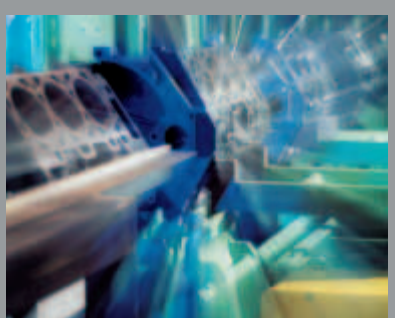
Industrial security
Security for network and data

Brochure • April 2006

simatic net
SCALANCE S



SIEMENS

SCALANCE – scalable performance

Totally Integrated Automation from Siemens demonstrates in a host of successful applications around the world the extent to which integrated solutions can be created today with shared tools and standardized mechanisms. Selective further development of industrial communication with SIMATIC NET is linked with this at a fundamental level.

A pioneering milestone in this development is SCALANCE, the new generation of active network components for establishing integrated networks.

These active network components are optimally coordinated with each other. They have been designed for harsh industrial environments and enable integrated, flexible and secure setup of a high-performance network.

SCALANCE

S Security

SCALANCE S –
for industrial security

Thanks to security mechanisms such as authentication, data encryption or access control, SCALANCE S protects networks and data within an organization against spying, manipulation and unauthorized access.

SOFTNET Security Client enables secure access to devices protected by SCALANCE S

W Industrial Wireless LAN

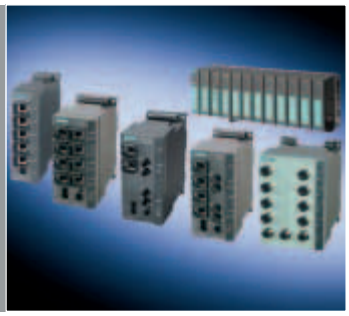
SCALANCE W –
reliable radio technology for Industrial Wireless LAN

Based on Industrial Wireless LAN, SCALANCE W supports integrated communication into areas that until now have been difficult or even impossible to access. It does this by reserving data rates or monitoring the wireless connection. SCALANCE W uses the WLAN standards in accordance with IEEE 802.11a/b/g/h.

X Switched Networks

SCALANCE X –
Industrial Ethernet Switches from the entry level to high-performance networks

SCALANCE X offers a graded portfolio of Industrial Ethernet switches with different functions, e.g. for diagnostics via PROFINET, SNMP or the Internet, to meet different requirements such as network structure, data rate and number of ports.



Industrial security with SCALANCE S

Modern automation technology is based on communication and the trend toward increased networking of individual production islands. It is becoming more and more important to integrate all the manufacturing components into an end-to-end network that merges with the office network and the corporate Intranet. This applies also to the use of IT mechanisms, such as Web servers and e-mail with programmable controllers, as well as to the use of wireless LANs.

The integrated networking of individual automation components with each other or with components from the office IT world offers the possibility of using familiar technologies from the office area in conjunction with the automation network. However, this simultaneously constitutes an increased danger in the form of attacks from the external network.

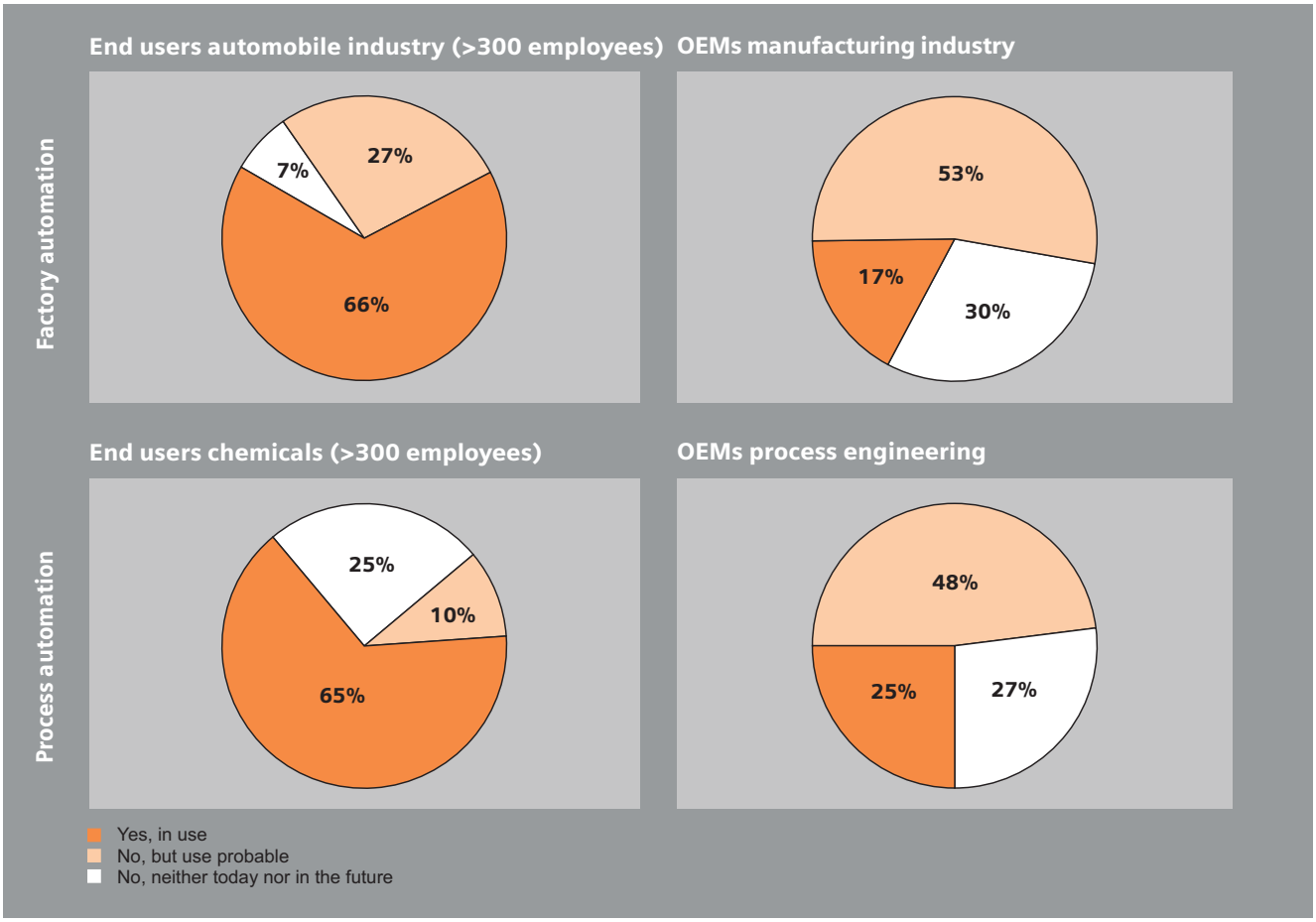
Interaction with the IT world results in industrial communication being exposed to the hazards familiar from the office and IT environment, including hackers, worms and Trojan horses.

It is necessary to reliably protect automation networks against unauthorized access and interference from the external network. Current security concepts are especially designed for the office world and require constant administration and specialist knowledge. They are not usually conversant with the typical protocol landscape of industrial communication and are not equipped to withstand the special environmental conditions involved.

The need for network security is increasing

An independent market study has analyzed the status of network security for users of Ethernet networking solutions in production and automation networks, and investigated the potential hazards from the viewpoint of Ethernet users. The study shows that network security products are already used to a large extent for protecting the network or they are planned for future use.

Use of network security products



Industrial security – security in automation engineering

The attempt to use typical IT strategies from the office world is generally doomed to failure because the automation level presents a different context with different security aims than the office area (e.g. other requirements, other risks).

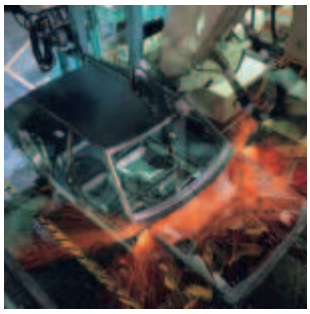
The direct integration of IT security into the automation solution has a decisive advantage over conventional IT solutions because only this avoids any conflict or negative mutual influence between the aims of IT security and those of the automation application.

Industry is experiencing three trends that are already making their influence felt and will continue to do so in the future:

- Production and office networks are increasingly merging: As a result, the same technologies are used in the office environment and the production environment (e.g. Ethernet), resources are shared (e.g. uniform network), and problems and dangers familiar from the IT world (e.g. viruses) are transferred to the automation level.
- Software and software-based systems play an increasingly important role for the production sequence, with the result that typical IT requirements from the office world also become relevant for the automation level.
- Since the IT world is still extremely heterogeneous in many companies, there is a tendency in every industrial sector toward IT consolidation resulting in reorganization and rationalization of company-wide infrastructures. The production plants are included here.

Benefits of industrial security

- High IT security of the plant or machine
- More stable systems thanks to rugged components
- Avoidance of possible costs involved in subsequent closing of security gaps or in damage limitation
- OEMs can meet end customer demands with regard to security
- Legal requirements in the security environment can be easily met
- Improved handling of security updating (patch management, updates, etc.)

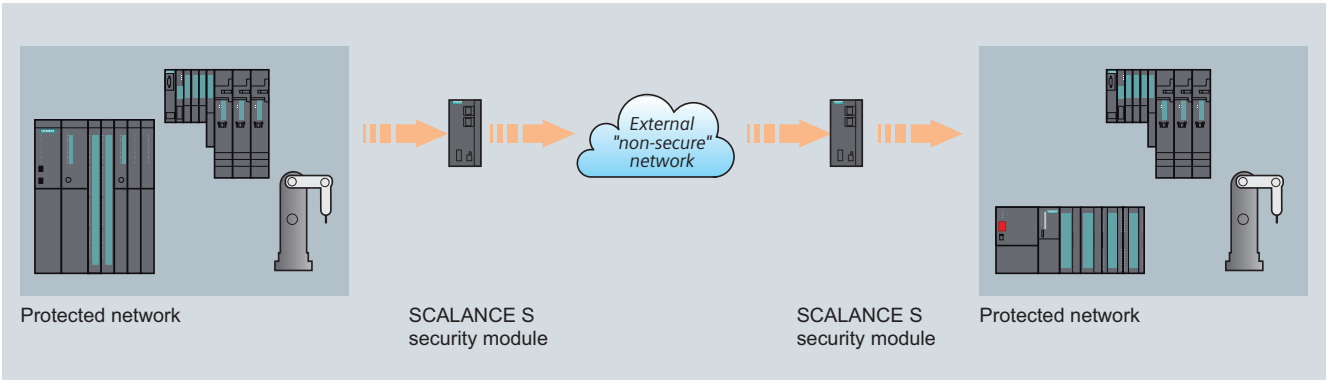


With its security concept, Siemens offers a security solution specially designed for industrial automation engineering that satisfies the specific requirements of industrial communication. The concept uses the integrated Ethernet structures and protects the production areas and other sensitive areas within the company against the risks associated with Internet technology.

Siemens is the only global player in automation engineering that has all the expertise and products for IT security at its disposal: From the network infrastructure to the automation technology itself, Siemens is the only manufacturer in the world to offer all the necessary components.

SCALANCE S protects automation cells against unauthorized access and unnecessary communication load. Even in the event of interference in the external network, data traffic within the automation cell remains unaffected.

SCALANCE S modules protect communication independently of the application protocol used. All IP-based protocols and the still widely used Layer-2 protocols of automation engineering can be easily protected in this way without restricting permissible productive data traffic.



Secure communication with SCALANCE S

Segmented networks with SCALANCE S

With the security concept SCALANCE S, the network can be segmented for security purposes. This offers crucial advantages.

The security modules support learning mode. They automatically detect every station (also other security modules) in the network. The stations thus do not have to be configured and when a plant is expanded, existing security modules do not have to be reconfigured.

Advantages of the industrial security concept:

- Protection against spying and data manipulation - diagnostics and logging of attempted attacks
- Protection against overloading of the communication system
- Protection against mutual influence
- Protection against addressing errors
- User-friendly and simple configuration and administration without specialist knowledge of IT security
- No changes or modification of the existing network structure are necessary
- No changes or modification of the existing applications of the network stations are necessary
- Scalable for different security requirements
- Rugged, industry-compatible design

Products for secure communication

SCALANCE S security modules

SCALANCE S security modules offer scalable security functionality:

- Stateful Inspection Firewall for protecting the programmable controllers from unauthorized access regardless of the size of the network to be protected.
- Supplementary or alternative VPN (Virtual Private Network) for reliable authentication of the communication partners and encryption of the transmitted data

SCALANCE S602

- Protects with Stateful Inspection Firewall, address conversion (NAT/NAPT), DHCP server and Syslog

SCALANCE S612

- Protects with Stateful Inspection Firewall
- Protects up to 32 devices while supporting up to 64 simultaneous VPN tunnels

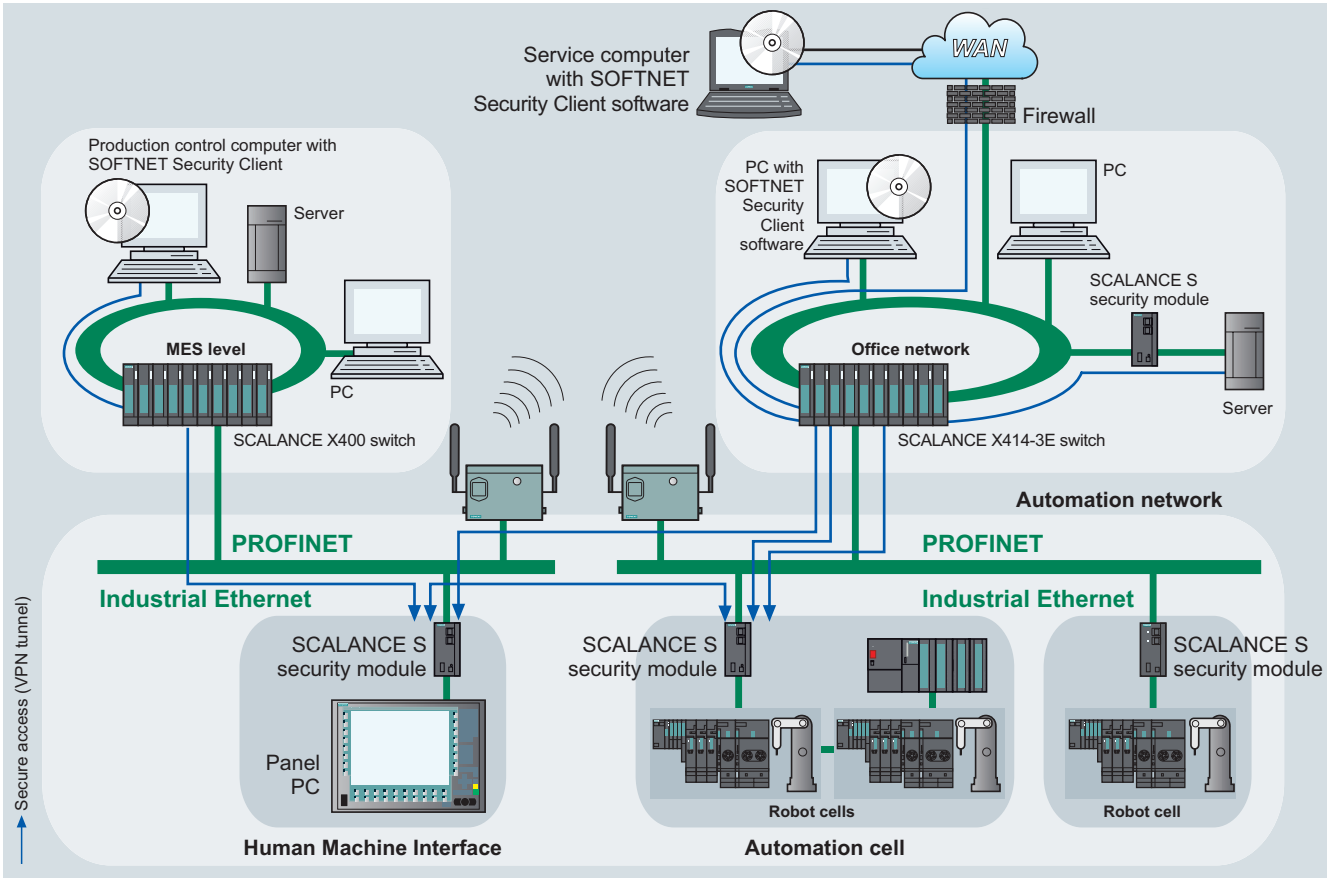
SCALANCE S613

- Protects with Stateful Inspection Firewall
- Protects up to 64 devices while supporting up to 128 simultaneous VPN tunnels
- Extended temperature range from -20 °C to +70 °C

SOFTNET Security Client

The SOFTNET Security Client software is used as the VPN client for programming devices, PCs and notebook computers in the industrial environment.
It permits secured VPN-Client access to automation systems protected by SCALANCE S.

Secure communication between programmable controllers with SCALANCE S



Applications and solutions
Protection of the production network when combined with the office network

Task specification

- The production network must be protected against unauthorized access from the office network and the automation cells must be protected against mutual influence.
- Integration from the control level to the field level must be enabled in order to be able to generate integrated diagnostics for field devices and network components.
- Cells with predominantly identical structures (same private IP addresses) must be protected against unauthorized access.
  - A Syslog server is to log all accesses, e.g. hacker attacks, or overloads.
  - Process data such as unit quantities, product numbers and type designations are to be recorded.
- Configuring must be easy to carry out since personnel without expert security knowledge is to implement startup and service.

Solution

SCALANCE S602 can be used as a firewall to filter data packages and to permit communication connections that comply with the firewall rules. Incoming and outgoing communication can also be filtered in the same way as IP and MAC addresses, and communication protocols (ports). In addition, an overload limit can also be set.

The firewall integrated into the security modules can be configured in such a way as to permit access to specific stations only.

The logging functionality enables access monitoring and logs accesses and attempted attacks to enable preventive measures to be taken.

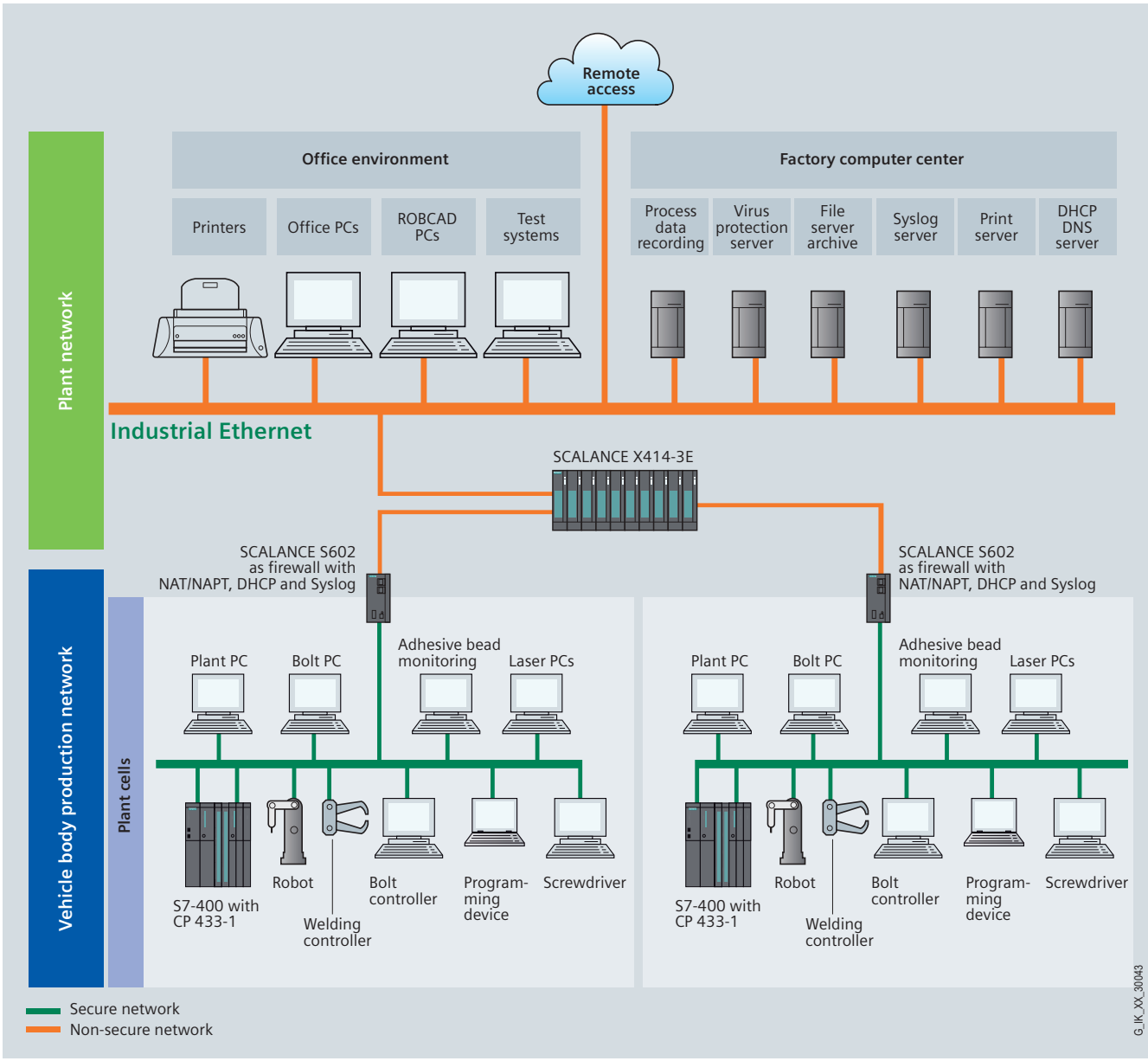
IP address conversion is necessary for effective protection of identically structured cells. SCALANCE S602 security modules with NAT/NAPT functionality are used for this purpose.

Syslog information such as process data is automatically sent to the Syslog server.

This effectively protects the production network against unauthorized access from the office network but it also secures the office network against influence from the production network.

Benefits

- Protection of the plant against unauthorized access and communication overload through the use of SCALANCE S
- Effective protection against mutual influence between the production network and the office network
- Continuous monitoring of accesses to the production network
- Cost savings through saving on public IP addresses
- Simple maintenance and diagnostics since all protected cells have the same structure



Plant network protected with SCALANCE S

Protection of the automation system against influence from the office network

Task specification

- The automation system must enable integration from the control level to the field level and thus also integrated diagnostics for field devices and network components.
- The system must be expandable for other applications thanks to the use of open standards as well as future-oriented bus systems.
- The security mechanisms must rule out possible dangers such as the influence of overload in the communication system, or faulty access.
- Configuring must be easy to carry out because untrained personnel are to implement startup and service.

Solution

Vertical and horizontal integration is implemented by using the new PROFINET communication standard based on Industrial Ethernet.

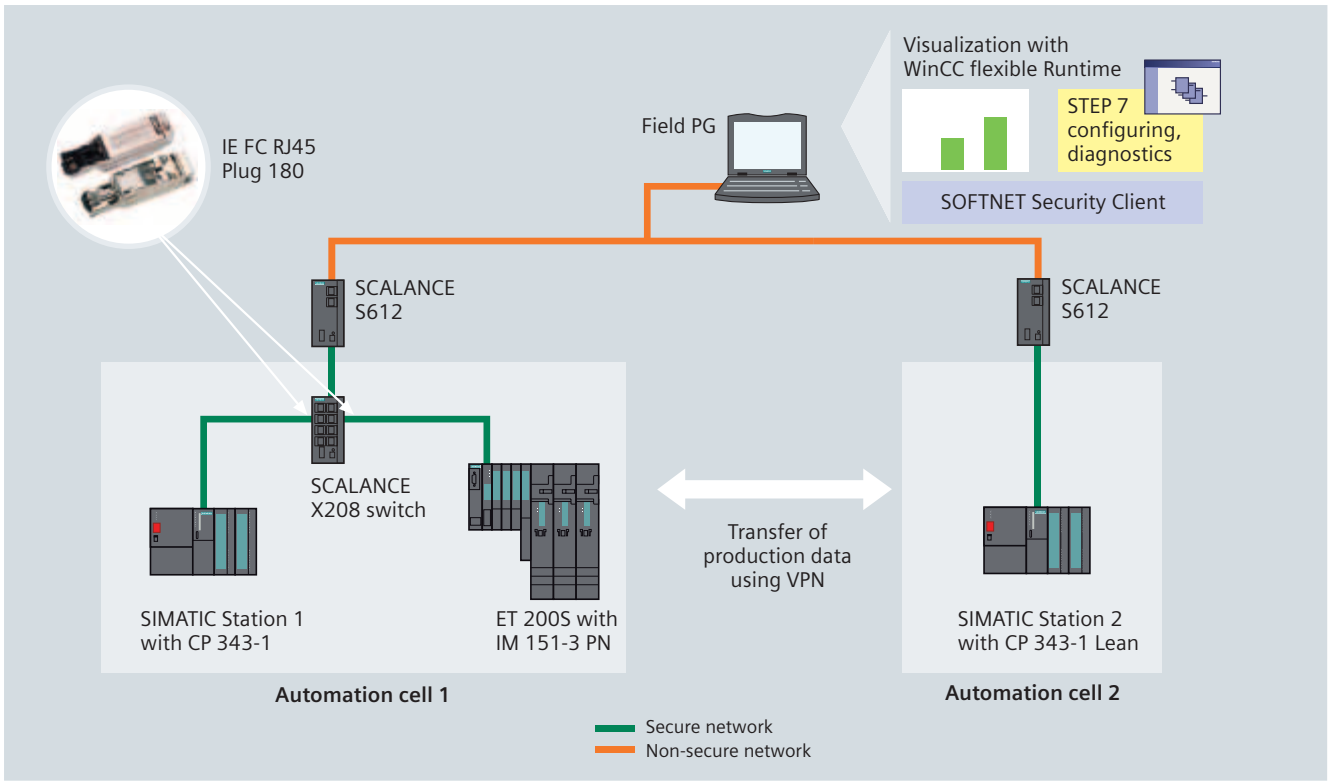
The network structure is based on Industrial Ethernet switches of the SCALANCE X-200 product family. The SCALANCE S-600 security modules, operated as a firewall, are used for protecting the automation network against influences from the office network.

The firewall filters data packets and disables or enables communication links in accordance with the filter list (packet filter firewall). Incoming and outgoing communication can also be filtered in the same way as IP and MAC addresses as well as communication protocols (ports). In addition, an overload limit can also be set.
The firewall integrated into the security modules can be configured in such a way as to permit access to individual stations only.
The logging functionality enables access monitoring and it logs accesses and attempted attacks to enable preventive measures to be taken. This data is saved by the security module in a log file.

Benefits

- Protection of the plant against unauthorized access and communication overload through the use of SCALANCE S
- Simple and reaction-free integration into existing networks
- Higher data throughput thanks to the use of Industrial Ethernet
- Greater flexibility through the use of open standards
- Simpler configuring of the diagnostics both of the SCALANCE X network components and the field devices
- Simpler maintenance through centralized diagnostics functions

Protection of automation cells using VPN tunnels



Encrypted data security

Task specification

- Programmable controllers must also be protected within the automation cell without their own security functionality.
- Existing network settings such as topologies, addresses or the protocols used must remain unchanged by the implementation of security.
- Mechanisms for authentication and data encryption must be used to prevent falsification of IP addresses, manipulation and spying.

Solution

VPNs (Virtual Private Networks) enable secure authentication of the communication stations and encryption of data transmission.

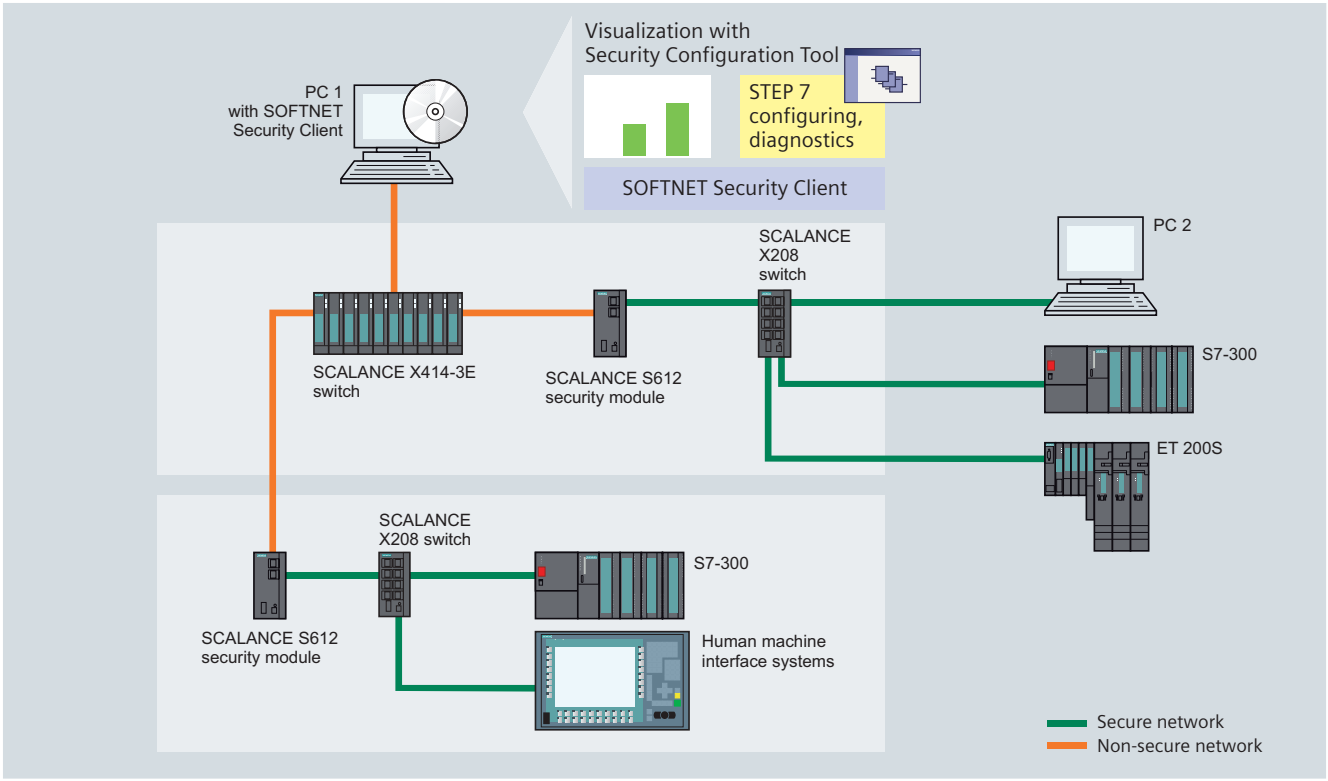
The SCALANCE S security modules are used for protecting automation networks and for secure data exchange between automation systems. They only allow communication between authenticated and authorized devices. This protects against operator error, prevents unauthorized access, and avoids interference and communication overload.

In addition, data transmission is encrypted and thus protected against spying and manipulation.
The SOFTNET Security Client software is used for establishing secure VPN connections of PGs/PCs with network segments. This permits secure VPN client access from PCs/notebook computers to automation systems or cells protected by SCALANCE S.

Benefits

- Extended protection of the plant against unauthorized access, manipulation, spying and communication overload thanks to the use of VPN technology with SCALANCE S and SOFTNET Security Client
- Easy configuring of the security mechanisms is possible without specialist knowledge
- No changes or modifications need to be made to the existing network structure/applications or network stations, and thus simple integration into existing structures is possible.

Protection of automation cells using a firewall



Data protection with mobile communication

Task specification

- Mobile access for commissioning, service and maintenance of field devices, control engineering and mobile operator control and monitoring must only be enabled for authorized personnel.
- Personnel must be able to move freely and have access to the data of machines and controller sections within the radio field.
- This should minimize downtimes and personnel costs.
- Indoor and outdoor use of the components must be possible.
- Configuration of restricted access must be as easy as possible to parameterize since the plant is operated exclusively by automation engineers.

Solution

The radio field is planned and the coverage checked in advance to ensure optimum coverage of the wireless area.

A SCALANCE W788-1PRO access point is used for coverage of the affected area. It can be used both indoors and outdoors thanks to its rugged metal housing in degree of protection IP65. Stations can move freely within the radio field thanks to the roaming function of Industrial Wireless LAN (IWLAN).

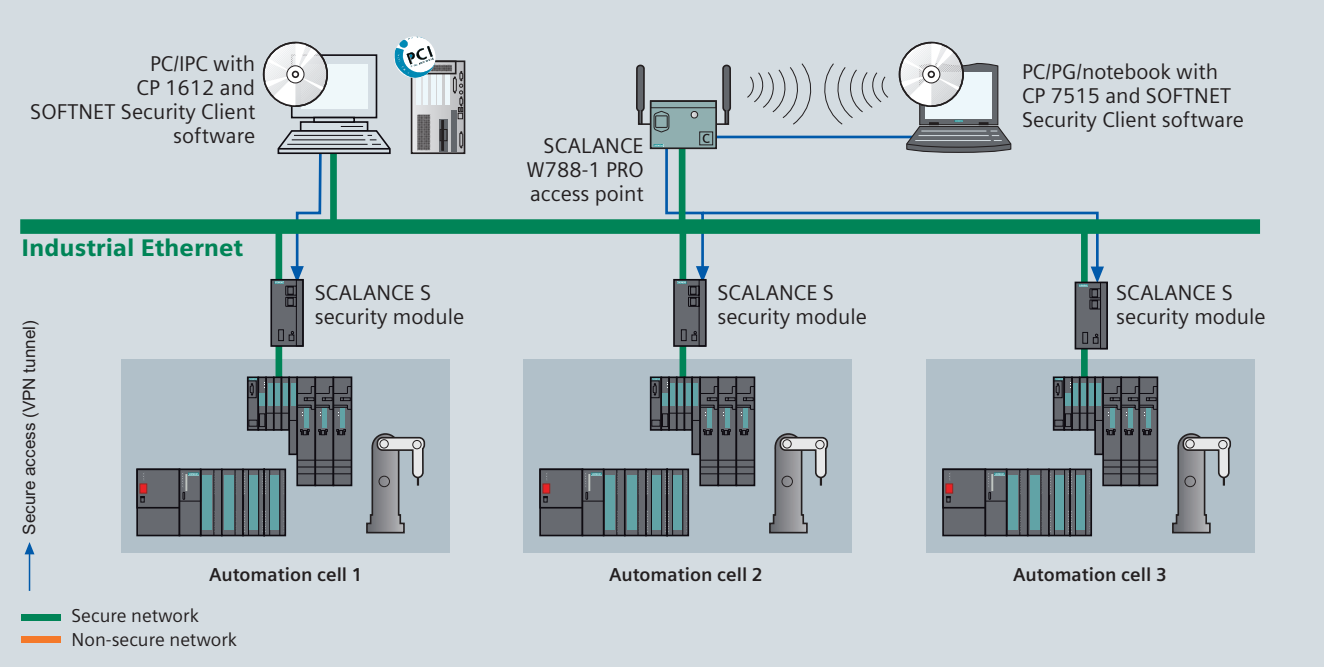
A Field PG is used as a mobile terminal unit.

The use of SCALANCE S security modules and the SOFTNET Security Client software implements secure authentication of the communication stations and encryption of data transmission through VPN tunnels. Operator errors and unauthorized access are prevented along with spying and manipulation.

Benefits

- Mobile communication is protected against unauthorized access, manipulation, spying and communication overload
- Simple integration of other mobile stations even into existing automation systems
- Saving of service and maintenance resources
- Easy configuring of the security mechanisms, without specialist knowledge

Secure access to automation cells protected by SCALANCE S with SOFTNET Security Client



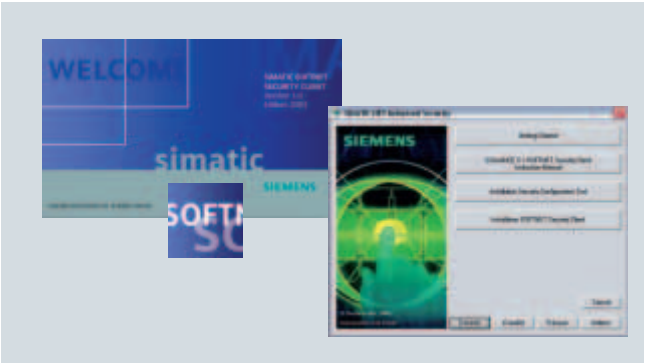
Acknowledged security

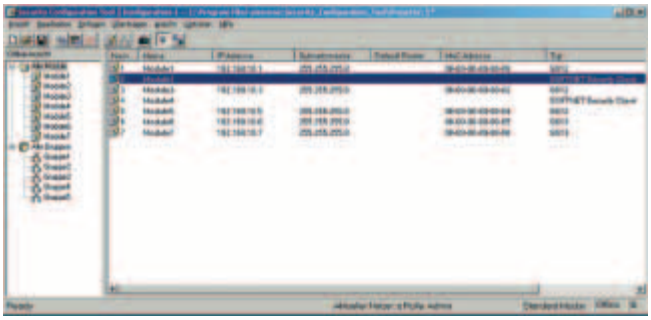
The SCALANCE S family was subjected to a security evaluation by the company "escrypt GmbH" (*www.escrypt.com*) which concluded that "...the security module (SCALANCE S) allows allround secure configuration through manual tightening of the rules... The device can be easily integrated into existing networks thanks to its bridge functionality. The security module performs its task and secures an automation network. Simplicity of configuring without detriment to security is a feature worth emphasizing here. The SCALANCE S602 module has an extremely rugged design and meets the special requirements of the automation sector extremely well."

The SIMATIC NET security products also fulfill the requirements laid out in the PROFINET Security Guideline (*www.profinet.com*)

SCALANCE S602/S612/S613 security modules

- The security modules protect automation networks and enable secure data exchange between automation systems
- Security modules only permit communication between authenticated and authorized devices:
  - Protection against operator errors
  - Prevention of unauthorized access
  - Prevention of interference and communications overload
- Encryption of data transmission
  - Protection against spying
  - Protection against manipulation
- Easy handling thanks to minimal configuration and no special knowledge of IT security is required
- No changes or modification of the existing network structures, applications or network stations are necessary
- The security of the communication is independent of the protocol used (PROFINET, Ethernet/IP, MODBUS TCP, etc.)
- Module replacement without the need for a programming device, using the C-PLUG swap medium for backing up the configuration data (not included in the scope of supply)





SOFTNET Security Client

The SOFTNET Security Client is an integral component of the industrial security concept for protecting automation devices and for security during data exchange between automation systems:

- Integrated, intuitive configuring without specialist security knowledge
  - A shared configuration tool with a shared database for SCALANCE S and SOFTNET Security Client
  - Automatic generation of the certificates through Security Configuration Tool
  - Automatic learning of the stations of the internal network and detection of SCALANCE S modules in the external network
- Uses the tried and tested IPSec mechanisms for setting up and operating VPNs.
- Gives programming devices, PCs and notebooks secure access to programmable controllers or complete automation cells protected by SCALANCE S

Security in automation with solution partners

Initiation of the security process

Production networks are turned into open networks when linked to an office network through increased use of Industrial Ethernet and IT solutions. But security risks increase in direct proportion to the growth in ways of accessing the network. Security concepts designed and implemented by experts counter these risks.

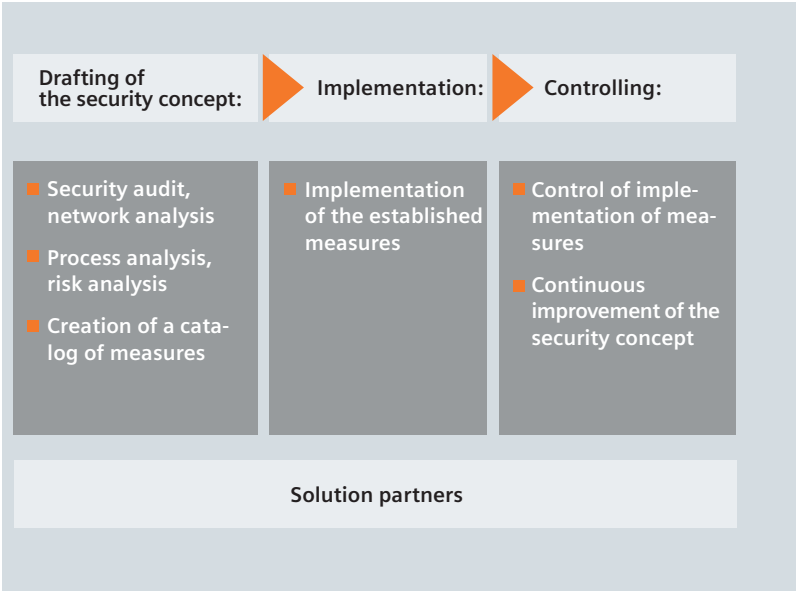
The aim of a security concept is to minimize or eliminate all potential risks. Our solution partners are specialists in the area of data security with experience in the office area. They offer comprehensive consulting for an optimally adapted and cost-efficient security concept with different measures. These are carried out depending on the potential danger and graded to the desired security level.

Your benefits

- Up-to-date expert knowledge for data security
- Comprehensive consulting
- Individual, custom-tailored security concept
- Professional implementation of the security measures
- Accompanying support

Risk analysis of the existing networks is a central component and must take a holistic approach. It covers the Internet-Intranet interface as well as the wireless LAN infrastructures and makes use of valid technical standards in doing so.

An exclusively technical solution, such as the installation of a firewall or the use of a security appliance for specific production cells, is not sufficient. What is important are additional personnel and organizational measures that must ensure that the drafted security concept can also work in reality. Security cannot be achieved with temporary measures but only through a continuous process.

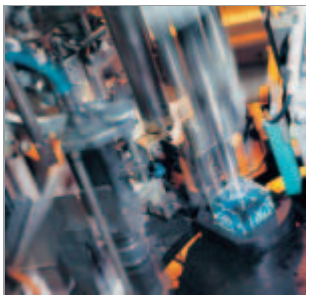


You can find more information in the Internet at:
http://www.siemens.com/simatic-net/partner

Advantages of industrial security at a glance

- **Protection from:**
  - **- Unauthorized access**
  - **- Spying**
  - **- Manipulation**
  - **- Excessive communication load**
- **Can be used without specialist security knowledge**
- **Use of field-proven and certified security standards**

- **No changes or modification of the existing network topologies, applications or network stations are necessary**
- **Low configuring overhead thanks to automatic learning of the protected network stations and automatic generation of the certificates by the configuring tool**
- **Rugged, industry-compatible design**



Further information

- **You can find more information on industrial security in automation at:**
  www.siemens.com/industrial-security
- **Visit our SIMATIC NET homepage in the Internet:**
  www.siemens.com/automation/simatic-net
  Here you will find information about products and solutions, all the latest news about SIMATIC NET as well as information about events and technical publications.
- **For a personal discussion, you can locate your nearest contact at:**
  www.siemens.com/automation/partners
- **In the A&D Mall you can place orders electronically using the Internet:**
  www.siemens.com/automation/mall

In various SIMATIC NET components (e.g. SCALANCE, OSM/ESM, CPs with IT functions), extensive parameterizing and diagnostics functions (e.g. Web server, network management) are made available via open protocols and interfaces. These open interfaces provide access to those components and could also be used for illicit activities.
When using the above-mentioned functions and these open interfaces and protocols (such as SNMP, HTTP and Telnet), suitable security measures must be implemented that block unauthorized access to the components or the network especially from the WAN/Internet.
For this purpose, automation networks must be isolated from the remaining corporate network using appropriate firewall systems such as SCALANCE S.

Subject to change without prior notice | Order No. 6ZB5530-1AP02-0BA0 | Dispo 26000 | BS 0506 5. ROT 16 EN / 601319 | Printed in Germany |

www.siemens.com/industrial-security

Siemens AG

Automation and Drives
Industrial Communication
Postfach 48 48
90327 NÜRNBERG
GERMANY

www.siemens.com/simatic-net