WHITEPAPER 2025

Cybersecurity for Industry

SIEMENS

siemens.com/cybersecurity-industry

Foreword

This white paper provides an overview of the topic of Cybersecurity for Industry.

It outlines the threats and hazards facing industrial automation systems and production plants and presents best-practice approaches for minimizing these risks. The aim is to help establish an appropriate level of protection that is both economically viable and technically sound.

The paper also addresses the growing need to respond to escalating threats driven by digitalization trends such as universal connectivity and the increasing value and volume of data, which collectively make cyberattacks more feasible and more frequent.

Further information about Cybersecurity for Industry at Siemens is available at

siemens.com/cybersecurity-industry ↗

Security disclaimer

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

To protect these environments against cyber threats, it is essential to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions form one key element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines, components, and networks. These 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, such as firewalls and/or network segmentation, are in place.

Siemens continuously develops its products and solutions to enhance their security. Siemens strongly recommends applying updates as soon as they become available and always using the latest supported product versions. Using outdated or unsupported versions and failing to apply updates may increase the customer's exposure to cyber threats.

To stay up to date on product updates, subscribe to the Siemens Security Advisories at:

Siemens Security Advisories ↗

Contents

1.

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

Introduction

Industrial enterprises worldwide face many challenges that are evolving rapidly. To overcome them, companies must collect, understand, and make intelligent use of the data they generate and that are available in the Industrial Internet of Things (IIoT). The key is to combine the real and the digital worlds to become a true Digital Enterprise.

As Digital Enterprises, companies can digitalize and optimize processes, reduce costs, increase flexibility, and improve sustainability. To make the most of their data, they need to become more connected by linking operational technology (OT) with information technology (IT) systems and the cloud. Combining the real and the digital worlds with a comprehensive Digital Twin approach and cutting-edge technologies enable a continuous loop of optimization in near real-time.

The emergence of the Industrial Metaverse, which is about connecting the real and digital worlds even more closely and fluidly, has led to an increase in data flows beyond company boundaries, driven by integration with partners and suppliers as well as more frequent remote access to plants and systems.

With data becoming a new kind of gold, it also attracts cybercriminals. Greater connectivity makes their job easier, leading to a steady rise in cyberattacks. The costs of such attacks can be severe, threatening the very existence of a company and, in critical infrastructure, even human lives.

Cybersecurity must protect industrial enterprises against a constant stream of evolving threats. IT and OT require equal safeguards because their convergence exposes both to the same risks. Yet, the unique demands of IT and OT must also be considered. OT's special conditions, such as continuous operation, high performance, and availability, require deep knowledge of industrial processes to design and implement effective security concepts. For many companies, managing this complexity has become overwhelming. They need a partner experienced in both industrial requirements and cybersecurity to guide and support them.

Summary

Digital transformation cannot succeed without cybersecurity. Industrial cybersecurity protects the data, expertise, and productivity of industrial enterprises from the shop floor to the top floor against the growing cyber threats targeting OT and the IIoT.

Through its integrated Charter of Trust initiative and extensive partner ecosystem, Siemens provides a multilayer defense-in-depth approach to safeguard industrial production, enhanced by Zero Trust principles, because effectively countering cyber threats requires a comprehensive strategy applied across all relevant levels.

These levels include plant security, network security, and the system integrity of automation systems. Siemens provides a broad range of network and automation components with integrated security functions and the associated security services to support the implementation of multilayer protection in industry.

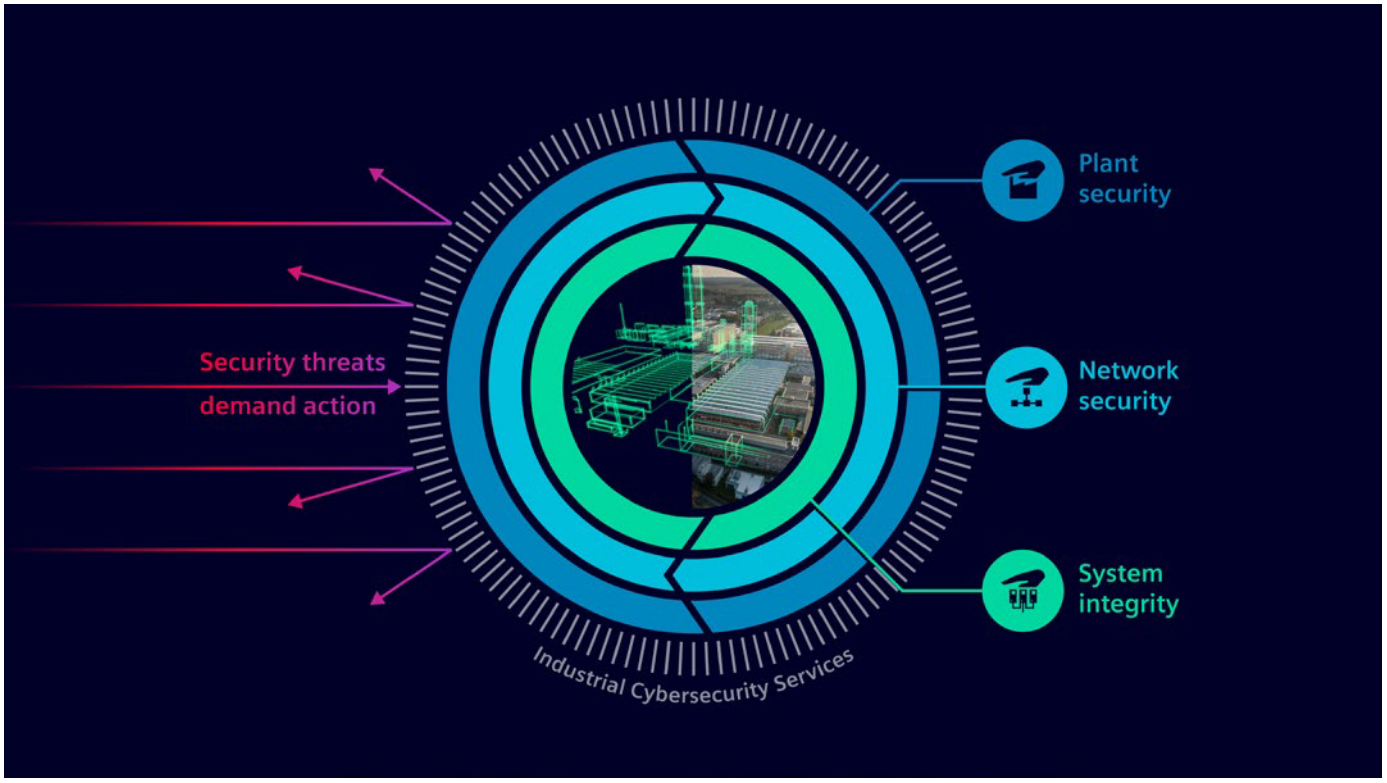
This white paper explains how to implement a comprehensive cybersecurity concept to protect industrial plants, detailing the essential elements involved.

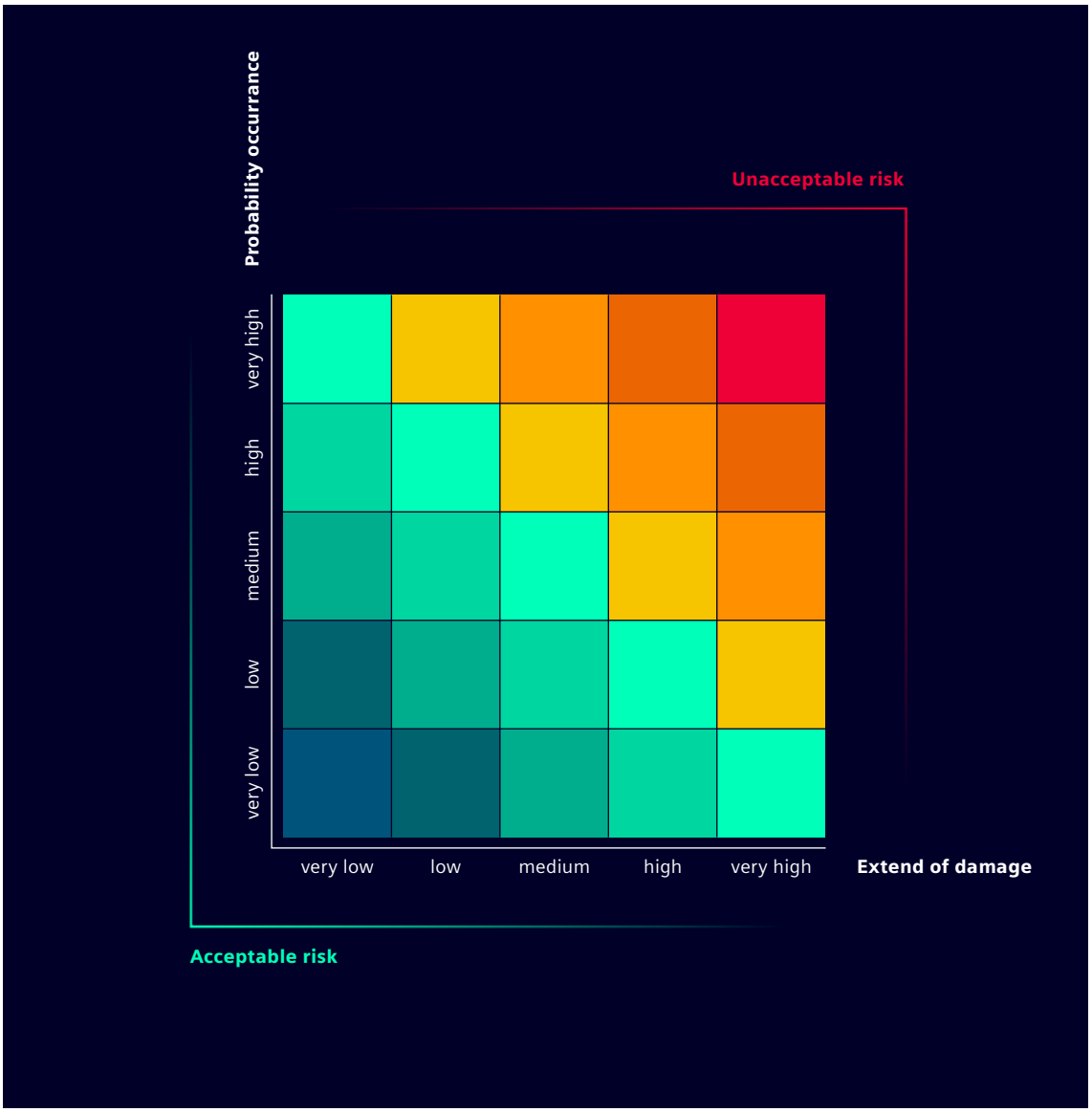
2.

Overview of the Siemens industrial cybersecurity concept

To effectively protect industrial systems from internal and external cyberattacks, all areas must be addressed in parallel. This includes everything from the operating and field levels to physical access control, network security, and terminal protection. A defense-in-depth strategy, based on the leading IEC 62443 standard for industrial automation security, offers the most effective approach.

At Siemens, industrial cybersecurity is built on three essential pillars: plant security, network security, and system integrity. This comprehensive approach covers all critical aspects, including physical access protection, organizational measures such as policies and processes, and technical safeguards that protect networks and systems from unauthorized access, espionage, and manipulation. Multiple layers of protection and the combined effect of coordinated measures help ensure a high level of security. This reduces the risk of successful attacks and supports improved availability and productivity across the plant.





Risk assessment decision table for use along with a prior plant-specific risk analysis. The risks involved are reviewed regularly

Security management

Appropriate organizational measures and the introduction of effective security processes are vital for plant security. Organizational measures must be closely coordinated with technical measures, because the effectiveness of one strongly depends on the effectiveness of the other. In most cases, security objectives can only be achieved through a combination of both.

Organizational measures include the establishment of a security management process. The first step in determining which measures are required in a given situation is to analyze the specific risks and identify which of them cannot be tolerated. The significance of an identified risk depends on the potential damage and the likelihood of its occurrence.

Without a proper risk analysis and clearly defined security objectives, the measures implemented may prove ineffective or unnecessarily expensive, and some weaknesses may remain undetected.

The risk analysis defines security objectives that form the basis for specific organizational and technical measures. These measures must be reviewed after implementation. The risk should be reassessed periodically or after significant changes to account for any shifts in the threat landscape or underlying conditions. The risk analysis provides the foundation for implementing protective and, where applicable, monitoring measures.

3.

Plant security

Plant security establishes the conditions needed to ensure that technical IT security measures cannot be bypassed by other means. These measures include physical access protection systems such as barriers, turnstiles, surveillance cameras, and card readers. Organizational measures include a defined security management process to maintain and enforce security throughout the plant.

3.1 Security transparency in plant operations

To support this security approach, our industrial security experts assist operators in designing secure production environments. They bring together expertise in automation, digitalization, and cybersecurity to offer comprehensive support.

A risk analysis provides transparency on a plant's current security status and identifies vulnerabilities. It forms the basis for assessing corresponding risks. The resulting measures are compiled into a structured action plan ("roadmap") that outlines how to improve the plant's overall security level.

Security Assessments, for example, define the steps needed to bring a plant in line with international standards such as IEC 62443 or NIS2 directive. Scanning Services can be used on their own or in combination to assess existing computing devices and detect vulnerabilities, including checks against defined security levels. This approach is supported by Industrial Security Consulting, which focuses on site-specific guidelines and network architecture. It also includes Incident Analysis, where our experts provide immediate assistance and help uncover root causes to prevent future incidents. Together with you, we develop a tailored security roadmap to protect your system.

Industrial Security Trainings are also available to raise awareness and reduce the risk of security incidents caused by human error.

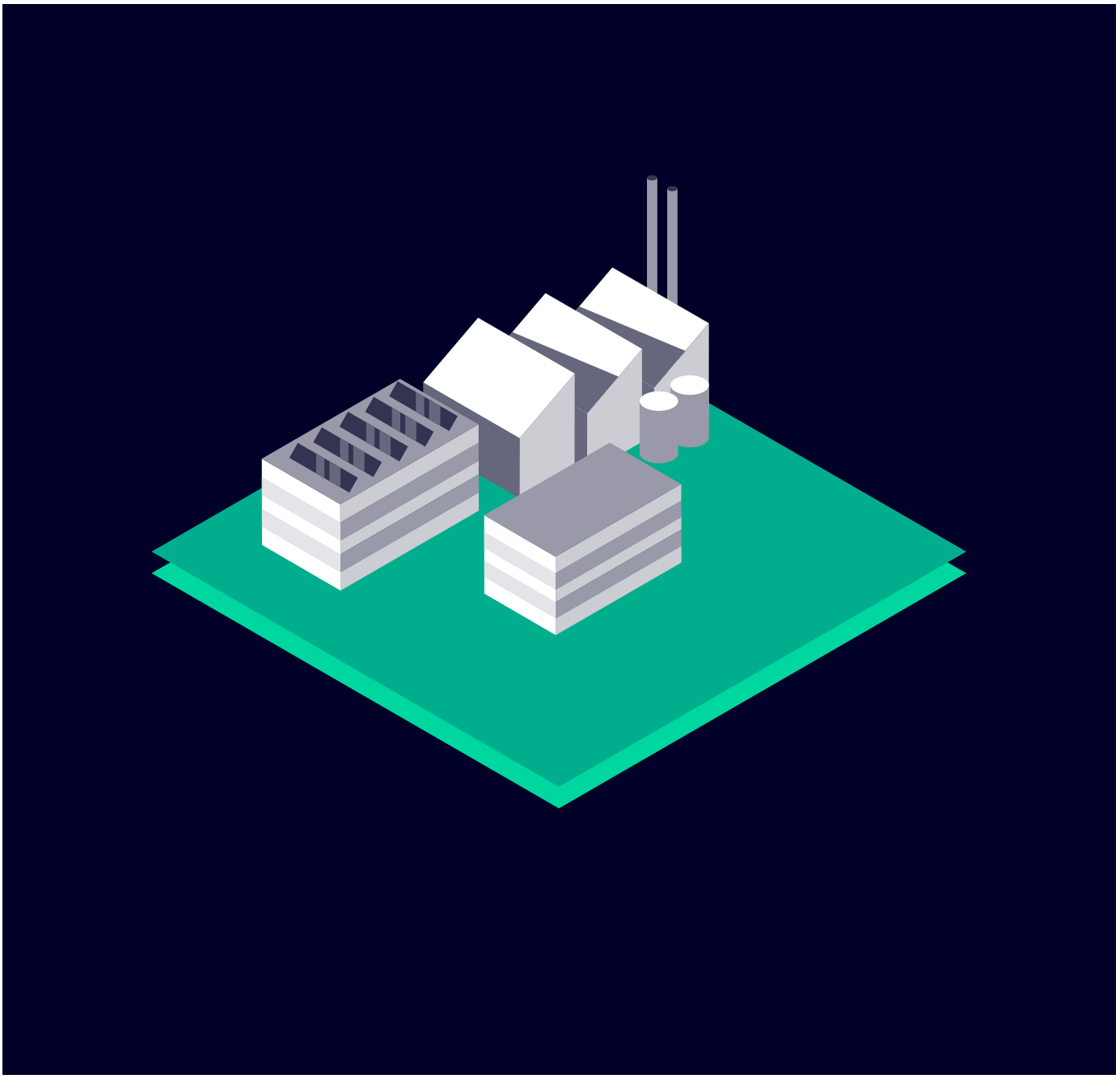
3.2 Physical access protection

This includes measures and processes designed to prevent unauthorized individuals from entering the plant or surrounding areas. Key aspects include:

- Restricting access to the plant premises through defined security procedures.
- Physically separating production areas based on access rights and responsibilities.
- Physical access protection for critical automation components, such as locking control cabinets.

Physical access protection also influences the type and strength of IT security measures required. For example, if access to a specific area is tightly restricted to authorized personnel only, the network interfaces or automation systems in that area may not require the same level of protection as those in more accessible zones.

Physical protection
against unauthorized access
to production areas



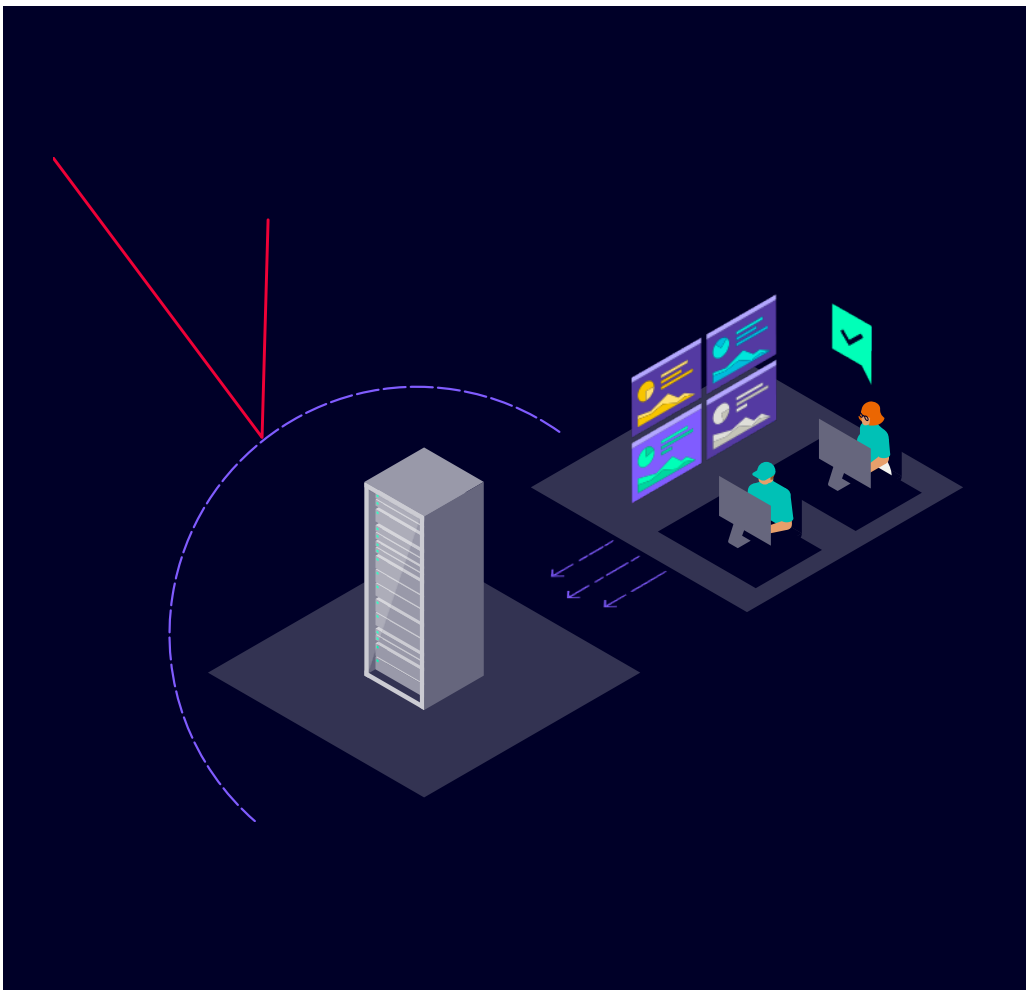
3.3 Managed security services and IT/OT Security Operations Center

Cybersecurity is not a one-time action but an ongoing process. However, you do not have to manage everything alone or build and maintain your own resources. Remote Industrial Operations Services provide a team of proven experts who monitor and manage the health and security of your IT/OT infrastructure remotely, 24/7, allowing you to focus on your core business.

These modular services are tailored to your individual infrastructure and needs. Managed security services range from vulnerability management and anomaly monitoring to a full OT Security Operation Center (SOC) as a service for holistic, continuous protection of your OT systems. By leveraging the SOC that reliably safeguards Siemens' own factories worldwide, we also protect your plants. Log files are collected and forwarded to a Security Information and Event Management (SIEM) system. Our experts monitor and triage security alerts to prioritize real threats and trigger remediation. Critical incidents are managed closely with you, supporting containment and threat eradication during remediation and recovery. The service includes comprehensive dashboards and reporting to assist with reporting critical incidents to authorities. Additionally, Siemens experts handle patching, backup, and restore management, maintaining system integrity through regular backups and verifications. They provide disaster recovery support to quickly restore critical systems and minimize disruption impact.

For plants with a high degree of IT/OT integration seeking full vertical coverage up to the corporate IT level, we offer comprehensive managed IT/OT SOC services in collaboration with Accenture.

The security strategy is continuously adapted to new situations, threats, and regulations to provide optimal protection. Remote Industrial Operations Services help you stay compliant with cybersecurity laws and regulations such as NIS2.



Remote Industrial Operations Services provide managed security services and SOC as a Service to continuously protect against cyber threats.

SINEC NMS software is a network management system for the central monitoring and managing of industrial networks.

3.4 Network asset discovery and management

Industrial networks are becoming increasingly complex. Powerful industrial networks are not defined by hardware alone – effective network management is essential.

With the network management system SINEC NMS, it is possible to centrally monitor, manage, and configure networks of up to several thousand nodes across different industry sectors, 24 hours a day, seven days a week. SINEC NMS also supports efficient security management in accordance with IEC 62443. For example, system access and the range of functions available to each authorized user can be precisely controlled through user role administration. The system ensures security through encrypted data communication, using certificates and passwords, between the central SINEC NMS control instance and the distributed SINEC NMS operations within the network. Data communication between SINEC NMS and infrastructure components can also be encrypted. Additionally, SINEC NMS provides local documentation through audit trails. Audit log entries record which user performed which activities in the system and when, complete with timestamps. This feature results in significant time and cost savings during official tests.

Moreover, information such as audit logs, system events, and network alarms can be forwarded to a central location via syslog. SINEC NMS also offers central firewall and NAT management. Firewall components such as SCALANCE SC-600/S615 and RUGGEDCOM RX1400/1500 can be configured centrally. Firewall rules are created using a graphical description of permitted communication relationships within the network, and the system automatically generates device-specific rules. It is also possible to use the NAT management function independently of firewall management, or vice versa.

SINEC INS (infrastructure network services) is a software tool for central network services specifically tailored to OT in a simple and structured way. Separated from IT services, the operator can establish and host a self-sufficient network, for example in an OT data center, using SINEC INS. The tool includes several security-relevant clients, such as a RADIUS server for user and device authentication (MAC authentication), which verifies who may access which device within the network. The secure syslog client allows sending and receiving security messages in syslog format, meaning audit log entries from SINEC NMS can be sent to the SINEC INS syslog client as syslog messages for further analysis.

4.

Network security

Network security is a crucial factor in protecting against potential cyberattacks. Until recently, it was generally accepted that both the network itself and all connected devices must be protected against threats using various technological tools. Single production cells were typically segmented by firewalls, and connections to the IT environment were made through so-called perimeter networks. In recent years, however, interconnectivity and resulting communication have increased dramatically, pushing traditional defense concepts to their limits. As a result, new security approaches have emerged that no longer assume implicit trust within the local network. Instead, the Zero Trust security concept relies on verifying and authorizing both entities involved in communication. Protection is therefore shifted toward the network participants.

To fully implement Zero Trust in the OT area, each device must offer specific functions to ensure device integrity, authenticate communication requests, and encrypt data. Since most OT devices lack these capabilities, Zero Trust cannot be applied in full to these networks. Consequently, both Zero Trust principles and firewalls with perimeter-based networks must be combined to ensure a reliable security concept. It is important to consider both approaches within a defense-in-depth framework, supported by process and device-specific measures such as integrity protection. Consequently, there are multiple options to achieve in-depth protection of industrial networks.

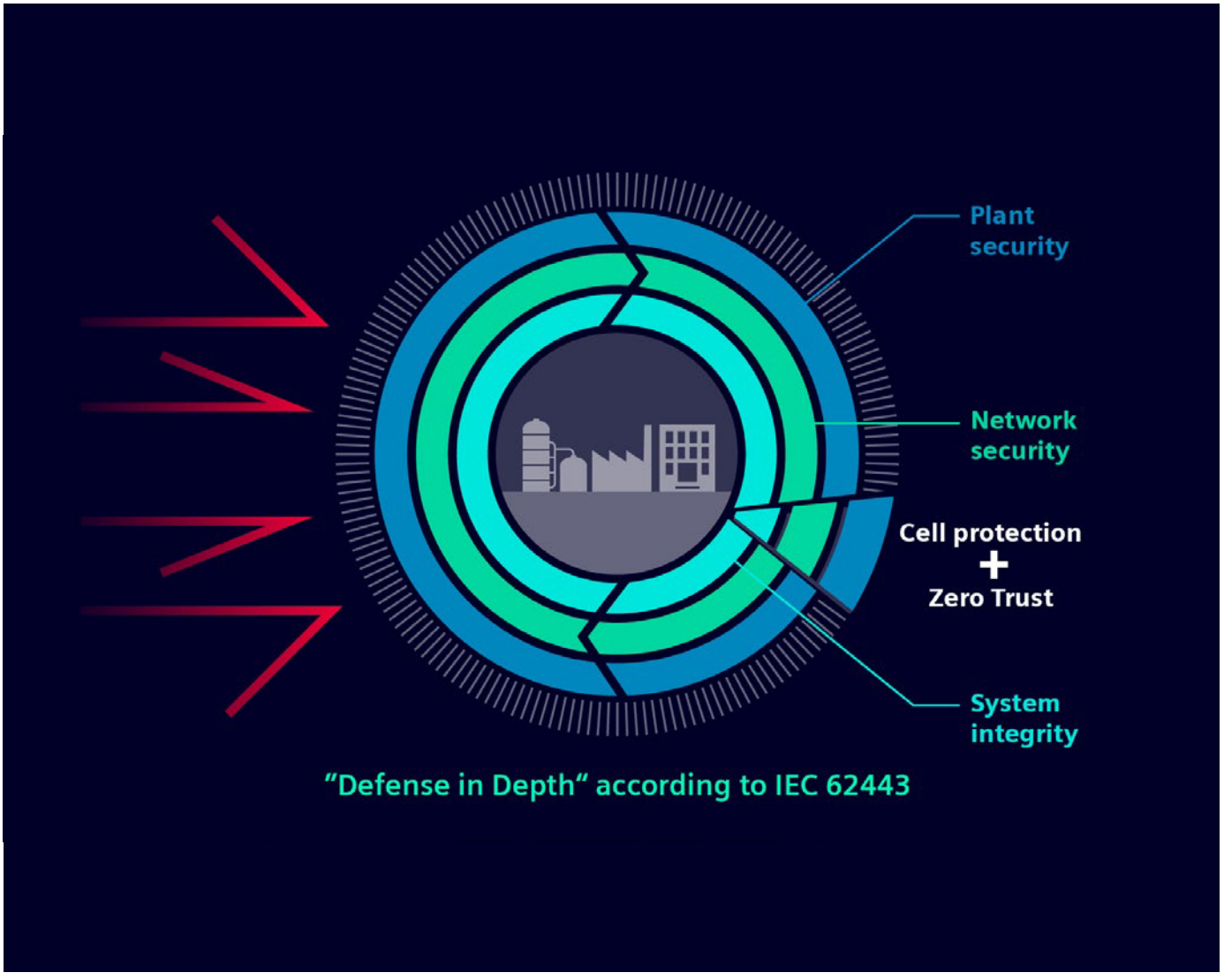
4.1. Secure access to OT networks based on Zero Trust principles

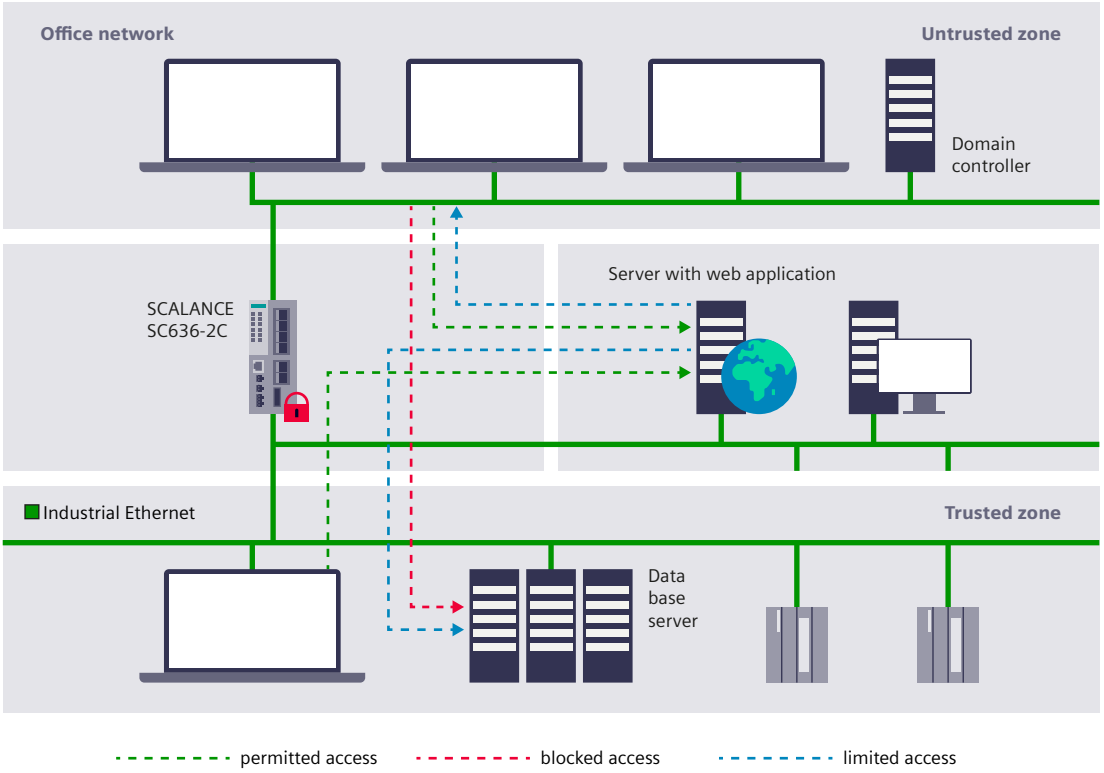
For many years, IT and OT were kept as separate as possible. However, with increasing IT/OT collaboration, the networks are now growing closer together, and flexible access to applications in the production network is becoming essential. Artificial intelligence-driven use cases such as predictive maintenance, process optimization, and security analytics require as much information as possible, which in turn demands high connectivity between network assets and cloud environments, whether private or public. Given this vast amount of communication, a security concept is needed that provides fine-grained access control for users and applications. Zero Trust security architectures enable such scenarios.

Building on existing network designs and perimeter-based security concepts, network participants will identify themselves using digital identities. Communication requests can then be allowed or denied based on these identities. This approach provides fine-grained access control for all types of requests, local or remote, and may also allow verification of an asset's integrity before granting access.

Currently, most OT environments are not yet ready to implement a full Zero Trust network architecture for every network participant. However, the journey toward Zero Trust can begin today using traditional cell protection concepts and encrypted communication. Introducing digital identities and certificates into devices and applications within the OT environment will establish the foundation for holistic future Zero Trust architectures.

Proven defense-in-depth security concept enriched by the Zero Trust principles.





Using a demilitarized zone (DMZ) for data transfer between the company network and a plant network

4.2. Securing interfaces to other networks

Interfaces to other networks can be monitored and protected by using firewalls and, where appropriate, by establishing a demilitarized zone (DMZ). A DMZ is a network area where technical security measures protect access to data, devices, servers, and services within that area. The systems installed inside the DMZ are shielded from other networks by firewalls that control access.

This separation allows data from internal networks, such as the automation network, to be provided on external networks without granting direct access to the automation network. A DMZ is typically designed so that it does not allow access to the automation network, ensuring the automation network remains protected even if a hacker gains control of a system inside the DMZ.

Using innovative, state-of-the-art technology, service experts close existing security gaps in your network, thereby improving your plant's protection against cyberattacks. Siemens relies on collaboration with professional, best-in-class partners to identify the best solution for your plant.

One example is the Industrial Next Generation Firewall, such as the RUGGEDCOM-APE1808 industrial application hosting platform with Palo Alto Networks' VM Series virtual firewall or appliances from Palo Alto Networks. This perimeter protection meets the security requirements for industrial automation and is tested and approved for use with the Siemens process control system. The high-quality firewalls are available in various performance classes and not only function as port filters but also analyze layer 7 data traffic at the application level. Additional security subscriptions, such as threat detection and URL filtering, and a service contract complete the offering.

The firewalls are also part of the Industrial DMZ Infrastructure solution. This turnkey concept provides IT/OT network segmentation with integrated security features. Through a DMZ with redundant front and back firewalls, OT systems are shielded from corporate IT. This network segmentation allows access to systems that require data from the internet while protecting the system network from unauthorized outside access, in line with IEC 62443. Services provided within the DMZ, such as remote access, file exchange, and active directory, are made available as virtual machines on a separate high-performance virtualization host.

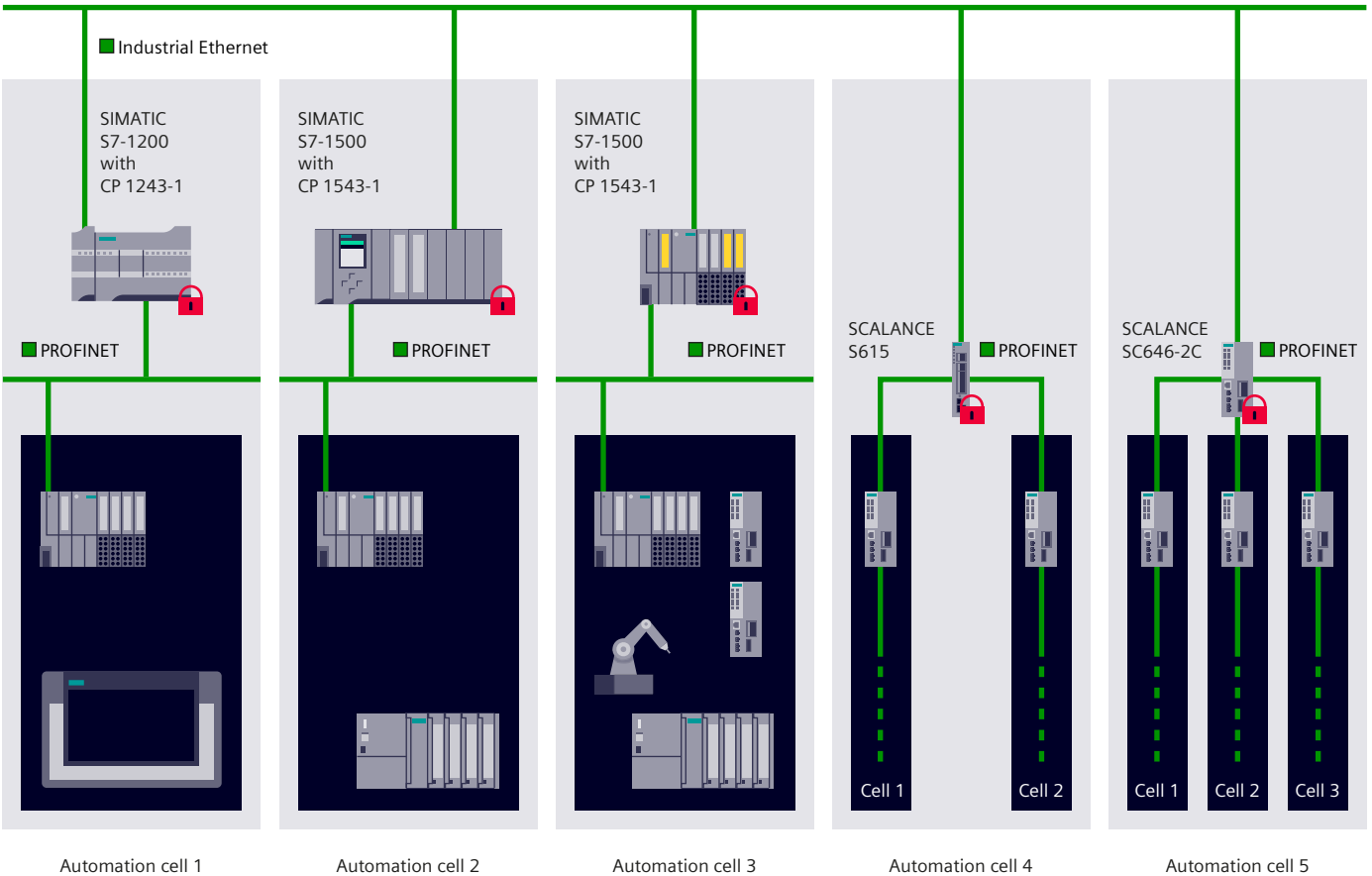
4.3. Network segmentation and cell protection concept

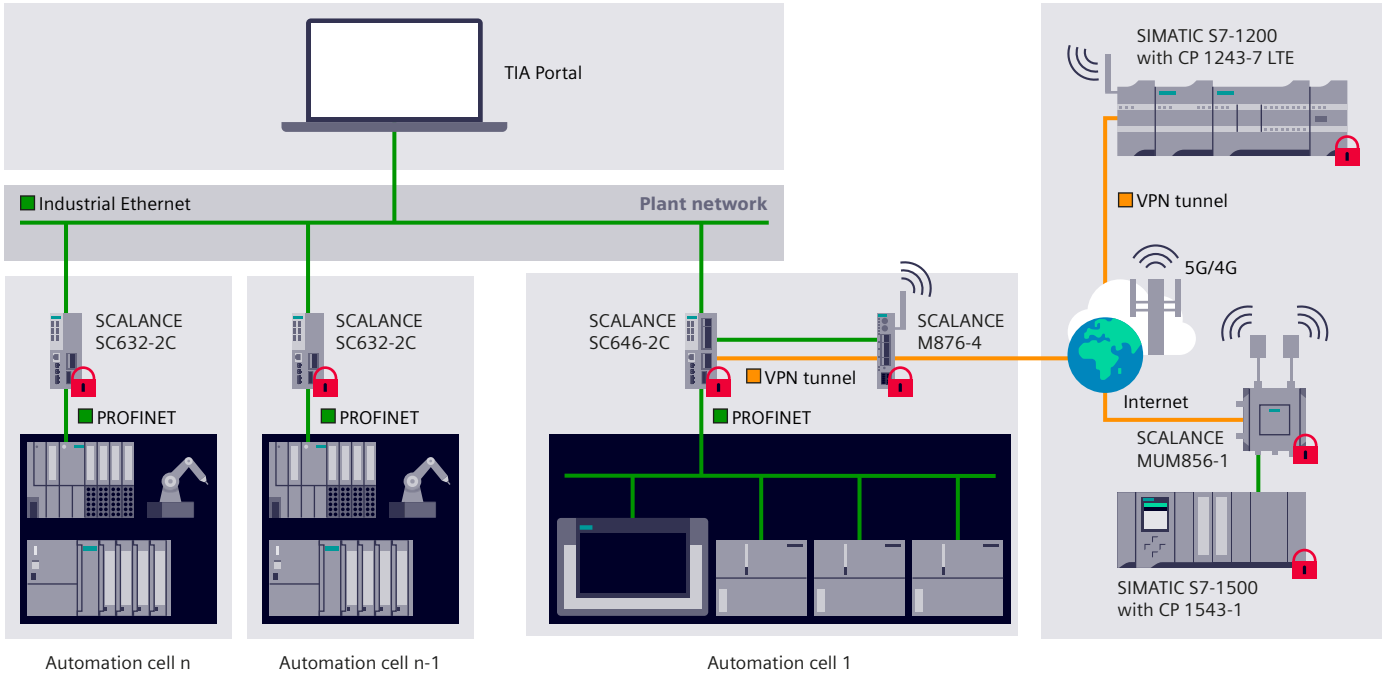
The segmentation of the plant network to create separated automation cells protected by technical security measures helps to further minimize risk and increase security. Network segmentation involves protecting parts of a network, such as an IP subnet, with an industrial security appliance that separates 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 any compromise in real-time capability, performance, or other functions.

The firewall controls access attempts to and from the cell. It is even possible to specify which network nodes are allowed to communicate with each other and, where appropriate, which protocols they may use. This means unauthorized access attempts can be blocked first and foremost, and it also reduces network load, as only explicitly permitted communications can proceed.

The division of cells and the allocation of devices reflect the communication and protection requirements of the network stations. Data transmission to and from the cells can also be encrypted by the security appliances using a VPN to protect against data espionage and manipulation. This comprises authenticating communication participants and, where applicable, authorizing access attempts. The cell protection concept can be implemented, and communication between cells protected, by using components such as SCALANCE S industrial security appliances or the security communications processors for the SIMATIC S7 automation. The SCALANCE S industrial security appliances provide the ability to define and protect network cells flexibly based on VLANs.

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





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

4.4. Secure remote access

It is becoming increasingly common to connect plants directly to the internet and to link remote plants via mobile networks such as LTE (4G) and 5G. This enables remote maintenance, the use of remote applications, and monitoring of machines installed worldwide.

Securing access is especially important in this context. Attackers can easily and cheaply find unsecured entry points using search engines, port scanners, or automated scripts. It is therefore crucial to ensure communication nodes are authenticated, data transmission is encrypted, and data integrity is protected, especially for critical infrastructure plants. Incidents such as unauthorized intrusion, espionage of confidential data, and manipulation of parameters or control commands can cause enormous damage, including environmental harm and risk to personnel.

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

Typically, devices used for secure communication are authenticated as trustworthy nodes using certificates, and the relevant IP addresses or DNS names are applied in firewall rules to permit or block access. The SCALANCE M industrial routers and the SCALANCE S industrial security appliances also support user-specific firewall rules. This creates the option to link access rights to specific users. Users must log on to a web interface with their login credentials to temporarily unlock a specific set of firewall rules matched to their personal access rights. One particular advantage of this time-limited and user-specific activation is that there is always a clear record of who accessed the system and when, which can be very important for maintenance and services.

The SCALANCE S variants with more than two ports also provide a solution to a common dilemma faced by many system integrators, OEMs, and end users: Machine builders need access to their machines on the end user's premises for maintenance, but end-user IT departments are often highly reluctant to allow outsiders into the connected network. With these variants of the industrial security appliances, it is possible to connect the machine both to the plant network and, via the additional firewall-protected port, to the internet. This means the machine can be accessed from the internet without allowing internet access to the plant network. Thus, remote maintenance access to the machine is possible without giving the service technician direct access to the plant network.

Facilitation of secured remote access using management platforms

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

Remote management platforms are especially suitable for use in series and special-purpose machine manufacturing. This enables OEMs, for example, to clearly identify a large number of similar machines in use by different customers and address them for remote maintenance.

A remote management platform is an application that provides secure management of VPN tunnels between remote experts and installed equipment. Service technicians and machines each establish a connection to the remote management platform, where their identities are verified through an exchange of certificates before access is granted. This prevents unauthorized attempts to access the company network to which the plant or machine is connected. Access rights to machines can be centrally controlled 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 allow incoming connections to the plant.

Siemens offers two robust solutions for secure remote access to meet all customer use cases:

SINEMA Remote Connect and
common Remote Service Platform (cRSP)

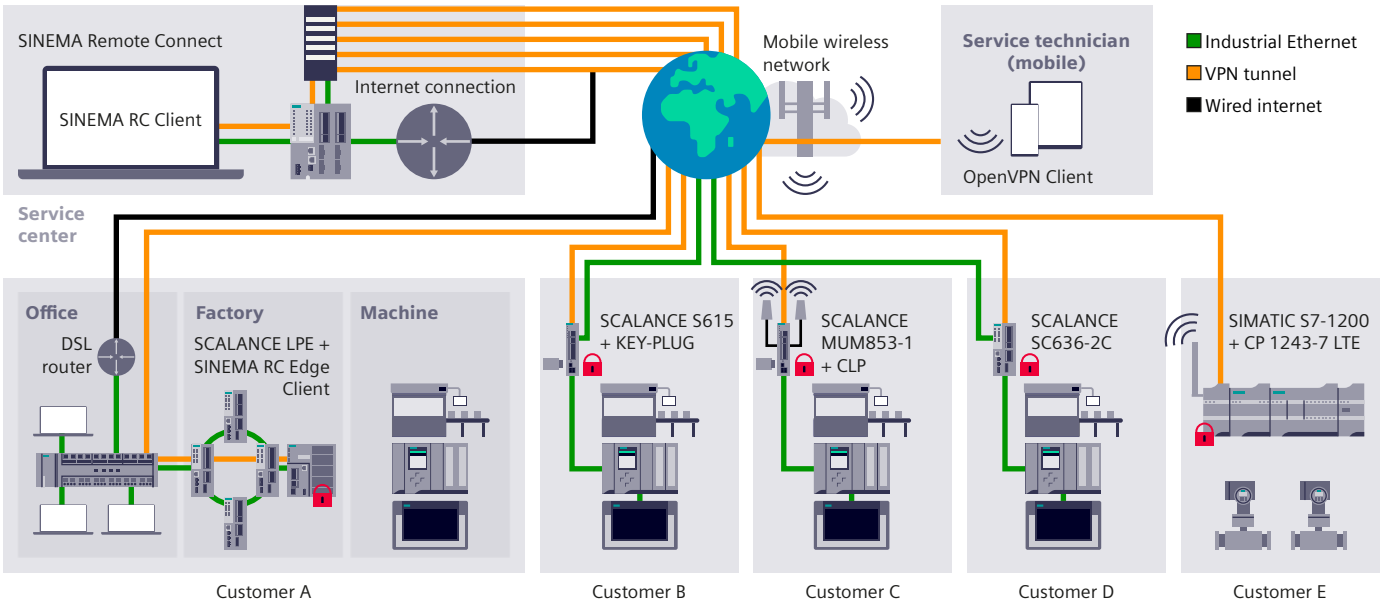
Both solutions ensure secure and continuously available remote access to customer equipment, with protocol-based access.

The SINEMA Remote Connect management platform is a server application designed for a dynamic business environment, offering a customized, flexible, and cost-effective solution. SINEMA Remote Connect meets individually defined remote access requirements perfectly. With SINEMA Remote Connect as a Service (SaaS), installation, maintenance, and updates require no effort. Siemens manages the hosting according to the latest cybersecurity standards in an ISO/IEC 27001 certified data center. Whether deployed on-premise, cloud-based, or directly hosted by Siemens, SINEMA Remote Connect offers the versatility to adapt seamlessly to each customer's unique needs.

SINEMA Remote Connect is a management platform for efficient and secure remote access to globally distributed plants and machines

Key benefits of SINEMA Remote Connect:

- Individual, independent, and flexible use of the remote management platform
- Seamless integration and easily expandable
- Cost-effective solution
- Comprehensive security approach
- Zero effort for installation, maintenance, and updates with SaaS

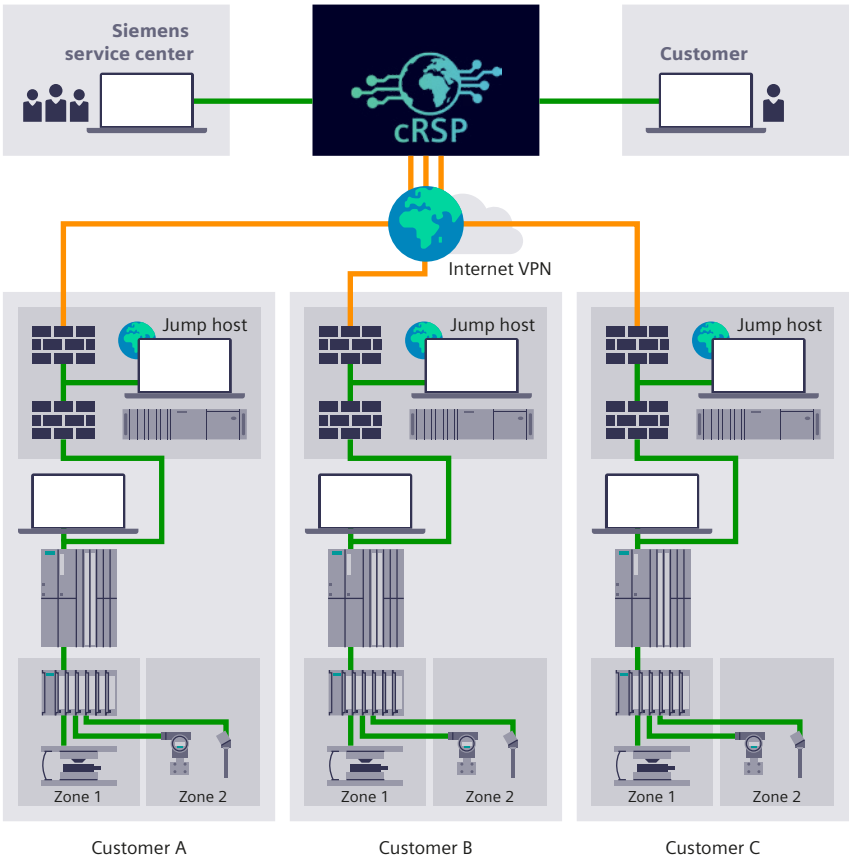


Secure remote access to distributed plants using the SINEMA Remote Connect management platform for remote networks

With Remote Platform SaaS based on the common Remote Service Platform (cRSP), customers can enhance remote platform capabilities and unlock new opportunities for growth and efficiency.

Designed for maximum performance, scalability, and availability, cRSP is the ideal solution for business-critical remote management needs. Hosted on high-performance server infrastructure across three state-of-the-art data centers, cRSP delivers a consistently reliable and secure experience. cRSP is ISO/IEC 27001 certified and complies with the latest security standards such as IEC 62443 and NIS2. Backed by Siemens' holistic operation and security concept, customers can trust cRSP to handle the complexities of remote service management, allowing them to focus on their core business activities.

Secure remote access to distributed plants using the common Remote Service Platform (cRSP) management platform for remote networks



Key benefits of cRSP:

- Standardized, consistent platform for all customer's remote use cases
- Optimized for maximum performance, scalability, and availability
- Comprehensive security approach
- Fast, efficient and first-class remote service delivery
- Siemens' expertise and responsibility for holistic platform operation and monitoring

4.5. Continuous security monitoring detects threats at an early stage

In today's interconnected industrial landscape, OT environments face unprecedented cybersecurity challenges. Traditional industrial control systems and machinery, originally designed to operate in isolation, are now increasingly connected to corporate networks and the internet. It is more challenging than ever to maintain oversight of the rapidly expanding complexity of connected devices and growing data volumes, creating a vastly expanded attack surface for cybercriminals.

AI has lowered the barrier of entry for potential attackers, enabling more sophisticated and automated cyber threats. A successful attack can result in production downtime, equipment damage, safety risks to workers, and potentially catastrophic environmental incidents. Traditional IT security solutions are unsuitable for OT environments because they do not meet the specific requirements of industrial networks and could interfere with ongoing production.

What companies need is a holistic overview of their OT security situation to help them understand their security posture and make informed decisions to protect critical operational systems. An effective solution provides continuous security monitoring specifically designed for industrial networks – an intrusion detection system (IDS) made for OT.

By mirroring and analyzing network traffic, assets can be detected passively without interfering with ongoing production. The detected assets are correlated with known vulnerabilities to identify affected vulnerable devices. This enables a proactive security approach, allowing companies to address vulnerabilities before they can be exploited.

Cyberattack detection occurs through two complementary mechanisms: signature-based anomaly detection based on an extensive database of threat intelligence and signatureless anomaly detection with built-in AI that can identify previously unknown attack patterns.

SINEC Security Monitor from Siemens offers precisely these capabilities. It was specifically developed for industrial environments and features monitoring down to segmented network zones, for example at aggregation and cell levels, through the optional "distributed sensor add-on." Monitoring Windows-based PCs is also possible – for example, the system can detect when USB storage devices are connected or new applications are installed, implemented through the optional "PC agent add-on."

To complement this powerful technology platform, the industrial anomaly detection service provides 24/7 remote continuous security monitoring for industrial customers. This service is delivered by cybersecurity experts from the remote industrial operations services team, who combine deep industrial knowledge with security expertise.

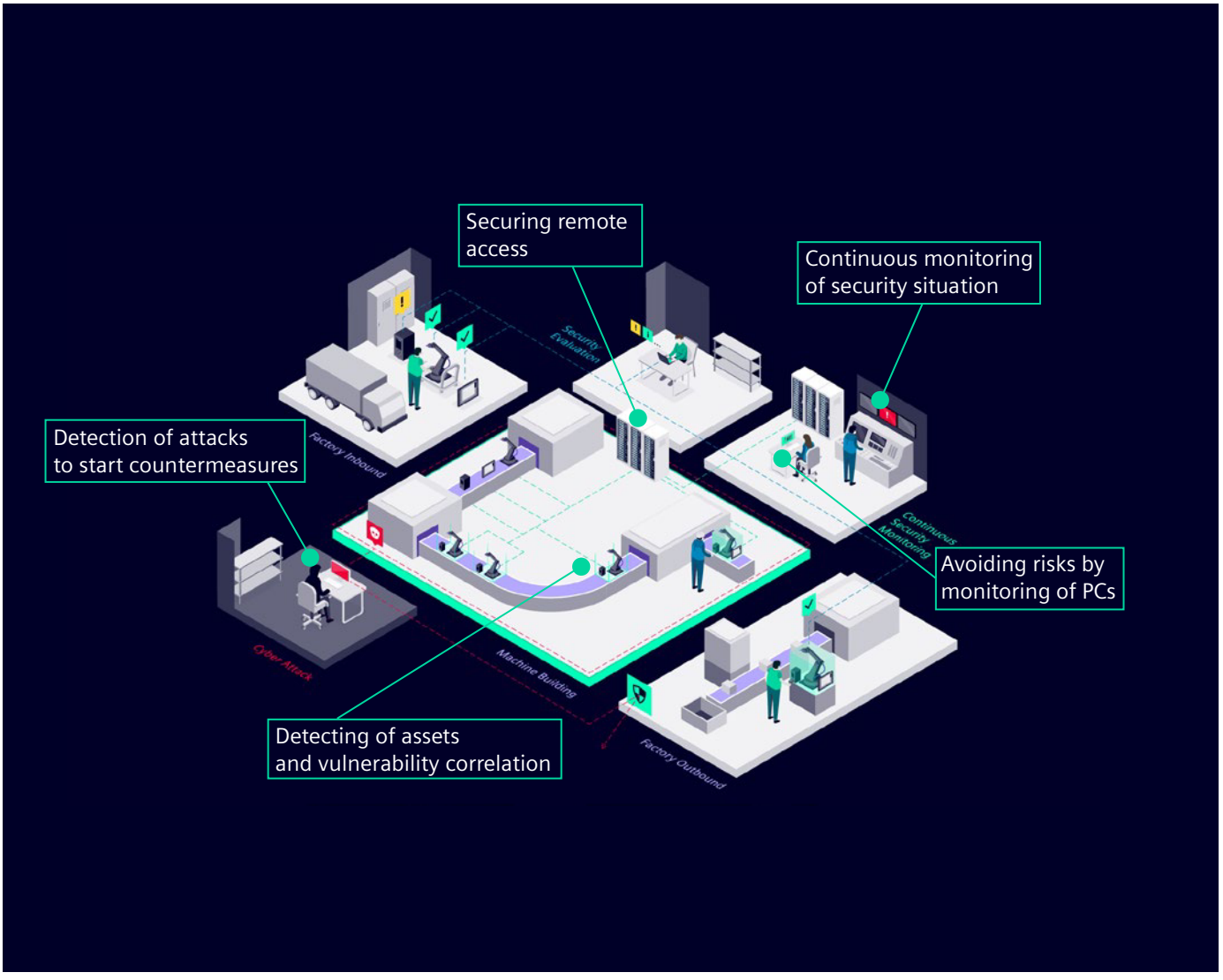
The service helps detect and act on threats through specialists who understand OT security's unique challenges. These experts provide context-aware threat analysis, regular security reports, and actionable recommendations tailored to your specific industrial environment. This human-in-the-loop approach ensures that automated alerts are properly interpreted within the operational context of your facility.

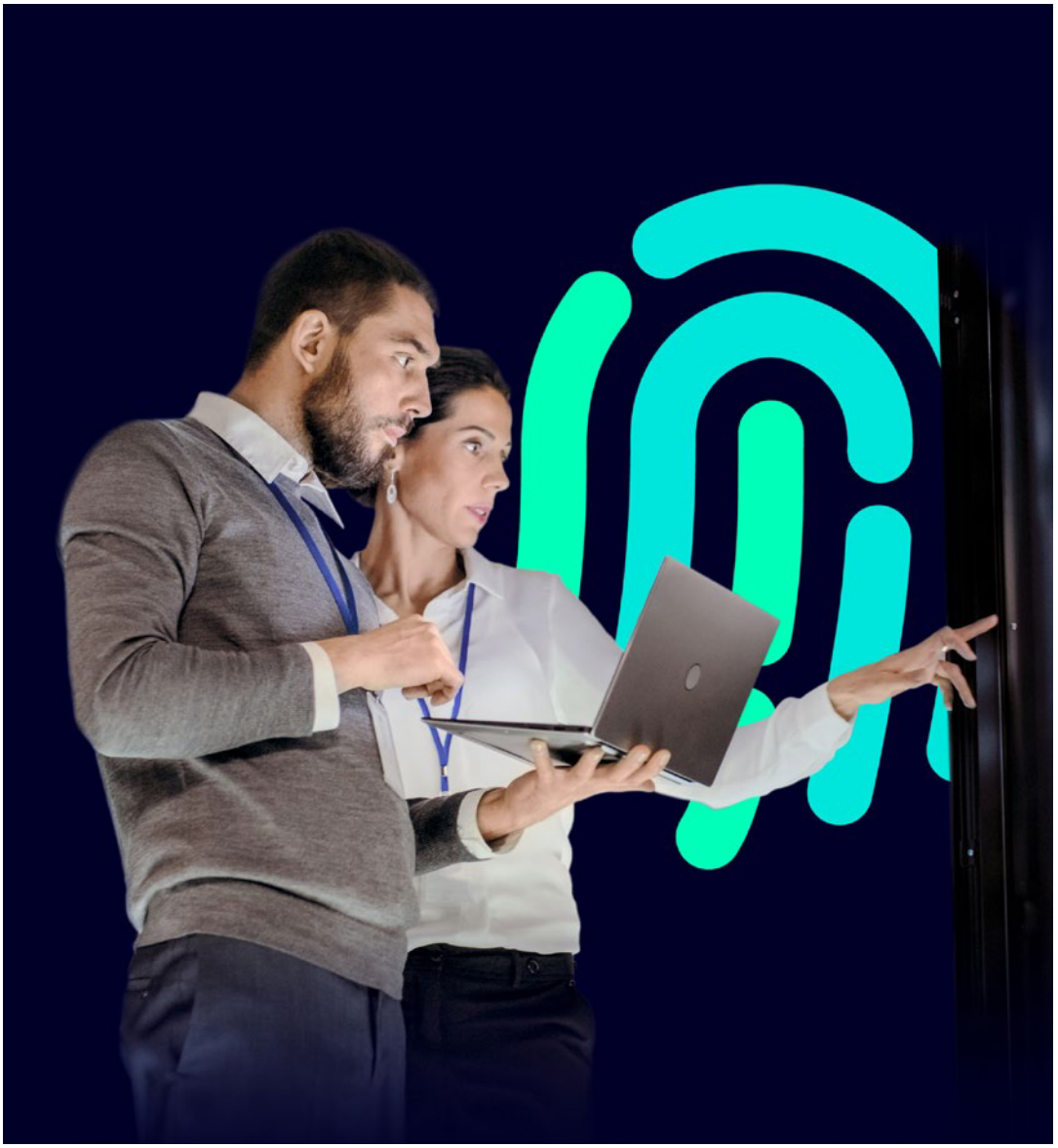
The comprehensive security monitoring approach delivers multiple strategic advantages:

- Zero impact asset discovery: Identify assets, including firmware and topology, through passive analysis without disrupting production processes – crucial in environments where downtime costs can be substantial.
- Vulnerability intelligence: Discover multi-vendor vulnerabilities across the entire network by correlating detected assets with leading vulnerability databases, providing a clear picture of your actual risk exposure.
- Early threat detection: Combine signature-based detection with AI-powered anomaly recognition to identify both known threats and suspicious behavioral patterns before they cause damage.
- Regulatory compliance support: Meet increasing compliance requirements such as IEC 62443, NIST frameworks, or regional regulations such as the NIS2 Directive in Europe through comprehensive monitoring and documentation.
- Holistic security dashboard: Gain a complete overview of your OT security posture through intuitive visualizations that help stakeholders across different organizational levels understand and address security challenges effectively.

By combining advanced technology with expert human analysis, continuous security monitoring provides the visibility and intelligence necessary to protect modern industrial operations in an increasingly threatening digital landscape.

SINEC Security Monitor analyzes network traffic and detects anomalies with passive, non-intrusive, continuous monitoring. Both tools are on-premises.



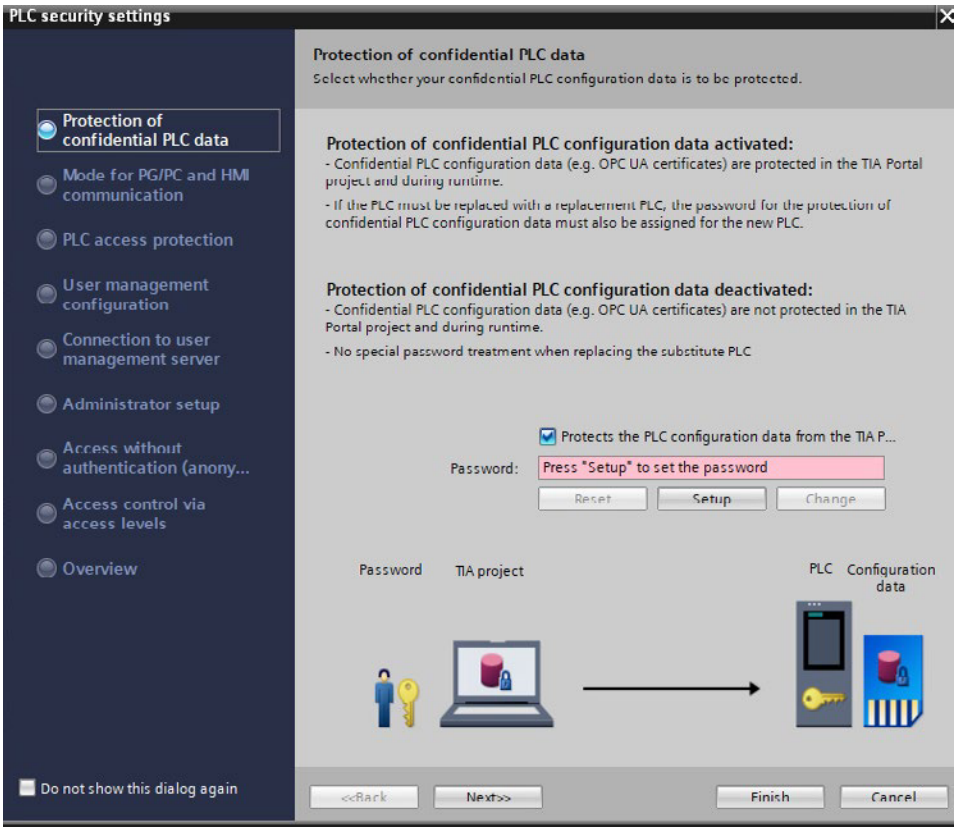


5.

System integrity

The third pillar of a balanced security concept is system integrity. This involves protecting control components and automation systems, as well as SCADA and HMI systems, from unauthorized access and malware. It also includes safeguarding intellectual property and ensuring secure communication.

Relying solely on perimeter-based defenses is insufficient, as attackers will likely penetrate these measures eventually. Therefore, it is safer to assume breaches will occur and to prepare multiple layers of defense. This defense-in-depth approach includes maintaining the system integrity of automation systems and utilizing their integrated security functions.



Screenshot of “security wizard” in TIA Portal

5.1. Protection of the control level

Efforts to protect the control level primarily focus on ensuring the availability of the automation solution. The security mechanisms integrated into standard automation components provide the foundation for control level protection. These mechanisms are enabled and configured according to the protection requirements of the specific machine or plant. Configuring these security features and developing engineering programs for the automation solution can be done conveniently and efficiently using TIA Portal.

However, the increasing interconnection and integration of IT mechanisms into automation technology are changing the requirements for production plants, especially regarding access protection and defense against manipulation – both essential for modern control systems. These capabilities are already built into the SIMATIC S7-1200 and S7-1500 controller families, including the software controller.

The protection includes multi-level access control with differentiated access rights and secure communication protocols for controller configuration or HMI connections, which include integrated security mechanisms for significantly enhanced detection of manipulation attempts.

Secure PG/HMI communication: provided through TLS (transport layer security), this protects communication between S7 controllers and engineering stations with TIA Portal or HMI stations and encrypts communication by applying individual certificates. This true end-to-end encryption between engineering or HMI stations prevents any manipulation of controller programs or parameters. With this state-of-the-art secured communication based on TLS (v1.3), automation systems benefit from high-level protection, helping avoid production loss, data theft, manipulation, or sabotage.

For configuration in TIA Portal, the user is guided by a security wizard that assists with security settings. This includes protecting confidential configuration data, managing the access level of the SIMATIC controller, and securing PG/HMI communication.

Safeguarding intellectual property is an increasingly important concern. Machine builders invest heavily in product development and cannot afford to have their proprietary expertise compromised. Siemens controllers provide convenient and effective support through know-how protection and copy protection functions.

The know-how protection function enables highly specific protection of program modules, preventing access to their content as well as copying and modification of algorithms.

The copy protection function links program components to the serial number of the memory card or CPU, helping prevent unauthorized copying of machines, since protected programs can only be used in the intended machines.

These functions assist machine builders in safeguarding their investment and maintaining their technological edge.

Additional security features, such as 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. Their protection extends to the connected controllers and, where necessary, to communication between them, thus supplementing and enhancing the cell protection concept within a plant by using firewall and VPN.

All these security-integrated products are compatible and can connect securely with each other via VPN, effectively protecting every part of a plant and all automation components.

5.2. Protection of PC-based systems in the plant network

PC systems used in office environments are typically protected against malicious software, with vulnerabilities in their operating systems or applications addressed through regular updates and patches. Similar protective measures may also be necessary for industrial PCs and PC-based control systems, depending on their usage. Protective tools common in office settings, such as antivirus software, can generally be applied in industrial environments, provided they do not negatively impact automation tasks.

Allowlisting solutions can complement antivirus software. Allowlisting involves creating approved lists that explicitly specify which processes and programs are permitted to run on the computer. Any attempt by a user or malware to install or execute an unapproved program is denied, preventing potential damage.

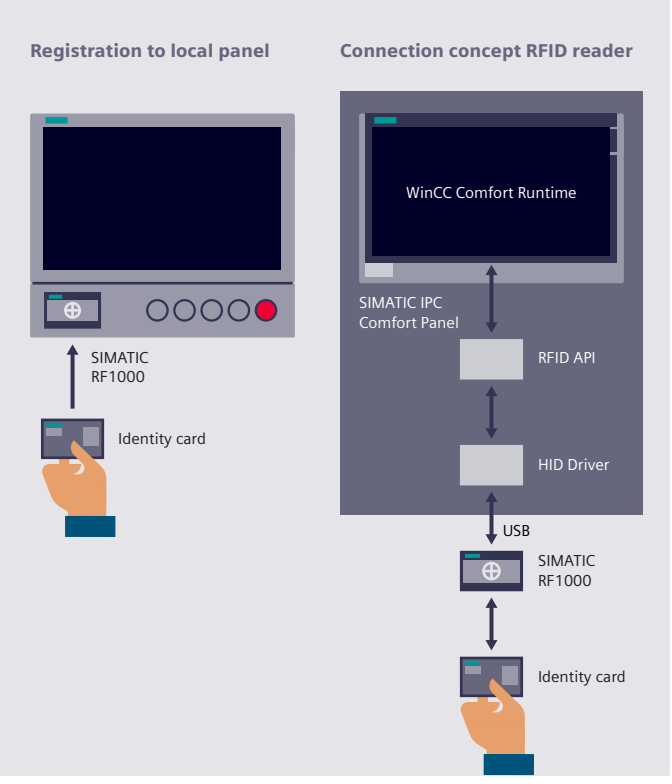
As an industrial software vendor, Siemens supports the protection of industrial PCs and PC-based systems by testing its software for compatibility with virus scanners and allowlisting software.

Additionally, the numerous integrated security mechanisms available in Windows operating systems can be employed to harden systems as needed. These include user management and rights management as well as finely configurable security policies. Siemens provides comprehensive guidelines to assist with these measures.

5.3. Secure access management for machines and plants

One of the essential mechanisms for protecting automation components is consistent, logged access control. The SIMATIC RF1000 access control reader enables reliable identification of personnel operating machines and plants, allowing assignment of appropriate access rights.

Depending on your needs and security requirements, login can be restricted to RFID card authentication such as an employee ID – or require both an RFID card and user-specific login credentials. Logging all access attempts ensures transparent traceability in the event of security incidents.



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

SIMATIC RF1000 for controlling access to machines and equipment

5.4. Security testing in industrial environments: addressing unique challenges

Industrial environments present unique challenges for security testing. Traditional penetration testing methods can be complex, expensive, and often require the involvement of external cybersecurity experts. Moreover, many industrial components were not originally designed with security in mind, making vulnerabilities more difficult to detect without specialized tools.

Misconfigured network devices, such as systems with open ports or insecure communication protocols, pose significant risks. In many cases, incomplete inventories of OT assets further erode the overall security posture. This lack of visibility into networked devices makes comprehensive security testing essential for protecting industrial operations and developing secure products.

As IT and OT systems continue to converge, the attack surface expands rapidly. Industrial networks are becoming increasingly connected to enterprise IT and cloud environments, which amplifies the need for testing solutions capable of identifying vulnerabilities across both products and network infrastructures.

Unauthorized remote access – often caused by misconfigured OT devices – can lead to production downtime, data breaches, and the exposure of sensitive information. Security testing can mitigate these risks by analyzing network configurations (e.g., protocols and ports in use) and detecting assets, including device types, firmware versions, and known vulnerabilities.

To be truly effective, modern security testing tools must be user-friendly and flexible enough to accommodate the diverse industrial environments.

Testing methods should be accessible to both non-specialist engineers and cybersecurity professionals alike, and scalable from individual devices to entire industrial facilities.

SINEC Security Inspector:
a tailored solution for industrial security

Siemens' SINEC Security Inspector offers a specialized approach to industrial security testing. This on-premises platform integrates multiple security tools into a unified solution tailored for industrial networks.

The SINEC Security Inspector identifies assets, network configurations, and device vulnerabilities. Vulnerabilities are detected through two primary methods: comparison of collected data with a vulnerability database, and active penetration testing techniques such as brute-force attacks on OT devices. The system uncovers security gaps across multiple layers, including network segmentation and unauthorized access points.

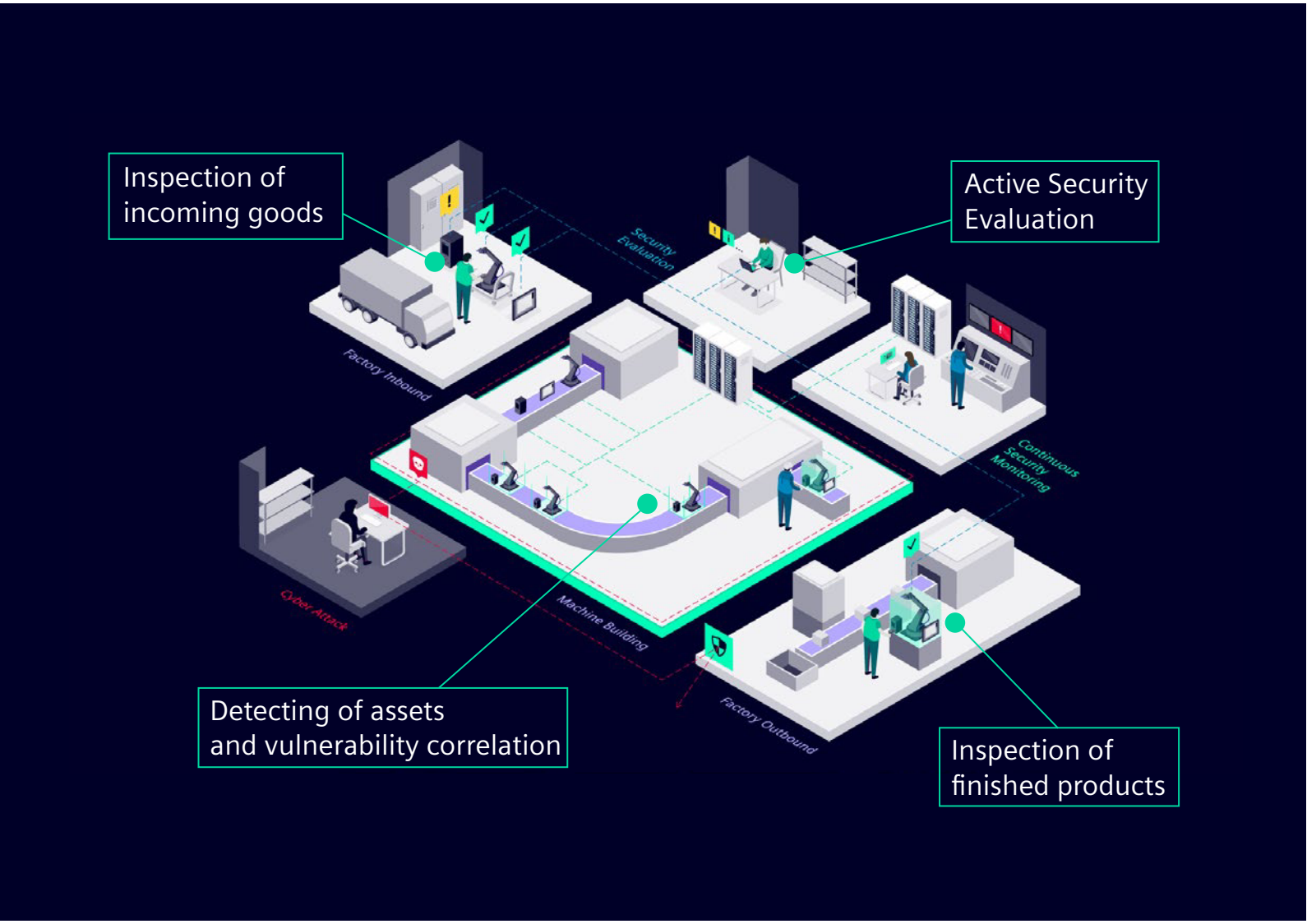
The software includes predefined test cases specifically designed for industrial environments, drawing on the expertise of the Siemens ProductCERT community.
Its intuitive, web-based interface supports the entire security testing workflow from asset discovery to remediation planning with clear, actionable results.

Moreover, the platform allows test cases to be customized to specific environments and validated against network specifications. This flexibility enables comprehensive security evaluations of both entire networks and individual products, tailored to unique operational requirements.

Transforming the industrial cybersecurity posture

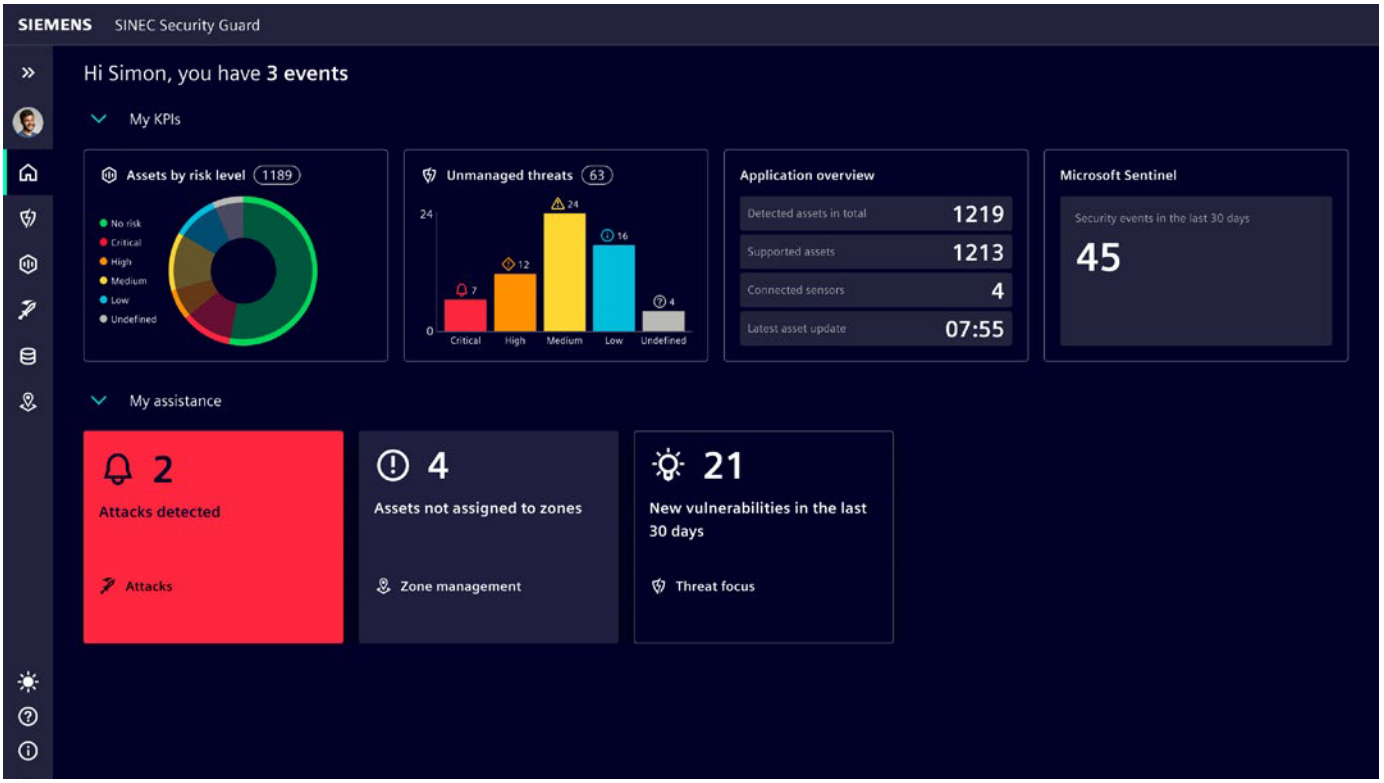
Systematic vulnerability and network configuration testing with SINEC Security Inspector fundamentally enhances an organization's cybersecurity posture. The solution delivers full visibility into all OT network components, enabling proactive security through early vulnerability detection. This shifts the security approach from reactive to preventive.

OT-specific testing methods ensure that critical processes remain uninterrupted during assessments. Risk-based evaluations help prioritize limited resources toward addressing the most critical vulnerabilities. Additionally, the solution supports regulatory compliance through detailed documentation, laying the foundation for holistic protection of industrial environments and the secure development of future products.



SINEC Security Inspector determines the security status of individual components or entire production networks, so that you can detect gaps within minutes.

5.5. Vulnerability management: systematically combating vulnerabilities



The SINEC Security Guard home dashboard provides an overview of the current threat situation for OT systems in order to prioritize measures.

The acute lack of dedicated cybersecurity expertise for OT environments poses significant problems for companies. While IT security experts are relatively common, there is a shortage of professionals who deeply understand both industrial processes and cybersecurity.

Managing OT assets is extraordinarily complex. Industrial components with lifecycles of 15-20 years meet modern network technologies, creating a heterogeneous environment with numerous potential vulnerabilities. The sheer number and variety of devices – from PLCs to HMIs to engineering workstations – make manual monitoring nearly impossible.

Particularly problematic is the insufficient visibility of threats. Without specialized tools, many vulnerabilities remain undetected until exploited by attackers. The reactive approach of acting only after an incident is unacceptable, especially in critical infrastructures where failures can have catastrophic consequences.

Regulatory pressure is also continuously increasing. The European Union's NIS2 Directive, for example, significantly tightens cybersecurity requirements for critical as well as noncritical infrastructures and demands systematic risk management – including efficient strategies for handling vulnerabilities.

Effective vulnerability management for industrial environments requires a holistic, systematic approach. The foundation is a complete inventory of all assets – only what is known can be protected. Based on this, automated vulnerability detection can proceed, comparing identified assets with current vulnerability databases.

Crucial is the risk-based prioritization of discovered vulnerabilities. Not every vulnerability poses the same risk – factors such as the criticality of the affected system, the exploitability of the vulnerability, and potential impacts on the production process must be incorporated into the assessment. This risk evaluation must consider the special requirements of industrial environments, where different priorities apply compared to IT networks (availability, integrity, confidentiality – AIC – instead of CIA).

The process must be rounded off by integrated mitigation and tracking mechanisms. For each identified vulnerability, concrete mitigation measures should be developed and their implementation tracked – whether through patching, network segmentation, or alternative protective measures.

SINEC Security Guard from Siemens offers precisely this comprehensive solution for vulnerability management in industrial networks. As a cloud-based SaaS offering, it combines accessibility with maximum efficiency – without elaborate local installation or maintenance. The platform automates vulnerability detection and correlates these with identified assets, enabling precise risk assessment.

The risk-based threat analysis considers industry-specific factors, thus delivering relevant prioritizations for OT environments. Through continuous monitoring, new vulnerabilities are immediately detected and evaluated. The solution also supports the planning of remediation measures with concrete action recommendations and tracks their implementation.

Systematic vulnerability management with SINEC Security Guard fundamentally transforms cybersecurity in industrial environments. Companies gain immediate transparency about their security situation and can target resources where they deliver the greatest benefit. The industry-specific risk assessment ensures that truly critical vulnerabilities are addressed first.

Through continuous monitoring and automatic updates of the vulnerability database, protection stays constantly up to date – a decisive advantage in a rapidly evolving threat landscape. Enhanced compliance supports companies in efficiently meeting and proving adherence to regulatory requirements.

Ultimately, the proactive handling of vulnerabilities leads to a significant reduction in overall risk. In an era of increasing cyberattacks on industrial infrastructures, this is not just a competitive advantage but an operational necessity.

Expert services

Complementing SINEC Security Guard's comprehensive protection, our Vulnerability Services offer additional robust monitoring solutions employing advanced technologies and expert analysis to deliver timely, actionable vulnerability intelligence across your full product stack and infrastructure. Through the Management Portal, Data Service (API), and Managed Service, you can tailor your approach to cybersecurity, whether you require hands-on management, seamless data integration, or comprehensive outsourced monitoring. These services are designed to reduce the time-to-patch by quickly identifying new vulnerabilities affecting both software and hardware components. They ensure compliance with new regulatory standards like NIS2 for the EU, enhancing protection against cyber threats.

5.6. Enhancing endpoint security and recovery strategies

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

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.

Furthermore, implementing an effective Disaster Recovery strategy is an extremely important factor in restarting production after a breakdown and preventing data loss. Additionally, new security regulations (e.g. NIS2 for EU) require operators to have a system for backup, disaster recovery and crisis management in place. Backup and Restore (as part of Managed IT/OT Infrastructure) provides a powerful and preconfigured IT infrastructure for disaster recovery in industrial environments.

With these proven technologies and partnerships, Siemens expertly enhances system integrity, resilience, and security across diverse operations.

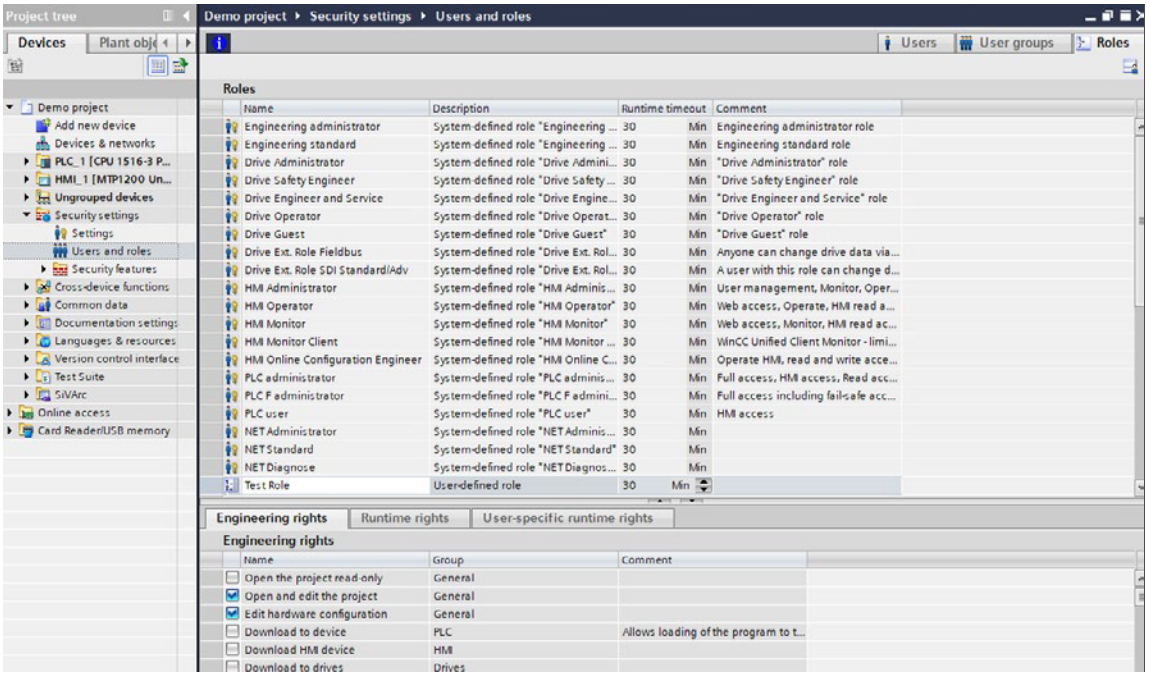
6.

Roles and rights concepts

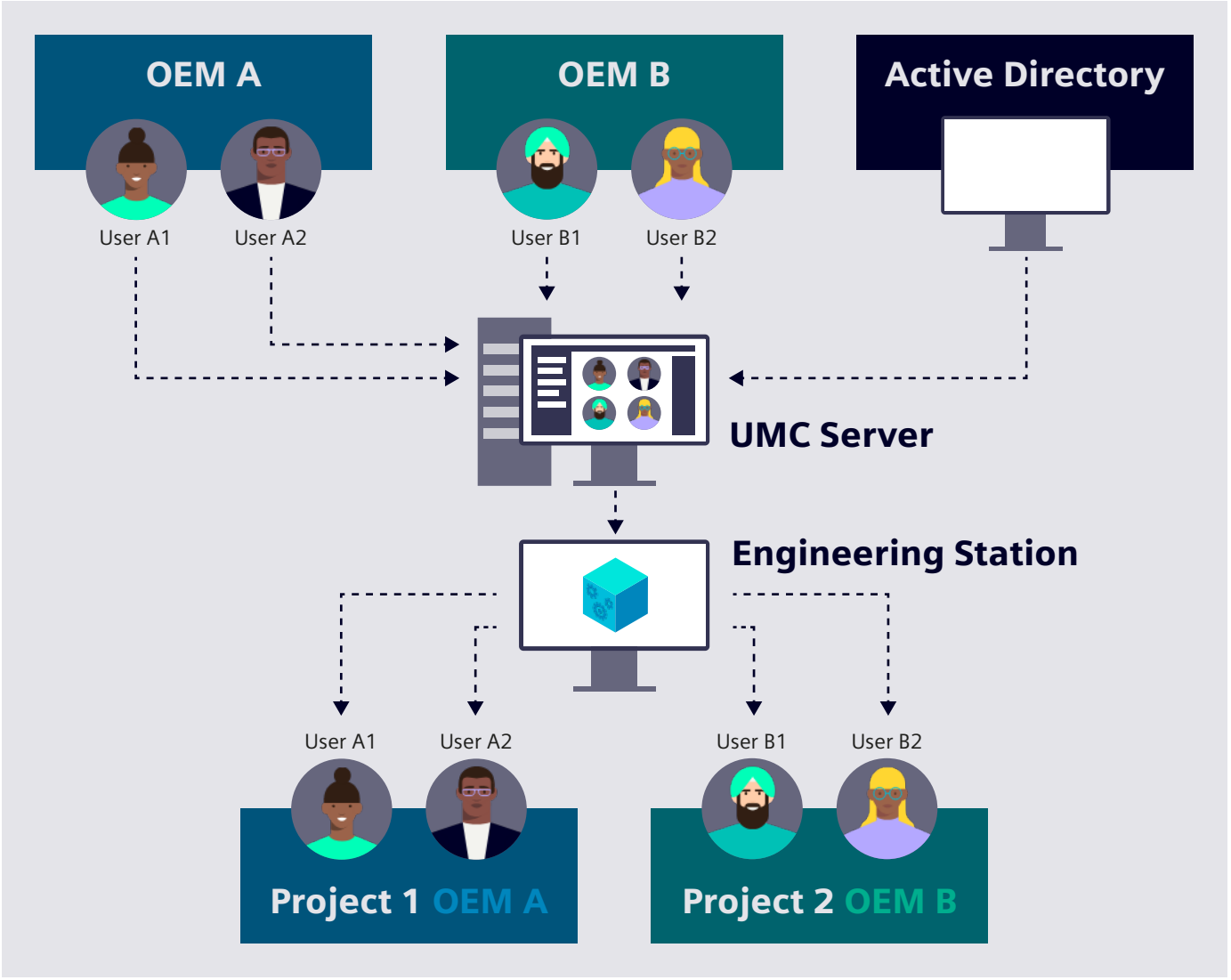
Defending against various threats and achieving an appropriate level of protection requires a defense-in-depth concept that creates multiple obstacles for potential attackers. These obstacles, of course, must not hinder authorized users. It is common practice to establish a system of graduated access rights, where users are assigned different levels of access to specific plant units, devices, or applications. For example, some users may have administrator rights, while others are limited to read or write access.

Implementing a security concept therefore supports not only protection against direct attacks, but also the introduction of a structured authorization model. Such authorization concepts ensure that access is limited to authorized individuals based on predefined rights. Rather than assigning unique permissions to every user, roles are typically defined, each carrying a specific set of access rights. Users or user groups are then assigned to these roles, streamlining permission management.

Effective user and rights management is a critical component of industrial security. A universal configuration across all automation components simplifies this task, as roles and rights for all relevant personnel can be centrally defined and maintained. The figure shows a screenshot of user and rights management in TIA Portal.



User management in TIA Portal with assignment of roles and rights



Central user management

The user management component (UMC) is a centralized user and group directory configured on a separate server. It enables centralized management of users and user groups across systems.

With UMC, users and groups, such as those from Microsoft Active Directory, can be imported into TIA Portal. The UMC Agent is installed along with TIA Portal and operates independently of individual projects.

The primary advantage of UMC lies in the efficiency it brings to user management and role assignment across multiple projects and engineering stations. When users are added or removed, or when passwords are changed, these updates are made once on the UMC server. The updated users or user groups can then be imported into TIA Portal as needed.

In essence, this approach allows centralized user maintenance for the entire system, avoiding redundant configuration across projects or locally per product. It provides an easy-to-use foundation for efficient and secure administration of personalized access throughout 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 that security aspects must be considered as an integral part of product development and production (see security standard IEC 62443). An automation product must be tracked and embedded within a holistic security concept (HSC) from its creation, through production, and into its operational use.

Assets in this context can include source code, IT processes, and production machines. The security requirements pertaining to assets and organization, with respect to processes and methods, become progressively more demanding as the targeted security level increases. The product owner is responsible for specifying the security level applicable to the product and the associated assets.

The need for robust security is especially high when developing and manufacturing automation products with built-in security functions. For this reason, protective and monitoring measures are particularly relevant for manufacturers of such products.

However, not only the portfolio of dedicated security products benefits from the HSC. All standard products, such as the engineering tool TIA Portal and the SIMATIC S7-1200 and SIMATIC S7-1500 controllers, also profit from this approach. These products help reduce risks for end users, provided they are tested for vulnerabilities during development and further optimized through structured 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

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

8. Summary: Industrial cybersecurity for production plants

Industrial cybersecurity has become an essential business imperative in today's hyperconnected manufacturing landscape. Today, cyber threats are an everyday reality, with manufacturing consistently ranking among the most targeted sectors for cyberattacks globally.

Spectacular incidents on production facilities and numerous critical infrastructure attacks have demonstrated that industrial systems are prime targets. Nation-state actors, ransomware-as-a-service operations, and advanced persistent threats targeting OT have created an unprecedented risk environment. Threat intelligence shows attacks on industrial targets have risen by over 300% since 2020.

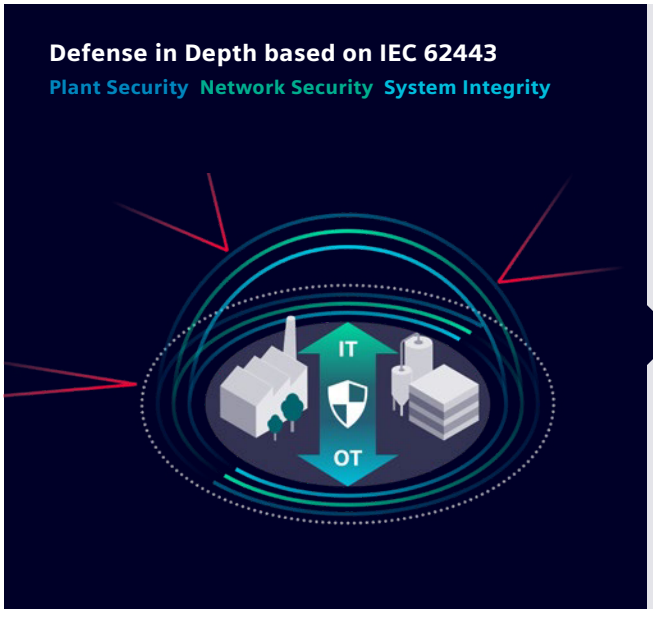
The rapid shift to smart manufacturing, IIoT, and cloud-integrated operations has significantly expanded the attack surface. IT/OT convergence, remote access, and emerging technologies like AI and edge computing introduce vulnerabilities beyond the scope of traditional security measures. Still, these advances are essential for staying competitive in global markets.

Today's regulatory landscape extends far beyond the General Data Protection Regulation (GDPR) to include industry-specific requirements like IEC 62443, the NIS2 Directive in Europe, and critical infrastructure protection mandates worldwide. These frameworks increasingly hold executives personally accountable for cybersecurity failures, making compliance a boardroom-level concern.

Siemens is a recognized leader in industrial cybersecurity, offering end-to-end solutions that cover every aspect of protection. Through its integrated Charter of Trust initiative and partner network, Siemens delivers defense-in-depth strategies spaning from individual components to full enterprise security. This includes asset discovery, vulnerability management, anomaly detection, and secure automation system design.

Modern cybersecurity goes beyond technology, requiring a mix of technical controls, organizational processes, and people-focused measures. Siemens' Industrial Cybersecurity Services include OT security operations centers, incident response, and specialized training to help companies build resilience.

As digital and physical systems become more interconnected, cybersecurity provides the basis for sustainable digital transformation. The focus is no longer on whether to invest in industrial cybersecurtity, but on how to implement it effectively to enable innovation while managing evolving threats.



Siemens products offer integrated security

- ✓ Know-how and copy protection
- ✓ Authentication and user management
- ✓ Firewall and VPN
- ✓ System hardening, continuous monitoring and anomaly detection

Siemens Industrial Cybersecurity Services

- ✓ Transparency about the current security status
- ✓ Increased security level by closing security gaps
- ✓ Long-term protection through continuous security management

Siemens' Cybersecurity for Industry offerings are part of the Siemens Industrial Operations X portfolio. Industrial Operations X offers IT-empowered automation to move from an automated to an adaptive production fast and easily. The open and interoperable portfolio, available on Siemens Xcelerator Marketplace, enables industrial companies to integrate and use both IT capabilities and the automation of software development processes. It accelerates faster idea generation and implementation, intuitive cross-disciplinary collaboration, improved operations and decision-making, and easier scaling of operations.

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-B10376-00-7600

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