SIEMENS


Industrial Security

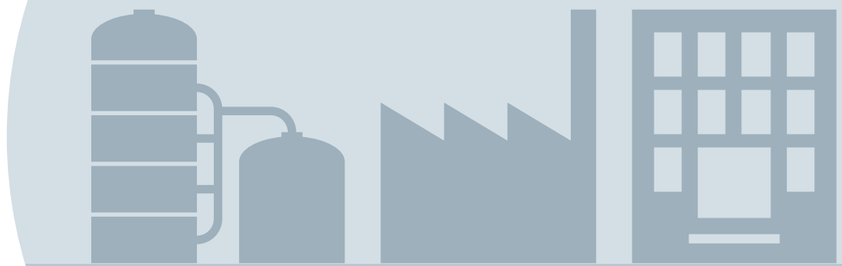
# Network Security

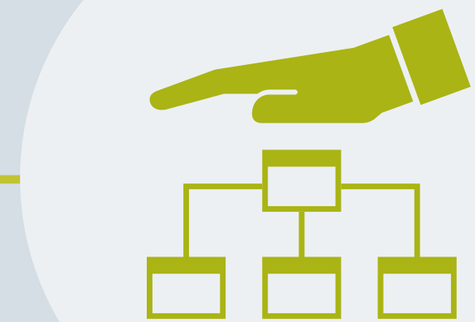
Brochure

Edition 11/2020

siemens.com/network-security

© Siemens 2020





**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 therefore 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.**

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

The topic of cybersecurity is also becoming increasingly important due to the constantly growing number of convergent networks in companies and the increased frequency of cyberattacks and has long been the focus of standardization efforts by international committees such as the International Electrotechnical Commission (IEC). Moreover, security is also regulated at the national level by laws and regulations addressing critical infrastructures in particular in order to accommodate increased security requirements. Examples include the IT Security Act in Germany, the ANSSI Certification in France, NERC CIP in the USA and many more. Thanks to these standards and regulations, it is now possible to take advantage of the tremendous opportunities offered by open communication and the increased networking of production systems while also appropriately addressing the accompanying high risks. Siemens supports you here in adequately protecting your industrial plant from cyberattacks – as part of an integrated portfolio for industrial security.



# Contents

# Industrial Security

## A look at the threat situation

| No. | Threat | Explanation |
|---|---|---|
| 1 | Introduction of malicious code via removable media and external hardware | The use of removable media and mobile IT components by external personnel always entails a major risk of malware infections. However, personnel are often unaware of the effects of malware. |
| 2 | Malware infection via Internet or intranet | Standard components used in company networks (e.g., operating systems, databases, browsers and email clients) usually contain vulnerabilities which an attacker can exploit to infiltrate the company network. From the infiltrated intranet or office network, the attacker can often proceed into the production network, either directly or with a follow-up attack. |
| 3 | Human error and sabotage | Deliberate actions – regardless of whether by internal or external offenders – are a massive threat to all security goals. Security can never be guaranteed through technical measures alone; organizational rules must always be established and followed. |
| 4 | Compromising of extranet and cloud components | Outsourcing of IT components to cloud solutions in some cases leads to system owners having only very limited control over the security of these components and the possibility of their being compromised. However, the components themselves may be connected directly to the local production. |
| 5 | Social engineering and phishing | Social engineering is a method of gaining unauthorized access to information or IT systems through mostly non-technical actions and through exploitation of human traits, such as curiosity, helpfulness, trust, fear or respect for authority. Fraudulent emails – so-called phishing emails – which induce recipients into opening manipulated links or attachments with malware represent a classic example of this. |
| 6 | (D)DoS attacks | (Distributed) denial of service attacks can be used to disrupt both wired and wireless network connections as well as required system resources and cause systems to crash, e.g., to disrupt the functionality of an ICS. |
| 7 | Control components connected to the Internet (ICS) | Despite manufacturer recommendations, ICS components are often connected directly to the Internet without having an adequate level of security and security mechanisms. |
| 8 | Intrusion via remote maintenance access | External access to ICS installations for maintenance purposes is a common practice. Access with default or hard-coded passwords is widespread. Access by manufacturers and external service providers for maintenance purposes is sometimes not limited to specific systems. As a consequence, further systems are accessible. |
| 9 | Technical malfunctions and force majeure | Failures due to extreme environmental influences or technical defects are always possible – the risk and the potential for damage can only be minimized here. |
| 10 | Compromising by smartphones in the production environment | The ability to display and change operating and production parameters on a smartphone or tablet is increasingly being used in the production environment. Remote maintenance access via a smartphone or tablet represents a special case and adds an additional point of attack. |

Threat overview

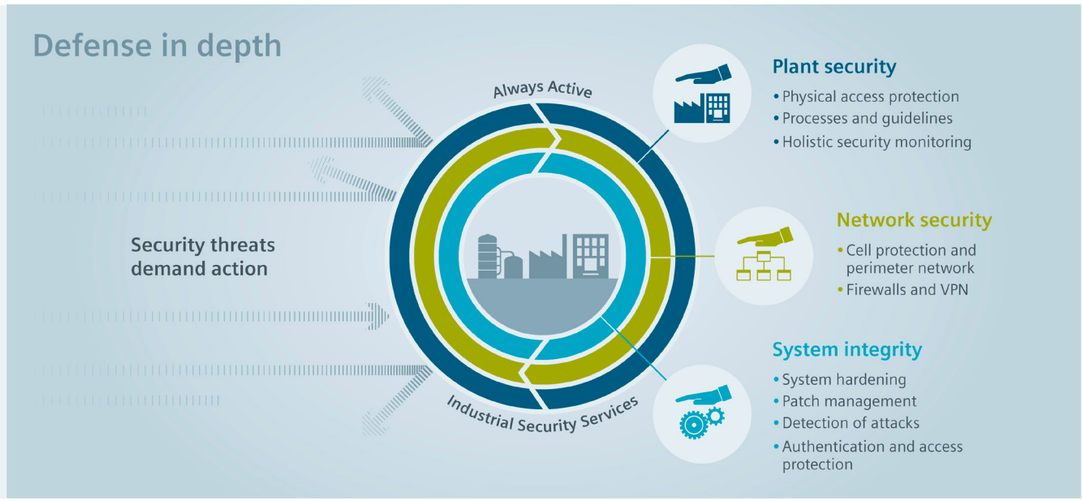
**Source:**
Based on BSI-CS 005 | Version 1.30 dated 1 January, 2019
**Note:**
This list of threats was compiled in close cooperation between BSI (German Federal Office for Information Security) and representatives of industry.
Using BSI analyses, the Federal Office for Information Security (BSI) publishes statistics and reports on current topics relating to cybersecurity.



© Siemens 2020

INDUSTRIAL SECURITY

## Defense in depth




Network security as a central component of the Siemens industrial security concept

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

### Plant security

Plant security uses a number of different methods to prevent unauthorized persons from gaining physical access to critical components. This starts with conventional building access and extends to securing sensitive areas by means of key cards. Comprehensive security monitoring leads to transparency with regard to the security status of production facilities. Thanks to continuous analyses and correlations of existing data and through comparison of these with threat indicators, security-relevant events can be detected and classified according to risk factors. On this basis and through regular status reports, plant owners receive an overview of the current security status of their production facilities, enabling them to react swiftly to threats.

### Network security

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

### 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 SIMATIC 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 possible attacks.

© Siemens 2020

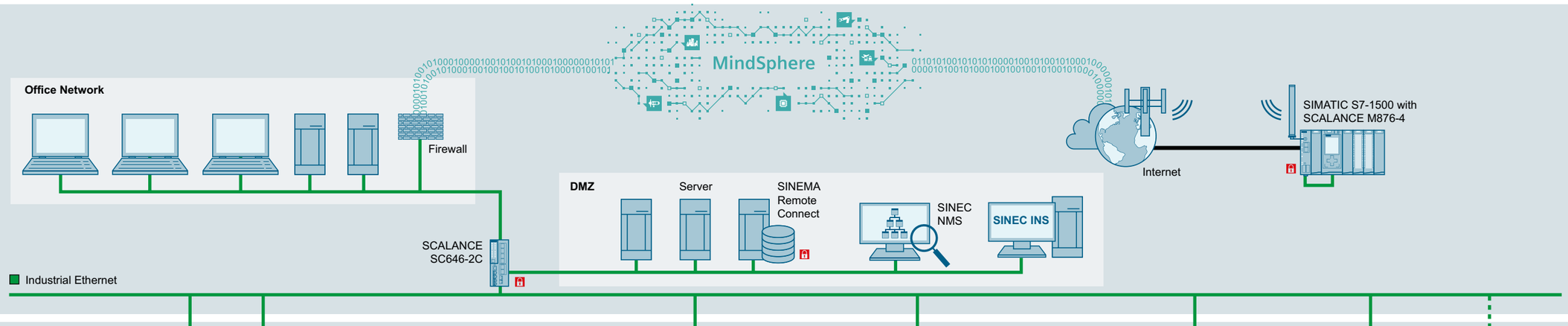


INDUSTRIAL SECURITY

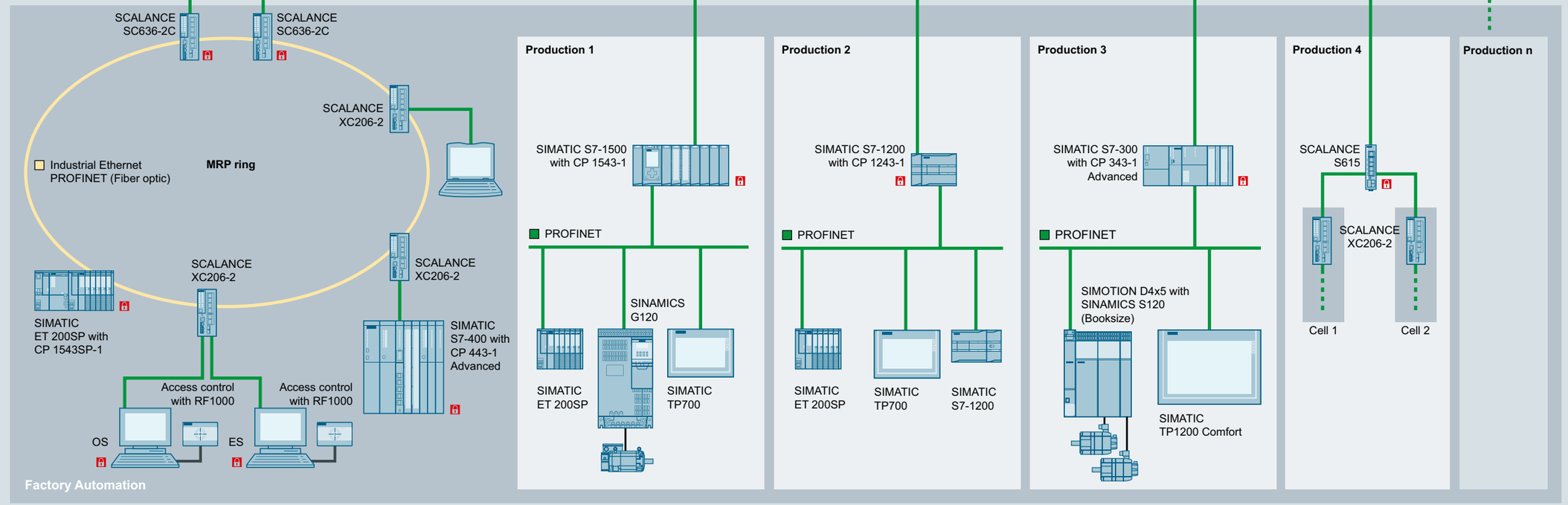
# Industrial security at a glance

**Plant Security**


**Network Security**




**System Integrity**



## Industrial security – more than just product functions



With the aim of taking a further step toward a secure digital world, Siemens is the first company to receive TÜV SÜD (German Technical Inspectorate/South) certification based on IEC 62443-4-1 for the interdisciplinary process of developing automation and drive products and is also the initiator of the "Charter of Trust".

Based on 10 key principles, the members of the "Charter of Trust" set themselves the three goals of protecting the data of individuals and companies, preventing harm to people, companies and infrastructures as well as creating a reliable basis upon which trust is established and can grow in a connected, digital world.

## Industrial security as part of Totally Integrated Automation

Totally Integrated Automation (TIA): maximum consistency from the automation level to the IT

TIA Portal

TIA stands for total integration: hardware, software and services are seamlessly interconnected. Information flow horizontally and vertically and new technologies are constantly integrated. To ensure that systems and machines are as secure as possible despite increasing interconnectedness, TIA is consequently based on the security concept defense in depth.

All Industrial Security Appliances and remote networks components are integrated in the TIA Portal and can be configured there. In addition to a central user management with the UMC option of the TIA Portal, the firewall rules for the security communications processors are also automatically assigned via the TIA Portal.

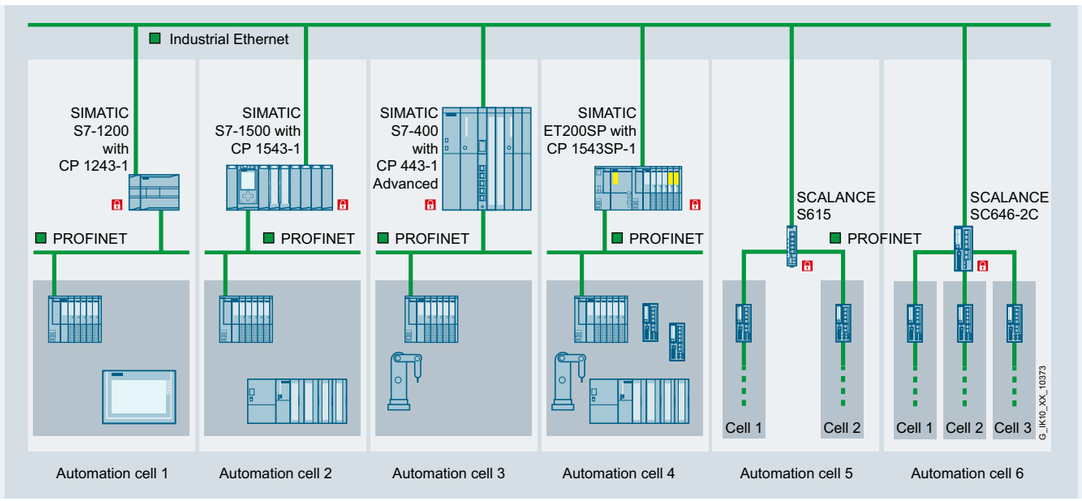


© Siemens 2020



# Network Security

## Cell protection concept




Secured communication between components with Security Integrated in separate automation cells

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

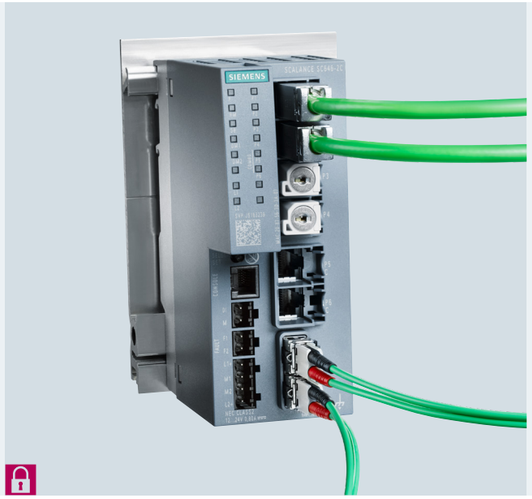
### Cybersecurity – comprehensive security mechanisms

Siemens helps its customers benefit from technological progress while keeping risks in areas such as cybersecurity as low as possible. A security solution can only be implemented optimally when it is continuously adapted to new threats. Taking this into account, the products, solutions and services from Siemens for cybersecurity offer proven protection in industrial plants, automation systems and industrial networks, even for those in harsh environments.

### Cell protection concept

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

# SCALANCE S Industrial Security Appliances



SCALANCE S Industrial Security Appliances offer protection of devices and networks in discrete manufacturing and in the process industry and protect industrial communication with mechanisms such as Stateful Inspection Firewall and Virtual Private Networks (VPN). The devices are suitable for industry-related applications. Depending on the requirements, they are available with different port configurations (2 to 6 ports) and range of functions (firewall or firewall + VPN). All versions enable configuration over Web Based Management (WBM), Command Line Interface (CLI), Simple Network Management Protocol (SNMP), SINEC NMS network management as well as TIA Portal. Furthermore, the Industrial Firewall Appliances allow the realization of a network segmentation in the PROFIsafe environment.

**All Industrial Security Appliances support:**

- User-specific firewall
- Network Address Translation (NAT), Network Address Port Translation (NAPT) for communication for serial machines with identical IP address bands
- Autoconfiguration interface for easy connection configuration to SINEMA Remote Connect
- Digital input (DI) for connection of a transducer (e.g., key-operated switch) for controlled setup of a tunnel connection
- Simple device replacement with C-PLUG
- Redundancy mechanisms through VRRPv3

**Industrial Firewall Appliances**

SCALANCE SC622-2C, SC632-2C and SC636-2C

- Firewall performance approx. 600 Mbps
- Communication between separate network segments through a bridge firewall (except SC622-2C)
- Connection via 10/100/1000 Mbps ports and fiber optic for large distances (up to 200 km)
- Secured redundant MRP/HRP connection for SCALANCE SC636-2C

**Industrial VPN Appliances**

SCALANCE S615

- Firewall performance approx. 100 Mbps
- Management of up to 20 VPN connections with a data rate of up to 35 Mbps
- Connection via 10/100 Mbps ports

SCALANCE SC642-2C and SC646-2C

- Firewall performance approx. 600 Mbps
- Bridge tunnel for secure layer 2 communication
- Communication between separate network segments through a bridge firewall
- Management of up to 200 VPN connections with a data rate of up to 120 Mbps
- Connection via 10/100/1000 Mbps ports and fiber optic for large distances (up to 200 km)
- Secured redundant MRP/HRP connection for SCALANCE SC646-2C

For more information on Industrial Security Appliances, visit: **siemens.com/scalance-s**
Additional information on SINEMA Remote Connect on page 18.

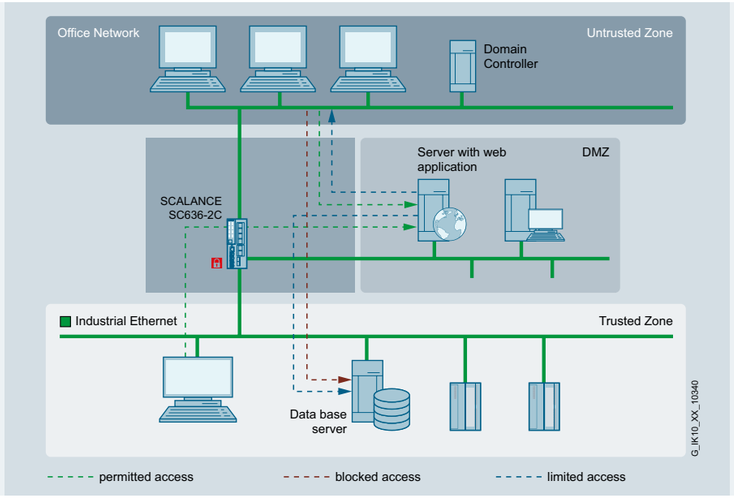


© Siemens 2020

NETWORK SECURITY

## Application example

# Network access protection with DMZ




Network security as a central component of the Siemens industrial security concept

**Task**

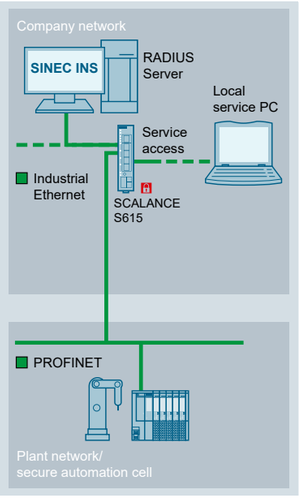
Network nodes or servers (e.g., MES servers) are to be accessible from both the secured network and the unsecured network without a direct connection between the networks.

**Solution**

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

**Advantages at a glance**

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




Connection of a local service PC via SCALANCE S615

**Task**

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

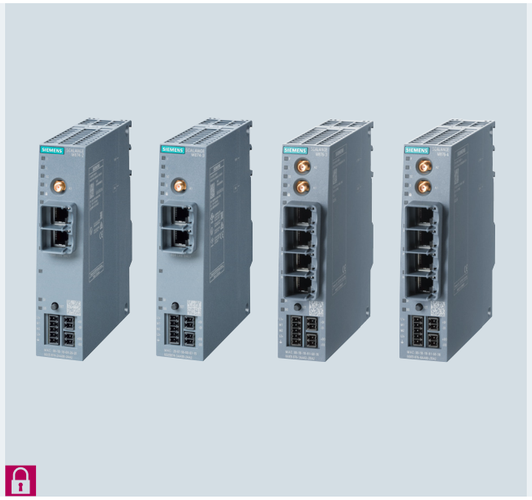
**Solution**

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

**Advantages at a glance**

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

# SCALANCE M Industrial Routers



The SCALANCE M portfolio consists of routers for Industrial Remote Communication applications such as Telecontrol and Teleservice. The integrated firewall and VPN (IPsec; OpenVPN as client and for connection to SINEMA Remote Connect) security functions protect against unauthorized access and make data transmission secure.

### Wireless connection to remote networks

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

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

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

SCALANCE M876-3 supports dual-band CDMA2000 and the UMTS data service HSPA+. Thus, the device enables high transmission rates of up to 14.4 Mbps in the downlink and up to 5.76 Mbps in the uplink.

SCALANCE M876-4 supports LTE (Long Term Evolution) and enables high transmission rates of up to 100 Mbps in the downlink and up to 50 Mbps in the uplink.

### Wired connection to remote networks

The wired routers of the SCALANCE M product family support the cost-effective and secured connection of Ethernet-based subnets and automation devices. The connection can be made over existing two-wire or stranded cables or wired telephone or DSL networks. The connection of PROFIBUS networks is also possible without any additional adapters or software.

SCALANCE M804PB supports PROFIBUS/MPI. This enables the device to have secured remote access to existing systems. Transmission rates up to 12 Mbps can be achieved.

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

SCALANCE M826-2 is an SHDSL modem for connection via existing two-wire or stranded cables and supports the ITU-T standard G.991.2. Thus, the device enables high symmetrical transmission rates of up to 15.3 Mbps per wire pair.

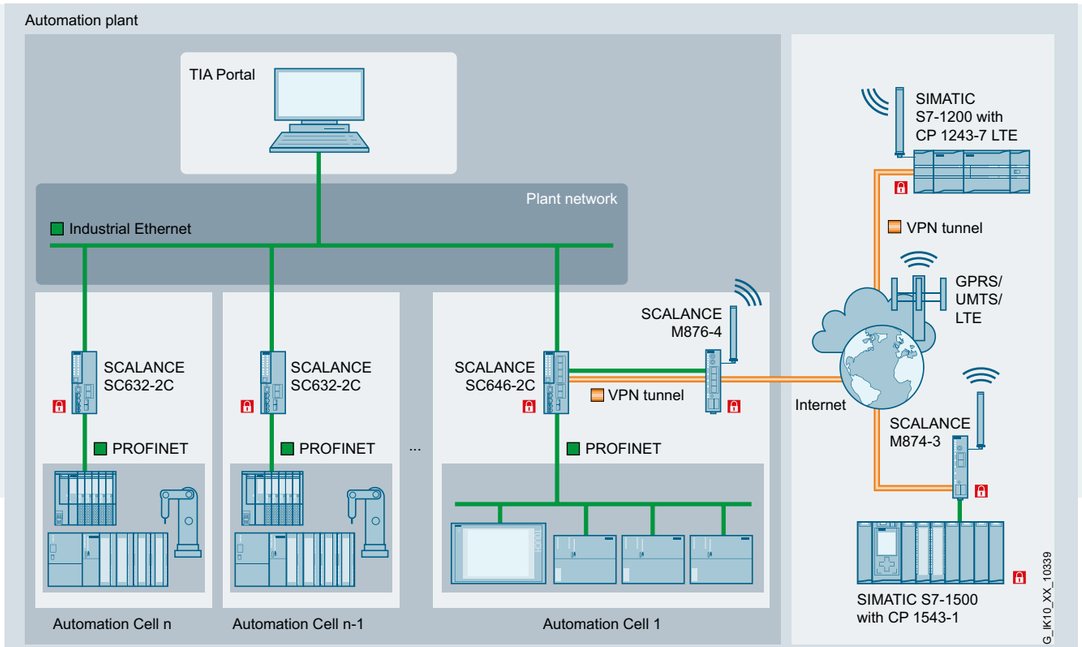


© Siemens 2020

NETWORK SECURITY

## Application example

# Secured remote maintenance with SCALANCE M and SCALANCE S




Secured remote access without direct connection to the automation network with industrial security components

### Task

For servicing purposes, a system integrator requires secure access via the Internet to his/her machine or equipment at the end user. However, the integrator is to be given access only to specific devices and not to the plant network. In addition, a secured connection from the plant to a remote station via mobile networks (e.g., UMTS or LTE) is to be established.

### Solution

Starting points for the connection of the system integrator are the VPN clients (in this case CP 1243-7 LTE, SCALANCE M874-3) with the end point SCALANCE SC646-2C as VPN server in the automation system.

### Advantages at a glance

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

### Task

Access of a system integrator to the machine is to be unlocked for individual end devices and services on a user-dependent and role-dependent basis.

### Solution

User-specific firewall rules can be temporarily enabled on the SCALANCE S Industrial Security Appliances with personalized user data for the duration of the service work.

### Advantages at a glance

- Reduced security risk during service and maintenance
- Controlled and logged device access
- User-based and protocol-based access control to end systems of a network cell

# Security Communications Processors for Basic Controllers, Advanced Controllers and Distributed Controllers

Security Communications Processors protect controllers with integrated firewall and VPN against data manipulation and espionage.

**For SIMATIC Basic Controllers**

**CP 1243-1, CP 1243-7 LTE and CP 1243-8 IRC**

The CP 1243-1 and CP 1243-7 LTE communications processors connect the SIMATIC S7-1200 controller to Ethernet networks (CP 1243-1) or mobile wireless networks (CP 1243-7 LTE). The CP 1243-8 IRC communications processor connects the controller to a telecontrol center via the telecontrol protocols SINAUT ST7, DNP3 and IEC 60870-5-104. With integrated firewall and VPN security functions, the communications processors protect S7-1200 stations and lower-level networks from unauthorized access and data transmission against manipulation and espionage by means of encryption.

**For SIMATIC Advanced Controllers**

**CP 1543-1**

The CP 1543-1 communications processor securely connects the SIMATIC S7-1500 controller to Ethernet networks. With its integrated firewall and VPN security functions and protocols for data encryption such as FTPS and SNMPv3, the communications processor protects S7-1500 stations and lower-level networks from unauthorized access and data transmission against manipulation and espionage by means of encryption. The CP 1543-1 also allows encrypted email communication via SMTPS (Ports 587 & 25) and secure open communication via TCP/IP.

**CP 1545-1**

The CP 1545-1 with CloudConnect functionality enables easy and reliable transfer of all data from SIMATIC S7-1500 to MindSphere or a cloud solution which supports the standardized MQTT protocol, e.g., Microsoft Azure or IBM Cloud. CP 1545-1 protects the SIMATIC S7-1500 station from unauthorized access with the integrated Stateful Inspection Firewall. Integration into an IPv6 infrastructure is also possible. In parallel with the connection to cloud applications, the CP 1545-1 supports the connection to additional automation devices, such as HMIs, via Industrial Ethernet with the SIMATIC S7 protocol.

**For SIMATIC Distributed Controllers**

**CP 1543SP-1**

The CP 1543SP-1 communications processor allows the ET 200SP Distributed Controller to be flexibly expanded to include an Industrial Ethernet interface. This enables the setup of identical machines with the same IP addresses through network segmentation. It also offers extended security functions such as encryption of all transmitted data using VPN with IPsec and Firewall for secure access to the ET 200SP Distributed Controller.

## Advantages at a glance

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

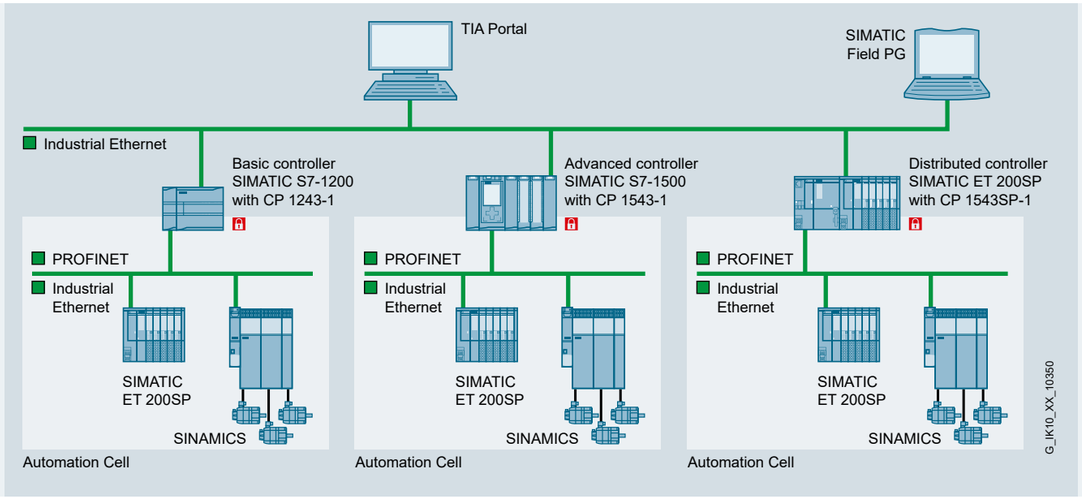


© Siemens 2020

NETWORK SECURITY

## Application example

# Network segmentation with Security Communications Processors




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

**Task**

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

**Solution**

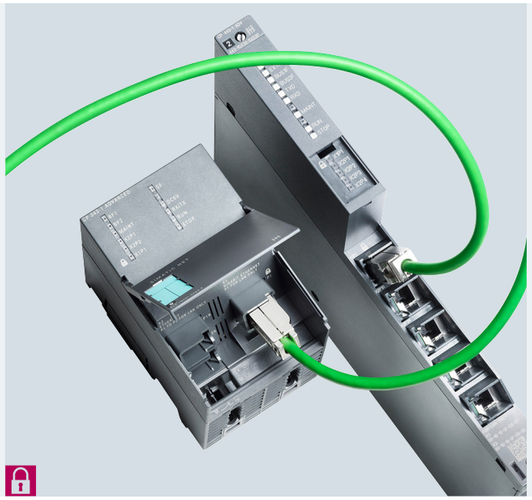
The communications processors are placed in the rack of the respective target systems (SIMATIC S7-1200, SIMATIC S7-1500, SIMATIC ET 200SP Distributed Controller) upstream of the automation cells to be protected. In this way, the communication to and from the SIMATIC CPU and lower-level automation cell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

## Advantages at a glance

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

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

# Security Communications Processors for SIMATIC S7-300 & SIMATIC S7-400



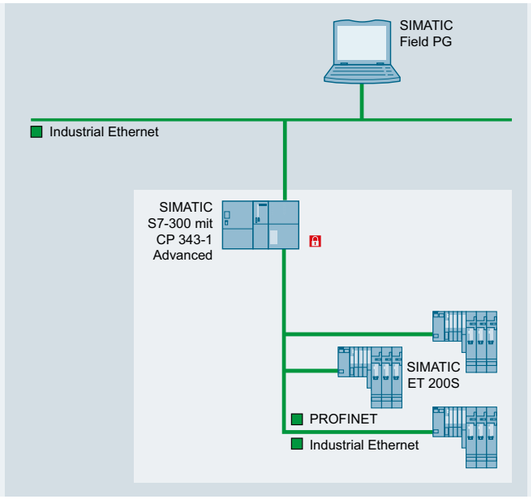
**CP 343-1 Advanced and CP 443-1 Advanced**

Alongside the familiar communication functions, an integrated switch and Layer 3 routing functionality, the Industrial Ethernet communications processors CP 343-1 Advanced and CP 443-1 Advanced for SIMATIC S7-300 and SIMATIC 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.

**Advantages at a glance**

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

## Application example
# Network segmentation




**Task**

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

**Solution**

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

**Advantages at a glance**

- In addition to their communication functions, Advanced CPs also come with integrated firewall and VPN security functions for implementing a protected automation cell and for protecting data transmission.
- Secure communication integration: CPs are easily configured with STEP 7/TIA Portal; VPN tunnels can be set up between the CPs or to the SCALANCE S Industrial Security Appliances and the SCALANCE M Internet and mobile wireless routers.
- All CP 343-1 Advanced and CP 443-1 Advanced users get Security Integrated and do not need separate hardware or special tools besides SIMATIC S7 to configure the security of industrial plants.



© Siemens 2020

NETWORK SECURITY

# Software for secured networks

**Efficient and secure network management**

With the powerful and future-proof Network Management System (NMS), the possibility exists for central, 24/7 monitoring, management and configuration of networks of up to several thousand nodes across industry sectors.

SINEC NMS also enables efficient security management in accordance with IEC 62443. For example, access to the system and the range of functions available to each authorized user can be precisely controlled via the user role administration. The system provides system security through, among other things, encrypted data communication (via certificates and password) between the central SINEC NMS control instance and the SINEC NMS operations distributed in the network. Data communication between SINEC NMS and the infrastructure components in the network can also be encrypted (SNMPv3).

In addition, SINEC NMS provides a local documentation function via Audit Trails. For example, audit log entries can be traced by automatically documenting which user performs which activities in the system and when with a time stamp. This also produces significant time and cost savings for official tests.

Furthermore, information such as audit logs, system events and network alarms can be passed to a central location via syslog. SINEC NMS also offers central firewall and NAT management. Firewall components (SCALANCE SC-600/S615 and RUGGEDCOM RX1400/1500) can be centrally configured. The firewall rules are created using a graphical description of the permitted communication relationship in the network. The system then automatically generates the device-specific rules. It is also possible to use only the NAT management function independent of firewall management, or vice versa.

**Infrastructure Network Services SINEC INS**

SINEC INS (Infrastructure Network Services), the software tool for central network services, offers central network services which are specifically tailored to Operational Technology (OT) in an easy and structured way. Separated from IT services, the OP can establish a self-sufficient network which it can host by itself, e.g., in an OT data center with SINEC INS. The tool includes different security-relevant clients such as a RADIUS server for user and device authentication (MAC authentication) within the network, for example to check who may access which device. The Secure Syslog Client allows sending and receiving security messages in the Syslog format meaning, for example Audit Log entries from SINEC NMS can be sent to the SINEC INS Syslog Cleint as Syslog messages. A (D) Dos ((Distributed) Denial of Service) attack, meaning an unauthorized user tried to gain access with force, can be discovered here.

For more information visit:
www.siemens.com/sinec

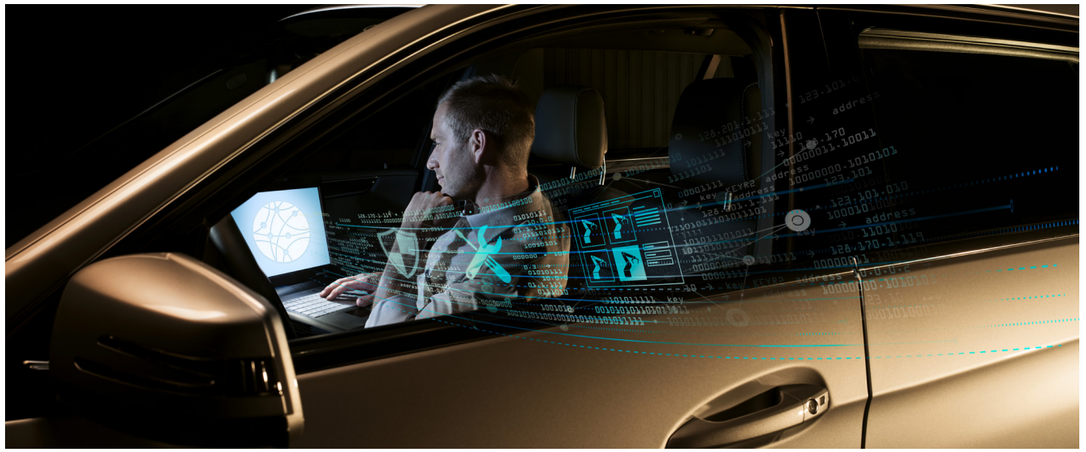
# Software for secured networks


**SINEMA Remote Connect**

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

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

With the SCALANCE M804PB Industrial Router, it is also possible to easily and economically connect existing PROFIBUS/MPI systems directly to SINEMA Remote Connect for secured remote access.



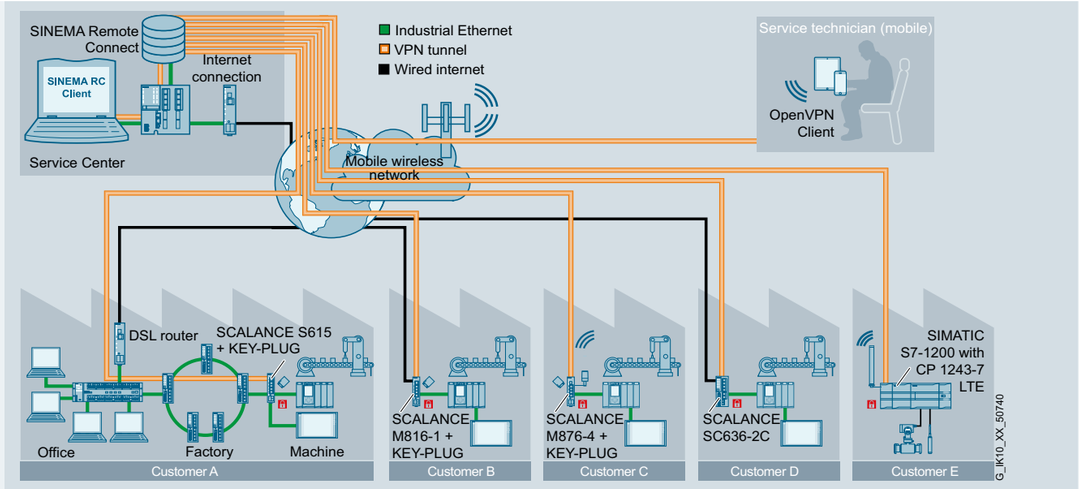


© Siemens 2020

NETWORK SECURITY

## Application example

# Secured access to plant sections with SINEMA Remote Connect




Configuration example for SINEMA Remote Connect – general overview

**Task**

Remote access for remote maintenance is to be possible for serial machines and larger plants with identical subnets. The remote access to special-purpose machines and sensitive areas, in particular, requires central management of the connections needed to acquire status and maintenance data. Easy and convenient creation of the corresponding routers with routing/NAT information should also be possible.

**Solution**

SINEMA Remote Connect – the management platform for remote networks – is used to centrally manage the connections between machines and service technicians. SINEMA Remote Connect manages both user rights and access authorizations and ensures that only authorized personnel are given access to remote machines.

**Typical areas of application**

- Plant and machine building
- 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
- Local and central logging of all activities
- Central user administration
- Secured and easy access to plant sections from anywhere in the world
- Optimum connection of machines including machines with identical IP addresses in local subnets (NAT)
- Convenient management of different users (service technicians) through group management, including user-specific access rights, also to explicit IP addresses in the subnet (dedicated device access)
- Quick and effortless connection setup thanks to address book function
- Easy integration into industrial facilities
- No special IT know-how required thanks to simple user interface with autoconfiguration for end devices and SINEMA RC Client
- Secure and convenient multifactor authentication with user name/password and PKI Smartcard
- Operation in virtual environment is possible

# Technical specifications

## SCALANCE S Industrial Security Appliances

| Product type designation | Industrial Firewall Appliances | | | Industrial VPN Appliances | | |
|---|---|---|---|---|---|---|
| | SCALANCE SC622-2C | SCALANCE SC632-2C | SCALANCE SC636-2C | SCALANCE S615 | SCALANCE SC642-2C | SCALANCE SC646-2C |
| Article number | 6GK5622-2GS00-2AC2 | 6GK5632-2GS00-2AC2 | 6GK5636-2GS00-2AC2 | 6GK5615-0AA00-2AA2 | 6GK5642-2GS00-2AC2 | 6GK5646-2GS00-2AC2 |
| **Transmission rate** | | | | | | |
| Transmission rate | 10/100/1 000 Mbps | 10/100/1 000 Mbps | 10/100/1 000 Mbps | 10/100 Mbps | 10/100/1 000 Mbps | 10/100/1 000 Mbps |
| **Interfaces** | | | | | | |
| Electrical connection | 2 x RJ45 port | 2 x RJ45 port | 6 x RJ45 port | 5 x RJ45 port | 2 x RJ45 port | 6 x RJ45 port |
| Optical connection | 2 x combo port with SFP | 2 x combo port with SFP | 2 x combo port with SFP | – | 2 x combo port with SFP | 2 x combo port with SFP |
| for signaling contact | 1 x 2-pin terminal block | 1 x 2-pin terminal block | 1 x 2-pin terminal block | – | 1 x 2-pin terminal block | 1 x 2-pin terminal block |
| for power supply | 1 x 4-pin terminal block | 1 x 4-pin terminal block | 1 x 4-pin terminal block | 1 x 5-pin terminal block | 1 x 4-pin terminal block | 1 x 4-pin terminal block |
| C-PLUG removable data storage medium | Yes | Yes | Yes | Yes | Yes | Yes |
| **Supply voltage, current consumption, power loss** | | | | | | |
| Supply voltage, external | 24 V DC | 24 V DC | 24 V DC | 24 V DC | 24 V DC | 24 V DC |
| Range | 9.6 V ... 31.2 V DC | 9.6 V ... 31.2 V DC | 9.6 V ... 31.2 V DC | 10.8 V ... 28.2 V DC | 9.6 V ... 31.2 V DC | 9.6 V ... 31.2 V DC |
| **Permissible ambient conditions** | | | | | | |
| Ambient temperature during operation [°C] | -40 °C ... +70 °C | -40 °C ... +70 °C | -40 °C ... +70 °C | -40 °C ... +70 °C | -40 °C ... +70 °C | -40 °C ... +70 °C |
| Degree of protection | IP20 | IP20 | IP20 | IP20 | IP20 | IP20 |
| **Design** | | | | | | |
| Module format | Compact | Compact | Compact | Compact | Compact | Compact |
| **Product function: Security** | | | | | | |
| Firewall type | Stateful Inspection | Stateful Inspection | Stateful Inspection | Stateful Inspection | Stateful Inspection | Stateful Inspection |
| Bridge firewall | No | Yes | Yes | No | Yes | Yes |
| Bridge tunnel | No | No | No | No | Yes | Yes |
| User-specific firewall | Yes | Yes | Yes | Yes | Yes | Yes |
| Password protection | Yes | Yes | Yes | Yes | Yes | Yes |
| Product function with VPN connection | OpenVPN (as client for SINEMA Remote Connect) | OpenVPN (as client for SINEMA Remote Connect) | OpenVPN (as client for SINEMA Remote Connect) | IPsec, OpenVPN (as client for SINEMA Remote Connect) | IPsec, OpenVPN (as client for SINEMA Remote Connect) | IPsec, OpenVPN (as client for SINEMA Remote Connect) |
| IPsec VPN data throughput | – | – | – | 35 Mbps | 120 Mbps | 120 Mbps |
| Number of possible connections with VPN connection | 0 | 0 | 0 | 20 | 200 | 200 |
| Firewall data throughput | 600 Mbps | 600 Mbps | 600 Mbps | 100 Mbps | 600 Mbps | 600 Mbps |
| NAT/NAPT | Yes | Yes | Yes | Yes | Yes | Yes |
| VRRPv3 coupling | 6 | 6 | 6 | 2 | 6 | 6 |
| MRP client/HRP client | No | No | Yes | No | No | Yes |
| Network segmentation in PROFIsafe environment | Yes | No | No | No | No | No |



© Siemens 2020

TECHNICAL SPECIFICATIONS

## SCALANCE M Industrial Routers

| Product type designation | SCALANCE M wireless | |
|---|---|---|
| | M874-2, M874-3 | M876-3, M876-4 |
| Article number | 6GK5874-2AA00-2AA2<br>6GK5874-3AA00-2AA2 | 6GK5876-3AA02-2BA2<br>6GK5876-4AA00-2BA2 |
| **Transmission rate** | | |
| at interface 1/2 | 10/100 Mbps | |
| GPRS transmission uplink/downlink, max. | 85.6 Kbps | 85.6 Kbps |
| EDGE transmission uplink/downlink, max. | 237 Kbps | 237 Kbps |
| HSPA+ transmission uplink/downlink, max. | 5.76 Mbps | 14.4 Mbps |
| EV-DO transmission forward link/reverse link | – | 3.1 Mbps/1.8 Mbps (M876-3 only) |
| LTE transmission uplink/downlink, max. | – | 50 Mbps/100 Mbps (M876-4 only) |
| ADSL2+ transmission uplink/downlink, max. | – | – |
| SHDSL transmission, max. | – | – |
| **Interfaces** | | |
| Number of electrical connections | | |
| ■ for internal network | 2 | 4 |
| ■ for external network | 1 | 2 |
| ■ for power supply | 2 | 2 |
| Electrical connection | | |
| ■ for internal network | RJ45 port (10/100 Mbps, TP, autocrossover) | RJ45 port (10/100 Mbps, TP, autocrossover) |
| ■ for external network | SMA antenna sockets (50 ohms) | SMA antenna sockets (50 ohms) |
| ■ for power supply | Terminal strip | Terminal strip |
| **Supply voltage, current consumption, power loss** | | |
| Supply voltage/range | 10.8 V ... 28.8 V | 10.8 V ... 28.8 V |
| **Permissible ambient conditions** | | |
| Ambient temperature during operation [°C] | -20 °C ... +60 °C | -20 °C ... +60 °C |
| Degree of protection | IP20 | IP20 |
| **Design** | | |
| Module format | Compact | Compact |
| **Product function: Security** | | |
| Firewall type | Stateful Inspection | Stateful Inspection |
| Bridge firewall | No | No |
| User-specific firewall | Yes | Yes |
| Password protection | Yes | Yes |
| Packet filter | Yes | Yes |
| Product function with VPN connection | IPsec, OpenVPN (as client) | IPsec, OpenVPN (as client) |
| Number of possible connections with VPN connection | 20 | 20 |
| Key length | | |
| ■ 1 \| 2 \| 3 with IPsec AES for VPN | 128 bit \| 192 bit \| 256 bit | 128 bit \| 192 bit \| 256 bit |
| ■ with IPsec 3DES/with virtual private network | 168 bit | 168 bit |
| ■ VRRPv3 coupling | 2 | 2 |
| ■ MRP client/HRP client | No | No |

**Suitable accessories such as antennas and cables can be found on the Internet at:**
**www.siemens.com/mall-remote-networks-accessories**

# SCALANCE M Industrial Routers

| Product type designation | SCALANCE M wired | | | |
|---|---|---|---|---|
| | M812-1/M816-1 | | M826-2 | M804PB |
| Article number | 6GK5812-1BA00-2AA2<br>6GK5816-1BA00-2AA2 | | 6GK5826-2AB00-2AB2 | 6GK5804-0AP00-2AA2 |
| **Transmission rate** | | | | |
| at interface 1/2 | 10/100 Mbps | | 10/100 Mbps | 10/100 Mbps |
| GPRS transmission uplink/downlink, max. | – | | – | – |
| EDGE transmission uplink/downlink, max. | – | | – | – |
| HSPA+ transmission uplink/downlink, max. | – | | – | – |
| EV-DO transmission forward link/reverse link | – | | – | – |
| LTE transmission uplink/downlink, max. | – | | – | – |
| ADSL2+ transmission uplink/downlink, max. | 1.4 Mbps/25 Mbps | | – | – |
| SHDSL transmission, max. | – | | 15.3 Mbps | – |
| **Interfaces** | | | | |
| Number of electrical connections | | | | |
| ■ for internal network | 1 | 4 | 4 | 2 |
| ■ for external network | 1 | 1 | 2 | 1 |
| ■ for power supply | 2 | 2 | 2 | 2 |
| Electrical connection | | | | |
| ■ for internal network | RJ45 port (10/100 Mbps ,TP, autocrossover) | | | RJ45 port (10/100 Mbps, TP, autocrossover), D-SUB |
| ■ for external network | RJ45 DSL port | – | Terminal strip | RJ45 port (10/100 Mbps, TP, autocrossover) |
| ■ for power supply | – | – | – | Terminal strip |
| **Supply voltage, current consumption, power loss** | | | | |
| Supply voltage/range | 10.8 V ... 28.8 V | | 10.8 V ... 28.8 V | 10.8 V ... 28.8 V |
| **Permissible ambient conditions** | | | | |
| Ambient temperature during operation [°C] | 0 °... +60 °C | | -40 °C ... +70 °C | -20 °C ... +60 °C |
| Degree of protection | IP20 | | IP20 | IP20 |
| **Design** | | | | |
| Module format | Compact | | Compact | Compact |
| **Product function: Security** | | | | |
| Firewall type | Stateful Inspection | | Stateful Inspection | Stateful Inspection |
| Bridge firewall | No | | No | No |
| User-specific firewall | Yes | | Yes | Yes |
| Password protection | Yes | | Yes | Yes |
| Packet filter | Yes | | Yes | Yes |
| Product function with VPN connection | IPsec, OpenVPN (as client) | | IPsec, OpenVPN (as client) | IPsec, OpenVPN (as client) |
| Number of possible connections with VPN connection | 20 | | 20 | 20 |
| Key length | | | | |
| ■ 1 \| 2 \| 3 with IPsec AES for VPN | 128 bit \| 192 bit \| 256 bit | | 128 bit \| 192 bit \| 256 bit | 128 bit \| 192 bit \| 256 bit |
| ■ with IPsec 3DES/with virtual private network | 168 bit | | 168 bit | 168 bit |
| ■ VRRPv3 coupling | 2 | | 2 | 2 |
| ■ MRP client/HRP client | No | | No | No |

**Suitable accessories and details can be found on the Internet at: www.siemens.com/mall-remote-networks-accessories**



© Siemens 2020

TECHNICAL SPECIFICATIONS

# Communications Processors

| Product type designation | CP 1243-1 | CP 1243-7 LTE | CP 1243-8 IRC | CP 1543-1 | CP 1543SP-1 | CP 1545-1 |
|---|---|---|---|---|---|---|
| Article number | 6GK7243-1BX30-0XE0 | 6GK7243-7KX30-0XE0 | 6GK7243-8RX30-0XE0 | 6GK7543-1AX00-0XE0 | 6GK7543-6WX00-0XE0 | 6GK7545-1GX00-0XE0 |
| **Transmission rate** | | | | | | |
| ■ at interface 1 | 10/100 Mbps | Mobile wireless 4G/3G/2G | 10/100 Mbps | 10/100/1 000 Mbps | 10/100 Mbps | 10/100/1 000 Mbps |
| **Interfaces** | | | | | | |
| Number of electrical connections | | | | | | |
| ■ to interface 1 | 1 x RJ45 port | Antenna connection SMA socket | 1 x RJ45 port | 1 x RJ45 port | 2 x RJ45 ports using ET 200SP BusAdapter | 1 x RJ45 port |
| ■ for power supply | – | 1, 3-pin plug-in terminal strip | 1, 3-pin plug-in terminal strip | – | – | - |
| ■ C-PLUG swap medium | – | – | – | – | – | - |
| **Supply voltage** | | | | | | |
| ■ 1 from backplane bus | 5 V DC | – | 5 V DC | 15 V DC | – | 15 V DC |
| ■ external | – | 24 V DC | 24 V DC | – | 24 V DC | |
| **Permissible ambient conditions during operation** | | | | | | |
| ■ when installed vertically | -20 °C ... +60 °C | -20 °C ... +60 °C | -20 °C ... +60 °C | 0 °C ... +40 °C | 0 °C ... +50 °C | 0 °C ... +40 °C |
| ■ when installed horizontally | -20 °C ... +70 °C | -20 °C ... +70 °C | -20 °C ... +70 °C | 0 °C ... +60 °C | 0 °C ... +60 °C | 0 °C ... +60 °C |
| Degree of protection | IP20 | IP20 | IP20 | IP20 | IP20 | IP20 |
| **Design** | | | | | | |
| Module format | Compact S7-1200, single width | Compact S7-1200, single width | Compact S7-1200, single width | Compact S7-1500, single width | Compact module for ET 200SP | Compact S7-1500, single width |
| **Product function: Security** | | | | | | |
| Firewall type | Stateful Inspection | Stateful Inspection | Stateful Inspection | Stateful Inspection | Stateful Inspection | Stateful Inspection |
| Product function with VPN connection | IPsec, SINEMA Remote Connect | IPsec, SINEMA Remote Connect | IPsec, SINEMA Remote Connect | IPsec | IPsec, SINEMA Remote Connect | - |
| Number of possible connections with VPN connection | 8 | 1 | 8 | 16 | 4 | - |
| **Product function** | | | | | | |
| ACL – IP-based | No | No | No | No | No | No |
| ACL – IP-based for PLC/routing | No | No | No | No | No | No |
| Deactivation of services that are not needed | Yes | No | No | Yes | Yes | Yes |
| Log file for unauthorized access | No | No | No | Yes | Yes | Yes |

## Communications Processors

| Product type designation | CP 343-1 Advanced | CP 443-1 Advanced |
|---|---|---|
| Article number | 6GK7343-1GX31-0XE0 | 6GK7443-1GX30-0XE0 |
| **Transmission rate** | | |
| at interface 1/2 | 10/1 000 Mbps/10/100 Mbps | 10/1 000 Mbps/10/100 Mbps |
| **Interfaces** | | |
| Electrical connection | | |
| ■ to interface 1 acc. to Industrial Ethernet | 1 x RJ45 port | 1 x RJ45 port |
| ■ to interface 2 acc. to Industrial Ethernet | 2 x RJ45 port | 4 x RJ45 port |
| ■ for power supply | 2-pin plug-in terminal strip | – |
| ■ C-PLUG swap medium | Yes | Yes |
| **Supply voltage, current consumption, power loss** | | |
| Type of power supply voltage | – | – |
| Supply voltage | | |
| 1 from backplane bus | 5 V DC | 5 V DC |
| 2 from backplane bus | – | – |
| external | 24 V DC | – |
| Range | – | – |
| **Permissible ambient conditions** | | |
| during operation | | 0 °C ... +60 °C |
| ■ when installed vertically | 0 °C ... +40 °C | – |
| ■ when installed horizontally | 0 °C ... +60 °C | – |
| Degree of protection | IP20 | IP20 |
| **Design** | | |
| Module format | Compact | Compact S7-400 single width |
| **Product function: Security** | | |
| Firewall type | Stateful Inspection | Stateful Inspection |
| Bridge firewall | No | No |
| User-specific firewall | Yes | Yes |
| Product function with VPN connection | IPsec | IPsec |
| Number of possible connections with VPN connection | 32 | 32 |
| **Product function** | | |
| Password protection for Web applications | Yes | Yes |
| ACL – IP-based | Yes | Yes |
| ACL – IP-based for PLC/routing | Yes | Yes |
| Deactivation of services that are not needed | Yes | Yes |
| Blocking of communication via physical ports | Yes | Yes |
| Log file for unauthorized access | No | No |
| MRP client | Yes | Yes |



© Siemens 2020

## Software for industrial networks

| Product type designation | SINEC NMS | SINEC INS | SINEMA Remote Connect | SINEMA RC Client |
|---|---|---|---|---|
| Article number | 6GK8781-1....-.... | 6GK8751-1....-.... | 6GK1720-1AH01-0BV0 | 6GK1721-1XG01-0AA0 |
| Firewall management | Yes | – | – | – |
| Product function with VPN connection | – | – | OpenVPN | OpenVPN |
| Operating system | Desktop:<br>Windows 10 (64 bit, Professional, Enterprise) as of version 1809<br>Server:<br>Windows Server 2016 (64 bit), Windows Server 2019 (64 bit)<br>Virtualization:<br>ESXi V6.7 | Linux Ubuntu 18.04.2 LTS Desktop (64 bit)<br>Linux Ubuntu 18.04.2 LTS Server (64 bit)<br>SIMATIC OS V1.3<br>RX1500 APE 1808<br>Debian 9.6.0 | SINEMA RC Virtual Appliance has its own operating system | Windows 10 Pro, Windows Server 2008, 2012 R2, 2016, 2019 (64 bit) |
| Web browser | Internet Explorer V11.0, Firefox V 68.3 or higher, Google Chrome V78.0 or higher | Google Chrome 67.0 or higher<br>Firefox 60.0 or higher<br>Microsoft Edge 83 or higher<br>Internet Explorer 11.0 *) | Internet Explorer V11.0, Firefox V65.0 or higher, Google Chrome V72.0 or higher | – |
| System Integrity Check | Yes | – | – | – |
| User/Device authentication | Yes | Yes | Yes | Yes |
| Central user authentication with UMC | Yes | Yes | Yes | Yes |
| Security-relevant Syslog messages | Yes/Syslog-Client | Yes/Syslog-Client | Yes/Syslog-Client | No/but via SINEMA RC Server |

# Industrial Security

## IE RJ45 Port Lock


IE RJ45 Port Lock

### Physical network access protection with IE RJ45 Port Lock

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

## SIMATIC RF1000 Access Control Reader


SIMATIC RF1000 for controlling access to machines and equipment

### SIMATIC RF1000 Access Control Reader

The growing demand for security and traceability increasingly calls for solutions which regulate and document access to machines and equipment. With SIMATIC RF1000, Siemens provides an RFID-based solution for easy and flexible implementation of electronic access management. Existing employee IDs are used as the basis for identification. This increases user friendliness and reduces costs. SIMATIC RF1000 series readers allow realization of finely-graded access concepts, documentation of processes and storage of user-specific instructions – according to the customer-specific application. And all with a single card. The compact size, low overall depth, high degree of protection (IP65 at the front) and temperature range from -25 to +55 °C allow the access control reader to be used directly on machines and equipment in harsh industrial environments.

**Highlights:**

- Use in the HF range (13.56 MHz) and LF range (125 kHz)
- OEM version with neutral front foil for customer-specific design
- Diagnostics via 3-color LED status display
- Prevention of misuse through protected and documented access to machines
- Simple integration into existing hardware
- ATEX II approval (for SIMATIC RF1060R and RF1070R only)
- Reading and writing of data on ID/card
- Creation of customer-specific parameter assignments for reader via the config card
- Handling and storage of customer-specific key material in the reader for data access



## Security with SCALANCE X and SCALANCE W

SCALANCE X-200 product line

SCALANCE W product line

### SCALANCE X

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

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

- Management ACL (Access Control List)
- IEEE 802.1X (RADIUS)
- 802.1Q-VLAN – enables logical separation of the data traffic between pre-defined ports on the switches
- Broadcast/Multicast/Unicast Limiter
- Broadcast blocking

In addition, the following secured protocols are supported:

- SSH, HTTPS, SNMPv3

### SCALANCE W

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

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

- Management ACL (Access Control List)
- IEEE 802.1X (RADIUS)
- Access protection according to IEEE 802.11i
- WPA2 (RADIUS)/WPA2-PSK with AES

In addition, the following secured protocols are supported:

- SSH, HTTPS, SNMPv3

Inter AP-Blocking increases the security in a network environment with multiple SCALANCE W access points. WLAN clients which are connected via a layer 2 network (switches) using different access points can communicate directly with one another. 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. SCALANCE W-1700 devices include the function without KEY-PLUG.



© Siemens 2020

MORE ON INDUSTRIAL SECURITY

# Cybersecurity with RUGGEDCOM

RUGGEDCOM Multi-Service Platform

RUGGEDCOM APE1808 Application Processing Engine line module with the RX1500

With increasing connectivity, industrial networks in harsh environments such as those in electric power, transportation and oil & gas industries are exposed to cyber threats. RUGGEDCOM, a family of rugged networking devices from Siemens, is perfect for these industries. RUGGEDCOM devices exceed the requirements of the IEC 61850-3 and IEE 1613 standards for error-free operation despite electromagnetic interference, humidity, vibration and temperature extremes from -40° to +85°C. These devices are built to be secure and enable the integration of advanced cybersecurity applications onto any industrial network.

### RUGGEDCOM Multi-Service Platform

RUGGEDCOM Multi-Service Platform: a family of rugged, hot-swappable and modular Ethernet devices which function as an all-in-one switch, router with VPN and firewall and which are typically used as the main point of entry between the local area network and the WAN. It includes the RX1400 compact Edge router and the RX1500 series of compact (RX1510, RX1511 and RX1512) and rack mount (RX1501 and RX1500) devices.

**Their cybersecurity capabilities include:**

- Stateful Inspection Firewall with Network Address Translation (NAT)
- IPsec VPN for encryption and authentication of all IP packets at the network layer
- Strong encryption to further secure all network traffic with algorithms like AES, RSA and ECC

### RUGGEDCOM APE1808

RUGGEDCOM APE1808 is a powerful application processing engine based on Intel Quad core CPU and x86_64 architecture which supports either Linux or Windows 10 in the form factor of a line module for the RX1500 series of devices. The RUGGEDCOM APE1808 provides a standards-based platform to install applications such as Next Generation Firewalls, Intrusion Detection Systems with Deep Packet Inspection and Intrusion Prevention Systems, Siemens proprietary software such as CROSSBOW for Secure Access Management and SINEC NMS (Operations) for network management, providing a cost-effective way to ensure comprehensive cybersecurity for any industrial network.

### RUGGEDCOM CROSSBOW

A proven Secure Access Management solution designed to provide NERC CIP compliant access to Intelligent Electronic Devices (IEDs). It provides remote IED access, activity logging, data privacy and secure connection to field devices without having to go to the field, delivering productivity gains for administrators and users alike.

RUGGEDCOM Layer 2 Ethernet switches provide security at the local area network level, including MAC-based port security, RADIUS authentication, SSH/SSL encryption for passwords, VLANs and the ability to enable/disable ports.

Siemens offers end-to-end cybersecurity solutions, including network appliances, consultation, design and implementation support with the Siemens Professional Services team.

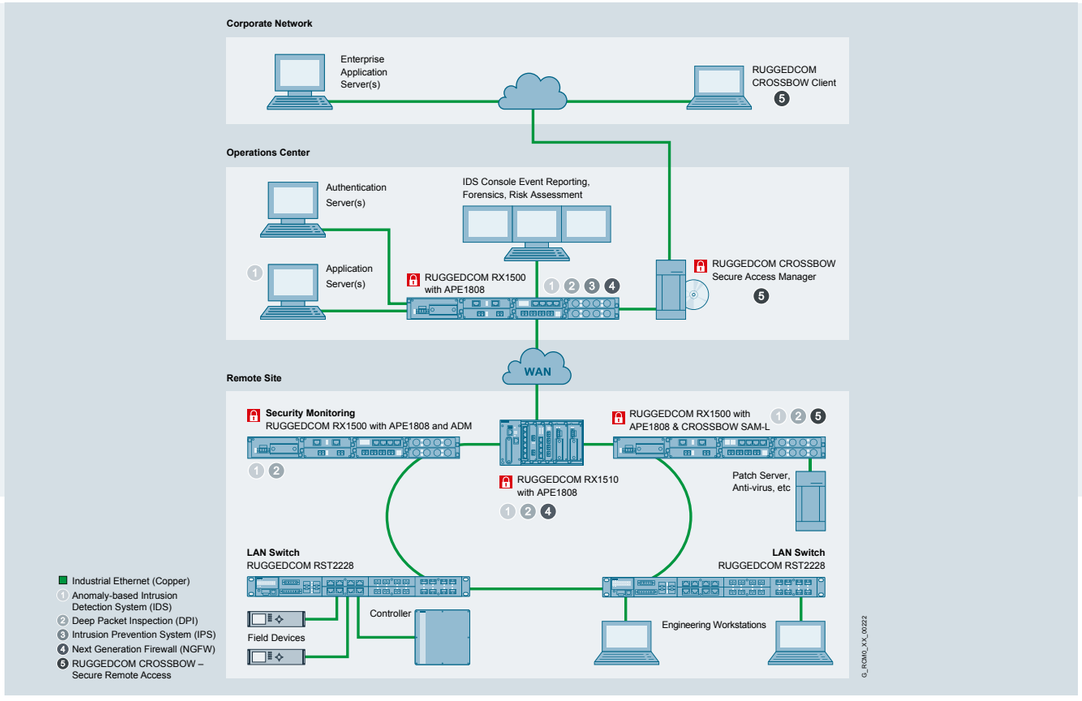


© Siemens 2020

MORE ON INDUSTRIAL SECURITY

## Application example

# Cybersecurity solutions with RUGGEDCOM




RUGGEDCOM cybersecurity solutions hosted on the RUGGEDCOM APE1808

### Task

Secure a typical OT network in harsh environments from malicious events (cyberattacks, malware, misuse and unauthorized access) without affecting network availability

### Solution

RUGGEDCOM APE1808 installed with a NGFW application is used with the RUGGEDCOM RX1510 gateway router for application level protection from cyberattacks. It is also equipped with an integrated Intrusion Prevention System (IPS) to monitor activity, prevent suspicious behavior and report events to a SIEM server.

Integrated Intrusion Detection System with Deep Packet inspection for OT protocols (IDS/DPI) solution is installed on the APE1808 module in the Operations Center and at the remote site to collect, analyze and report on all traffic passing through the sensor (Northbound or Southbound).

RUGGEDCOM CROSSBOW Secure Access Manager in the Operations Center and the CROSSBOW SAM-L installed on the RUGGEDCOM APE1808 in the remote site router provide NERC-CIP compliant remote access.

### Advantages at a glance

- Passive implementation of a comprehensive cybersecurity solution with zero disruptions
- Includes real time monitoring and risk alerts with IDS, analysis of OT protocols with DPI, Next Generation Firewall and IPS for blocking threats and secure remote access to the field assets
- Eliminates the need for specialized cybersecurity appliances, reducing training and operational costs
- One box integrated solution with the RUGGEDCOM Multi-Service Platform and APE1808 with bundled software from leading cybersecurity providers
- All in one customized hardware, software and services solution offered by Siemens Professional Services

# SIMATIC PCS neo Security and SIMATIC PCS 7 Security

**SIMATIC PCS neo Security**

The 100% web-based SIMATIC PCS neo process control system also relies on the proven defense in depth strategy. The issue of security is also top priority in SIMATIC PCS neo. Evidence of this can be seen in the TÜV certification of the product life cycle process based on IEC 62443-4-1. Security is a “built-in” element of SIMATIC PCS neo. This means that comprehensive protection is guaranteed from the outset. Unneeded functionalities can be turned off when required in order to adapt systems to individual requirements.

The access protection of SIMATIC PCS neo is multifaceted. Of course, all functionalities and interventions require a corresponding authentication and authorization. In the case of especially critical functionalities, two-factor authentication is required in order to guarantee maximum security. In addition, the system provides a central user administration.

**SIMATIC PCS 7 Security**

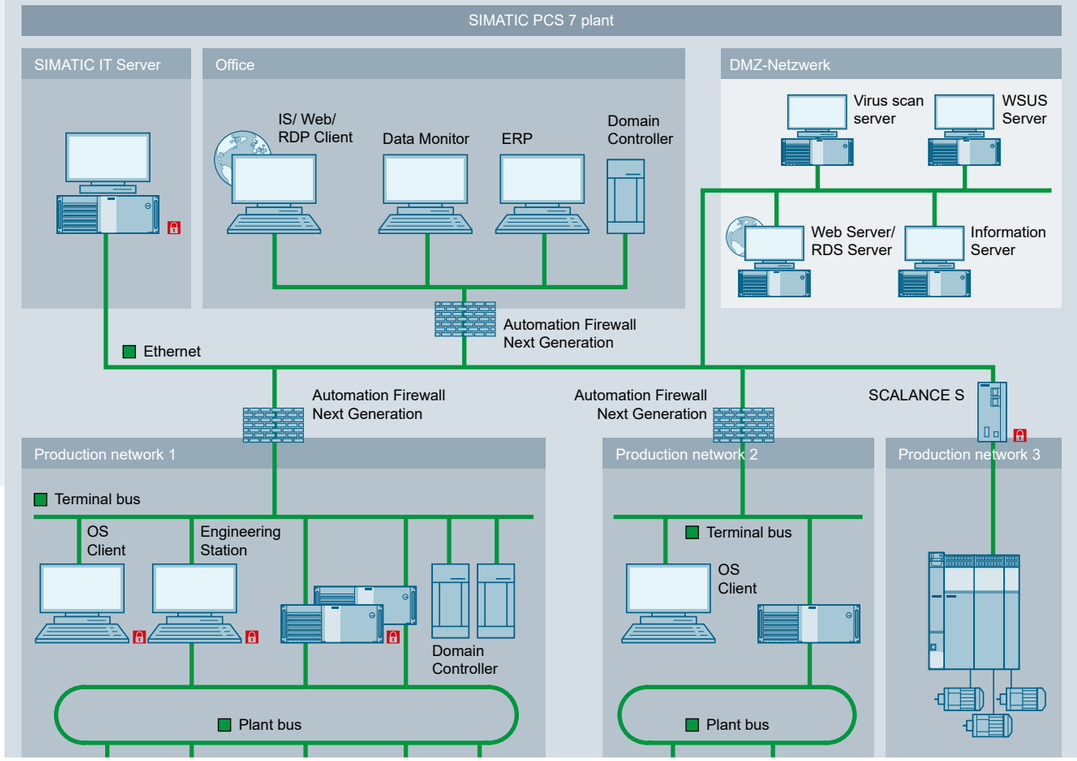
A top priority in SIMATIC PCS 7 is that operating personnel always retain control over production and processes even when security threats occur. Full operator control and monitoring capabilities are to be retained when actions are being taken to prevent or contain security threats in plants and networks. The purpose of the security concept for SIMATIC PCS 7 is to ensure that only authenticated users can perform authorized operator inputs on authenticated devices using the possible operator inputs assigned to them. These operator inputs may only be performed using clearly-defined and planned access paths in order to ensure reliable production or coordination of an order without endangering people, the environment, the product, the goods to be coordinated or the company’s business. The SIMATIC PCS 7 security concept describes a defense in depth strategy based on the international standard IEC 62443. The implementation of this strategy in a system is described in detail in “PCS 7 Compendium Part F - Industrial Security“. SIMATIC PCS 7 is certified based on this recommended system configuration in accordance with IEC 62443-3-3 (TÜV Süd).



© Siemens 2020

MORE ON INDUSTRIAL SECURITY

# SIMATIC PCS 7 Security




SIMATIC PCS 7 Security – secure architecture from defense in depth

Multiple protection levels are created in order to minimize risks and to increase the security of systems.

**Elements of the SIMATIC PCS 7 Security concept**

- Physical access protection
- Cell segmentation using firewalls
- System hardening
- Patch Management
- User administration (SIMATIC Logon)
- Malware detection and prevention
- Training and processes

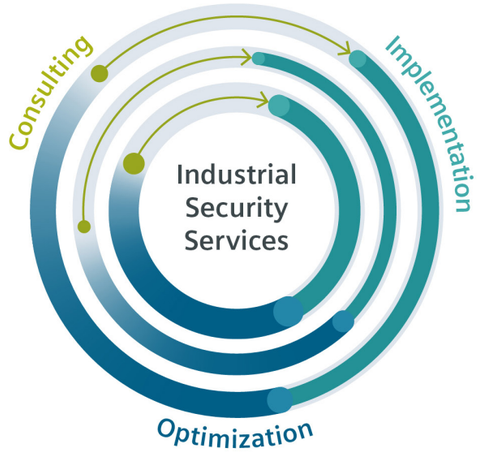
- Access protection: systems and access controls secured by factory security including access authorizations by means of typos
- Firewalls: segmentation of networks, formation of perimeter networks (DMZ), restriction and logging of network communication
- VPN: use for encrypted communication between networks (e.g., remote access)
- Whitelisting: specification of the programs which are permitted to be run on your system
- Patch management: the system is kept current using an update strategy (e.g., with operating system, software and firmware updates). This minimizes the risk of an attack on known security gaps.
- User administration: use of a central user administration in order to explicitly define access rights, group memberships, roles and policies for system users. This is done following the principle of limiting rights to those needed for the respective task.
- Virus scanner: use of an up-to-date virus scanner to minimize the risk of harm and negative impacts on systems and system operation.
- Regular training of all personnel for the purpose of adhering to all defined processes and ensuring the security of the system.

# Industrial Security Services

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

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

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




## Security Consulting for a risk-based security roadmap

Security Consulting includes comprehensive analysis of threats, identification of risks and concrete recommendations of security measures.

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

## Security Implementation for risk reduction measures

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

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

## Security Optimization for comprehensive, continuous protection

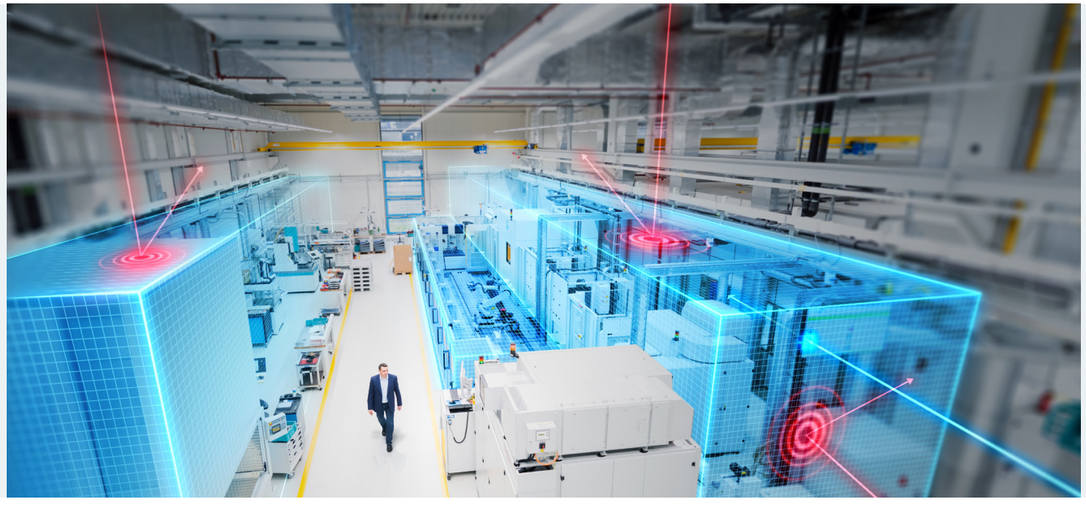
Security Optimization means continuous monitoring, regular adjustment and updating of the implemented measures through our security tools.

- You benefit from: maximum transparency with regard to the security status of your plants and proactive prevention of potential threat scenarios thanks to our security tools which are designed specifically for your industrial environment.



© Siemens 2020

# Automation Firewall Next Generation



In order to avoid the loss of production and downtimes, the data traffic between networks must be checked, analyzed and selectively released without affecting the process control system function. This is the only way to optimally protect the system without any disadvantages for productivity. Firewalls with complementary services are predestined for this. With the Automation Firewall Next Generation, Siemens offers a tested and validated standard firewall in three performance classes (220, 820, 850). It is designed for use with SIMATIC PCS 7 and WinCC.

The Automation Firewall Next Generation cooperates perfectly with the communication products of SIMATIC NET. It features comprehensive hardware and software functions for SIMATIC PCS 7 and WinCC projects, e.g.,

- Application Layer and Stateful Inspection Firewall
- Classification of all applications, on all ports, at any time
- Enforcement security policies for each user and site
- High availability (active/active and active/passive)
- Redundant power supply input for increased reliability (PA-220 and PA-850)
- Hardened operating system (PanOS is Linux-based)
- Possibility to check Layer 7 traffic, such as of the S7 protocol (detection of start, stop, read, write) or of OPC
- Secure System Architecture

**Advantages at a glance**

- Tested and released for SIMATIC PCS 7
- Protection against known and unknown threats
- Very good value for money
- First-class firewall solution for the segmentation of IT/OT networks based on the «Zones & Conduits» model of IEC 62443
- Time savings, as many application protocols are integrated by default

**Service by Siemens**

- Checking the plant network
- Development of a perimeter firewall concept
- Installation and configuration of a perimeter firewall in automation systems
- Documentation of the firewall configuration

**Support by Palo Alto Networks (3 or 5 years)**

- Premium Support Available 24/7
- Spare parts shipment and hardware replacement the following working day
- Feature releases and software updates, updates for subscriptions
- Documentation and FAQs, online portal for customer support



MORE ON INDUSTRIAL SECURITY

# Terms, definitions

### Cybersecurity

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

### Demilitarized zone (DMZ)

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

### Firewall

Security components which allow or block data communication between interconnected networks according to specified security restrictions. Firewall rules are 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 a 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 involves the disabling of unneeded interfaces and ports, thereby reducing the vulnerability of the network to external and internal attacks. Every level of an automation system is considered: the control system, network components, PC-based systems and programmable logic controllers.

### Virtual Private Network (VPN)

A VPN tunnel connects two or more network nodes (e.g., security components) and the network segments behind them. Encrypting the data within this tunnel makes it impossible for third parties to listen in on or falsify the data when it is transmitted over a non-secure 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 network, which exists only once physically. 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 which are actually required can be executed.



© Siemens 2020

## Get more information

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF (6ZB5530-1AP02-0BB0)
BR 1120 36 En
Printed in Germany




## Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place.

For additional information on industrial security measures that may be implemented, please visit
**https://www.siemens.com/industrialsecurity**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under
**https://www.siemens.com/industrialsecurity**