SIEMENS

Technical article

Industrial Security

# IT Security of Automation Systems

## Staggered Protection down to the Plant Structure

**IT security in the automation is extremely important for our industrial location, since the automation and process control systems required are used in virtually all industrial sectors: From energy generation and distribution to water supply to manufacturing, traffic control systems and facility management. In order to protect people and plants, plant-specific measures are necessary. Help is provided by a staggered protection portfolio that reaches deep into the specific plant structure.**

Especially due to the increasing networking of Ethernet connections down to the field level, the industry is becoming more concerned with the related security issues. Because open communication and increasing networking of production systems not only hold enormous opportunities, but equally big risks, whose potential damage to these networked systems must be identified.

The era of sealed off automation systems – based on proprietary protocols and inaccessible from the outside – is a thing of the past. A connection of automation systems to the Internet or to existing office networks is a given nowadays, although the requirements for automation networks differ greatly.

### Different Requirements for Automation Networks

In the current "ICS Security Compendium" of the German Federal Office for Information Security (BSI), the different requirements for classic IT networks and automation networks are pointed out. It is intended to serve as basic guide for the operation of industrial plants with respect to safeguarding the production and processing systems, and is addressed to utility companies and water suppliers, providers of traffic control systems, and companies in the facility management sector.

A significant difference is the assessment of the risks concerning the different systems. While an attack on the IT infrastructure "only" affects the data integrity and at worst results in a loss of company data, a hacker attack on the processes and the automation environment can endanger people, destroy production capacities and uncontrollably damage the environment.

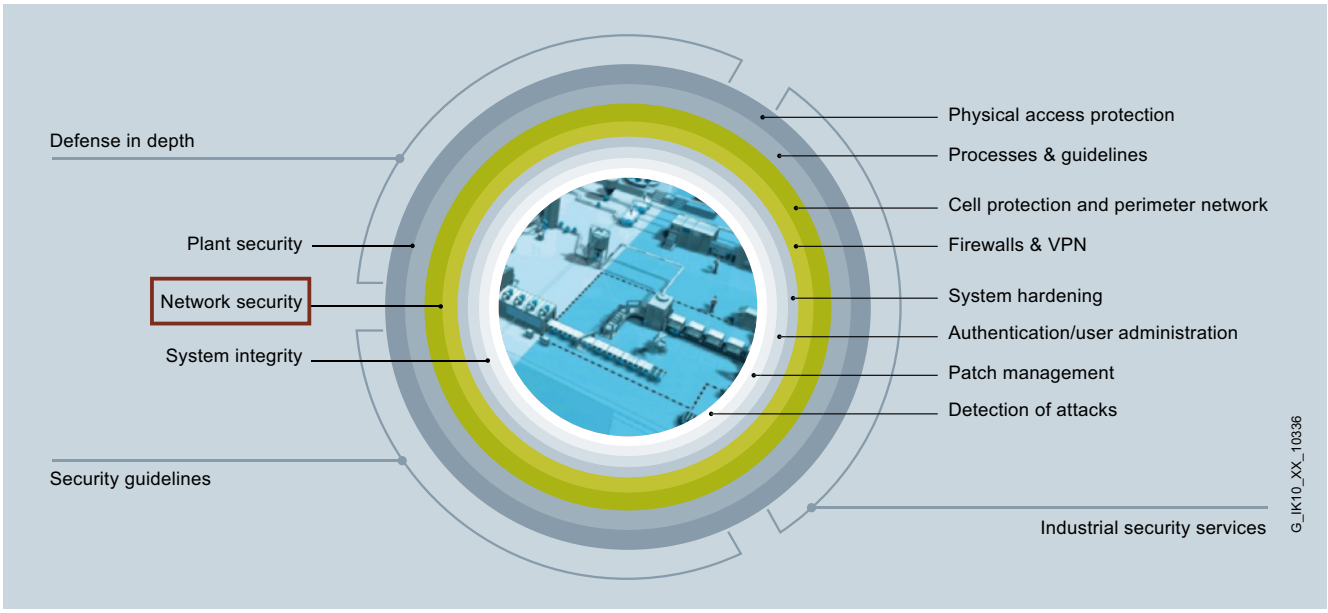


Image 1: Siemens industrial security strategy: Defense-in-depth

To comprehensively protect an industrial plant against attacks in terms of security, appropriately staggered and coordinated measures must be taken.

It is not enough to just implement a simple password-protected system access, since attacks from the outside can take place at several levels. For a comprehensive protection of industrial plants, the Siemens AG has developed a defense-in-depth concept, which is depicted in Image 1.

### Complete Protection that also goes deep

With defense-in-depth, Siemens is offering a multilayered concept for industrial users that protects industrial plants against attacks from the outside as well as the inside in several layers. The concept is based on the components of plant security, network security and system integrity – according to the recommendations from ISA 99 / IEC 62443, the leading standard for security in industrial automation. While classic plant protection wards off physical access, network protection and system integrity protection prevent cyber-attacks and access by unauthorized operators or non-company personnel. The advantage here is that an attacker has to overcome multiple security mechanisms, and that the security requirements of the individual layers can be taken into consideration plant-specifically.

### Success Factor: Network Security

Network security means protection of automation networks against unauthorized (external as well as internal) access. This includes the monitoring of all interfaces, such as between office and plant networks, or the monitoring of the teleservice access to the Internet, which can be carried out by means of firewalls and, where necessary, the setup of a DMZ (demilitarized zone = security-relevant shielded zone). The DMZ is intended for supplying data to other networks, without granting direct access to the automation network. The security-relevant segmentation of the plant network into individually protected automation cells minimizes the risk and increases the security. The segmentation into cells and the assignment of the devices follow the plant-specific communication and protection needs. The data transmission between the cells is exclusively established via VPN connection (virtual private network), which is also encrypted and thus protected against data espionage and manipulation. The communication participants are securely authenticated. With the “Security Integrated” components from Siemens (e.g., the SCALANCE S security modules or security CPs for SIMATIC controllers), a cell protection concept can be effortlessly realized and the communication be secured.

## Components for Network Security

For the implementation of such protection concepts, two means of security have proven themselves: the firewall and the VPN tunnel.

The firewall is used for the content-related protection of the data traffic. Through filtering, suspicious/prohibited packets can be discarded and, where appropriate, network access be blocked or granted packet-dependently. To secure the physical communication, the tunneling method is most often used (Image 2).

The firewall and VPN functions are supported by the Security Integrated" products (red padlock icon) and thus provide the user with protection down to the automation cell.

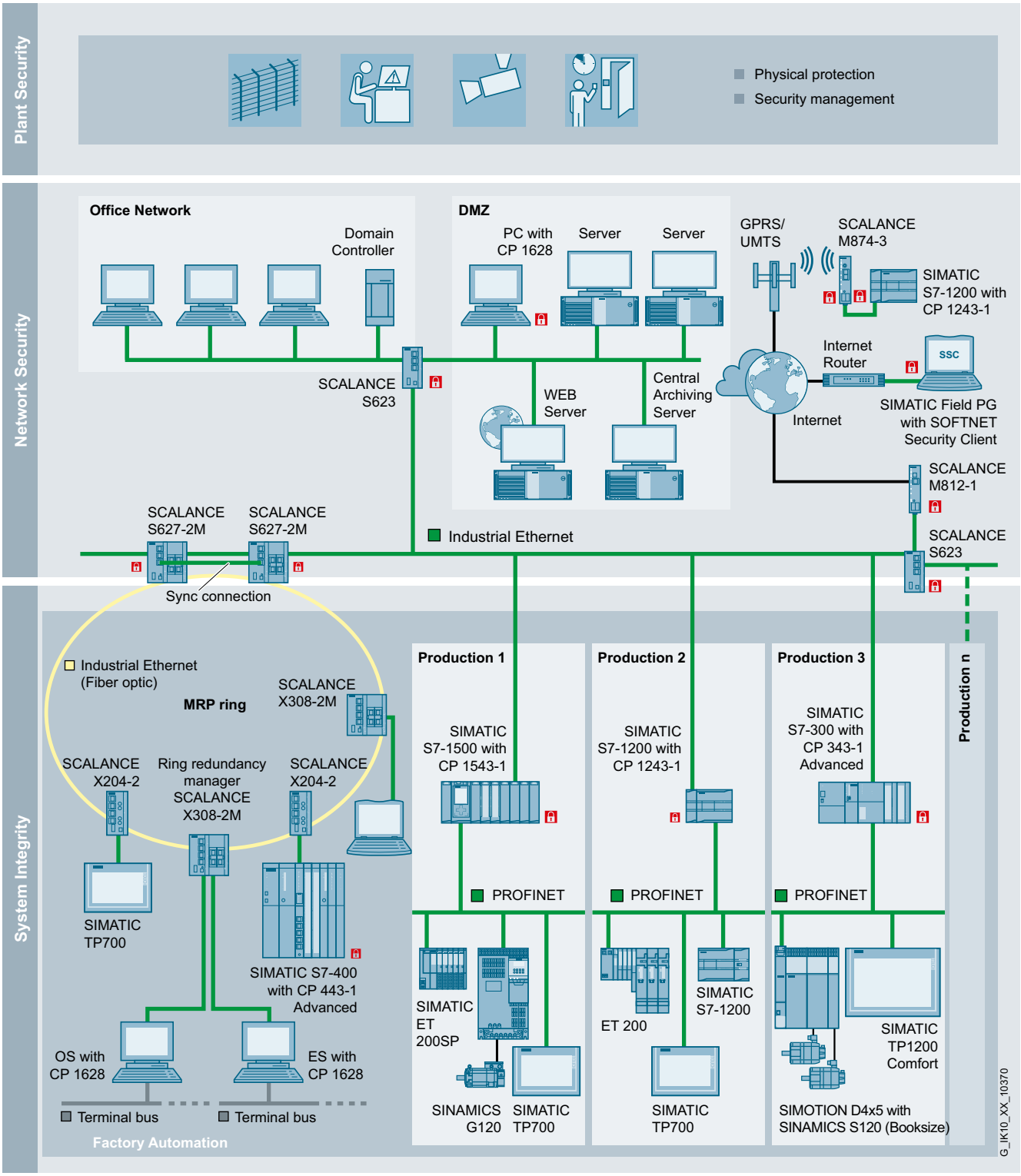


Image 2: Secure communication, network access protection and network segmentation with "Security Integrated" products (Siemens plant image)

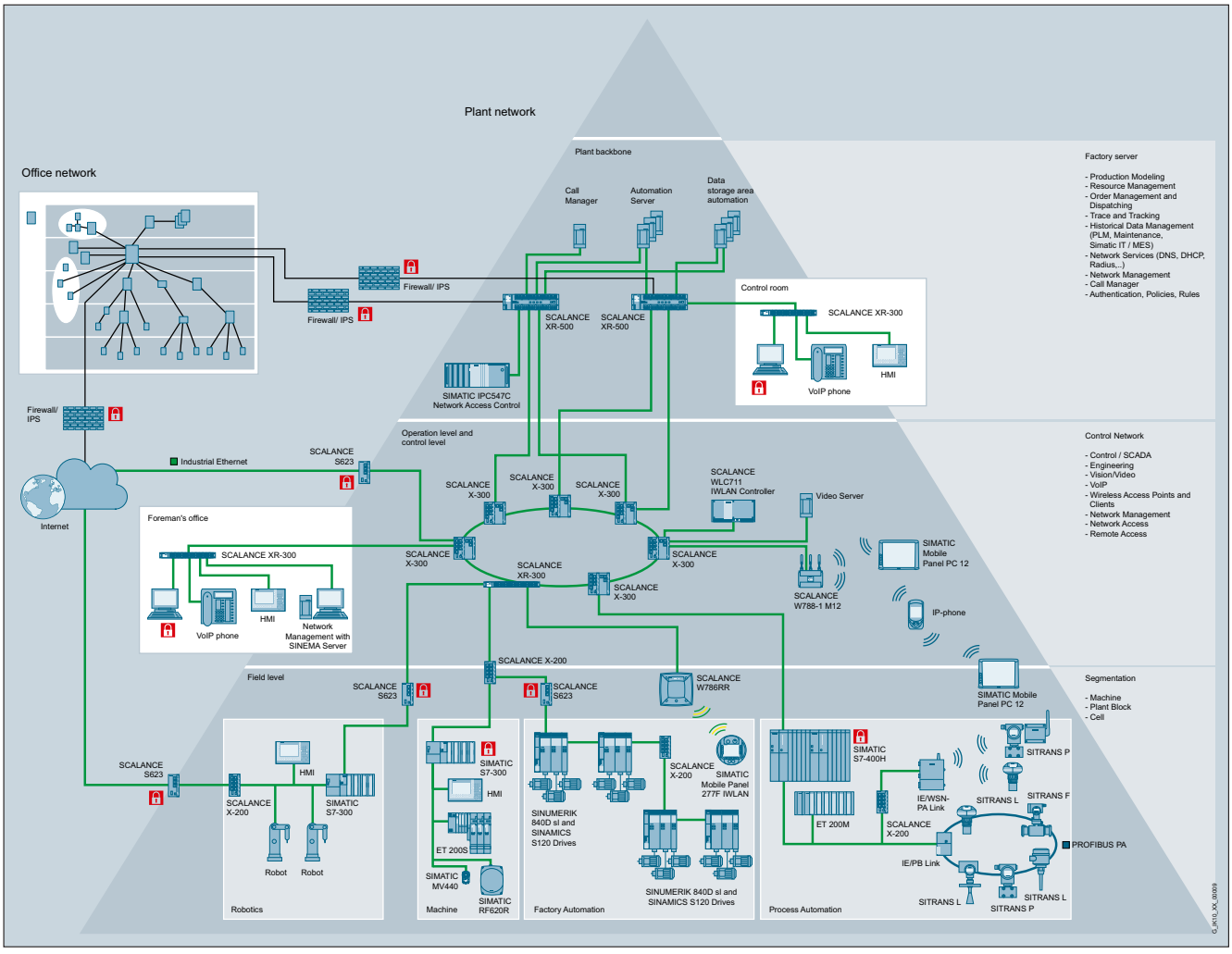


Image 3: Secure industrial communication, set up with SIMATIC Net components (Siemens plant image)

## Choice of various Security Products for application-specific Plant Security

To make it possible for almost all plant operators to effortlessly set up secure networks, Siemens is offering a wide range of "Security Integrated" products. A distinction is made between stand-alone modules, such as DSL modems/routers or cellular phone network routers, and communication processors, which directly integrate the security functionality into the controller world (Image 3).

These products are marked with the typical red padlock. The "Security Integrated" products are designed for harsh industrial use and offer proven protection for production plants.

In addition to the security product offering, Siemens supports the user in the implementation of the defense-in-depth concept through Plant Security Services. The service offering is comprised of the elements depicted in Image 4.

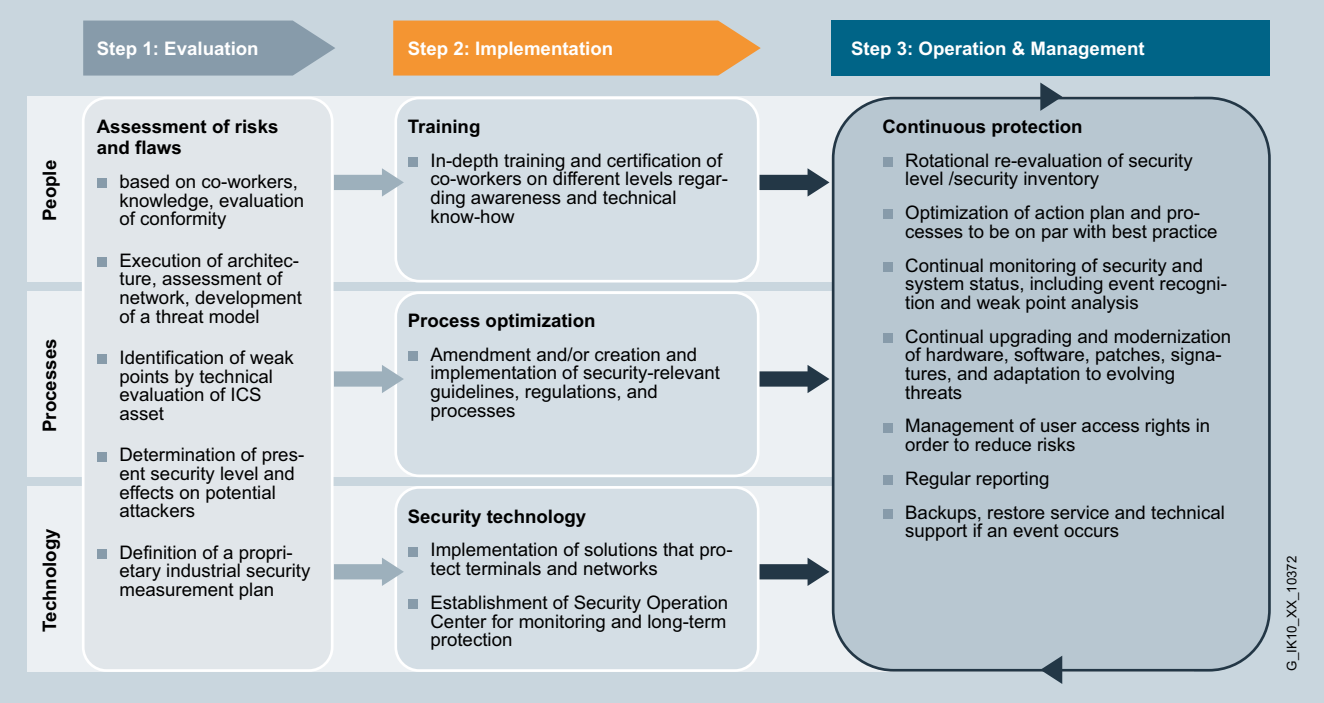


Image 4: Steps for a secure communication in industrial plants

### Security is a continuous Process

Industrial security, however, is not only a purely technical subject, but also must be consciously embedded in the minds of management and personnel. Security is a continuous process that must be taken into account at all times. It is important to understand that the requirements of the classic office IT differ from those of the automation IT. It is therefore critical to employ proven security products in the automation environment. In the ideal case, the component manufacturers integrate the required/necessary security functions directly into their automation products as standard.

### Excerpt from the "Security Integrated" portfolio of the Siemens AG:

- Cellular Phone Network Router SCALANCE M874 / M875 and DSL Router SCALANCE M812
- Security Module SCALANCE S
- Software SOFTNET Security Client
- Communication Modules CP 1628, CP 343-1 Advanced, CP 443-1 Advanced and (new) CP 1543-1 for the High-End Controller SIMATIC S7-1500

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 NÜRNBERG
GERMANY

Subject to change without prior notice
PDF
Technical article
FAV-634-2014
DR.PN.PA15.XXXX.95.11
Produced in Germany


**www.siemens.com/industrialsecurity**