Protecting productivity

Industrial Security

siemens.com/industrial-security

Defense in depth

Security threats force you to take action

Defense in depth

As the level of digitalization increases, so too does the importance of comprehensive security concepts for automation applications. That's why Industrial Security is an essential element of Digital Enterprise, the Siemens way to Industrie 4.0. With defense in depth, Siemens provides a multi-layer concept that gives your plant both all-round and in-depth protection. The concept is based on plant security, network security and system integrity as recommended by ISA 99/IEC 62443.

Plant security

Plant security uses various methods to protect critical components against physical access by individuals, from classic building access to the protection of sensitive areas with code cards. Plant security also covers the integration of processes and guidelines as well as continuous monitoring of the security status of production facilities to provide comprehensive protection.

Network security

Today, protecting production networks against unauthorized access is essential, particularly at interfaces to other networks (e.g. office or Internet). Additional security is offered here by the segmentation of individual subnets, as in the cell protection concept with SCALANCE S or Security communication processors for SIMATIC. Data transmission can also be secured using a VPN, such as for connecting to remotely located plants via the Internet or cellphone networks from anywhere in the world, using SCALANCE M.

System integrity

The third pillar of defense in depth is safeguarding system integrity. This includes protecting automation systems and controllers such as SIMATIC S7, SCADA and HMI systems against unauthorized access or protecting the intellectual property contained within them. Furthermore, integrity also involves authenticating users and their access rights, as well as hardening the system against attacks.

Always active

Industrial Security is a continually changing challenge

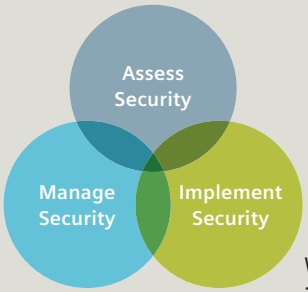
At Siemens, we know how important Industrial Security is, and throughout the development of our automation products and solutions, we have established a series of measures and procedures for just this aspect, including within our Product Lifecycle Management (PLM), Supply Chain Management (SCM) and Customer Relationship Management (CRM) processes.

We work closely with our suppliers to ensure a high standard of security across the entire supply chain, and also check software components from third-party suppliers for possible weaknesses.

When security issues arise, we react promptly, informing our customers and providing them with recommendations, updates and security patches as quickly as possible. This means that we are now already able to comply with future legal requirements, such as those laid out in the German IT Security Act.

In addition, we are linked to over 200 security organizations around the world through the Forum of Incident Response and Security Teams (FIRST).

As a partner for industry, Siemens will work to incorporate any future IT security requirements as and when they emerge. For more information on alerts, updates and patches, visit:
www.siemens.com/industrial-security



Plant Security Services

With Siemens Plant Security Services, industrial companies benefit from the comprehensive know-how as well as the technical expertise of a global network of experts for automation and cyber-security. The holistic approach of the industry-specific concept is based on state-of-the-art technologies as well as the applicable security rules and standards.

Threats and malware are detected at an early stage, vulnerabilities analyzed in detail, and suitable comprehensive security measures are initiated. Continuous monitoring gives plant operators the greatest possible transparency regarding the security of their industrial facility and optimal investment protection at all times.

Plant security

Plant security – physical protection and holistic security management for automation plants

Access control

Managed access control is an essential factor when it comes to safeguarding critical company areas. Siemens Building Technologies offers an extensive portfolio of products, solutions and services for the protection of critical infrastructure. The range extends from access solutions and video monitoring systems to command and control platforms.

Standards

Although there are hundreds of IT security standards, only a few have proven themselves useful for the protection of industrial systems. Building on our many years of experience, we advise you on the selection and implementation of appropriate standards.

In particular, IEC 62443/ISA99 is a well-proven international standard for the industrial automation environment.

Defining guidelines

We support you in defining appropriate guidelines for your own application, and take all the relevant rules and standards into consideration. For example, the handling of removable storage devices must be clearly regulated. These precise guidelines help to ensure a high level of security for all concerned, without placing any constraints on productivity. In this way, Industrial Security becomes a central management task.

Security monitoring

With continuous analysis and correlation of logs as well as comparison with our databases we detect and classify potential threats. In case of a security threat we notify you immediately and give a constant overview of the current security status of the plant through monthly status reports.

Network security

Network security for production networks

This involves the protection of automation networks against unauthorized access with access protection, segmentation (e.g. DMZ) and encrypted communication using security modules.

Security modules from Siemens have been optimized for use in automation systems and are designed for the specific requirements of industrial networks.

Siemens was the first supplier of automation technology to achieve Achilles Level 2 certification for communication robustness for multiple controllers, security S7 communication processors and security appliances.

These devices can be configured together in the TIA Portal for consistent, end-to-end security engineering.

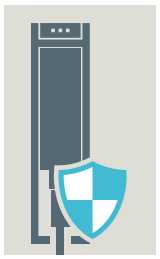
Secure remote maintenance and remote access using protected communication

Siemens offers a comprehensive range of products with integrated security functions (Security Integrated), such as the SCALANCE S security modules, the SCALANCE M Internet and mobile wireless routers as well as security communication processes for SIMATIC controllers to protect industrial networks and secure remote access.

These products support stateful inspection firewalls and secure VPN communication (virtual private network) against unauthorized access, data espionage and manipulation.

SCALANCE S – Security modules

SCALANCE M – Industrial modems and routers



Security communication processors

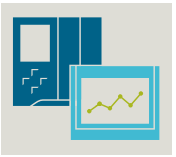
System integrity

System integrity – security for automation systems and control components

Protect automation components against cyber-attacks and unauthorized access and safeguard your expertise right in the TIA Portal.

Whether you want to protect existing know-how or rule out unauthorized access to your automation processes from the outset, thus preventing production downtimes, our comprehensive Industrial Security portfolio includes support for implementing targeted measures to protect against a variety of threats, as well as the design of complete solutions for maximum protection.

Our integrated security features provide comprehensive protection against unauthorized configuration changes at the control level as well as against unauthorized network access, preventing the copying of configuration data and making any attempts to manipulate such files easier to detect.



Controllers and HMI systems

Robust controllers and HMI systems with integrated security functions for multi-level access protection, know-how and copy protection.

PC-based systems

Security functions for PC-based automation systems with whitelisting, antivirus software and system hardening for greater OS security.

Motion control and drives

Integrated security functions in SINUMERIK, SIMOTION and SINAMICS for protecting your investment and maintaining productivity levels.

Process automation

Safeguard productivity in the process industry with the Industrial Security concept for SIMATIC PCS 7, based on the recommendations of the IEC/ISA99.

Plant security

- Physical access protection
- Processes and guidelines
- Security services protecting production plants

Network security

- Cell protection and perimeter network
- Firewalls and VPN

System integrity

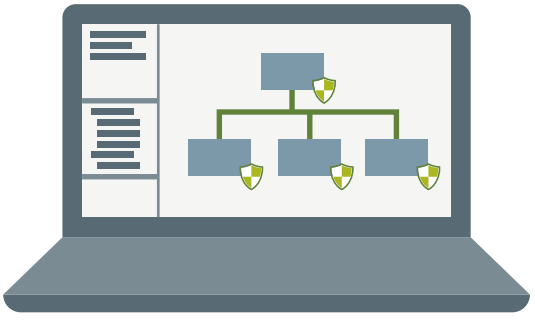
- System hardening
- Patch management
- Detection of attacks
- Integrated access protection in automation

Industrial Security as part of Totally Integrated Automation

With industry-standard security products for network security and system integrity which are integrated in the TIA Portal, your automation solutions can be efficiently safeguarded and the defense in depth concept for the protection of industrial plants and automation systems can be implemented. Integration into the TIA Portal enables the configuration of standard and security functions in one project. This avoids data being input more than once, reduces error rates and saves engineering time.

Industrial Security from Siemens makes it possible to:

- increase and maintain plant availability
- avoid data loss and protect confidential information
- maintain and improve competitiveness
- meet legal requirements and standards
- prevent manipulation and safeguard values



In TIA Portal integrated security functions

Find out more:

siemens.com/industrial-security

Experience and discover dependable Industrial Security:

Get acquainted with the defense in depth concept from Siemens and learn about all aspects of Industrial Security.

Industrial Security – at a glance!

Follow us at
twitter.com/siemensindustry
youtube.com/siemens

Published by
Siemens AG 2017

Digital Factory
P.O. Box 48 48
90026 Nuremberg
Germany

Article No.: DFFA-B10076-01-7600
Dispo 21507
170/74168
W-DFFA7-7P-21DE9
WS 03170.5
Printed in Germany

Security information:

Siemens provides products and solutions with Industrial Security functions that support the secure operation of plants, solutions, machines, equipment and/or networks. They are important components in a holistic Industrial Security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art Industrial Security concept. Third-party products that may be in use should also be considered. For more information on Industrial Security, visit:
http://www.siemens.com/industrial-security.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit:
http://support.automation.siemens.com.