WHITEPAPER 2022

Cybersecurity for Industry

This White Paper provides an overview of the subject of Cybersecurity for Industry. 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 cyber attacks easier and more likely.
Further information about Cybersecurity for Industry at Siemens can be found here:
siemens.com/cybersecurity-industry

SIEMENS

Security disclaimer

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

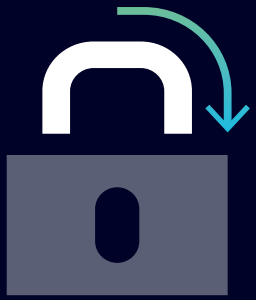
In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

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 Security Advisories under:
https://new.siemens.com/global/en/products/services/cert.html#SecurityPublications



Contents

OT/IT integration means new cyber-risks and requires a comprehensive security concept

1

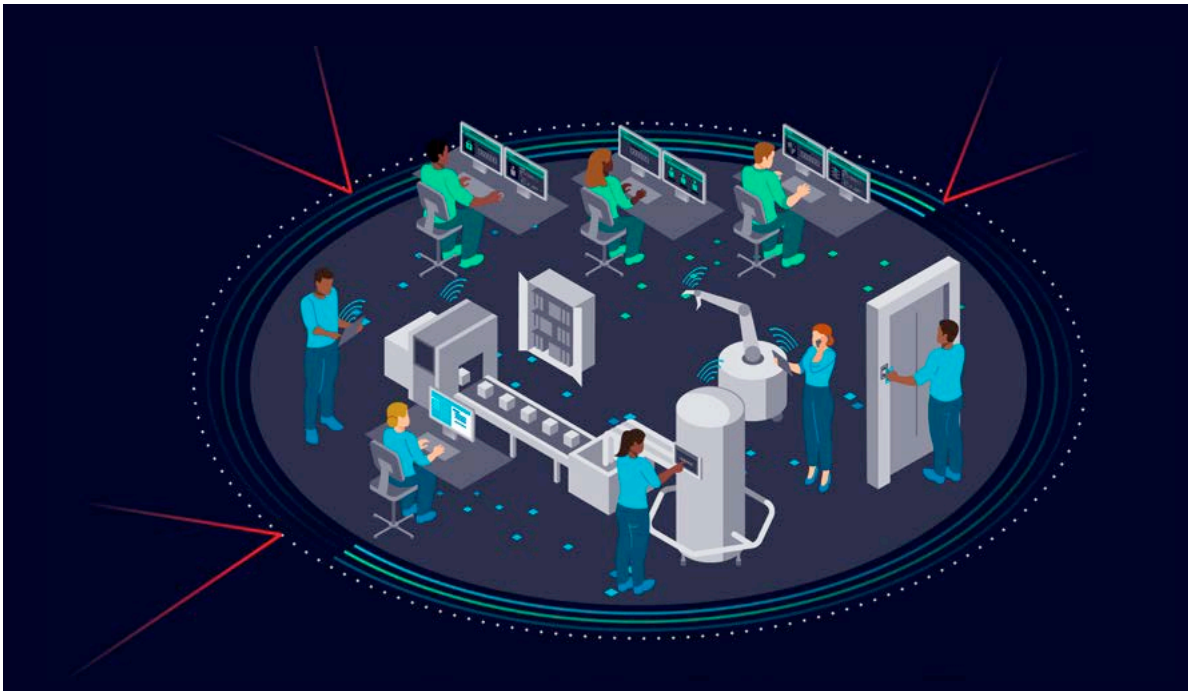
Introduction

Industrial enterprises the world over are facing numerous challenges that are changing dynamically. Overcoming these challenges requires that companies collect, understand, and intelligently use the data they generate. The way to do this is by combining the real and digital worlds and becoming a Digital Enterprise.

As Digital Enterprises they can digitalize and optimize their processes, reduce costs, increase flexibility, and above all, become more sustainable. To make optimal use of their data, they need to become increasingly networked, which means connecting OT (operational technology) to office IT systems and the cloud. The flow of data beyond company boundaries has also grown due to the integration of partners and suppliers and the fact that remote access to plants and systems is becoming more and more frequent – and not just during a global pandemic.

Because of the many benefits of utilizing data, it's become the new gold. But just as data becomes more valuable to companies, it also becomes more attractive to cyber criminals. Increasing connectivity makes their job even easier, resulting in the constant growth in the number of cyber attacks. Not only are the potential costs of these attacks high, they can also threaten a company's very existence and – in the case of critical infrastructure – they can even endanger human lives.

Cybersecurity must protect industrial enterprises from a constant barrage of new threats. IT and OT require equal protection, because the merging of these two domains means that they are subject to the same threats. At the same time, however, the specific characteristics of the IT and OT worlds also have to be taken into account. The special framework conditions in OT, including continuous operation, high performance requirements, and availability, demands an in-depth understanding of industrial processes so that security concepts can be optimally introduced and implemented. For many companies, this task has become too complex. They need a partner who is familiar with and has mastered the special requirements of industry and cybersecurity.



Summary:

Without cybersecurity, there can be no digital transformation. Industrial cybersecurity protects the expertise and productivity of industrial enterprises from the growing number of cyber threats in OT and the IoT.

To protect industrial production, Siemens relies on the multilayer defense-in-depth concept – extended by Zero Trust principles – because the only way to effectively counteract cyber threats is with a comprehensive concept that is applied at all the relevant levels.

These levels are plant security, network security, and the system integrity of automation systems. Siemens offers a wide range of network and automation components with integrated security functions and the associated security services for implementing multilayer security concepts for industry.

This white paper describes how to implement a comprehensive cybersecurity concept to protect an industrial plant and the specific elements that are required.

2

Overview of the Siemens industrial cybersecurity concept

All aspects, from the operating level to the field level and from physical access control to network and terminal protection, must 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.

The plant security, network security, and system integrity elements form the foundation for the industrial security concept at Siemens. All 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 provide a high degree of security, reducing the risk of successful attacks and ultimately improving plant availability and productivity (Figure 1).

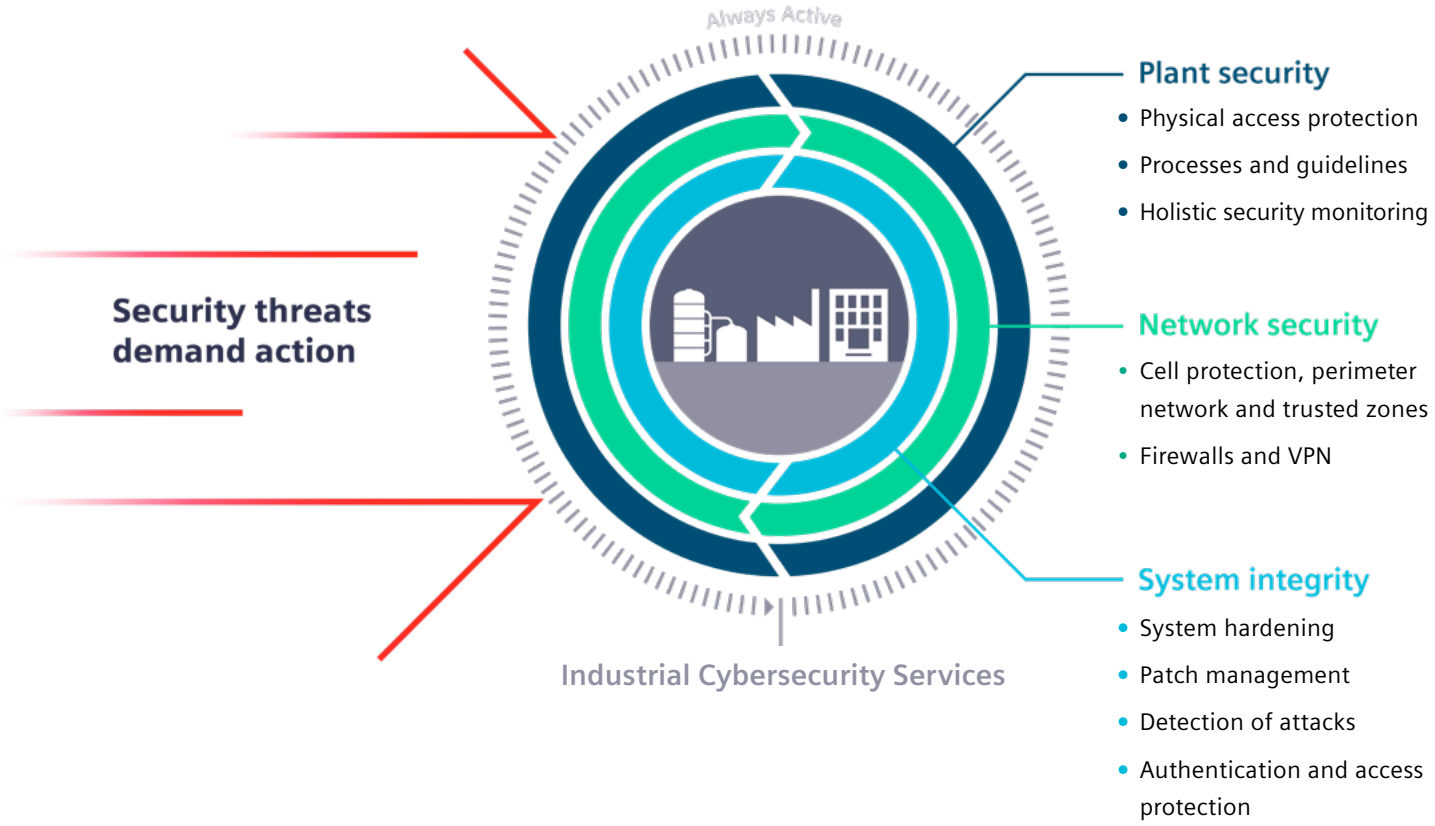


Figure 1: Defense-in-depth concept for industrial plants

3 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.

3.1 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).

Physical access protection policies also impact what IT security measures are required and at 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).

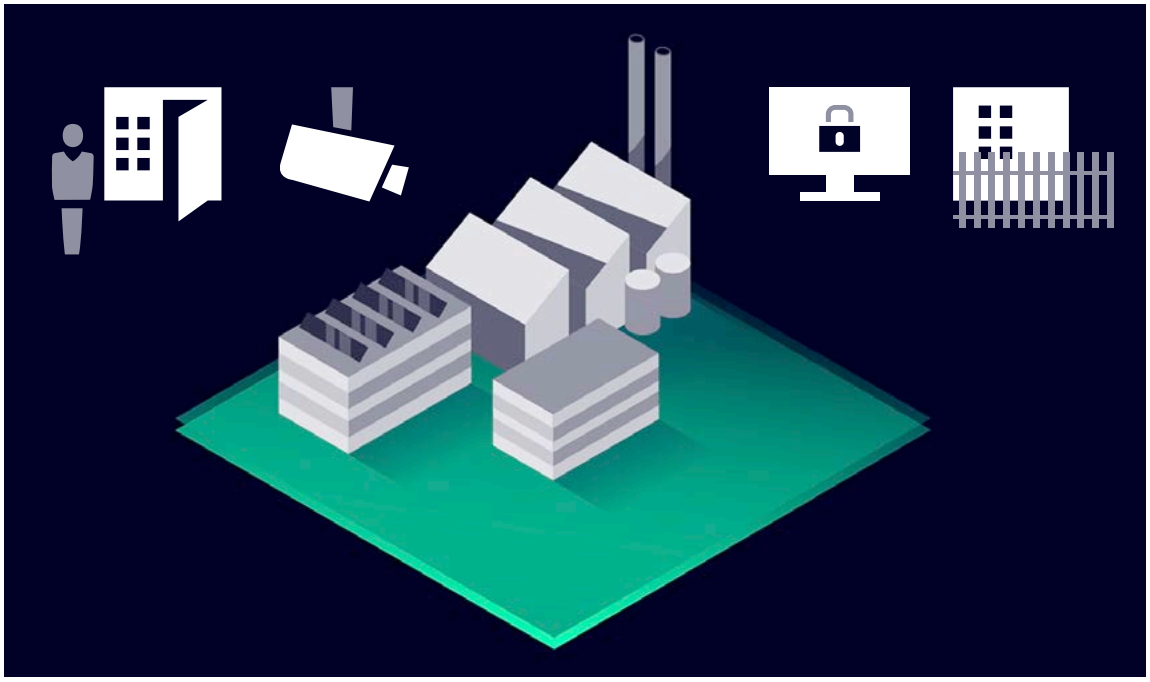


Figure 2: Physical protection against unauthorized access to production areas

3.2 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, because the effectiveness of one is highly dependent on the effectiveness of the other; in fact, most security objectives can be achieved only 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 of them cannot be tolerated. The significance of an identified risk 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.

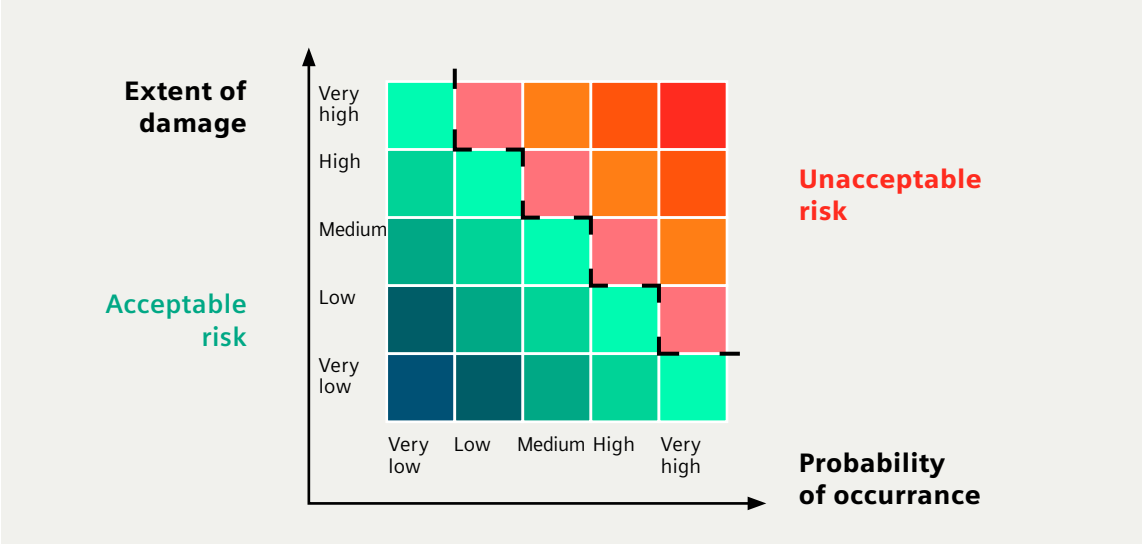


Figure 3: Risk assessment decision table for use in conjunction with a prior plant-specific risk analysis. The risks involved are reviewed regularly

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.

3.3 Plant security services

Our industrial security experts can assist operators in many respects with the design of secure production environments, as they combine know-how in automation, digitalization and cybersecurity. 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 are the **Security Assessments**, which establish the actions necessary to bring a specific plant into compliance with international security standards like the IEC 62443. **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 whole thing is rounded off by **Industrial Security Consulting** with a focus on guidelines and your plant-specific network. On this basis, a security roadmap to protect your system will be created together with you.

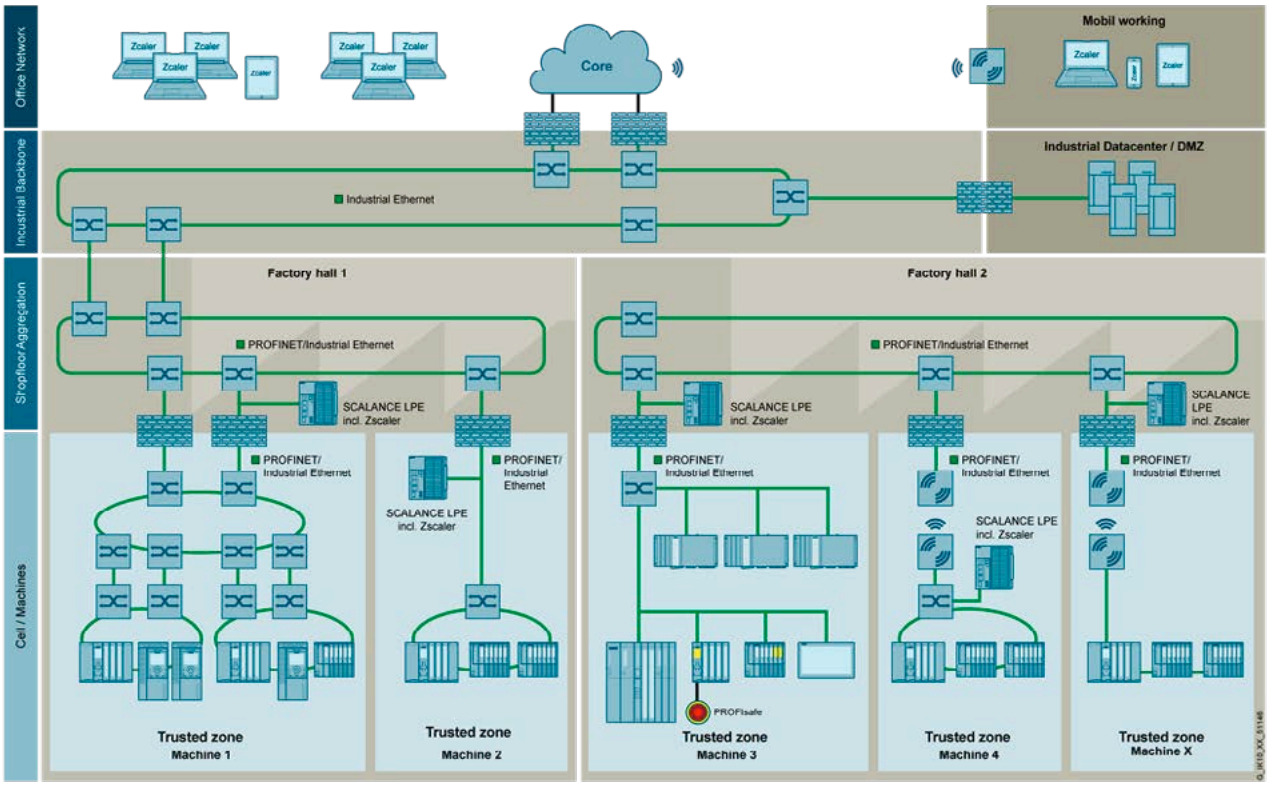
4

Network security

Network security is an essential factor for protection against potential cyber attacks. Until recently it was generally undisputed that the network itself as well as all connected devices need to be protected against any potential threats by means of different technological tools. Single production cells were usually segmented by firewalls and the connection to the IT space was realized through so-called perimeter networks. In recent years interconnectivity and the resulting communication relations are experiencing a massive increase which pushes the defense concept to its limits. Hence, new security concepts are being established that are no longer based on implicitly trusting the local network. Instead, the so-called Zero Trust security concept builds its foundation on verification and authorization of two communicating entities. Protection is hence shifted towards the network participants. To fully apply Zero Trust to the OT area, each device needs to provide specific functionality for ensuring device integrity, to authenticate communication requests, and for data encryption. As most OT devices do not provide such functionality, the concept of Zero Trust cannot be applied to these networks in its entirety. Hence, not only Zero Trust principles but also firewalls and perimeter-based networks need to be considered to ensure a reliable security concept. It is important to view both approaches in the context of defense in depth and that both are flanked by processual and device-specific measures like integrity protection. Consequently, there are several options to achieve in-depth protection of industrial networks.

4.1 Secure access to OT networks based on Zero Trust principles

For many years, IT and OT were kept separate as much as possible. However, due to the increasing OT/IT collaboration, the networks are now growing closer together and flexible access to applications in the production network is becoming essential. In the context of Zero Trust, there is an ideal approach for reliably and securely connecting IT and OT networks. While the devices in the automation network are still protected by firewalls that also offer NAT functions, maintain real-time communication or even functional safety, access to these specific devices is realized by utilizing the principles of Zero Trust. This is made possible by installing Zscaler Private Access, a cloud-based security solution from Zscaler Inc, on Siemens' SCALANCE LPE on-premises processing platform. No changes to the existing network are required for implementation – you simply deploy a SCALANCE LPE with Zscaler App Connector, connect to Zscaler Zero Trust Exchange and take advantage of flexible access, just as you are used to in your IT environment. The central management in the Zscaler cloud platform and the use of only outgoing connections mean that existing firewall rules can be configured even more restrictively. In this way, access to non-critical process steps can be implemented flexibly and securely in order to carry out monitoring and supporting measures without endangering production.



4.2 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 to access the automation network, which means that the automation network remains protected even if a hacker gains control of a system inside the DMZ (Figure 4).

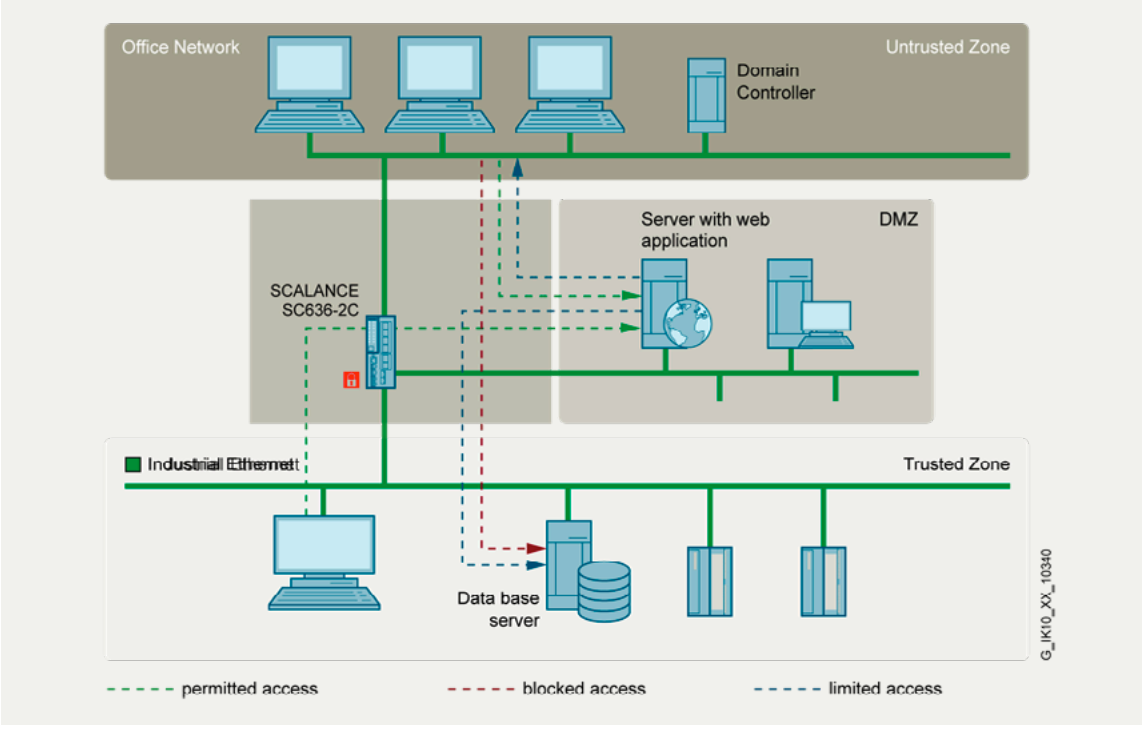


Figure 4: Using a demilitarized zone to transfer data between the company network and a plant network

4.3 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 an industrial 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 network load, 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 SCALANCE S industrial security appliances or the security communications processors for the SIMATIC S7 automation system (Figure 5). The SCALANCE S industrial security appliances provide the possibility to define and protect network cells flexible on the basis of VLANs.

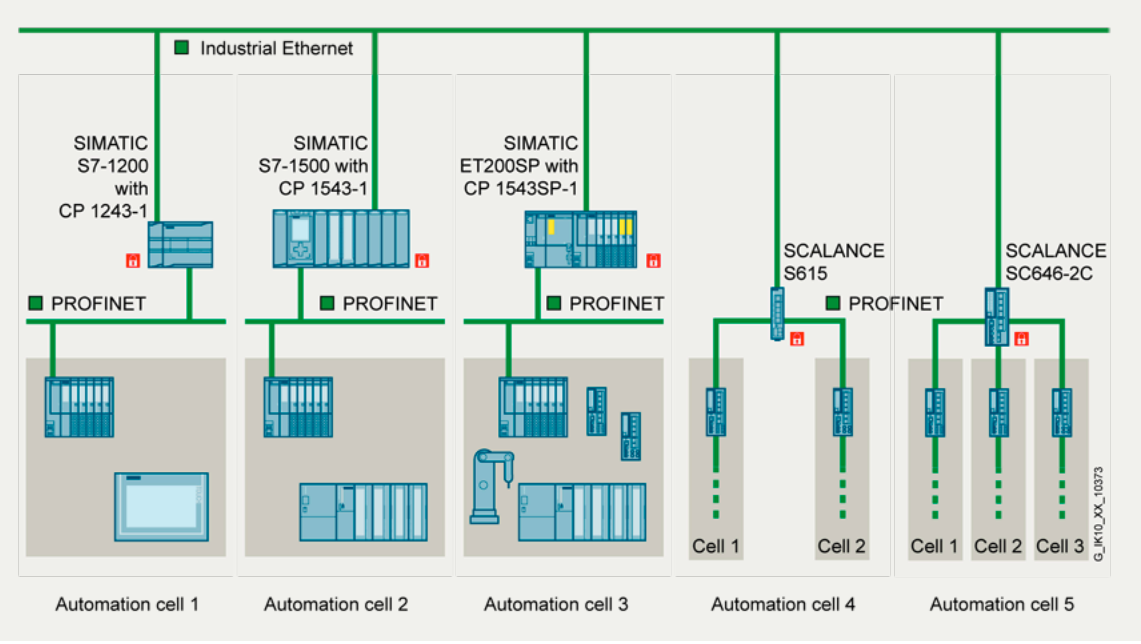


Figure 5: Network segmentation and cell protection with security integrated products (see red padlock symbol)

4.4 Secure remote access

It is becoming increasingly common to connect plants directly to the internet and to link up remote plants via mobile networks (LTE[4G], 5G). 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 entry 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 espionage 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 wireless 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 routers 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. Thus remote maintenance access to the machine is possible without having to allow the service technician direct access to the plant network (Figure 6).

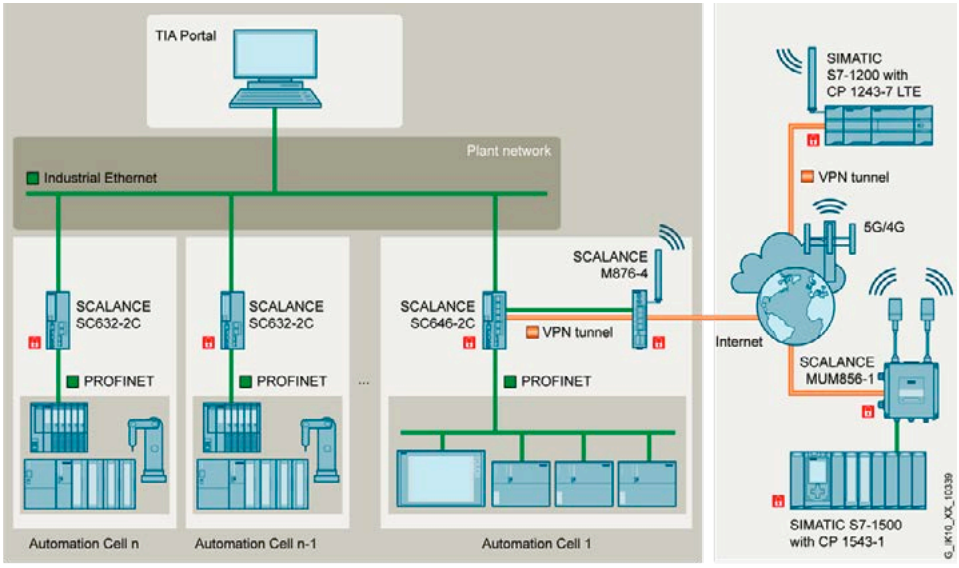


Figure 6: Secure remote access to plant units without direct access to the plant network with three-port firewall

Figure 7: SINEMA Remote Connect is a management platform for efficient and secured remote access to globally distributed plants and machines

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 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 service technician and the machine establish each a connection to a SINEMA Remote Connect server. There 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 function. 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 7 and 8).

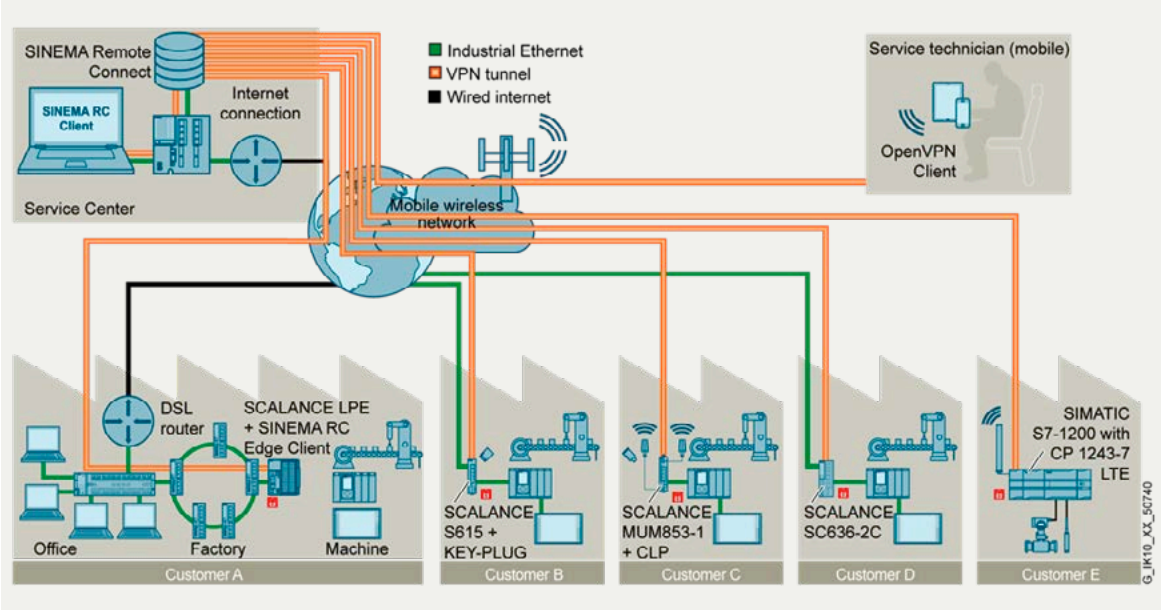


Figure 8: Secured remote access to distributed plants using SINEMA Remote Connect

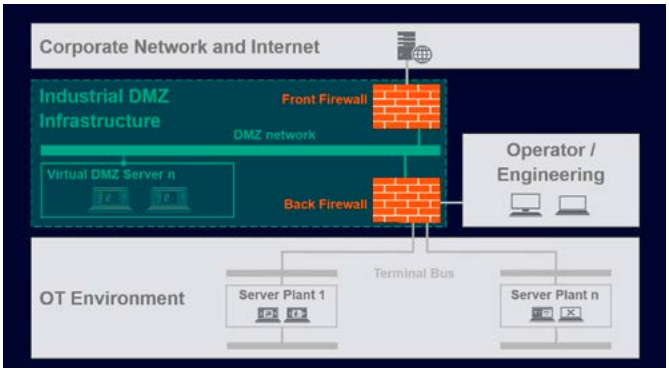
4.5 Efficient and secure network management

Industrial networks are growing more and more complex. Powerful industrial networks are not defined by hardware alone – the right network management is essential.

With the Network Management System SINEC NMS, the possibility exists for central, 24/7 monitoring, management and configuration of networks of up to several thousand nodes across industry sectors. SINEC NMS also enables efficient security management in accordance with IEC 62443. For example, access to the system and the range of functions available to each authorized user can be precisely controlled via the user role administration. The system provides system security through, among other things, encrypted data communication (via certificates and password) between the central SINEC NMS control instance and the SINEC NMS operations distributed in the network. Data communication between SINEC NMS and the infrastructure components in the network can also be encrypted. In addition, SINEC NMS provides a local documentation function via audit trails. For example, audit log entries can be traced by automatically documenting which user performs which activities in the system and when with a time stamp. This also produces significant time and cost savings for official tests. Furthermore, information such as audit logs, system events and network alarms can be passed to a central location via syslog. SINEC NMS also offers central firewall and NAT management. Firewall components (SCALANCE SC-600/S615 and RUGGEDCOM RX1400/1500) can be centrally configured. The firewall rules are created using a graphical description of the permitted communication relationship in the network. The system then automatically generates the device-specific rules. It is also possible to use only the NAT management function independent of firewall management, or vice versa.

SINEC INS (Infrastructure Network Services), the software tool for central network services, offers central network services which are specifically tailored to Operational Technology (OT) in an easy and structured way. Separated from IT services, the OP can establish a self-sufficient network which it can host by itself, e.g., in an OT data center with SINEC INS. The tool includes different security-relevant clients such as a RADIUS server for user and device authentication (MAC authentication) within the network, for example to check who may access which device. The secure syslog client allows sending and receiving security messages in the syslog format meaning, for example audit log entries from SINEC NMS can be sent to the SINEC INS syslog client as syslog messages for further analysis.

4.6 Network security services



Using innovative, state-of-the-art technology, service experts close existing security gaps in your network and thus improve your plant's protection against cyber attacks. In doing so, Siemens builds on its collaboration with professional, best-in-class partners to identify the best solution for your plant.

One example is the **Industrial Next Generation Firewall** based on appliances from Palo Alto Networks. This is a perimeter protection in accordance with the security requirements for industrial automation – tested and approved for use with the Siemens process control system. The first-class firewalls are available in various performance classes and not only function as port filters, but also analyze the layer 7 data traffic at the application level. Additional security subscriptions such as threat detection or URL filtering and a service contract complete the offer.

The firewalls are also part of the **Industrial DMZ Infrastructure** solution. This is a turnkey concept for OT/IT network segmentation with integrated security features. Due to a DMZ (demilitarized zone) with redundant front and back firewalls, the OT systems are shielded from the corporate IT. This network segmentation allows access to systems that require data from the internet and at the same time protects the system network from unauthorized access from outside – corresponding to the IEC 62443. The services forthcoming in the DMZ, e.g., remote access, file exchange, and active directory, are made available as virtual machines on a separate high-performance virtualization host. Furthermore, the DMZ itself is based on the zero trust concept, therefore the communication between the virtual machines within the DMZ is effectively prevented and only takes place via the firewalls.

In order to detect anomalies in the network at an early stage, we rely on **Industrial Anomaly Detection** based on Claroty's Threat Detection Software. It allows automatic asset identification and complete transparency of communication and data traffic within the plant network. By correlating the current traffic with the baseline of normal operations, anomalies are proactively detected. The monitoring is 100% passive without influencing the monitored systems. The powerful, easy-to-use dashboard enables monitoring and event management with minimal configuration. Here, too, a service contract is an integral part.

5 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, protection of intellectual property and secure communication.

Perimeter-based defenses alone cannot keep attackers out, at least not indefinitely. It is safer to assume that attacks will penetrate defenses sooner or later and be prepared with multiple layers that provide defense in depth, which includes the system integrity of automation systems and the use of their integrated security functions.

5.1 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 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 secure communication protocols for controller configuration or HMI connection. These include integrated security mechanisms for significantly enhanced detection of manipulation attempts.

Secure PG/HMI communication: TLS(Transport Layer Security)-based protection of communication between S7-Controllers and Engineering Stations with TIA Portal or HMI-Stations. Encrypts communication by applying individual certificates. This true end-to-end encryption between engineering station or HMI station can prevent any manipulation of the controller program or parameters. With this state-of-the-art secured communication based on TLS (V1.3) a high-level protection will be provided for the automation systems and avoid production loss, data theft and manipulation or sabotage.

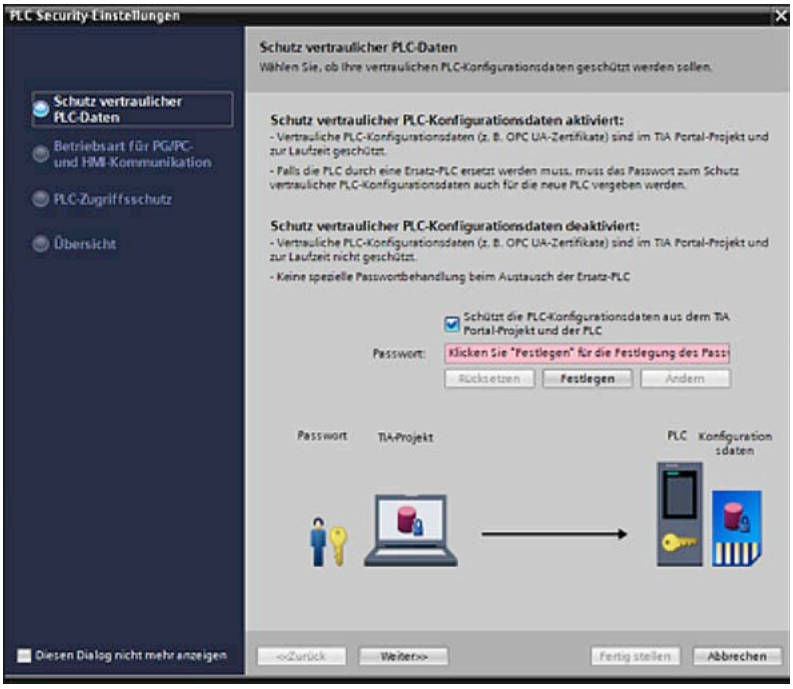


Figure 9:
Screenshot from "Security Wizard" in TIA Portal

For the configuration in TIA Portal the user is guided through a security wizard which assists them with the security settings. This includes the protection of confidential configuration data, the access level of the SIMATIC controller, and the secure PG / HMI communication (Figure 9).

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 communication processors for S7 controllers.

This makes the communication processors for the SIMATIC S7 controller 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 by use of firewall and VPN.

All these security-integrated products are compatible and can connect securely with each other via VPN, so that in effect every part of a plant and all automation components can thus be protected.

5.2 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.

5.3 Secure access management for machines and plants

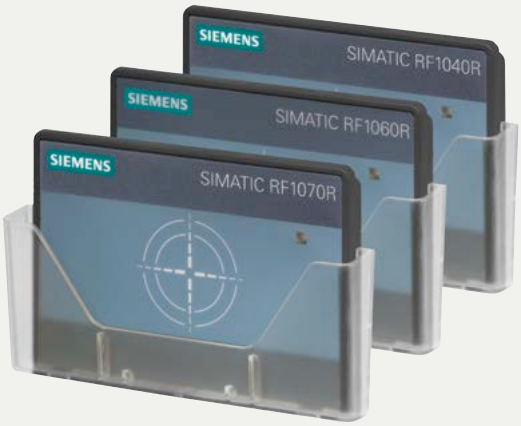


Figure 10: SIMATIC RF1000 for controlling access to machines and equipment

One of the essential mechanisms for protecting automation components is consistent, logged access control. With the SIMATIC RF1000 Access Control Reader, you can reliably identify the personnel operating machines and plants and assign them appropriate access rights.

Depending on your needs and security requirements, login can be exclusively via RFID card – such as an employee ID – or via RFID card and user-specific login data. Logging of accesses enables transparent tracing in the event of security incidents.

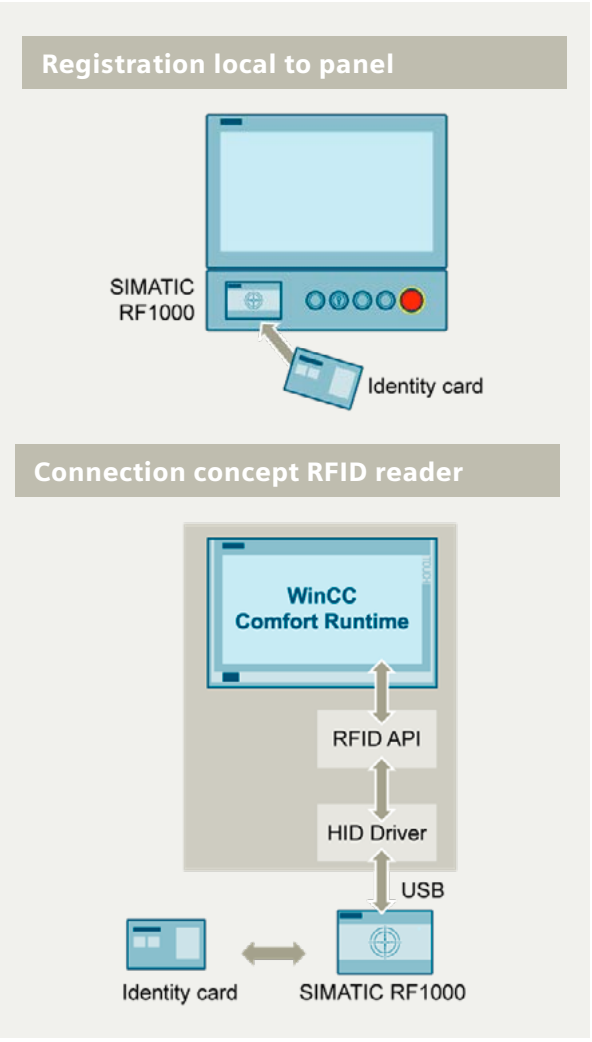


Figure 11: Electronic access control for machines and equipment with RFID-based identity card systems

5.4 System integrity services

Our service experts also rely on proven technologies and partners in the area of system integrity. With **Endpoint Protection**, Siemens offers two different approaches to malware protection of endpoints – based on software from Trellix. While Antivirus blocks malicious applications from running, Application Whitelisting only allows previously defined, trusted applications to run and blocks everything else. Siemens also offers additional services for customers with third-party EDR (Endpoint Detection and Response) solutions.

The **Industrial Vulnerability Manager** is an app that provides security information to enable manufacturers and operators of automation technology to proactively manage their cyber risks – tailored to their system, via one-stop. In the first step, the components to be monitored are defined. These are then continuously monitored for currently published vulnerabilities. If vulnerabilities are identified, a digital security bulletin including all information is generated. The management of the vulnerabilities and the patching can be done via the dashboard. The application is suitable for different requirements – as a cloud solution, on premise or on Siemens Industrial Edge as well as for OEMs.

The **Patch Management** service is also suitable for managing vulnerabilities and critical updates in Microsoft products. Here the patches released monthly by Microsoft are tested and released for compatibility with SIMATIC PCS 7 – this reduces the manual work of your employees and the risk of errors.

Our service experts also offer support for the SIMATIC S7-1500 – with the **Managed Hardening** service you can be sure that you are exploiting the full security potential of your controller.

6

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 12 shows a screenshot of user and rights management in the TIA Portal.

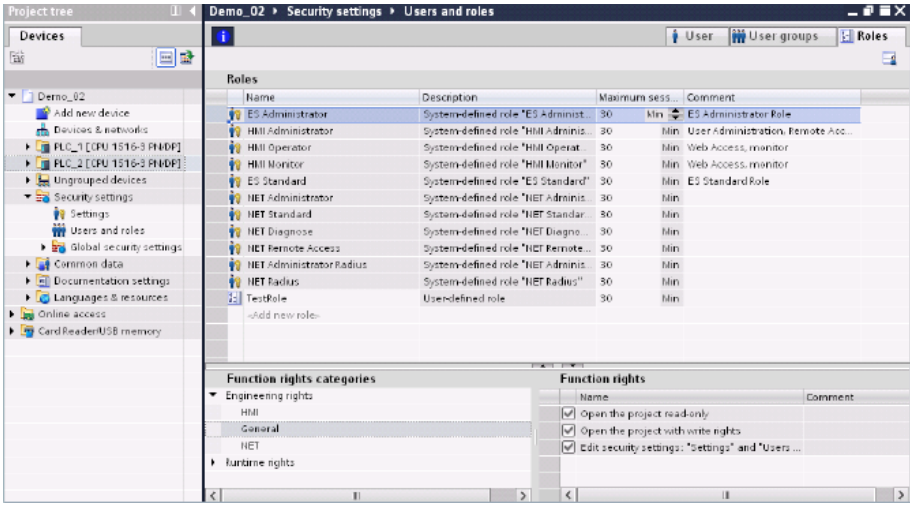


Figure 12: User management in the TIA Portal with assignment of roles and rights

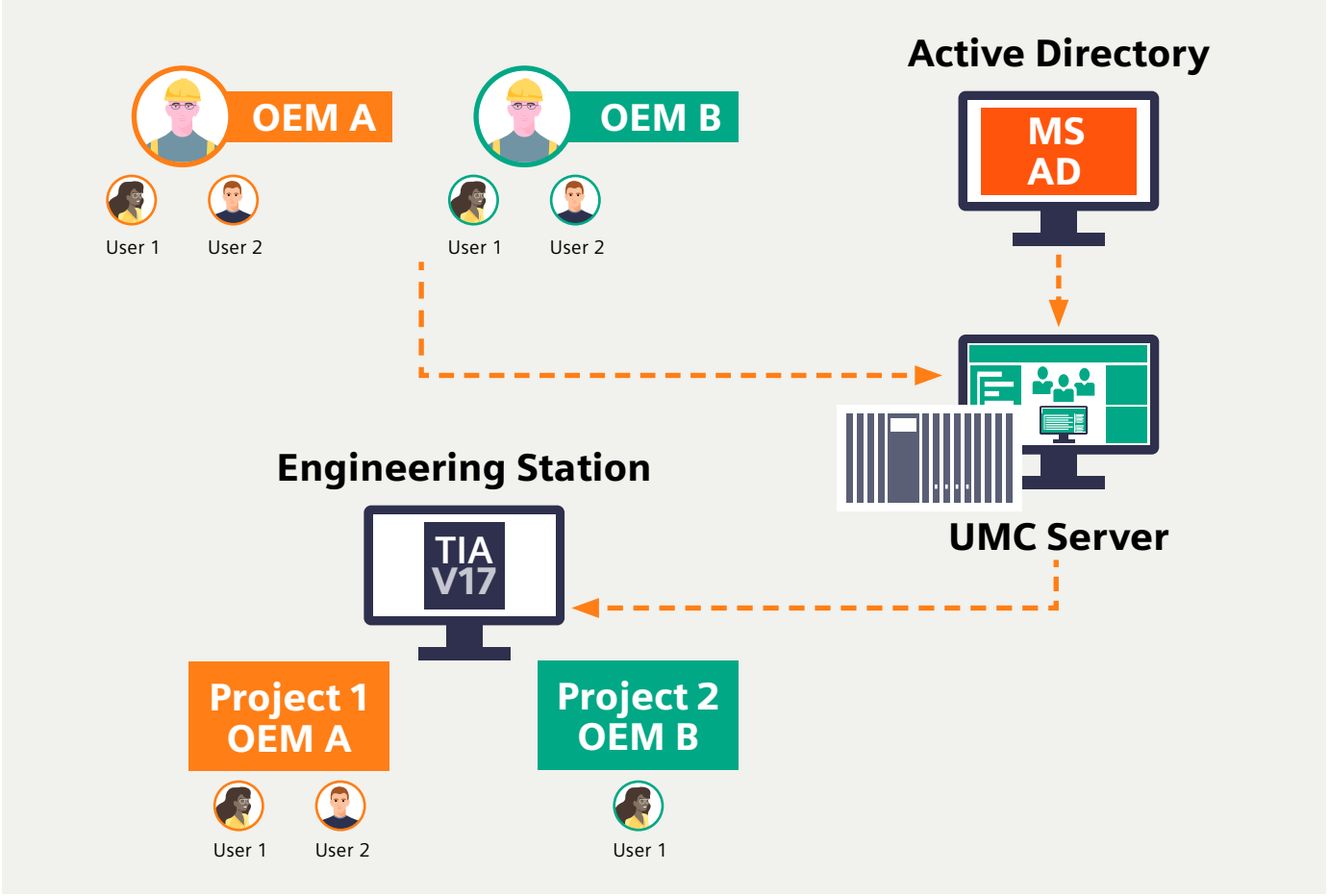
Central user management

The user management component or UMC is a pool of users and user groups configured on a separate server. This allows central users and user group management.

With UMC, it is possible to import the users and user groups e.g. from Microsoft Active Directory to TIA portal. The UMC Agent is installed with TIA portal and used independent of the project. The main benefit of UMC is the efficiency it provides when it comes to user management and role assignment between different projects, and different engineering stations.

When adding or removing users, or changing passwords, this is done ONCE on the UMC server. The users or user groups can then be imported to TIA portal.

This means: Maintenance of users only once for the system, not multiply across projects or even locally for a product as an “easy to use” basis for efficient administration of personalized security in the system.



7

Consideration of cybersecurity 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 13).

The need for security is particularly high when developing and manufacturing automation products with security functions. For this reason, these protective and monitoring measures are particularly relevant for manufacturers of products with security functions. But not only the portfolio of security products benefits from the HSC, but also all standard products, such as the engineering tool TIA Portal and the Simatic S7-1200 and Simatic S7-1500 controllers. Because these products can also reduce the risk for the end user if the products are tested for weaknesses during development and the design is optimized through risk analysis.

HSC answers key questions for security in business

„What in my business do I need to protect?“

Identification of the critical business assets is a core component of the concept

„Which level of security do I need?“

Security level drives requirements, in alignment with IEC 62443, to protect against attacks

„How do I protect the specific assets?“

Standards based security solutions are applied to protect and monitor the critical assets

HSC addresses 5 levers including the IT

Figure 13: Holistic security concept takes security on the next level – a holistic approach for IT and OT

8

Summary: Industrial cyber-security for production plants

Even just a few years ago, cybersecurity 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 industrial cybersecurity 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 14).

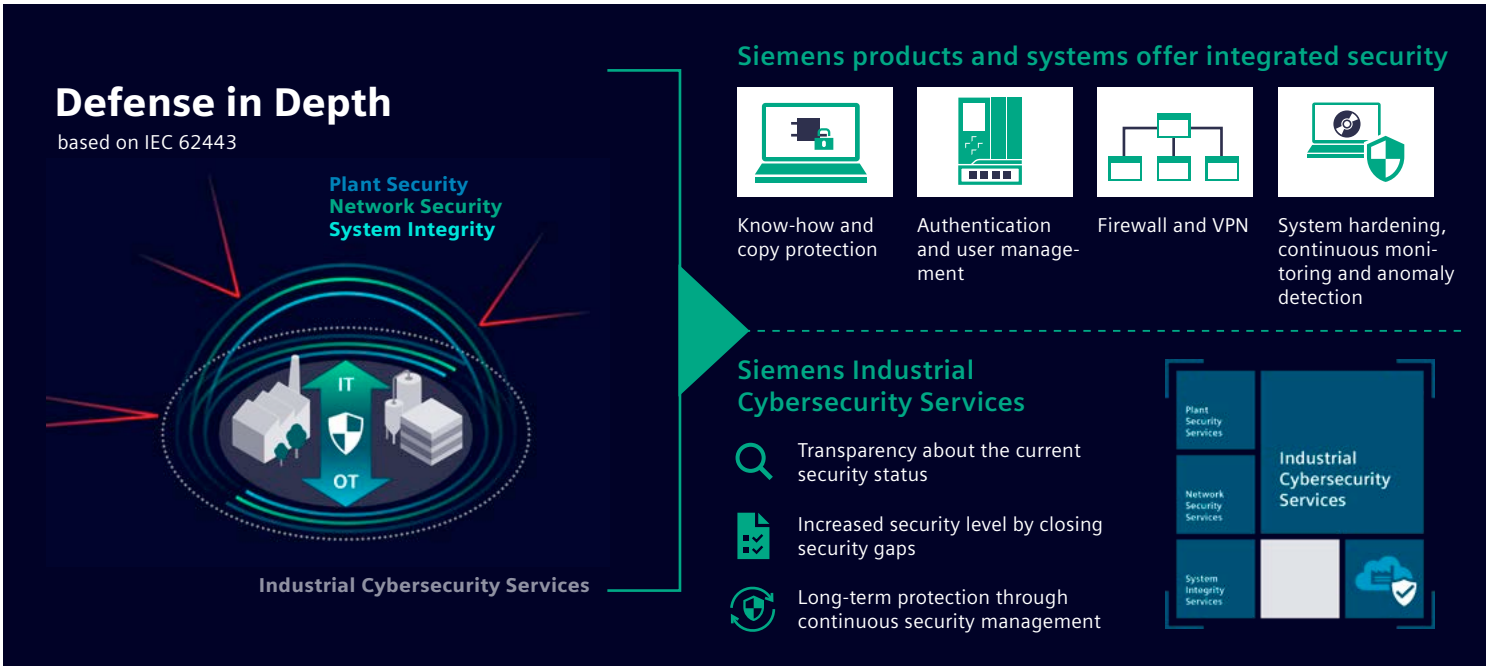


Figure 14: Industrial security portfolio: concept, products and services

Figure 15: Cybersecurity for Industry – for comprehensively protected production plants

Published by
Siemens AG

Digital Industries
Gleiwitzer Str. 555
90475 Nürnberg, Germany

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

100 Technology Drive
Alpharetta, GA 30005
United States

Article No. DIFA-B10222-00-7600

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