Security concept for process and discrete industries

Industrial Security
# Contents

4 Introduction

5 Overview of the Siemens industrial security concept

6 Plant security
   Physical access protection
   Security management
   Industrial Security Services

10 Network security
   Securing interfaces to other networks
   Network segmentation and cell protection concept
   Secure remote access

15 System integrity
   Protection of PC-based systems in the plant network
   Protection of the control level

17 Roles and rights concepts

18 Consideration of attack scenarios during product development and production

19 Summary: Industrial security for production plants
Preface

This White Paper provides an overview of the subject of Industrial Security. It describes the threats and hazards to which industrial automation systems and production plants are exposed and introduces best practice concepts for minimizing these risks and instituting a level of protection that is acceptable on economic as well as security grounds. It also covers the need to face the increasing threats, due to the trends of the Digitalization, like universal connectivity and valuable large amounts of data, which make Cyberattacks easier and more likely.

Further information about industrial security at Siemens can be found here: https://www.siemens.com/industrialsecurity

The information presented in this White Paper is current as of June 2018.

Publisher
Siemens AG
Digital Industries
Gleiwitzer Str. 555
90475 Nuremberg, Germany

Support:
Please direct any questions in connection with this White Paper to your Siemens contact person at your representative/sales office.
Security disclaimer

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.
Introduction

Hand in hand with the increasing digitalization of industrial automation systems go ever-deeper integration, vast volumes of data and the adoption of open standards to provide the necessary direct access across all levels. The enormity of the opportunities and benefits – in both discrete manufacturing and the process industries – promised by these changes has led commentators to speak of a new industrial revolution and the dawn of what they call "Industry 4.0".

However, this trend has a significant dark side in the form of increasing vulnerability to cyber-attack. Far-reaching integration, mushrooming data volumes and universal standards make it much easier for attackers and malware to access systems. Studies and incidents show, not only are OT networks and production areas recognized as lucrative targets for attacks, but the people behind these attacks are becoming more aggressive in their tactics, using more effective tools, and applying more resources to the attacks.

The reality today is that industrial systems face also professionally implemented attacks. The "cyber war" is already upon us. The changed threat situation demands a fundamental rethink of information security, access protection and the whole process of establishing industrial security concepts. The attackers are upgrading their arsenal; never has it been more important for automation and production system vendors and operators to take on the threat they pose.

Fortunately, it is entirely possible to mount an effective defense. While 100 % security is out of the question, there are certainly ways and means of reducing the risk to an acceptable level. Bringing risk under control in this way requires a comprehensive security concept that takes account of the different features and the professional nature of attacks and promotes strong cooperation between the various parties involved (that is to say automation system operators, integrators, machine builder and vendors).

Organizational and technical measures must be carefully coordinated: a holistic security concept relies on people, processes and technology in unison to achieve the necessary level of protection.

This White Paper describes such a comprehensive security concept for the protection of industrial plants.
Overview of the Siemens industrial security concept

All aspects, from the operating level to the field level and from physical access control to network and terminal protection, have to be tackled simultaneously in order to protect industrial systems against internal and external cyber-attacks. The most suitable approach for this is a defense in depth concept in accordance with the recommendations set out in IEC 62443, the leading standard for security in industrial automation.

![Defense in depth concept for industrial plants](image)

**Figure 1: Defense in depth concept for industrial plants**

The plant security, network security and system integrity elements form the foundation for the industrial security concept at Siemens. All of the key factors are considered in this approach, including physical access protection and organizational measures such as guidelines and processes as well as technical measures to protect networks and systems against unauthorized access, espionage and manipulation. Protection at multiple levels and the combined effect of different protective measures provides a high degree of security, reducing the risk of successful attacks and ultimately improving plant availability and productivity (Figure 1).
Plant security

Plant security puts in place the conditions necessary to ensure that the technical IT security measures implemented cannot be circumvented by other means. Plant security measures include physical access protection infrastructure, such as barriers, turnstiles, cameras and card readers. Organizational measures include most notably a security management process to ensure the security of a plant.

Physical access protection

The following points can be covered here:

- Measures and processes that prevent unauthorized persons from entering the vicinity of the plant.
- Physical separation of different production areas with differentiated access authorizations.
- Physical access protection for critical automation components (for example securely locked control cabinets)

The guidelines pertaining to physical access protection measures also have impact on the question of which IT security measures are required and in what strength. If, for example, access to a particular area is already strictly limited to selected authorized persons, the network access interfaces or automation systems do not need to be secured as robustly as would be the case in generally accessible areas (Figure 2).

Figure 2: Physical protection against unauthorized access to production areas
**Security management**

Appropriate organizational measures and the introduction of effective security processes are vital for plant security. Organizational measures must be tightly coordinated with technical measures, as the effectiveness of the one depends to a significant degree on the effectiveness of the other; indeed, most security objectives can only be achieved through a combination of organizational and technical measures.

Organizational measures include the establishment of a security management process. The first step in determining which measures are likely to be required in a given situation is to analyze the specific risks that exist and identify which cannot be tolerated. The significance of an identified risk in this connection depends on the damage associated with its materialization as well as its probability of occurrence (Figure 3). Failure to conduct a proper risk analysis and ascertain security objectives is more than likely to result in both the measures implemented being ineffective or unnecessarily expensive and some weaknesses not being identified or addressed.

![Risk assessment decision table](image)

*Figure 3: Risk assessment decision table for use in conjunction with a prior plant-specific risk analysis. The risks involved are reviewed regularly.*

The risk analysis yields security objectives that form the basis of specific organizational and technical measures. The measures must be reviewed after implementation. The risk must be assessed again from time to time or after material changes just in case the threat situation or underlying factors have altered. The risk analysis provides the foundation for the procedure to implement protective and, where applicable, monitoring measures.
Industrial Security Services

Special security services can assist operators in many respects with the design of secure production environments. This assisted process extends from an analysis of the risk (assess security) and the design and realization of a secure production operation (implement security) to the continuous monitoring of the industrial security status (manage security) (Figure 4).

Figure 4: Siemens Industrial Security Services provide assistance with risk analysis, the implementation of measures and the continuous management of the plant

The risk analysis brings transparency as to the security status of a plant and identifies weaknesses, thus providing a basis on which the corresponding risk can be derived. The measures required are then compiled in an action plan (roadmap) showing how the security status of a plant can be raised to a new, higher level. One example is the IEC 62443 Assessment, which establishes the actions necessary to bring a specific plant into compliance with the IEC 62443 standard. Scanning Services can be used as alternative or in combination to achieve transparency on existing computing devices in the asset as well as vulnerabilities, including checks against pre-defined security levels.

The next step is to implement the measures proposed to close the gaps identified. Resources encompassing both hardware (such as firewalls) and software (such as antivirus, whitelisting and anomaly detection) are available for this purpose. Also included are clear instructions and guidelines on IT security. Ultimately, security solutions can only work properly if employees have been educated and trained accordingly. Employee awareness and understanding should be promoted continuously through workshops, web-based training or equivalent measures.
Another key aspect of the Siemens service in this area is support for customers with the ongoing continuous monitoring of industrial plants and production machines as well as the management of vulnerabilities and patches, thus reaching transparency on increasing cyber threats.

The defense in depth strategy creates a suitable basis for enhancing security in industrial plants. Siemens Industrial Security Services provide assistance for companies with the implementation of corresponding measures. The comprehensive range of services offered, from security assessments to firewall installation and training to continuous monitoring and attack detection, help customers in industry to reduce the security risk associated with their plants (Figure 5).

Figure 5: The Industrial Security Services portfolio built around industrial standard IEC 62443
Network security

A central element of the industrial security concept is the network security. It comprises mainly the protection of automation networks against unauthorized access as well as the control of all interfaces to other networks, such as the conduit to the office network. In particular the remote maintenance gateways to the internet need to be protected in this context. Protecting communications against interception and manipulation by means of encrypted data transmission and communication node authentication is also in the scope of network security.

Securing interfaces to other networks

Interfaces to other networks can be monitored and protected by using firewalls and, where appropriate, by setting up a demilitarized zone (DMZ). A DMZ is a network area in which technical security mechanisms protect access to data, devices, servers and services within this area. The systems installed within the DMZ are shielded from other networks by firewalls that control access. This separation makes it possible to provide data from internal networks (for example the automation network) on external networks without having to admit direct access to the automation network. A DMZ is typically designed so that it also does not permit access automation network, which means that the automation network remains protected even if a hacker gains control of a system inside the DMZ (Figure 6).

---

**Figure 6**: Using a demilitarized zone to transfer data between the company network and a plant network
Network segmentation and cell protection concept

The segmentation of the plant network to create separated automation cells protected by technical security mechanisms helps to minimize risk further and to increase security. Network segmentation involves protecting elements of a network, such as an IP subnet, with a security appliance that separates them from the rest of the network for technical security purposes. The devices within a segmented cell are protected against unauthorized access from outside without the need of any compromise in terms of real-time capability, performance or other functions.

The firewall is able to control access attempts to and from the cell. It is even possible to stipulate which network nodes are permitted to communicate with each other and, where appropriate, which protocols they are allowed to use. This means that unauthorized access attempts can be blocked, first and foremost, and also makes it possible to reduce the load on the network, as only those communications that are explicitly desired and permitted are able to proceed.

The division of the cells and the allocation of the devices reflect the communication and protection requirements of the network stations. Data transmission to and from the cells can in addition be encrypted by the security appliances using a VPN to protect against data espionage and manipulation. This comprises the authentication of communication participants and, where applicable, authorization of access attempts. The cell protection concept can be implemented and the communication between the cells can be protected by using components such as the Industrial Security Appliances SCALANCE S or the security communications processors for the SIMATIC S7 automation system (Figure 7). The Industrial Security Appliances SCALANCE S provide the possibility to define and protect network cells flexible on the basis of VLANs.

*Figure 7: Network segmentation and cell protection with Security Integrated products (see red padlock symbol)*
Secure remote access

It is becoming increasingly common to connect plants directly to the internet and to link up remote plants via mobile networks (GPRS, UMTS, LTE). This is done to enable remote maintenance, use remote applications and also to facilitate monitoring of machines installed all over the world.

Securing access is particularly important in this context. Attackers can find unsecured access points easily and inexpensively using search engines, port scanners, or automated scripts. It is therefore very important to ensure that communication nodes are authenticated, data transmission is encrypted and data integrity is protected, especially in the case of critical infrastructure plants. Incidents such as intrusion by unauthorized persons, the escape of confidential data and the manipulation of parameters or control commands can result in enormous damage, including to the environment and endanger even personnel.

VPN mechanisms, which provide the very functions (authentication, encryption and integrity protection) required, have proven to be particularly effective in securing communications in this context. Siemens industrial internet and mobile communication routers support VPN, allowing data to be sent securely over these networks with protection against unauthorized access.

Typically devices for use in secure communication are authenticated as trustworthy communication nodes using for instance certificates and the relevant IP addresses or DNS names are applied in the firewall rules to permit or block access. The SCALANCE M industrial router and the SCALANCE S Industrial Security Appliances support also user-specific firewall rules, creating the additional possibility of linking access rights to specific users. Therefore, a user must log on to a web interface using its login credentials to temporarily unlock a specific set of firewall rules matched to his or her personal access rights. One particular advantage of this temporal and user-specific activation is that there is always a clear record of exactly who has gained access when, which can be very important for maintenance and services.

The SCALANCE S variants with more than two ports also provide a way around a dilemma all too familiar to many system integrators, OEMs and end users: machine builders need to be able to access their machines on the end user's premises for maintenance purposes, but end-user IT departments are most reluctant to allow outsiders into the network to which the machine is connected. With the variants of the Industrial Security Appliances it is possible to connect the machine both to the plant network and, using the additional firewall-protected port, to the internet. This means that the machine can be accessed from the internet without allowing access to the plant network from the internet, so have direct access to the plant network (Figure 8).
Facilitation of secured remote access using management platforms

Industrial plants are often widely distributed, sometimes even spread across different countries. In these cases, public infrastructure is often used to access plants and machines in discrete manufacturing and process industries. In other instances, particularly complex connections are involved. One valuable option for secured and efficient remote access is to deploy a management platform to manage these connections and to secure, authenticate and authorize all communications.

Management platforms are particularly suitable for use in connection with series and special-purpose machine manufacturing. This enables OEMs, for example, to definitively identify a large number of similar machines in use with different customers and address them for remote maintenance.

The SINEMA Remote Connect management platform is a server application that provides secure management of VPN tunnels between HQ, the service engineers and the installed plants. The identity of the nodes is determined by an exchange of certificates before access to the machines can proceed. Unauthorized attempts to access the company network to which the plant or...
machine is connected can thus be prevented. The allocation of rights for access to machines can be controlled centrally via the management platform’s user management facility. The fact that the connection is only ever set up from the plant to the server and only when actually required further enhances security, as there is no need to permit incoming connections to the plant (Figures 9 and 10).

Figure 9: SINEMA Remote Connect is a management platform for efficient and secured remote access to globally distributed plants and machines.
Figure 10: Secured remote access to distributed plants using SINEMA Remote Connect.

**System integrity**

The third pillar of a balanced security concept is system integrity. The systems whose integrity is to be protected in this context comprise control components and automation, SCADA and HMI systems. These require protection against unauthorized access and malware or have to meet special requirements in areas such as the protection of expertise.

**Protection of PC-based systems in the plant network**

PC systems used in the office setting are typically protected against malicious software and have any weaknesses detected in their operating system or application software rectified by the installation of updates or patches. Equivalent protective measures can also be required for industrial PCs and PC-based control systems, depending on how they are used. Protective mechanisms familiar from the office environment, such as anti-virus software, can also be used in industrial settings in principle, although it is essential to ensure that they have no adverse impact on the automation task.

Whitelisting solutions can be used in addition to antivirus software. Whitelisting involves the creation of approved lists in which the user explicitly specifies those processes and programs that
are permitted to run on the computer. Any attempt by a user or malware package to install a new program is then denied, preventing the associated damage.

Siemens supports the protection of industrial PCs and PC-based systems in its capacity as an industrial software vendor by testing its software for compatibility with virus scanners and whitelisting software.

The numerous integrated security mechanisms provided in the Windows operating systems are of course also available for use in hardening systems to the extent required. These include not just user management and the management of rights, but also options such as finely differentiated settings using security policies. Siemens provides support here too in the form of thorough guidelines.

**Protection of the control level**

Efforts to protect the control level are concerned primarily with ensuring the availability of the automation solution. The security mechanisms integrated into the standard automation components provide the starting point for protecting the control level. These mechanisms are enabled and configured in line with the level of protection required for the machine or plant concerned. Configurations of the security mechanisms of the automation components as well as developing the engineering programs for the automation solution are conveniently and efficiently accomplished using TIA Portal. Ever-increasing interconnection and the integration of IT mechanisms into automation technology are, however, changing the requirements for production plants in terms of access protection and protection against manipulation, which are absolutely essential for modern control systems. These features are already integrated into the SIMATIC S7-1200 and S7-1500 controller families – including the software controller.

The protection afforded consists in part of multi-access protection with differentiated access rights and in part of communication protocols for controller configuration or HMI connection. These include integrated security mechanisms for significantly enhanced detection of manipulation attempts.

Safeguarding intellectual property is another matter of growing concern: machine builders invest heavily in the development of their products and they cannot afford to see their proprietary expertise compromised. The know-how protection and copy protection functions provided by the Siemens controllers give users convenient and straightforward support in this area as well.

The know-how protection function enables highly specific protection of program modules to prevent access to their content and the copying and modification of algorithms.
The copy protection function links program components to the serial number of the memory card or CPU. This helps to prevent copying of the machines, as protected programs can only be used in the machines for which they are intended. These functions assist machine builders to safeguard their investment and maintain their technological edge.

Further security features like Stateful Inspection Firewall and VPN are integrated into the security communications processors for S7 controllers. Amongst others, this makes the CP343-1 Advanced communications processor for the SIMATIC S7-300 controller, the CP443-1 Advanced communications processor for the SIMATIC S7-400 controller, the CP1543-1 communications processor for the S7-1500 controller and others the secure interfaces to the entire plant network. The protection they provide extends to the respective controllers connected, to the underlying networks and, where necessary, to communication between them and thus supplements and enhances the cell protection concept in a plant (see figure 7).

Used with PCs is the CP1628 Ethernet card, which can also protect communication with industrial PCs by means of VPN and firewall. All of these Security Integrated products are compatible with one another and can establish secure VPN connections with one another, making them suitable to protect just about any plant unit and all kinds of automation components.

**Roles and rights concepts**

Defending against the various threats posed and realizing an appropriate level of protection demands a defense-in-depth concept that sets up multiple obstacles for would-be attackers to overcome. These obstacles, of course, cannot be allowed to hinder authorized users. It is common in practice to establish a system of graduated access rights or categories of rights under which some users are only able to access specific plant units, devices or applications, for example, some have administrator rights and some have only read or write access rights.

The implementation of a security concept therefore helps not only to defend against direct attacks, but also to institute an authorization concept. Authorization concepts are intended to ensure that access is restricted to authorized persons based on the specific rights assigned to them. Usually this involves defining roles, each of which confers a specified set of rights, rather than creating a separate rights profile for every user. Users or user groups are then assigned these roles and thereby receive the corresponding access rights. Proper management of users and rights is therefore very important for Industrial Security.

A universal configuration for all of the automation components facilitates user management in this case, because the roles and rights of the different people involved can be defined and
maintained centrally. Figure 11 shows a screenshot of user and rights management in the TIA Portal.

![Image of user management in TIA Portal]

*Figure 11: User management in the TIA Portal with assignment of roles and rights*

**Consideration of attack scenarios during product development and production**

A security by design approach is increasingly being required of product manufacturers. This means to consider security aspects as part of product development and production (see Security Standard IEC 62443). An automation product shall be tracked and embedded in a holistic security concept (HSC) from creation to production to use. Assets in this context can include source code, IT processes and production machines. The security requirement pertaining to assets and organization, with respect to processes and methods, grows progressively more difficult as the desired security level increases. The product owner is responsible for specifying the security level to be applied to the product and associated assets (Figure 12).

Security requirements are particularly high when developing and manufacturing automation products that have security functions. The security keys used must be reliably protected against unauthorized access in storage. In the event of a security breach, for example, generating and distributing new keys would be a very laborious operation. Delays in detecting the breach – or a breach that passes completely undetected – would have high security risks.
The benefits of a holistic security concept extend to the portfolios of both security products and standard products. Security products such as the Industrial Security Appliances SCALANCE S, the Industrial Router SCLANCE M, or the communications processors for SIMATIC with integrated firewall and VPN, and others address specific security requirements. Standard products contain several integrated security functions available in the TIA Portal Engineering tool, SIMATIC S7-1200, and SIMATIC S7-1500 controllers. These standard products can reduce risk for the end user thanks to the vulnerability testing, risk analyses and associated design optimization work carried out in the course of development.

Figure 12: Holistic Security Concept takes security on the next level - a holistic approach for IT and OT

**Summary: Industrial security for production plants**

Even just a few years ago, security for production plants was very much a peripheral issue. The threats seemed rather abstract and theoretical and few manufacturers and operators had much of an interest in the issues involved.

A series of security incidents, reported prominently in the media changed everything. Suddenly it was clear to all that automation systems and production plants were also on the target list for cyber-attacks, that they were vulnerable and that the potential consequences could be severe. A combination of the sheer number of cases recorded and investigations carried out using honeypots – traps set up to trick hackers into exposing their methods and to generate attack statistics – revealed the true extent of the threats posed.

The path to the digital factory is associated with numerous trends, such as increasing interconnection, ever-greater volumes of data for transmission and storage and the continuing spread of the open standards used, that increase the risk of cyber-attacks. Shying away from these
developments on security grounds alone is no solution, as this course would result in steadily decreasing competitiveness and a contraction in sales revenue. Defending against threats and attacks is consequently a fundamental prerequisite for the digital transformation. Companies would be well advised to conduct a careful review of their data security situation even without motivation from the EU General Data Protection Regulation that recently came into force.

Siemens is well placed to help integrators and operators meet these increasingly demanding challenges in its capacity as a vendor and single-source supplier of industrial automation and communication systems. Risks can be successfully minimized by taking security factors into account during the design, development and production phases by implementing a holistic security concept to create correspondingly robust components equipped with effective security functions.

But engineering and technology alone can never suffice: also processes and organizational measures must be implemented and the relevant specific requirements adapted. Siemens can assist here if necessary with its security services.

Figure 13: Industrial security portfolio: concept, products and services
Armed with expertise in both automation and security, Siemens is a strong partner for machine builders, integrators and operators of production plants and offers a capable portfolio of security products and services as well as an effective industrial security concept (Figure 13).

Figure 14: Industrial Security - for comprehensively protected production plants
Published by
Siemens AG

Digital Industries
Factory Automation
P.O. Box 48 48
90026 Nuremberg, Germany

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article No.: DIFA-B10035-00-7600

Subject to changes and errors.
The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.