible ambient conditions</th>
<th>Ambient temperature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>during operation</td>
</tr>
<tr>
<td></td>
<td>-20 °C ... +60 °C</td>
</tr>
<tr>
<td></td>
<td>during storage</td>
</tr>
<tr>
<td></td>
<td>-40 °C ... +85 °C</td>
</tr>
<tr>
<td></td>
<td>Degree of protection</td>
</tr>
<tr>
<td></td>
<td>IP20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Design, dimensions and weight</th>
<th>Width / height / depth</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>35 mm / 147 mm / 127 mm</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Product function: Security</th>
<th>Stateful Inspection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall configuration</td>
<td>Yes</td>
</tr>
<tr>
<td>Password protection</td>
<td>Yes</td>
</tr>
<tr>
<td>Packet filter</td>
<td>Yes</td>
</tr>
<tr>
<td>Product function with VPN connection</td>
<td>IPsec</td>
</tr>
<tr>
<td>Number of possible connections with VPN connection</td>
<td>20</td>
</tr>
<tr>
<td>Type of authentication with VPN PSK</td>
<td>Yes</td>
</tr>
<tr>
<td>Key length</td>
<td>56 bit</td>
</tr>
<tr>
<td>with IPsec DES for VPN</td>
<td>128 bit</td>
</tr>
<tr>
<td>1 with IPsec AES for VPN</td>
<td>192 bit</td>
</tr>
<tr>
<td>2 with IPsec AES for VPN</td>
<td>256 bit</td>
</tr>
<tr>
<td>3 with IPsec AES with VPN</td>
<td>168 bit</td>
</tr>
<tr>
<td>with IPsec 3DES / with Virtual Private Network</td>
<td></td>
</tr>
<tr>
<td>Type of Internet key exchange with VPN main mode</td>
<td>Yes</td>
</tr>
<tr>
<td>Type of Internet key exchange with VPN quick mode</td>
<td>Yes</td>
</tr>
<tr>
<td>Type of packet authentication with VPN</td>
<td>MD5, SHA-1</td>
</tr>
</tbody>
</table>
## TECHNICAL SPECIFICATIONS

### CP 1243-1 and CP 1543-1 communications processors

<table>
<thead>
<tr>
<th>Product type</th>
<th>Designation</th>
<th>CP 1243-1</th>
<th>CP 1543-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article No.</td>
<td>6GK7243-1BX30-0XE0</td>
<td>6GK7543-1AX00-0XE0</td>
<td></td>
</tr>
</tbody>
</table>

### Transmission rate

| at interface 1 / 2 | 10/100 Mbit/s / – | 10/100/1 000 Mbit/s / – |

### Interfaces

#### Electrical connection

| to interface 1 according to IE | 1x RJ45 port | 1x 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 with VPN connection | IPsec | IPsec |
| Type of encryption algorithms with VPN connection | AES-256, AES-192, AES-128, 3DES-168 | AES-256, AES-192, AES-128, 3DES-168, DES-56 |
| 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 with 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 services that are not needed | Yes | Yes |
| Blocking of communication via physical ports | No | No |
| Log file for unauthorized access | No | Yes |
### CP 343-1 Advanced and CP 443-1 Advanced communications processors

<table>
<thead>
<tr>
<th>Product type designation</th>
<th>CP 343-1 Advanced</th>
<th>CP 443-1 Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article No.</td>
<td>6GK7343-1GX31-0XE0</td>
<td>6GK7443-1GX30-0XE0</td>
</tr>
<tr>
<td>Transmission rate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>at interface 1 / 2</td>
<td>10 / 1000 Mbit/s</td>
<td>10 / 1000 Mbit/s</td>
</tr>
<tr>
<td>Interfaces</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electrical connection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>to interface 1 according to IE</td>
<td>1x RJ45 port</td>
<td>1x RJ45 port</td>
</tr>
<tr>
<td>to interface 2 according to IE</td>
<td>2x RJ45 ports</td>
<td>4x RJ45 ports</td>
</tr>
<tr>
<td>for power supply</td>
<td>2-pin plug-in terminal strip</td>
<td>–</td>
</tr>
<tr>
<td>C-PLUG swap media</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supply voltage, current consumption, power loss</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply voltage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 from backplane bus</td>
<td>5 V DC</td>
<td>5 V DC</td>
</tr>
<tr>
<td>External</td>
<td>24 V DC</td>
<td>–</td>
</tr>
<tr>
<td>Permissible ambient conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ambient temperature</td>
<td></td>
<td></td>
</tr>
<tr>
<td>during operation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- when installed vertically</td>
<td>0 °C ... +40 °C</td>
<td>–</td>
</tr>
<tr>
<td>- when installed horizontally</td>
<td>0 °C ... +60 °C</td>
<td>–</td>
</tr>
<tr>
<td>during storage</td>
<td>-40 °C ... +70 °C</td>
<td>-40 °C ... +70 °C</td>
</tr>
<tr>
<td>during transportation</td>
<td>-40 °C ... +70 °C</td>
<td>-40 °C ... +70 °C</td>
</tr>
<tr>
<td>Degree of protection</td>
<td>IP20</td>
<td>IP20</td>
</tr>
<tr>
<td>Design, dimensions and weight</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Module format</td>
<td>Compact</td>
<td>Compact S7-400, single width</td>
</tr>
<tr>
<td>Width / height / depth</td>
<td>80 mm / 125 mm / 120 mm</td>
<td>25 mm / 290 mm / 210 mm</td>
</tr>
<tr>
<td>Net weight</td>
<td>0.8 kg</td>
<td>0.7 kg</td>
</tr>
<tr>
<td>Product function: Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firewall configuration</td>
<td>Stateful Inspection</td>
<td>Stateful Inspection</td>
</tr>
<tr>
<td>Product function with VPN connection</td>
<td>IPsec</td>
<td>IPsec</td>
</tr>
<tr>
<td>Type of encryption algorithms with VPN connection</td>
<td>AES-256, AES-192, AES-128, 3DES-168 DES-56</td>
<td>AES-256, AES-192, AES-128, 3DES-168 DES-56</td>
</tr>
<tr>
<td>Type of authentication procedure with VPN connection</td>
<td>Preshared key (PSK), X.509v3 certificates</td>
<td>Preshared key (PSK), X.509v3 certificates</td>
</tr>
<tr>
<td>Type of hashing algorithms with VPN connection</td>
<td>MD5, SHA-1</td>
<td>MD5, SHA-1</td>
</tr>
<tr>
<td>Number of possible connections with VPN connection</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>Password protection for Web applications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ACL – IP-based</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ACL – IP-based for PLCrouting</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Deactivation of services that are not needed</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocking of communication via physical ports</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Log file for unauthorized access</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
# CP 1628 communications processor and SOFTNET Security Client

<table>
<thead>
<tr>
<th><strong>Product type designation</strong></th>
<th>CP 1628</th>
<th>SOFTNET Security Client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Article No.</strong></td>
<td>6GK1162-8AA00</td>
<td>6GK1704-1VW04-0AA0</td>
</tr>
</tbody>
</table>

## Transmission rate
- at interface 1 / 2: 10/1 000 Mbit/s / – dependent on the PC system

## Interfaces
- **Electrical connection**
  - to interface 1 according to IE: 2x RJ45 port
  - of the backplane bus: PCI Express x1
  - for power supply: 1x 2-pin terminal block

## Supply voltage, current consumption, power loss
- **Type of power supply voltage**: DC
- **Optional external supply**: Yes
- **Supply voltage**:
  - 1 from backplane bus: 3.3 V
  - 2 from backplane bus: 12 V
- **External Range**:
  - 24 V
  - 10.5 V ... 32 V

## Permissible ambient conditions
- **Ambient temperature**:
  - during operation: +5 °C ... +55 °C
  - during storage: -20 °C ... +60 °C
  - during transportation: -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 with VPN connection**: IPsec
- **Type of encryption algorithms with VPN connection**: AES-256, AES-192, AES-128, 3DES-168 DES-56
- **Type of authentication procedure with VPN connection**: Preshared key (PSK), X.509v3 certificates
- **Type of hashing algorithms with VPN connection**: MD5, SHA-1
- **Number of possible connections with VPN connection**: 64

- Unlimited or dependent on the computer configuration
Industrial Security
Security with SCALANCE X and SCALANCE W

SCALANCE X
The managed switches of the SCALANCE X product range are very well suited for the setup of line, star, and ring topologies. They offer high-speed redundancy in the ring for electrical or optical lines.

SCALANCE X-200, X-300, X-400 and X-500 can control network access and have the following security functions:
- ACL port/MAC and IP-based
- IEEE 802.1X (RADIUS)
- 802.1Q-VLAN – enables logical separation of the data traffic between pre-defined ports on the switches
- Broadcast/Multicast/Unicast Limiter
- Broadcast blocking

In addition, the following secure protocols are supported, each of which replaces the weak predecessor protocol:
- SSH (instead of Telnet)
- HTTPS (instead of HTTP)
- SNMP v3 (instead of SNMP v1/v2)

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

SCALANCE W access points and client modules have the following security functions:
- Management security with IP based ACL
- IEEE 802.1X (RADIUS)
- Access protection according to IEEE 802.11i
- WPA2(RADIUS)/WPA2-PSK with AES

In addition, the following secure protocols are supported:
- SSH
- HTTPS
- SNMP v3

Inter AP Blocking
Available in firmware version 4.x and higher. This increases the security in a network environment with multiple SCALANCE W access points. WLAN clients that are connected via a layer 2 network (switches) using different access points can communicate directly with one other. This could pose a security risk depending on the application. "Inter AP Blocking" is used to specify those communication partners or gateways that WLAN clients are permitted to communicate with, thereby minimizing the security risk. Communication with other devices in the network is prevented using KEY-PLUG W700 Security (6GK5907-0PA00). It can be used with all SCALANCE W access points with a KEY-PLUG slot.
Security with RUGGEDCOM

Security

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

- VPN (IPsec) – the integrated hardware encryption engine enables powerful IPsec data communication without use of the main processor
- Passwords – satisfy the NERC guidelines including the option for RADIUS-based authentication
- SSH / SSL – enhanced password protection with the option of encrypting passwords and data for transmission within the network
- Unblocking/blocking of ports – Ability to block ports so that unauthorized devices cannot establish a connection to unused ports
- 802.1Q-VLAN – enables logical separation of the data traffic between pre-defined ports on the switches

- SNMPv3 – encrypted authentication and access protection
- HTTPS – for secure access to the web interface
- 802.1X – ensures that only permissible field devices can be connected to the device
- MAC address list – access control for devices that do not support RADIUS

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

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

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

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

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

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

Today it is no longer just the office environment that is under threat from viruses, hacker attacks, etc. - production plants are also at risk of malfunctions, manipulation of data integrity and loss of know-how. 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 safeguarding of a plant against failure in the event of attacks, a multi-level service concept for industrial security (Assess, Implement and Manage) is available from Siemens.

In the first step "Assess", the existing plant is analyzed to start. 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 actions based on the results for improving the level of security.

In the second step "Implement", the measures defined in the assessment are implemented. These can be divided into three blocks:

- **Training**
  Personnel are given specific training so that they understand what IT and infrastructure security means in the industrial environment and know how they can contributed to a higher level of security.

- **Process improvement**
  Security-relevant regulations and guidelines relating to the existing plant requirements are drawn up and implemented, and compliance with them is monitored.

- **Security technologies**
  Protective measures are implemented for hardware and software, as well as in the plant network. Also included here is long-term protection through monitoring with the help of a Cyber Security Operation Center (CSOC).

The measures defined and implemented in the first two steps are continuously managed in the third step "Manage". Additional measures are added based on monitoring of the security status. This is carried out with the support of a Cyber Security Operation Center (CSOC), which analyzes the security-relevant data of a plant 24/7 and is activated under alarm conditions. This activity also includes periodic review of the level of security including optimized measures for the changing threat landscape. When changes are made to the plant network, software landscape, or management of access rights for users and administrators, it is also ensured that the relevant data remains inside the system, thereby reducing possible attack points. The "Implement" and "Manage" steps are customized to the specific requirements in each case.
Competency
- Access to leading experts in automation engineering and IT security
- Global Cyber Security Operation Center (CSOC)
- Proven holistic approach with state-of-the-art technologies

Engineering
- Simple modular portfolio including consultation, implementation and managed services
- Fast implementation
- Plant-specific custom-fit engineering
- Optimized for your requirements and your budget

Service
- Plant Security Services is a managed service
- Determination of the security level and, based on this, drawing up a plan of action for reducing the risks
- Concentration on your core business

Operation & Management
- Continuous monitoring of the security status of the plant
- Continuous protection of your investments
- Continuous adjustment to the threat situation
- Early detection and advice on eliminating security risks
Terms, definitions

Global Cyber Security Operation Center (CSOC)
Plant Security Services obviously face special requirements in the sensitive field of cyber security. The CSOCs specifically responsible for industrial security bundle the competencies and expertise of international threat intelligence and make this available to customers. As the first point of contact for customers, CSOCs provide support on all security-relevant matters.

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.

Firewall
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.

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

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

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

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

Virtual Private Network (VPN)
A "VPN tunnel" connects two or more network 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 LAN (VLAN)
VLANs (IEEE 802.1Q) enable logical separation of the data traffic between pre-defined ports on the switches. The result is several “virtual networks” on the same physical network. Data communication takes place only within a VLAN.

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

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