SIEMENS

More security where it matters in industrial automation

The comprehensive range for protecting your plant

Industrial Security

siemens.com/industrialsecurity

Systematic minimization of potential hazards

Due to the increased use of Ethernet connections all the way down to the field level, the associated security issues are also gaining in importance in industry. After all, open communication and increased networking of production systems involve not only huge opportunities but also high risks. To provide an industrial plant with comprehensive IT security protection against attacks, the appropriate measures must be taken. Siemens supports you in selectively implementing these measures – within the scope of our integrated range for industrial security.

Security services for systems and solutions

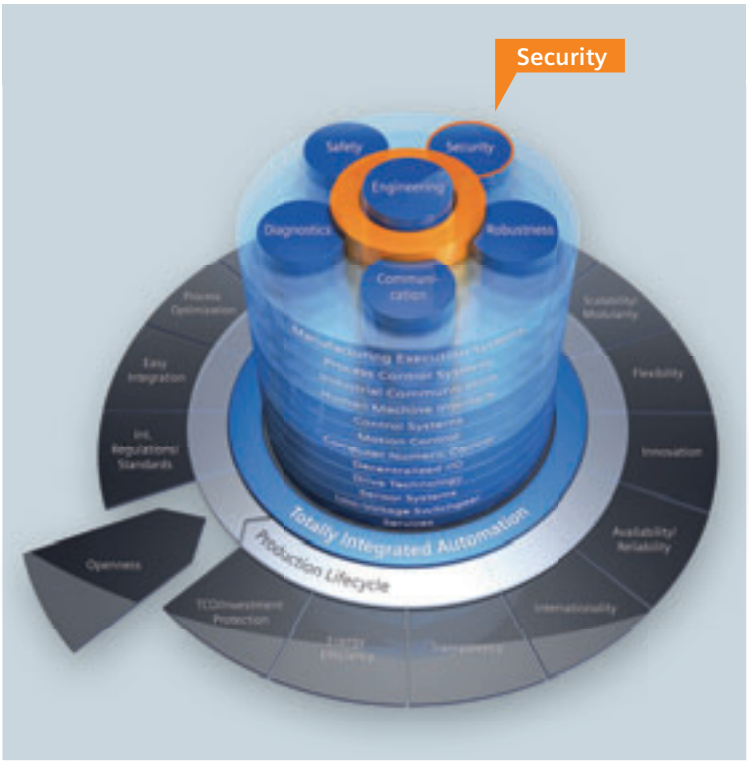
Industrial security cannot be achieved with products and systems alone. As an industry partner, we therefore support you comprehensively in this area – from the initial planning steps, through implementation and operation of a tailor-made security solution, right up to its modernization. Our professional consulting services encompass, for example:

- Establishment and expansion of know-how in **workshops and training courses**
- Analysis of **weak points**
- Configuration of **whitelists and firewall packages**
- Design of **customized** security solutions

Integral security in PCs and controllers

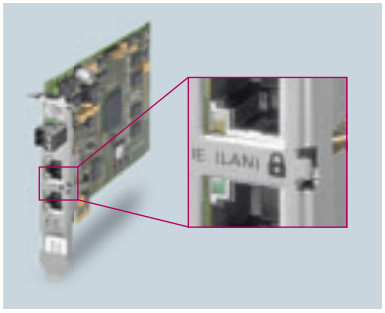
We offer you well thought-out concepts for the security of PCs and controllers, fully in keeping with the spirit of Totally Integrated Automation, our open system architecture for integrated automation.

- User administration and role-based access control with **SIMATIC® Logon** – for SIMATIC engineering and runtime systems
- Know-how protection by means of encryption of the user program for **SIMATIC Controllers**
- Whitelisting for secure operation of our **SIMATIC WinCC** SCADA system and our **SIMATIC PCS 7 process control system**
- Virus scanners for PCs









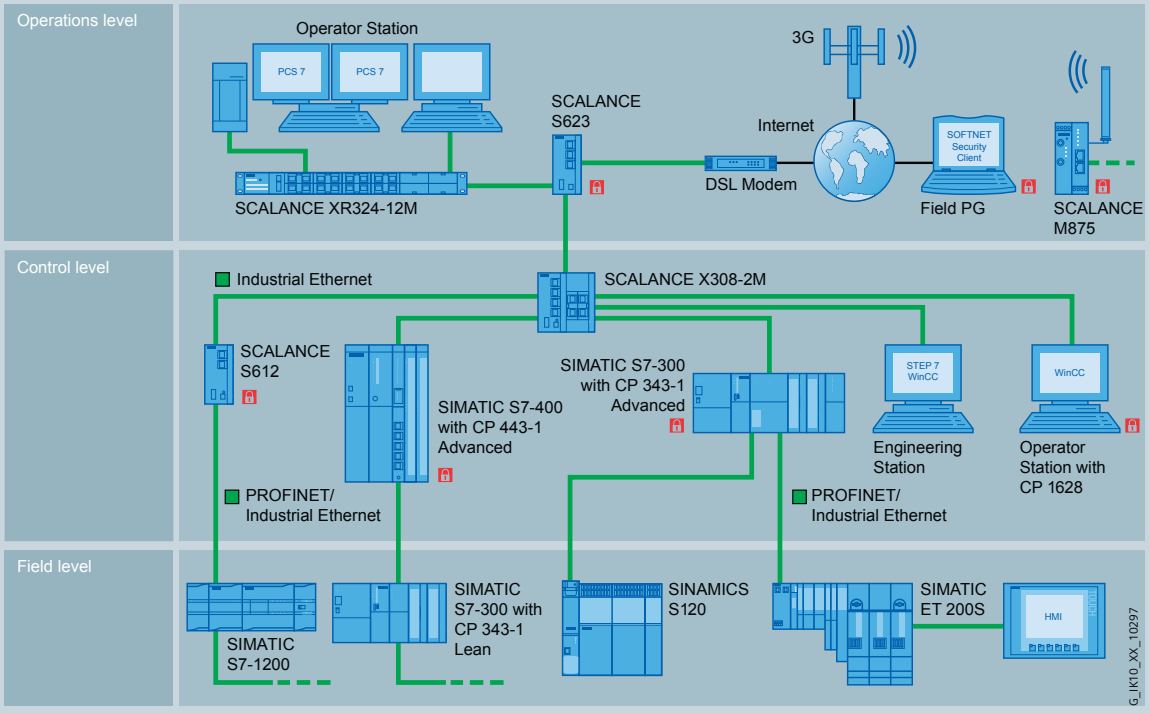
New security products for networking and communication

Protecting industrial communication and reducing the risk of an attack is a key factor for your corporate success. For this reason, we offer you security modules and software, as well as components with Security Integrated for implementing the cell protection concept.

- SCALANCE S security modules, e.g. S623 with additional DMZ (demilitarized zone) port that opens a separate and, if required, restricted network access point for service purposes, e.g. for remote maintenance over the Internet.
- The SOFTNET Security Client software enables access via the Internet or a company Intranet to automation cells or PCs protected by SCALANCE S or a component with Security Integrated.

Security Integrated

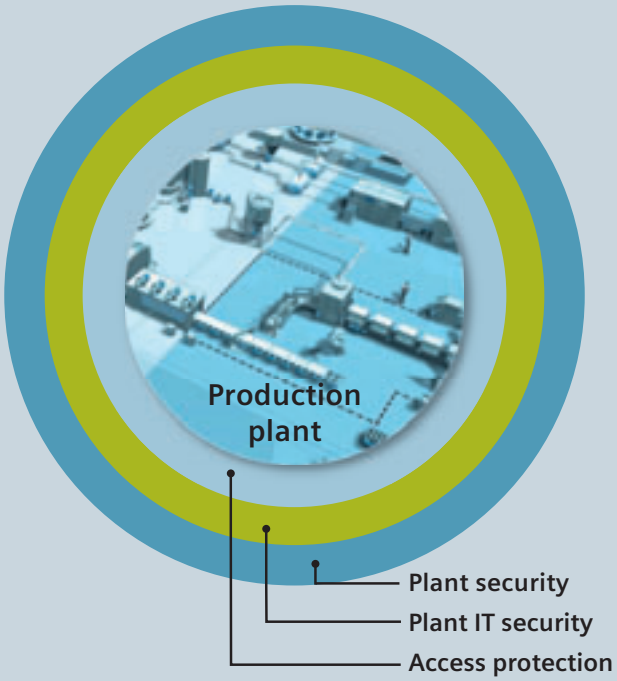
- Protection of controllers of the SIMATIC S7-300 and S7-400 type by means of CP 343-1 Advanced and CP 443-1 Advanced communications processors, whose latest versions contain both firewall and VPN (Virtual Private Network) functionalities.
- Via the CP 1628 communications processor, the industrial PCs are protected by firewall and VPN – for secure communication without special operating system settings. In this manner, computers equipped with the module can be connected to protected cells.
- SCALANCE M875 3G router for secure access to plant sections via the 3G mobile wireless network.



Cell protection concept

With this concept, a plant network is segmented into individual, protected automation cells within which all devices are able to communicate with each other securely. The individual cells are connected to the overall network protected by a VPN and a firewall.

Cell protection reduces the susceptibility to failure of the entire production plant and thus increases its availability. SCALANCE S and components with Security Integrated can be used for implementation.



Only total solutions offer maximum protection

Whether it's a question of inventions, patents, or other intellectual property: It is of crucial importance to your corporate success that you protect your existing know-how efficiently and on a sustained basis against espionage. In addition, you must exclude all unauthorized manipulation to your automation processes right from the start. Only in this way can you guarantee the integrity of your systems. Another important issue: Reliable protection against sabotage, in other words prevention of faults in your production processes, such as plant standstills resulting from a virus attack. Our response to these diverse threats: We view industrial security holistically and design total solutions that offer your plants maximum protection.

Whitelisting
Whether it's persons, companies, or programs: A whitelist – or positive list – refers to a collection of identical elements that are graded as trustworthy. Whitelisting for PCs ensures that only desired programs can be executed.

Key points for efficient industrial security solutions

When planning and implementing efficient industrial security solutions, the following five starting points must be taken into account:

Industrial Security Concept

- Implementation of an appropriate system-wide **security management system** with regard to the technology and the engineering and production processes.
- The **interfaces** to office IT and the Internet/Intranet are subject to clear regulations – and are monitored accordingly.
- Protection of **PC-based systems** (HMI, engineering and PC-based controllers) by means of antivirus software, whitelists, and integral security mechanisms.
- Protection of the **control level**
  - with automatically active security functions already integrated into the automation and drive components – e.g. IP hardening
  - with security functions that have to be activated by the programmer – e.g. setup of access passwords
- Monitoring of all **communication** with systems for the purpose of detecting intruders, and intelligent segmentation of the network with the help of firewalls.

The Industrial Security Concept is based on five key elements for protecting all three levels of your industrial plant.

For more information on selective measures against all conceivable threats, please contact the experts of our Consulting Team:

industrialsecurity.i@siemens.com

Siemens AG
Industry Sector
Industry Automation
P.O. Box 48 48
90026 NUREMBERG
GERMANY

Subject to change without prior notice 11/11
Order No.: E20001-A1020-P200-X-7600
DISPO 06303
Schö/36244 MI.AS.IS.52.2.01 SB 11110.5
Printed in Germany