SIEMENS

Background Information

Nuremberg, April 11, 2023

Industrial Cybersecurity

Siemens is the one-stop shop for industrial cybersecurity solutions

- **Convergence of IT and OT demands higher cybersecurity efforts**
- **Digital transformation and Cybersecurity – two sides of the same coin**
- **Multilayered defense-in-depth concept as gold standard**

The growing connection between production networks and office networks and the utilization of the Internet of Things (IoT) have many benefits for industrial companies, including digitalized processes and cross-company collaboration in ecosystems. At the same time, they also increase the risk of cyber threats. Industrial Cybersecurity protects the expertise and productivity of industrial enterprises from the growing number of cyber threats in Operational Technology (OT) and the IoT. To protect industrial production, Siemens relies on the multilayer defense-in-depth concept – extended by Zero Trust principles. According to Siemens, the only way to effectively counteract cyber threats is with a comprehensive concept that is applied at all the relevant levels.

“Without cybersecurity, there can be no digital transformation. Defending against threats and attacks is a fundamental prerequisite for the digital enterprise”, says Michael Metzler, Vice President Horizontal Management Cybersecurity for Digital Industries at Siemens. “Siemens is well placed to help integrators and operators meet these increasingly demanding challenges in its capacity as a single-source supplier of industrial automation and communication systems.” Security levels to be covered 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.

Siemens AG
Communications
Head: Lynette Jackson

Werner-von-Siemens-Straße 1
80333 Munich
Germany

The defense-in-depth concept is in accordance with the recommendations set out in IEC 62443, the leading standard for security in industrial automation. 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.

Starting point plant security

Plant security ensures that technical IT security measures are not bypassed by implementing physical access protection infrastructure and organizational measures. This includes barriers, turnstiles, cameras, and card readers, as well as a security management process. Physical access protection involves preventing unauthorized entry, separating production areas, and securing critical automation components. The strength of IT security measures depends on the level of physical access protection. Effective plant security requires a combination of organizational and technical measures, including risk analysis to identify security objectives and potential weaknesses. Industrial security experts help design secure production environments, assess security status, and create a security roadmap to comply with international security standards such as IEC 62443.

Securing production networks

Network security is crucial for protection against cyber-attacks. With increased interconnectivity, traditional defense concepts are pushed to their limits, leading to the adoption of the Zero Trust security concept, which focuses on verifying and authorizing communicating entities. However, as many OT devices lack the necessary functionality, a combination of Zero Trust principles, firewalls, and perimeter-based networks is needed for comprehensive security.

Secure access to OT networks based on Zero Trust principles can be achieved through solutions like Zscaler Private Access, which connects IT and OT networks reliably and securely. Siemens and Zscaler are partnering extensively for purposes like these. In this way, interfaces to other networks can be monitored and protected using firewalls and demilitarized zones (DMZ). Network segmentation and cell protection concepts involve separating automation cells with technical security mechanisms to minimize risk, control access attempts, and enable encrypted data transmission. Components

such as Siemens' SCALANCE S industrial security appliances can be used to implement these measures. As plants increasingly connect directly to the internet or through mobile networks for remote maintenance and monitoring, securing access is crucial. Using VPN mechanisms, data transmission can be encrypted, and communication nodes authenticated. SCALANCE M industrial routers and SCALANCE S industrial security appliances offered by Siemens provide user-specific firewall rules, allowing for temporary access tied to specific users.

Moreover, the SINEMA Remote Connect management platform enables secure and efficient remote access to globally distributed plants and machines, using VPN tunnels and central user management. SINEC NMS is a network management system that allows for central monitoring and configuration of networks, providing security through encrypted data communication and local documentation. Network security services include Industrial Next Generation Firewalls and Industrial DMZ Infrastructure solutions, which protect the system network from unauthorized access. Industrial Anomaly Detection based on Claroty's Threat Detection Software helps in early detection of network anomalies by comparing current traffic with a baseline of normal operations.

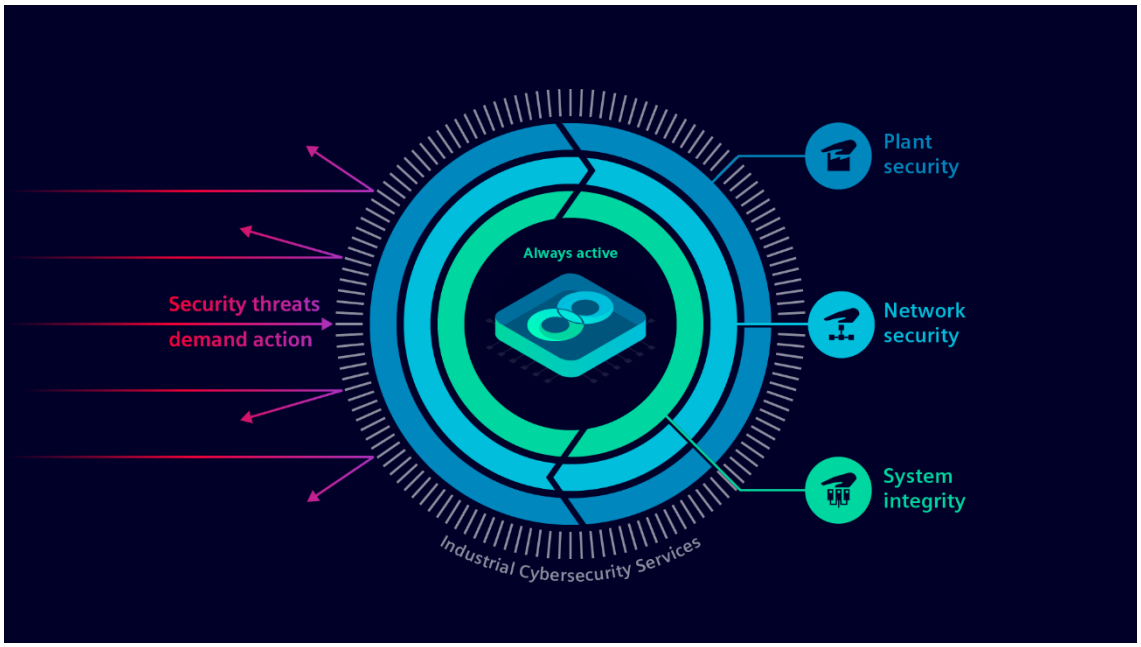
Maintaining system integrity

System integrity is the third pillar of a balanced security concept, focusing on protecting control components, automation, SCADA, and HMI systems. A multi-layered approach is necessary to maintain defense in depth. Protection at the control level is achieved through security mechanisms that are integrated into standard automation components and can be configured according to the level of protection required for the particular machine or plant.

The SIMATIC S7-1200 and S7-1500 controller families have integrated features for access protection and protection against manipulation. Secure communication between S7-Controllers and Engineering Stations or HMI-Stations is facilitated through TLS-based encryption. The TIA Portal Security Wizard assists users in setting up security configurations. Safeguarding intellectual property is also crucial, and Siemens controllers offer know-how protection and copy protection functions. Stateful Inspection Firewall and VPN are integrated into security communication processors for S7 controllers, creating secure interfaces to the entire plant network.

For protecting PC-based systems in the plant network, anti-virus software, whitelisting solutions, and integrated security mechanisms in Windows operating systems are used. Siemens supports the protection of industrial PCs and PC-based systems by testing software compatibility with virus scanners and whitelisting software, as well as providing guidelines for system hardening.

Secure access management for machines and plants can be achieved through the SIMATIC RF1000 Access Control Reader, which identifies personnel operating machines and assigns appropriate access rights using RFID cards and user-specific login data. This allows for transparent tracing in case of security incidents.
System integrity services rely on proven technologies and partners. Siemens offers Endpoint Protection with two approaches: Antivirus, which blocks malicious applications, and Application Whitelisting, which only allows trusted applications to run. Siemens also supports customers with third-party Endpoint Detection and Response (EDR) solutions. The Industrial Vulnerability Manager app helps manage cyber risks by monitoring components for published vulnerabilities. Furthermore, Siemens' Patch Management service is suitable for managing vulnerabilities and critical updates in Microsoft products, with tested and released patches for compatibility with control systems such as SIMATIC PCS 7. Additionally, service experts offer support for SIMATC controllers through the Managed Hardening service, ensuring the full security potential of the controller is utilized.



Defense in depth concept for Industrial Cybersecurity

Further information on Siemens Industrial Cybersecurity can be found at https://www.siemens.com/industrialsecurity

Press release regarding Zscaler partnership: https://press.siemens.com/global/en/pressrelease/siemens-and-zscaler-partner-integrated-zero-trust-security-solutions-otit

Contact for journalists
Christoph Krösmann
Phone: +49 162 7436402
Email: christoph.kroesmann@siemens.com

Follow us in **Social Media**:
Twitter: www.twitter.com/siemens_press and www.twitter.com/SiemensIndustry
Blog: https://blog.siemens.com

Siemens Digital Industries (DI) is an innovation leader in automation and digitalization. Closely collaborating with partners and customers, DI drives the digital transformation in the process and discrete industries. With its Digital Enterprise portfolio, DI provides companies of all sizes with an end-to-end set of products, solutions and services to integrate and digitalize the entire value chain. Optimized for the specific needs of each industry, DI's unique portfolio supports customers to achieve greater productivity and flexibility. DI is constantly adding innovations to its portfolio to integrate cutting-edge future technologies. Siemens Digital Industries has its global headquarters in Nuremberg, Germany, and has around 72,000 employees internationally.

Siemens AG (Berlin and Munich) is a technology company focused on industry, infrastructure, transport, and healthcare. From more resource-efficient factories, resilient supply chains, and smarter buildings and grids, to cleaner and more comfortable transportation as well as advanced healthcare, the company creates technology with purpose adding real value for customers. By combining the real and the digital worlds, Siemens empowers its customers to transform their industries and markets, helping them to transform the everyday for billions of people. Siemens also owns a majority stake in the publicly listed company Siemens Healthineers, a globally leading medical technology provider shaping the future of healthcare. In addition, Siemens holds a minority stake in Siemens Energy, a global leader in the transmission and generation of electrical power.

In fiscal 2022, which ended on September 30, 2022, the Siemens Group generated revenue of €72.0 billion and net income of €4.4 billion. As of September 30, 2022, the company had around 311,000 employees worldwide. Further information is available on the Internet at www.siemens.com.