Cybersecurity in the water industry: Essential protection

Attacks on automation and IT systems are on the rise, and, as a result, plant engineers and owners in the water and waste water industry have taken measures to protect their systems against manipulation and malware. However, the industry still requires suitable solutions to ensure that cybersecurity 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.

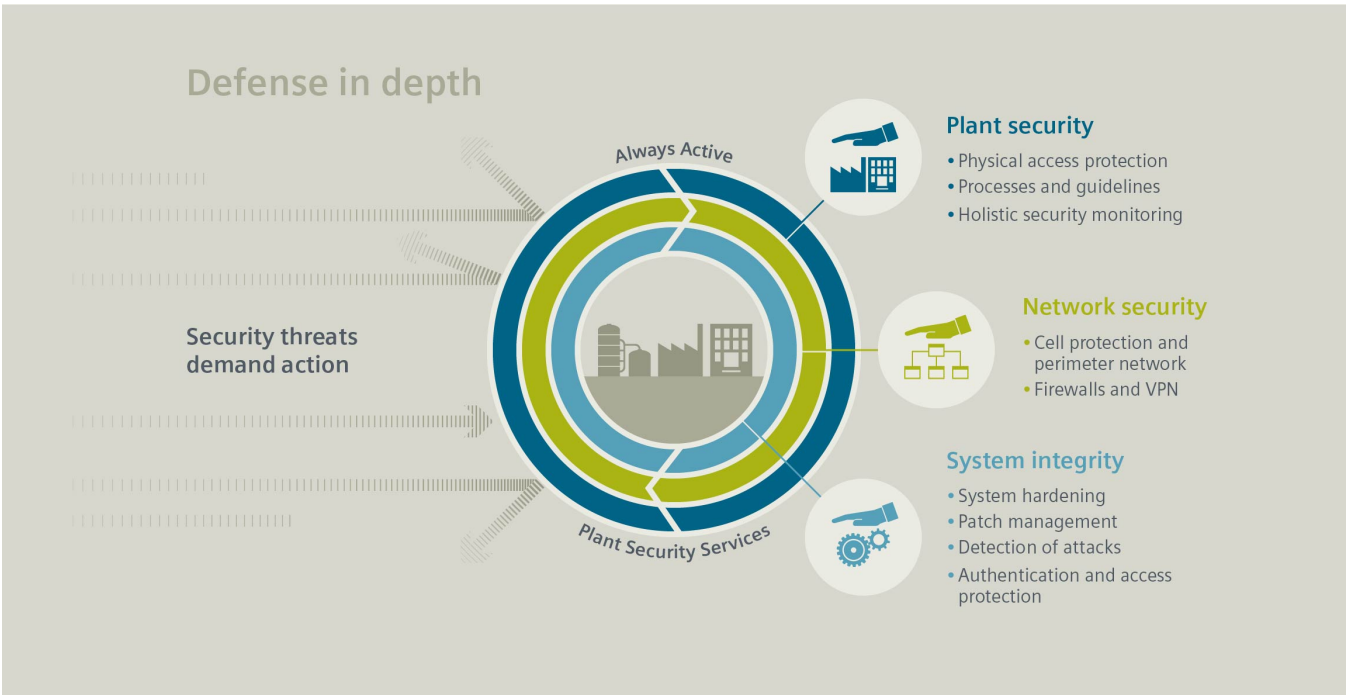
Connecting distributed systems via remote control – including connecting via public communication networks – , IT connections to regulatory systems, Internet technologies and mobile devices: coupled with the networked machines and processes these capabilities are based on, they help improve plant efficiency and facilitate plant monitoring and control. As a result, automation systems have become more networked with IT systems than many plant owners and operators are aware of, – especially in the water and waste water industry. Along with the benefits, however, networking these systems also brings risks. Modern standards such as Ethernet, TCP/IP, and mobile communication 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

That such vulnerabilities exist and represent a serious concern has become evident through cyberattacks such as the attacks on water supply systems in Switzerland in November 2018, which could be traced to origins in London and Korea. The potentially crippling effects of such attacks also were brought to the world's attention in May 2017, when, in a global cyberattack, the ransomware WannaCry is estimated to have affected more than 10,000 organizations and 200,000 computers across 150 countries. Fortunately, the attack was stopped within a few days, but it still caused substantial damage, notably in industrial systems and applications. What was especially troubling to IT and security experts was the fact that the cryptoworm exploited a known weakness that could have been eliminated by patching the systems – but 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 practices that include isolating critical systems, using appropriate software, and having the latest security patches installed should all be givens.

So why are industrial automation and control systems often not as well protected as they could and should 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 cybersecurity in industrial environments: an aging infrastructure paired with increasingly open industrial automation, insufficient management and user awareness, increased use of commercial off-the-shelf IT solutions, and, finally, inadequately trained workers with misconceptions about the cybersecurity lifecycle. According to ARC, one reason for reluctance to adopt security planning and implementation in some industries is that the task appears too daunting.

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



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.

This is why industrial facilities such as water and waste water plants require specific solutions for industrial cybersecurity that differ from established approaches in the general IT environment. Especially in the field of critical infrastructure, system availability – for example, security of supply in water systems – has top priority. Various automation suppliers are already addressing this demand with industry-specific products and services. For example, Siemens supports plant owners and operators in the water industry with an extensive service portfolio that includes a security status analysis and assistance with the design and implementation of security systems. Siemens' industrial security offering also includes industrial-grade security products for system integrity and network security. These features are complemented by threat and risk analyses as well as services for the installation, configuration, and management of security solutions, including an early alert system for monitoring industrial systems – for example, to identify network communication anomalies. 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 that extends from the plant management level to the field level. The concept integrates three components – system integrity, network security, and plant security – and is designed in accordance with IEC 62443, the leading standard for security in industrial applications that is recommended for product and system suppliers by national authorities such as the German Federal Office for Information Security (BSI).

Additionally, Siemens is continually developing and improving all its products, systems, and solutions with industrial security in mind, including obtaining certification under IEC 62443. In 2016, Siemens was 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. Since then, Siemens has received the certification at more than 30 development sites, covering all product families relevant in the water and waste water industry, such as Scalance communication products, Simatic components, and the Simatic WinCC and PCS 7 systems. In 2016, TÜV SÜD also certified the security functions of the Simatic PCS 7 process control system and the development and integration processes in accordance with IEC 62443-3-3 and 62443-4-1, respectively.

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.

Recurring audits – last performed in November 2019 – confirm that Simatic PCS 7 continues to meet the standard's requirements. This regular review also ensures continuous analysis of the security-relevant criteria of products and systems and continuous testing and delivery of security patches, including for third-party components and software.

Engineering secure plants and systems

To fully address the need for more secure systems, asset owners must consider all phases of the solution lifecycle, from development to system operation. The IEC 62443 series of standards considers the lifecycle to consist of five phases: product or system development, specification, integration and commissioning, operation and maintenance, and decommissioning. Each phase involves clear accountability and a primary objective, and therefore security issues must be coordinated and communicated between different stakeholders such as product suppliers, systems integrators, and plant operators.

Defense-in-depth security for a system requires addressing a broad and heterogeneous range of security domains, including network security, user authentication, secure configuration and hardening of the operating system, logging, encryption, and secure communication channels. In each of these areas, 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. Hence, it is common 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 support a secure design process in accordance with the international IEC 62443 standard. A key component of these blueprints is the IEC 62443-3-3 certified Simatic PCS 7 process control system and the Simatic Net portfolio of switches, routers, and firewalls. Since November 2018, Siemens has been certified in accordance with IEC 62443-2-4 for security-related capabilities offered as services to plant operators in the context of application engineering and integration and maintenance of an automation solution. As a result, project teams have access to guidance in the form of references to specific resources and can follow a process that ensures that the engineering project produces all security-relevant documents and that all security measures are applied to their fullest extent.

Moreover, Siemens is among the first system and solution providers to offer extended blueprints for water, waste water, and desalination projects that comprise features such as security components and procedures for encrypted – and, as a result, secure – communication for telecontrol via public networks. These extended blueprints and the corresponding documentation for secure process control system configuration are certified in accordance with IEC 62443-3-3 and are available to Siemens project teams and external systems integrators. In this way, Siemens supports integrators and partners during project design, engineering, and implementation as well as supporting utilities in the secure operation of water and waste water plants.

Security from experience

The 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 projects across the organization. The industrial security portfolio incorporates the expertise of Siemens' security engineers into products, systems, and a reproducible process that yields consistent 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 suite of tailored plant security services that range from assessing security, to implementing measures such as firewalls and 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 its own specialist organization, a global network of Siemens experts in automation and cybersecurity monitors current and developing threats, continuously analyzes products and systems for vulnerabilities, and proactively implements countermeasures, ensuring that Siemens control and automation solutions are and continue to be secure by design.

Published by Siemens AG 2020

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe