SIEMENS
Ingenuity for life

IT security in the water industry: Essential protection

The number of attacks on automation and IT systems is on the rise, and as a result, plant engineers and owners in the water and wastewater industry have taken measures to protect their systems against manipulation and malware. However, the industry still requires suitable solutions to ensure that IT security will not impact plant availability. Such solutions make IT security an integral part of plant design and operation, providing a security package tailored specifically to the individual environment.

Remote monitoring for distributed plants, Internet technologies, and mobile devices for accessing data – these capabilities, coupled with the networked machines and processes they are based on, help to improve plant efficiency and facilitate plant monitoring and control. As a result, automation systems have become increasingly networked with IT systems, as many plant owners and operators realize – especially in the water and wastewater industry. Along with the benefits, however, networking these systems also brings risks. Modern standards such as Ethernet and TCP/IP are replacing proprietary networks, and the office and automation environments are merging – making process control systems more vulnerable to outside attacks.

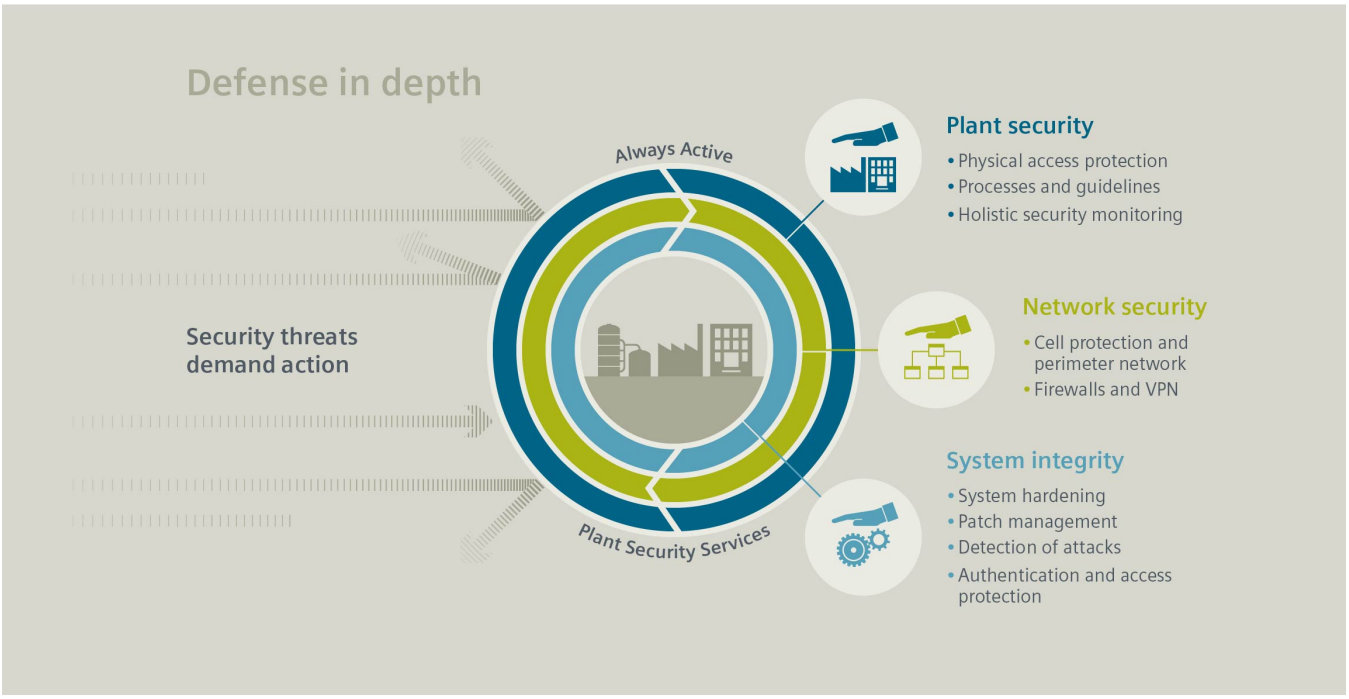
Taking threats seriously and adopting suitable measures

The potentially crippling effects of such attacks became evident in May 2017. In a worldwide cyberattack, the ransomware WannaCry is estimated to have affected more than 10,000 organizations and 200,000 computers across 150 countries. Luckily, the attack was stopped within a few days – but it still caused substantial damage, notably in industrial systems and applications. Especially troubling to IT and security experts, the cryptoworm exploited a known weakness that could have been eliminated by patching the systems – but obviously, many organizations had not applied such patches or were running legacy systems that could no longer be patched. Making regular and secure backups, implementing good cybersecurity that includes isolating critical systems, using appropriate software, and having the latest security patches installed should all be givens.

Then why are industrial automation and control systems often not as well protected as they could be? In its 2017 white paper "Cyber Security: Warding Off Threats with a Holistic Security Approach," the ARC Advisory Group listed several barriers to improving cyber security in industrial environments: increasingly open industrial automation, insufficient awareness among end-user managers, increased use of commercial off-the-shelf IT solutions, and finally, inadequately trained workers with misconceptions about the cyber security life cycle. According to ARC, one reason for reluctance to adopt security planning and implementation in some industries is that the task appears too daunting.

True enough, the specific environment of industrial systems has some unique requirements. Solutions and services for industrial security have to serve purposes that appear to be contradictory: production networks have to be 100% available, emergency stop signals always have to reach their destination without delay, a set value for a critical controller has to be processed with millisecond precision and at exact runtime intervals. On the other hand, scheduled virus and security scans, as well as authorizing and verifying of data packets, may result in a system load that affects the network's real-time capability.

This is why industrial facilities such as water or wastewater plants require matched solutions for IT security. Several automation suppliers are already addressing this demand with a set of products and services. Siemens' industrial security concept also includes industrial-grade security products for system integrity and network security.

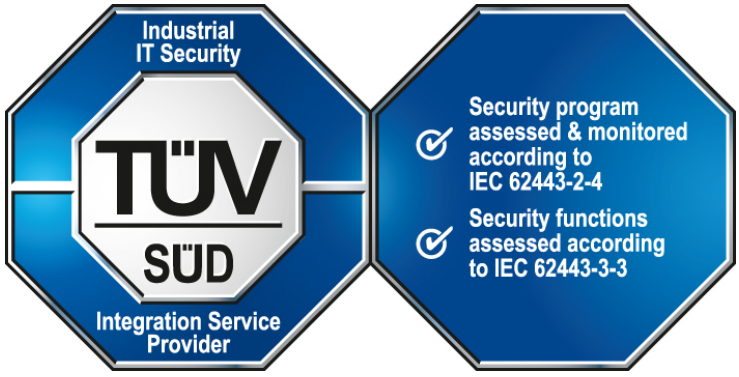


Deep staggered Defense - "Defense in Depth" - as a comprehensive protection concept, according to the recommendations of ISA99 / IEC 62443, the leading standard for security in industrial automation.

These features are complemented by threat and risk analyses as well as services for the installation, configuration, and management of security systems, including an early alert system for monitoring industrial systems. Finally, Siemens provides forensic analysis of events for documentation and reporting to authorities.

To minimize security risks, Siemens follows the “defense in depth” approach with a multilayer defense strategy from the plant management level to the field level. The concept integrates three components – system integrity, network security, and plant security – and is designed according to the recommendations of ISA99/IEC 62443, the leading standard for security in industrial applications.

Additionally, Siemens is continually improving all of its products and solutions with industrial security in mind, including obtaining certification under IEC 62443. As the first company to receive TÜV SÜD certification based on IEC 62443-4-1, for the interdisciplinary process of developing Siemens automation and drive products, including industrial software, Siemens received the certification at seven development sites in Germany in 2016. In the same year, TÜV SÜD certified that the security functions of the Simatic PCS 7 process control system and the development and integration processes conform to the security standard. Recurring audits make sure that Simatic PCS 7 continues to meet the standard’s requirements.



Siemens is the first company that recieved a TÜV-SÜD IEC 62443-4-1 certification for the overarching development process of Siemens products of the automation and drive technology, including industrial software.

Engineering secure plants and systems

To fully address the need for more secure systems, asset owners must consider all phases of the solution life cycle, from the development of systems to their eventual replacement. The IEC 62443 series of standards considers the life cycle to consist of five phases: product or system development, specification, integration and commissioning, operations and maintenance, and decommissioning. Each phase involves clear accountability and a primary objective, and therefore security topics have to be coordinated and communicated between different roles and stakeholders. Defense-in-depth security for a system requires covering a broad and heterogeneous range of security topics, including network security, user authentication, secure configuration and hardening of the operating system, logging, encryption, and secure channels. For each of these topics, there are plenty of technical solutions, tools, and best practices available – but project teams often lack the time and expertise to choose a suitable solution for each security topic. Hence, it is a common pitfall to focus on some topics in depth while overlooking others.

To facilitate security engineering and help engineers avoid this pitfall, Siemens has developed several blueprints for automation and control systems engineering that are certified according to IEC 62443 by TÜV SÜD. These blueprints provide guidance in the form of references to specific resources and make sure that the engineering project produces all security documents prescribed by IEC 62443-2-4. Based on a standard control solution using the Simatic PCS 7 process control system, the blueprints are designed to meet the requirements of a specific yet typical industry application.

Security from experience
Development of Siemens' secure framework and project blueprints was driven in large part by the company's own experience gained from more than 10 years of supporting security groups and engineering projectsacross the organization. The industrial security portfolio combines the expertise of Siemens' security engineers, incorporating it into products, systems, and a reproducible process that yields reproducible results – and mitigates project risk. Plant owners benefit by having a security solution engineered for their specific requirements that is ready for IEC 62443 certification. During plant operation, security documents advise them on system maintenance – and they can always draw on Siemens' industrial security expertise.

As cyber threats become more frequent and more creative, protecting processes and plants is a continuous task. This is why Siemens is offering a set of tailored plant security services that range from assessing security to implementing measures such as firewalls or antivirus software, to managing plant security through continuous monitoring. When Siemens experts detect a vulnerability, they alert the user and suggest proactive countermeasures. Supported by their own specialist organization, a global network of Siemens experts for automation and cybersecurity monitors current and developing threats, analyzes solutions for weaknesses, and develops suitable countermeasures, making sure that Siemens control and automation solutions are and continue to be secure by design.

Published by Siemens AG 2019

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe