SIEMENS

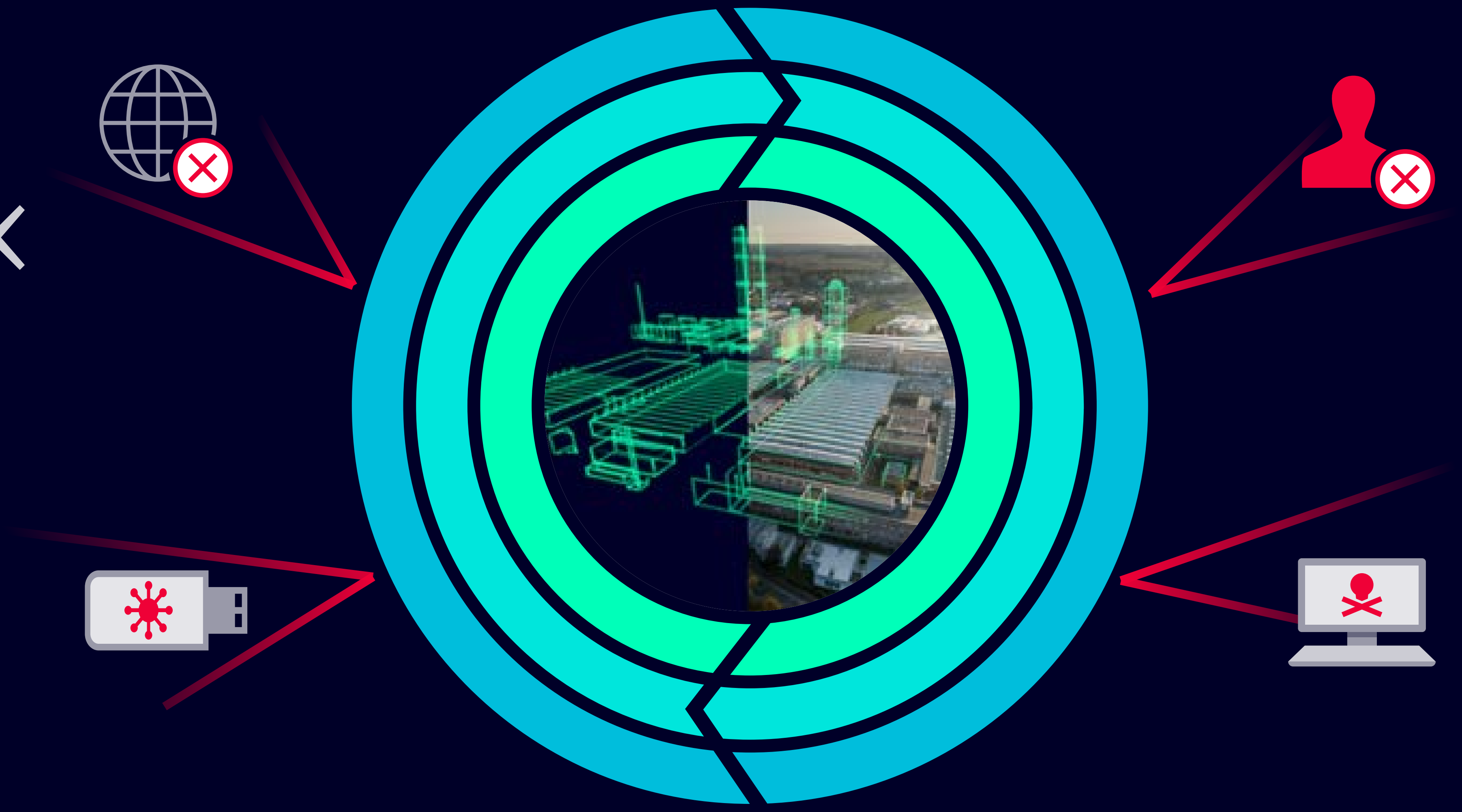
CYBERSECURITY FOR INDUSTRY

Combine the real and digital worlds **securely**

siemens.com/cybersecurity-industry

Defense in Depth | Plant security | Network security | System integrity | Industrial Cybersecurity Services | NIS 2 Directive | Siemens Xcelerator

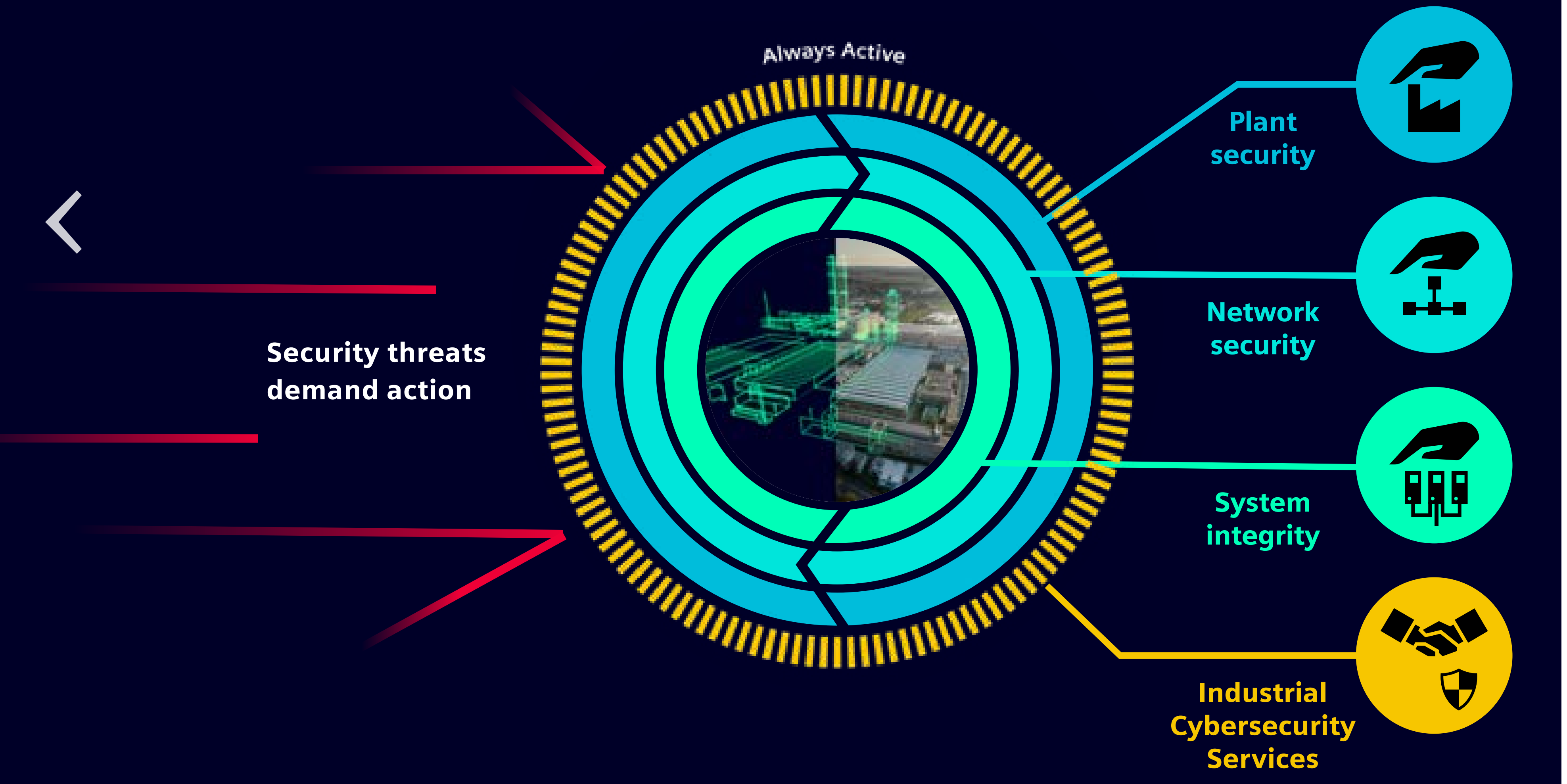
Defense in Depth



To protect industrial plants from internal and external cyber attacks, all levels must be protected simultaneously – from the plant management level to the field level and from access control to secure data communication.

With ”Defense in Depth“, Siemens provides a multi-layered security concept that ensures comprehensive and extensive protection for industrial facilities. It’s based on plant security, network security, and system integrity as it is recommended by IEC 62443.

Defense in Depth …


Always Active
Security threats demand action
Plant security
Network security
System integrity
Industrial Cybersecurity Services

Plant security

Protects physical access of persons to critical components. It starts with conventional building access and extends to securing of sensitive areas by means of key cards. In addition, plant security comprises the integration of processes and guidelines as well as continuous monitoring of the security status of production facilities.

Network security

Protects automation networks against unauthorized accesses and monitors all interfaces between IT and OT as well as remote accesses (e.g. with SINEMA Remote Connect) with the aid of network access protection, network segmentation (e.g. with SCALANCE S), encrypted communication, and zero trust principles. Reliable network management and security tools are additionally offered by the SINEC family.

System integrity

Securing system integrity means to protect automation systems and controllers like SIMATIC S7 controllers, control systems like SIMATIC PCS 7 and PCS neo, SCADA and HMI systems as well as the latest members of our new SINAMICS drive generation against unauthorized access or to protect the know-how contained therein. It also comprises user authentication and their access rights as well as system hardening against attacks.

Industrial Cybersecurity Services

Our experts in automation, digitalization and cybersecurity are the reliable partner for your secure digital transformation. They follow an end-to-end approach, starting with the evaluation of your security status over the implementation of security measures up to continuous monitoring and security management.

Charter of Trust

Cybersecurity is an essential factor for the success of the digital economy. If we expect people to support the digital transformation, the security of data and networked systems must be guaranteed.

As pioneers in the field of digitalization, we are well aware of our responsibility. That is why we and our partners in government, industry and civil society are committed to the development of binding rules and standards that will create a new basis for trust and fair competition.

That is why Siemens and its partners in industry, government and civil society are working to establish the “Charter of Trust” – a charter that pursues three important goals:

- Protect the data of individuals and companies
- Protect people, businesses and infrastructure from damage
- Establish a reliable foundation that supports and fosters the growth of trust in a networked digital world

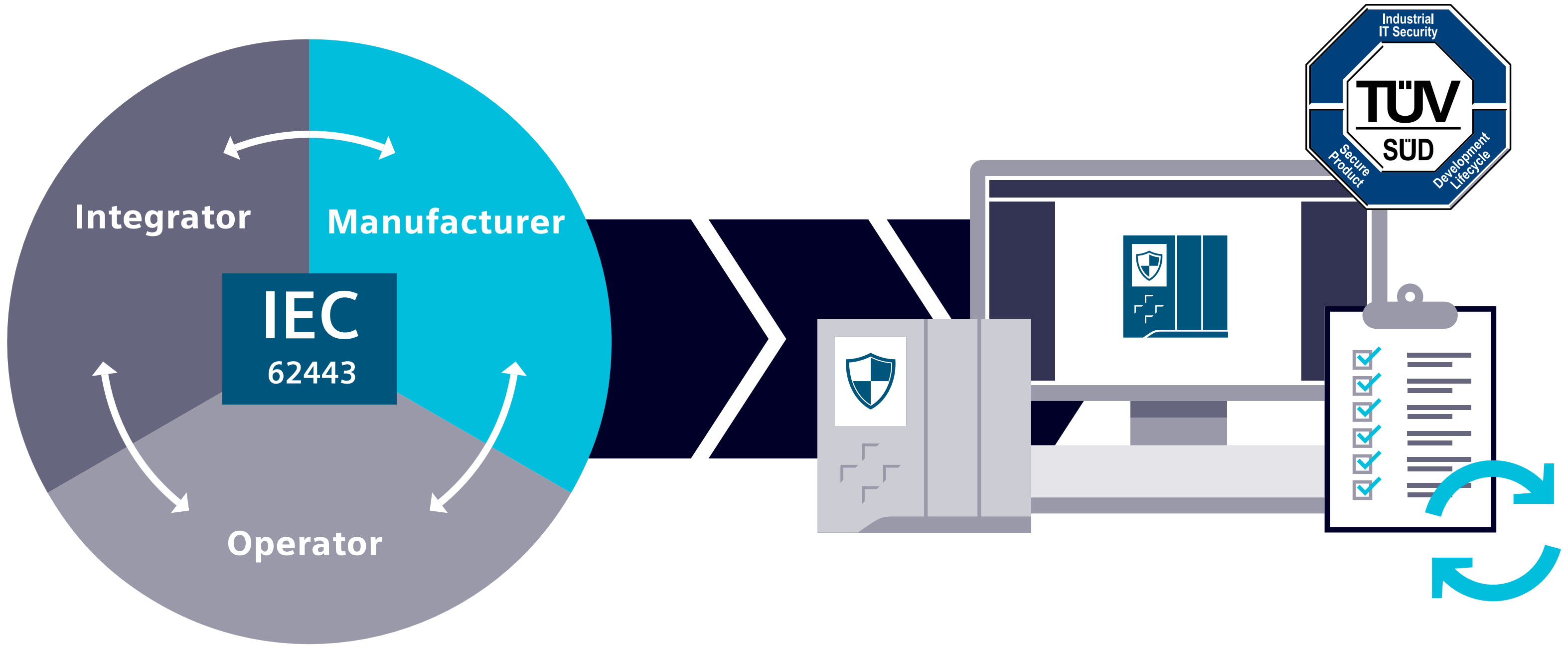
Basic principles

1. **Ownership of cyber and IT security**
2. **Responsibility throughout the digital supply chain**
3. **Security by default**
4. **User-centricity**
5. **Innovation and co-creation**
6. **Make Cybersecurity a mandatory element of educational and training programs**
7. **Certify critical infrastructures and IoT solutions**
8. **Increase transparency and reaction speed**
9. **Regulatory framework**
10. **Advance joint initiatives**

Plant security

Plant security starts with conventional building access and extends to securing of sensitive areas by means of key cards. Tailored industry security services include processes and guidelines for comprehensive plant protection. These range from risk analysis and the implementation and monitoring of suitable measures to regular updates.

Integrators, operators and manufacturers require insights into IT security measures in order to design and operate automation processes and automation systems.



Access control

Managed access control is an essential factor when it comes to safeguarding critical company areas. Siemens Building Technologies offers an extensive portfolio of products, solutions and services for the protection of critical infrastructure. The range extends from access solutions and video monitoring systems to command and control platforms.

Standards

Although there are hundreds of IT security standards, only a few have proven themselves useful for the protection of industrial systems. Building on our many years of experience, we advise you on the selection and implementation of appropriate standards.

In particular, IEC 62443/ISA99 is a well-proven international standard for the industrial automation environment.

Defining guidelines

We support you in defining appropriate guidelines for your own application, and take all the relevant rules and standards into consideration. For example, the handling of removable storage devices must be clearly regulated. These precise guidelines help to ensure a high level of security for all concerned, without placing any constraints on productivity. In this way, Industrial Cybersecurity becomes a central management task.

Security monitoring

With continuous analysis and correlation of logs as well as comparison with our databases we detect and classify potential threats. In case of a security threat we notify you immediately and give a constant overview of the current security status of the plant through monthly status reports.

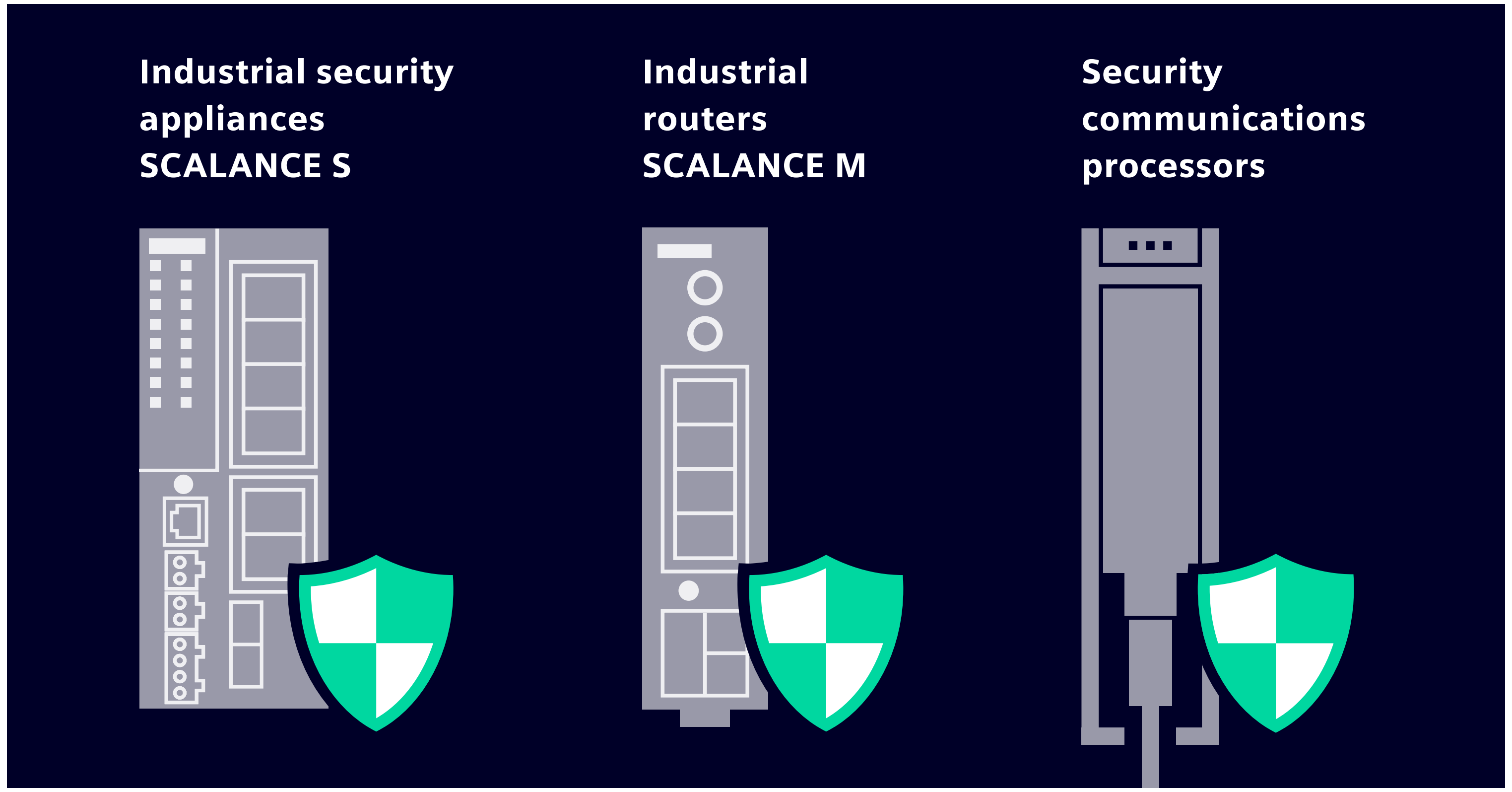
Network security

One of the key challenges for consistent communication is simply to establish adequate protection of the easily accessible open systems. The focus here is on availability and the protection of automation networks against unauthorized access. This includes monitoring all interfaces like the ones between office and automation networks or remote maintenance access to the internet. Automation networks and systems as well as industrial communication can be secured through network access protection, network segmentation (e.g. with “demilitarized zones”, DMZ) and encrypted communication with industrial Cybersecurity appliances, industrial routers, and zero trust network access (ZTNA).

Excellent components for network security

Industrial Cybersecurity components from Siemens are optimized specifically for being used with automation technology and are designed to meet the special requirements of industrial communication networks.

Certifications such as from TÜV Süd (IEC 62443) prove the effectiveness of the security functions that are implemented in our network components.



Industrial security appliances SCALANCE S

Industrial routers SCALANCE M

Security communications processors

Secure network architecture, remote access, and protected communication

To protect industrial networks and to enable using secured remote access Siemens offers a comprehensive product range with integrated security functions like SCALANCE S industrial Cybersecurity appliances, SCALANCE M industrial routers for wired and mobile wireless networks (4G/5G), and security communications processors for SIMATIC S7 controllers. These products support a stateful inspection firewall and also secured VPN communication for protection against unauthorized access, data espionage, and tampering.

All devices can be configured in the TIA Portal and enable consistent, end-to-end security engineering.

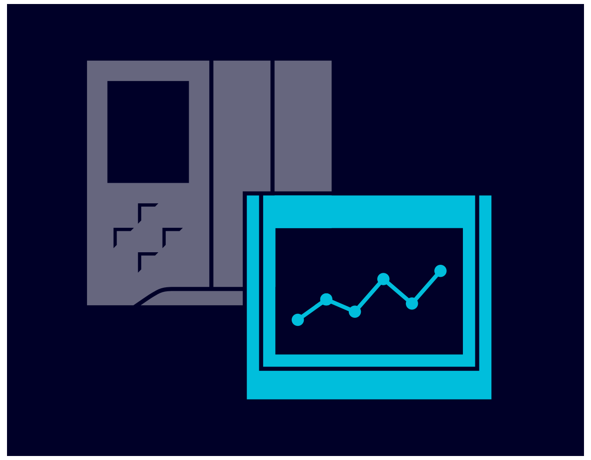
Software for efficient and secure networks

With the SINEC software solutions, it's also possible to monitor, manage, and configure complex industrial networks, including firewall rules (SCALANCE S), centrally and around the clock, including in security-related areas. SINEC Security Inspector and Monitor detect gaps and anomalies. SINEC Security Guard is an intuitive cloud-based software as a service which allows automated vulnerability mapping and security management optimized for non-security experts.

↗ siemens.com/networksecurity

System integrity

Protection of automation systems and control components. Our integrated security features provide comprehensive protection against unauthorized configuration changes at the control level as well as against unauthorized network access, preventing the copying of configuration data, and prevents any attempts to manipulate such sensitive data.

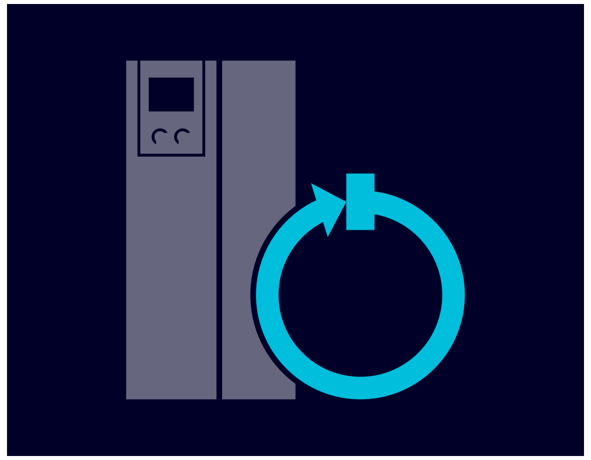


Controllers and HMI systems

Robust controllers and HMI systems with integrated security functions for multi-level access protection, know-how and copy protection and for secure communication: TLS based PG/HMI communication or via OPC UA.

PC-based systems

Security functions for PC-based automation systems with whitelisting, antivirus software and system hardening for greater OS security.

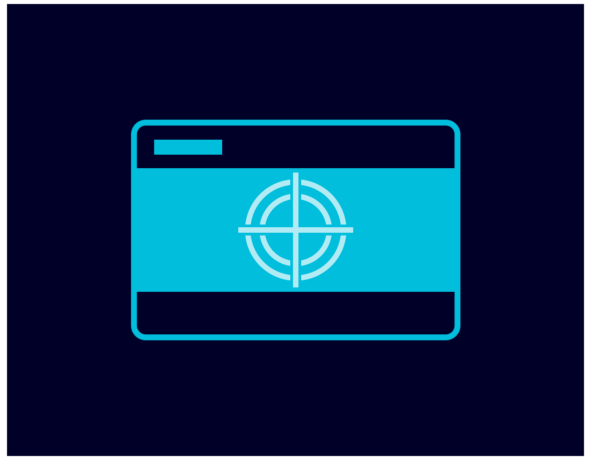


Motion control and drives

Integrated security functions in SINUMERIK, SIMOTION and SINAMICS for protecting your investment and maintaining productivity levels.

Process automation

Safeguard productivity in the process industry with the Industrial Cybersecurity concept for SIMATIC PCS 7 and SIMATIC PCS neo, based on the recommendations of the IEC 62443.



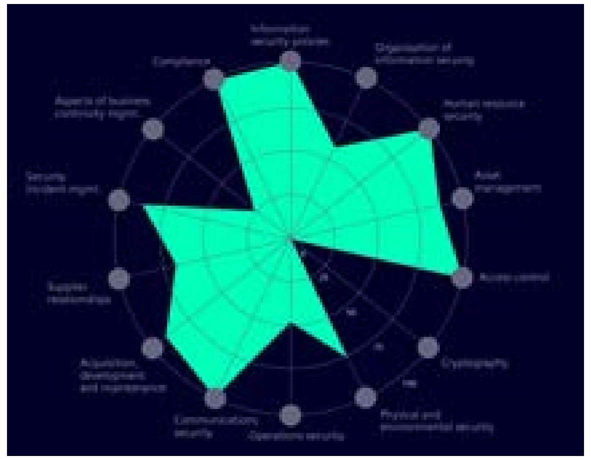
Secure access control with SIMATIC RF1000

The SIMATIC RF1000 system prevents unauthorized access, eliminating potential operating errors and production downtime.

Industrial Cybersecurity Services

With Industrial Cybersecurity Services, industrial plants benefit from the comprehensive expertise and technical experience of a global network of experts in automation, digitalization and Cybersecurity. The end-to-end approach of the industry-specific concept is based on state-of-the-art technologies as well as the applicable security rules and standards. Threats and malware are detected at an early stage, vulnerabilities analyzed in detail, and suitable comprehensive security measures are initiated. Continuous monitoring gives plant operators the greatest possible transparency regarding the security of their industrial facility and optimal investment protection at all times.

↗ siemens.com/icss

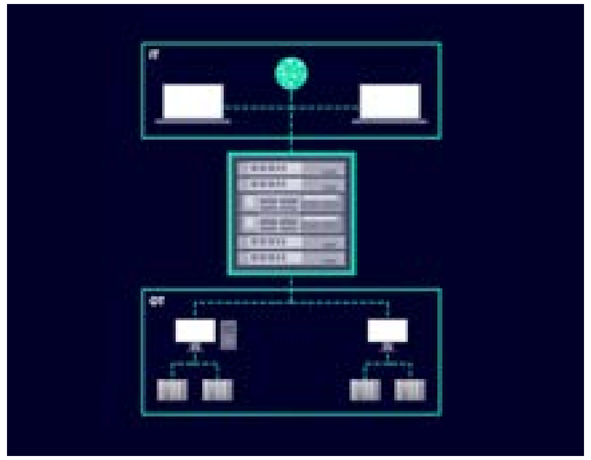


Security Assessments and Consulting

Security Assessments cover a holistic analysis of threats and vulnerabilities, the identification of risks and recommendations to close the identified gaps. They maximize transparency and provide a complete overview of the actual state of security of your automation systems. You can choose between a compact one-day on-site assessment (Industrial Security Check), or a deep assessment of compliance to IEC 62443 and NIS 2 (IEC 62443 / NIS 2 Assessment).

24/7 Infrastructure Monitoring

With Remote Industrial Operations Services, you have a team of proven experts behind you that covers your daily work regarding the operational continuity of your plant. As one of the leading industrial software companies, we have proven IT expertise in complex OT environments across all industries and can provide remote monitoring that's proactive, continuous, and integrated. We are your partner to remotely manage your infrastructure and thus align your IT and OT successfully.



Secure IT/OT Data Exchange

Industrial DMZ Infrastructure is a ready-to-run concept for IT/OT network segmentation with integrated security features. With front and back firewalls, the DMZ protects OT systems against unauthorized accesses from outside. Redundant, state-of-the-art Industrial Next Generation Firewalls not only function as port filters but also analyze the data at application level (Deep Packet Inspection). The services contained in Industrial DMZ, such as Remote Access, File Exchange, and Active Directory, are made available as virtual machines on a separate high-performance visualization host.

Vulnerability Management

Vulnerability Management empowers you to secure your infrastructure and product portfolio by providing relevant, actionable vulnerability intelligence. Based on a unique monitoring approach you receive vulnerability alerts for your individual system tailored to your needs – whether you need a comprehensive application including asset import and integrated reporting features, a seamless interface to your existing tools and processes via API, or the all-inclusive package with managed service by our experts.

Disaster Recovery

Backup and Restore offers comprehensive data protection without impact on plant performance. During operation, automatic backups are created from the computing cluster and stored on the backup server. In case of a failure, the virtual machines can easily be recovered from the backup server. This allows a fast recovery and prevents data loss. The solution is system-tested and pre-configured for OT environments. It includes hardware, software and services covering the complete life cycle – all from a single source and ready-to-run.

NIS 2 Directive

The NIS 2 Directive requires all operators of critical infrastructure and essential services within the EU to comply to stricter Cybersecurity regulations.

Siemens Security Assessments cover a holistic analysis of threats and vulnerabilities, the identification of risks and the development of a security roadmap with recommendations to close the identified gaps by experts with in-depth know-how in automation, digitalization and Cybersecurity.

↗ siemens.com/nis2-directive

NIS 2 Directive: support and solutions

The IEC 62443 / NIS 2 Assessment addresses the NIS 2 measures on risk management and information system security, supply chain security, access control and asset management. We support you with industrial Cybersecurity solutions and advise you if your company is affected by the NIS 2 directive in the EU.

Our deliverables:

- Identification of current security gaps based on the IEC 62443 security level target
- On-site workshop, coordinated by an ISA certified lead security consultant and a security engineer (min. 2 days)
- Questionnaire-based checklist to identify and classify risks
- Site survey of locations in scope
- More than 30 pages report containing recommendations for risk mitigation measures
- Additional report showing NIS 2 gaps on basis of assessment results

Siemens Xcelerator

Siemens Xcelerator provides integrated, scalable, and proactive Cybersecurity measures that keep pace with the speed of digital transformation. The key aspects of Siemens Xcelerator Cybersecurity approach are:

- Agility and Scalability: Siemens Xcelerator provides scalable Cybersecurity measures that include automated compliance checks, rapid vulnerability identification, and proactive monitoring to meet the growing demands of digital transformation.
- Rapid Incident Response and Regulatory Compliance: business disruption gets minimized and operational continuity is maintained. Automated compliance checks help businesses to meet regulatory standards and protect their reputation.
- Holistic Integration and Interoperability: Cybersecurity is integrated into all aspects of Siemens Xcelerator's portfolio, ensuring seamless security across IT and OT systems, and aligning with best practices for comprehensive Cybersecurity strategies.
- Ease of Configuration: Siemens Xcelerator provides Cybersecurity features that are based on industry standards and easy to configure. This reduces the complexity of managing security and empowers organizations to maintain strong defenses with minimal friction.

Siemens Xcelerator enables you to adopt new technologies and innovations without compromising your security posture, ensuring secure and sustainable digital transformation. Siemens Xcelerator ensures businesses to stay ahead of threats, mitigate risks, and maintain regulatory compliance across IT and OT systems. Siemens Xcelerator provides the necessary tools and measures to ensure that digital deployments are both secure and scalable.

Published by
Siemens AG

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

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

100 Technology Drive
Alpharetta, GA 30005
United States

For more information, please contact our
Customer Support Center
Phone: +49 180 524 70 00
Fax: +49 180 524 24 71
(Charges depending on provider)

Article No. DIFA-I10157-00-7600
Dispo 21507
WS 0924 iPDF

Subject to changes and errors.

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