Security concept for the protection of industrial plants
Prologue

This whitepaper gives an overview of Industrial Security. It describes the threats and risks to which industrial automation networks are exposed and presents concepts for minimizing these risks and achieving adequate protection from an economic standpoint. In addition, it also gives an insight into what direction the situation will take as it develops based on current trends and what security mechanisms will also be able to be used in industrial environments in the future.

You will find more information on the topic of Industrial Security at: http://www.siemens.com/industrialsecurity

Version of the information in this White Paper: August 2013

Published by
SIEMENS AG
Industry Sector

Gleiwitzer Str. 555
90475 Nuremberg, Germany

Additional support:

If you have any further questions, please contact your local representative at your nearest Siemens office.
Security information:

Siemens provides automation and drive products with industrial security functions that support the secure operation of plants or machines. They are an important component in a holistic industrial security concept. With this in mind, our products undergo continuous development. We therefore recommend that you keep yourself informed with respect to our product updates.

Please find further information and newsletters on this subject at:


To ensure the secure operation of a plant or machine it is also necessary to take suitable preventive action (e.g. cell protection concept) and to integrate the automation and drive components into a state-of-the-art holistic industrial security concept for the entire plant or machine. Any third-party products that may be in use must also be taken into account.

Please find further information at:

http://www.siemens.com/industrialsecurity
# Table of contents

Security information: ................................................................. 2  
1. Introduction ............................................................................. 4  
2. Overview of the Industrial Security concept from Siemens .......... 6  
3. Plant security ........................................................................... 8  
   3.1 Physical access protection .................................................... 8  
   3.2 Security management ......................................................... 9  
4. Network security ..................................................................... 11  
   4.1 Securing the interfaces between the company and plant network ... 11  
   4.2 Network segmentation and cell protection concept ............... 11  
   4.3 Secure remote access ....................................................... 12  
5. System integrity ...................................................................... 15  
   5.1 Protection of PC-based systems in the plant network ............. 15  
   5.2 Protection of the control level ............................................. 15  
6. Roles and rights concepts ....................................................... 16  
7. Consideration of attack scenarios in product development ........ 18  
8. Security services .................................................................... 20  
9. Summary: A comprehensive security concept for secure automation .... 21
1. Introduction

Cyber attacks on companies, associations and government centers have made it clear that the so-called "cyber war" has become a reality. More and more, industrial concerns and plants are being targeted, which is made clear by the increasing number of security incidents across the world in recent years. The targets and tactics of the attacks have changed. Attacks are becoming increasingly more aggressive and the tools are becoming more effective. This change in the threat situation requires a fundamental re-think of information and access protection measures, as well as the procedures for establishing security concepts. The attackers are upgrading – and both the manufacturers and operators of automation systems must counter these threats.

Headlines about industrial security feature prominently on the front page and in the news. Reports of cyber attacks are already on the daily agenda and we have to face the fact that more and more weak spots are discovered each year. In 1996, there was just a handful of reports about gaps in security that had been discovered. That number then rose exponentially to several thousand in recent years. The actual number of the existing weak points is probably several times higher.

Source: IBM X-Force® Research and Development
IBM X-Force 2012 Mid-year Trend and Risk Report
The fact that these weak points can be exploited and that the risks are real has been shown by investigations, such as the one by ICS-CERT, which found and investigated 198 attacks on control computers in the USA from October, 2011 to September, 2012 alone.

One reason why more and more weak points are being discovered is that fact that in industrial automation and control engineering, standardized hardware and software components are increasingly being used that also allow end-to-end networking among themselves and furthermore with office IT systems and the internet. These open systems simplify the integration of the individual components and reduce the dependency on certain suppliers, since, as a result, interoperability is significantly improved or even made possible in the first place. This speeds up production, allows a better overview and reduces development and production costs. Overall, the aim is for better efficiency to maintain or even improve competitiveness.

These advantages, however, involve risks since open systems are also more susceptible to attacks, manipulation, sabotage, and industrial espionage. Hackers naturally expend the majority of their resources targeting technologies that have the greatest worldwide presence, and the decreasing number of proprietary systems in favor of more open standards makes it easier for attackers and malware to gain access to automation systems.

However, when establishing security concepts, the situation in the automation environment looks very different from that in the office environment. Securing automation networks presents a huge challenge, because it comes into conflict with other important requirements such as performance capability, availability and user-friendliness. In addition, securing a network or system requires constant attention to detail and adaptations, and the job is not finished with a one-time installation the way it normally is when setting up an automation system. Even after the acceptance inspection, threats must be assessed and responded to with adaptations and updates if necessary, to ensure that the system remains secure.

If you are protecting your own systems, it is important to have a reasonable awareness of the risks. It is just as important, however, to be able to trust your own security precautions and to be able to believe in the reliability of your employees. Too little security is negligent and too much security is not cost-effective. In this area of conflict, one should use the right sense of proportion, based on need, when implementing measures which are adapted for industrial systems.
2. Overview of the Industrial Security concept from Siemens

The decisive question is: How can potential risks be significantly minimized and how can adequate, but affordable security be achieved in industrial automation?

Unfortunately, there is no standard solution that can always be applied because each system has individual boundary conditions, risks and protection goals. But there are proven procedures and a reasonable number of conceivable measures which must be taken into consideration for an efficient security concept. On their own, individual security measures always have gaps and are therefore insufficient. An individual measure is easier to by-pass than several in succession.

It is also true that multi-faceted threats must be countered with a variety of measures. For example, viruses cannot be effectively countered with firewalls and unauthorized accesses cannot be countered with virus scanners.

On their own, technical protective measures cannot cover all of the protection goals, which means that accompanying supporting organizational measures are indispensable. Thus, only one overall concept can minimize all of the risks and provide effective protection.

Consequently, the Industrial Security concept from Siemens corresponds to a multi-layer defense, the so-called "defense-in-depth" concept. This concept provides both all-round protection and in-depth protection for an automation system. On the one hand, this means that various, mutually complementary protective mechanisms are in place in order to be able to meet the various threats (all-round protection) and, on the other hand, that there are several barriers, which must be overcome by a potential attacker.

The concept contains the important components of system security, network security and system integrity (see Figure 1).
With a defense-in-depth approach, in which the required security measures shown here are seamlessly interwoven, it is possible to achieve comprehensive and reliable protection of an automated system.

Only the operator can ultimately ensure that the system is operated securely, but the manufacturer, e.g. Siemens, can assist by providing corresponding consulting and security-hardened products with security functions, so that the security concepts can actually be implemented.
3. Plant security

Plant security ensures that technical IT security measures cannot be by-passed in some other way. This includes physical access protection measures such as fences, turnstiles, cameras or card-readers and organizational measures, particularly a security management process, which ensures the long-term security of a plant.

3.1 Physical access protection

The following items can be categorized here:

- Measures and processes which prevent unauthorized persons from gaining access to the premises of the plant.
- Physical separation of different product areas with different access authorizations.
- Physical access protection for critical automation components (e.g. securely locked control cabinets)

The guidelines for physical access protection measures also have an influence on the required IT security measures and their extent. If, for example, only select personnel have access to an area from the beginning, then the network access interfaces or automation systems do not have to be secured to the same extent as would be the case for publicly accessible areas.

**Fig. 2: Physical protection against unauthorized access to production areas**
3.2 Security management

Organizational measures and the introduction of security processes are an indispensable component of plant security. Organizational measures must be closely tied in with the technical measures and they must be mutually supportive. Most protection goals can only be achieved by combining the two types of measures.

One organizational measure is to establish a security management process. In order to make well-founded decisions on which measures make sense, you must first analyze which concrete risks cannot be tolerated. Both the probability of a risk occurring and the possible extent of any damage play a role in this (Figure 3). If the operator neglects to perform a risk analysis or does not determine the protection goals, there is a considerable risk that unsuitable, overly expensive or ineffective measures will be taken and many weak points will not be detected or remedied.

Fig. 3: Decision-making table for assessing and regularly checking risks by means of a plant-specific risk analysis
The protection goals are derived from the risk analysis and serve as the basis for concrete, organizational and technical measures. The measures must be checked after the implementation. The risk must be assessed again from time to time, or if there have been changes, because the threat situation may have changed in the meantime. The process then starts over from the beginning (Figure 4).

**Fig. 4:** The four security management process steps to be continuously executed
4. Network security

The central element of the Industrial Security concept is network security. This includes the protection of automation networks from unauthorized access and the checking of all interfaces to other networks, such as an office network and particularly remote access to the internet. Network security also encompasses protecting communications from interception and manipulation, i.e. encryption of the data transfer and authentication of the respective communication nodes.

4.1 Securing the interfaces between the company and plant network

Transitions to other networks can be monitored and protected by means of firewalls and by setting up a DMZ, if necessary. "DMZ" stands for "demilitarized zone", which means a zone that is secured or shielded. The DMZ is used to provide data for other networks, without granting direct access to the automation network. Typically, a DMZ is designed in such a way that it is also not possible to access or connect to other systems from it, i.e. even if a computer in the DMZ has been taken over by a hacker, the automation network remains protected (Figure 5).

![Diagram of network security with DMZ](attachment:image)

**Fig. 5:** Use of a "demilitarized zone" for transferring data between the company and plant network

4.2 Network segmentation and cell protection concept

The secure segmenting of the plant network into individually protected automation cells minimizes risks and increases security even further. This means
that parts of a network, e.g. an IP subnet, are protected by a security appliance and thus the network is secured by segmentation. Thus, devices within this 'cell' can be protected from unauthorized access from outside without affecting the real-time capability, performance or other functions.

The firewall can now control the access to the cell, which allows the operator to define which network nodes can communicate with one another and what protocols they will use. This not only denies access to unauthorized persons, but also reduces the network load, because rather than allowing all forms of communication, only the desired and required forms of communication are allowed.

The cells are divided and devices are assigned according to the communication and protection needs of the network stations. Furthermore, data transmission from and to the cells can be encrypted by the security appliances by means of a VPN as required. It is thus protected from data espionage and manipulation. This authenticates the communication nodes, and authorizes them for access where necessary. For example, the cell protection concept can be implemented and communications can be secured using "Security Integrated" components such as SCALANCE S Security Appliances or Security CPs for the SIMATIC S7 automation system (Fig. 6).

**Fig. 6:** Network segmentation and cell protection with Security Integrated products (see red padlock symbol)

### 4.3 Secure remote access

More and more plants are being connected to directly via the internet and remote plants are being connected to via mobile networks (GPRS, UMTS, LTE) for
remote servicing, remote applications, and for monitoring machinery installed around the world.

Securing access is especially important here. With the aid of search engines, port scanners, or automated scripts, hackers can easily find unsecured access points without any great effort. This is why the authentication of the communication nodes, the encryption of the data transfer, and the integrity of the data must be ensured. Especially if you are dealing with infrastructures that are critical to the plant. Access by unauthorized persons, the reading of confidential data, and the manipulation of parameters or control commands can cause considerable damage, negatively impact the environment, and endanger personnel.

VPN mechanisms, which precisely provide authentication, encryption and integrity protection, have proven to be especially effective as protective functions for this. The internet-capable security products from Siemens Industry support VPN connections and can thus securely transfer data via the internet or mobile networks as well as control access.

Normally, devices are authenticated as trustworthy by means of certificates and IP addresses or DNS names are used in the firewall rules in order to block or allow access. The VPN appliance and SCALANCE S firewall use user-specific firewall rules to also give the capability of linking access rights to users as well. In this case, users log onto a web interface using their name and password and special firewall rules are assigned to each authorized user so that he or she can be granted access according to his or her access authorization. The advantage here is that you can clearly track who has accessed the system at a specific point in time.

The SCALANCE S623 variant with three firewall ports also provides a way out of a dilemma, which system integrators, OEMs and end users often have to face. On the one hand, machine builders should be able to access their machines at the end user's location for maintenance purposes, but, on the other hand, end user IT departments only grudgingly allows outsiders into the network to which the machine is connected. With the SCALANCE S623, the machine can be connected to the plant network and the firewall can be connected to the internet using the third port. This allows the machine to be accessed from the Internet, but access to the plant network from the Internet can be denied. Thus, it is possible to remotely access the machine from the internet for servicing without having to give the service technician direct access to the plant network (Figure 7).
Fig. 7: Secure remote access to plant units without direct access to the plant network with 3-port firewall.
5. System integrity

Securing a system's integrity should be regarded as the third pillar of a balanced security concept. This means using automation systems and controller components, SCADA and HMI systems, which are protected against unauthorized access and malware or that meet special requirements such as know-how protection.

5.1 Protection of PC-based systems in the plant network

Just as office PC systems are protected against malware and any weak points that are discovered in the operating system or in the user software must be eliminated by installing updates and patches, industrial PCs and PC-based control systems in the plant network also need corresponding protective measures. Many of the protection systems that have proven themselves in office environments can also be used here by using such things as virus scanners. Since virus scanners cannot detect all viruses and are powerless to stop new viruses before the pattern update, alternatives should be considered, if applicable, particularly because software cannot always be updated in a timely manner in an automation environment if no maintenance window is available, e.g. during 24/7 operations.

The use of so-called whitelisting software is an alternative to virus scanners. Whitelisting works with positive lists in which the user can define which processes or programs may run on the computer. If a user or malware then tries to install a new program, this is denied and the damage is prevented.

As a manufacturer of industrial software, Siemens supports the user by testing the software for compatibility with virus scanners or whitelisting software.

5.2 Protection of the control level

It is common knowledge that PCs and networks must be protected against threats. But what measures can be taken to protect manufacturer-specific, proprietary systems? How can one protect programmable logic controllers (PLCs) and operator stations that do not use a commercially available operating system or which use an older version, because they have been in operation for years or even decades?

Third-party security software generally does not provide a solution for this. Access to the system functions of the devices is mostly not possible or only possible to a limited extent. For security solutions for protecting the control level, the manufacturers of automation hardware are asked to implement corresponding security mechanisms and to provide users with system-specific setup options. At the same time, users are encouraged to ask the manufacturers about the existence of such mechanisms and to activate them if setup options are provided for this.
The protection of the control level is essentially aimed at ensuring the availability of the controllers in the field and also to protect intellectual property, because the development know-how with regard to the machine is a big investment for any machine builder. The requirements for access protection and protection against manipulation in production plants are changing, however, as a result of increased interconnection and integration within the IT world in automation technology. This is indispensable for modern control systems and is already integrated in the next generation of controllers, SIMATIC S7-1500. If, for example, Siemens controller functions, such as password protection, block protection or copy protection are used, another essential building block for securing the plant network has been laid.

Individual function blocks can be protected, meaning that unauthorized individuals have no access to their content and cannot therefore copy or change algorithms. At the same time machine reproduction is prevented using copy protection, i.e. linking the program parts with the memory card's serial number, meaning that protected programs can only be used in legitimate machines. These functions help every machine manufacturer to protect their investment and maintain their technological edge.

The cell protection concept described in Figure 6, which previously could only be implemented by special security appliances, has now been expanded by Siemens. The Stateful Inspection Firewall and VPN security functions are integrated into existing hardware, the communications processors for S7 controllers. Encrypted HTML pages via Secure Socket Layer (SSL), intercept-proof transmission of network analysis information to the network management system (SNMP V3), round off the security functions of the communication processors and represent a genuine added value for the user.

CP343-1 Advanced communication processors for Simatic S7-300 PLCs or CP443-1 Advanced for the Simatic S7-400 and CP1543-1 for the S7-1500 thus become "secure interfaces" to the entire plant network and protect their respective, connected controllers and the lower-level networks and, if need be, they also protect the communication between them, thus supplementing or expanding the cell protection concept in a plant.

The CP1628 Ethernet card is used to protect PCs. It can also protect industrial PCs and their communication by means of VPN and a firewall. All of these "security integrated" products are compatible with one another and can establish secure VPN connections with one another, so that practically any part of the system or any kind of automation component can thereby be protected.

6. Roles and rights concepts

We have seen that a defense concept which confronts an attacker with several hurdles (defense-in-depth concept) is required to defend against the various threats and to achieve an appropriate level of protection. At the same time, however, this means that authorized personnel must also overcome these
hurdles. In practice, there are normally different access rights or classes of rights. Specific users may only access specific parts of the system, devices or applications for example. Many have administrator rights, others only have read or write access rights.

Implementing a security concept thus not only serves to defend against attacks, but also implements a rights concept, i.e. to ensure that only authorized persons are able to access a system and even then only in accordance with the rights assigned to them. Typically, individual rights profiles are not created for each person. Instead, roles that have specific rights are defined. Users or groups of users are now assigned to the roles and thus their respective, corresponding access rights are assigned. User management is therefore an important aspect in connection with security.

A universal configuration for all of the automation components facilitates user management in this case, because the roles and rights of various persons can be defined and maintained centrally. Fig. 8 shows a screenshot of the user management in the TIA Portal.

![Fig. 8: User management in the TIA Portal with assignment of roles and rights](image-url)
7. Consideration of attack scenarios in product development

Security measures that are implemented by operators of production plants have been described above. Manufacturers like Siemens naturally support this by providing corresponding security products that are industry-capable in every regard, and concepts, guidelines and recommendations for use of the security products are created for this. Of course, manufacturers can do even more by scrutinizing the automation systems and devices during the development process for possible weak points and eliminating any that are found. Every weak point that is eliminated makes things more difficult for attackers and reduces the overall risk.

Manufacturer processes for increasing product security

Firstly, it is important to increase general understanding of the fact that the measures for preventing weak points must exist in a systematic, universal and sustainable way even during the development process and that they must be constantly checked. Those actively involved in structuring this process – both suppliers and in-house development departments – are, among other things, laying the foundations for security certifications, for example in accordance with ISA Secure (International Society of Automation) or NERC-CIP (North American Electric Reliability Corporation; critical infrastructure protection).

Experts then examine the development processes and the internal organization and evaluate them with regard to security aspects. The goal is to find improvement measures in the relevant processes and, if required or deemed useful, to also introduce new roles and responsibilities within the organization.

The following process improvements have been introduced at SIEMENS Industry in the context of these evaluations and corresponding improvement results have been achieved:

- **Creation of a new role in the Product Lifecycle Management process**
  - Product security experts monitor the PLM process following the "four eyes" principle and are responsible for the product data security.

- **Creation of programming guidelines**
  - The establishing of security programming guidelines in order to prevent known and standard weak points with statistical analysis in the source code.

- **Establishing product security risk management**
  - Expansion of the Siemens internal PLM process, which assesses the security risk in specific PLM steps and from which countermeasures are derived.
• **Optimizations in the development process**
  o Adaptations of the development process in order to proactively increase security against development weak points.

• **Creation of security awareness in development**
  o Create awareness among the developers in order to establish industrial security as a central element.

• **Expansion of the product strategy with security mechanisms**
  o Introduce data integrity, data confidentiality and data availability into the products as fundamental elements.

To deal with weak points found in products that are already in the field, reactive measures are required. If weak points are found in automation components during external or internal testing, they not only must be eliminated, but the relevant target group must also be notified. To do this, a dedicated process must be introduced in which security incidents are handled with a higher priority and the required experts are available quickly. Such a process reduced the processing times at Siemens for the discovered weak points by up to 80 percent and affected users were able to be notified within a few hours.

Of course, the elimination of weak points alone cannot ensure protection against specific cyber attacks such as unauthorized access or the detection of malware. These require active protection mechanisms such as secure authentication, access control or encryption.

But, nevertheless, the elimination of weak points and preventive measures is also an important and necessary component of securing automation systems. Only this combination of security-hardened products and active security measures can result in a consistent, high-performance security concept.
8. Security services

With the Industrial Security Services, Siemens offers its customers solutions and services that can be precisely adapted to the requirements of the automation environment.

The "Security Assessment" forms the basis for consultation. The customer is given a clear depiction of the possible threats, especially in the industrial environment. The result is a meaningful report, which contains the current risk level and recommendations for the effective and sustainable reduction of risks. This gives the customer an ideal basis for planning and implementing targeted measures. On the basis of the "defense-in-depth" concept, Siemens works with the customer to implement measures, which range from the implementation of firewalls, anti-virus/whitelisting software and system hardening to the access control systems with special signatures for the industrial environment (Intrusion Detection (IDS) / Intrusion Prevention (IPS)). The signatures are based on an analysis of the weak points of the components to be protected and ensure that they are protected.

Monitoring & Managed Service

To ensure that systems or machines maintain their security level over their entire lifespan, Siemens provides monitoring capabilities for the continuous monitoring or alarm notification if needed.

Threats are identified and eliminated in time thanks to the monitoring and alarm notifications, before processes or systems are damaged and values are destroyed. The success of the measures is validated by means of strict, cyclically recurring checks.

Many customers concentrate intensely on their core businesses. Therefore, the service line "Industrial Services and Security" can provide them with support within the framework of Managed Services in order to analyze, monitor and continually update their security architecture.
9. Summary: A comprehensive security concept for secure automation

Industrial Security is not only a question of technical implementation, rather it begins with an awareness of security at all levels of management and among employees. With the elements of plant security, network security and the protection of system integrity, it is possible to achieve a comprehensive and in-depth security concept, which can significantly minimize the risks that modern production networks are faced with (Figure 9).

Fig. 9: Implementation of a comprehensive security concept and in-depth defense with the elements of plant security, network security and system integrity.
Within the framework of a holistic industrial security package, Siemens provides products, systems, solutions and professional services in order to be able to implement comprehensive industrial security concepts. The Siemens solution pyramid for Industrial Security is thus comprised of the following three parts (see Figure 10):

**Fig. 10: With a comprehensive security concept for secure automation**

- **Industrial Security Services:** Comprehensive service packages over the entire lifecycle for a tailored security solution
- **Security management:** Processes and guidelines for increasing product security in the in-house development process and recommendations and guidelines for users on using the products and systems.
- **Products and systems:** Security-hardened and tested products and special security components and functions, which are tailored to the requirements of industrial automation.

This results in a comprehensive approach, which provides companies from all branches of industry with a way to a secure production network.