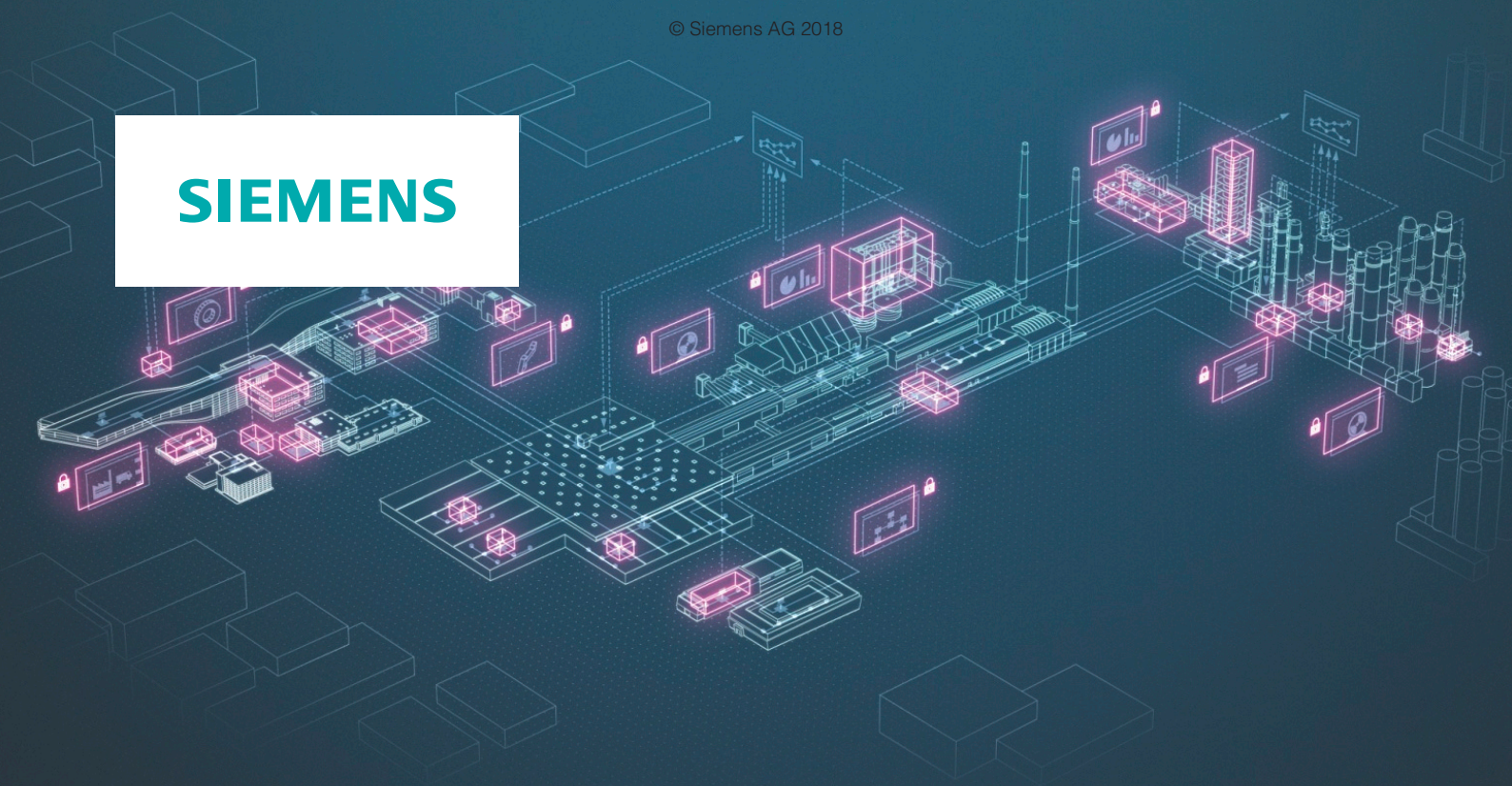
SIEMENS



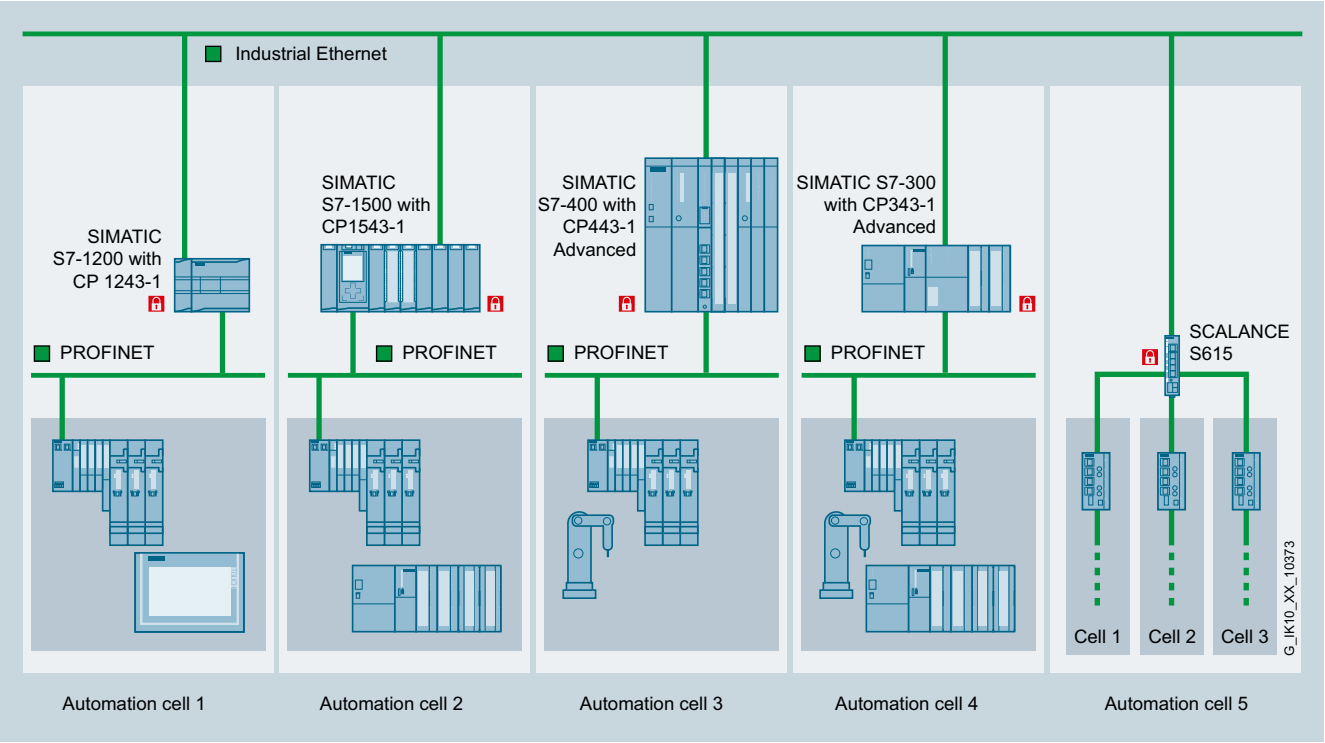
Technical article

Mastering the Industrie 4.0 security challenge

Factory and process automation are reaching new levels of integration that go far beyond just the automation. This not only opens the way to considerably higher degrees of efficiency, process control and flexibility, but also calls for increased security to protect the whole factory from malware and unauthorized intrusion.

Digitalization, Industrie 4.0 and similar initiatives are not mere buzzwords. They stand for no less than the next dimension of efficiency in industrial production systems and process plants. Automation systems and information technology will merge, while remote access, process monitoring, control and maintenance will reach new levels. Big data will offer new insights and help efficiently control processes and boost plant availability. With increasingly more connected devices in the Industrial Internet of Things (IIoT), islands of automation will disappear – which is why reliable, secure and future-proof industrial communication networks are crucial.

But in the opinion of many plant operators, Industrie 4.0 represents new challenges when it comes to protecting their automation systems from malware, unauthorized intrusion and security breaches – both intentional and unintentional. They are well aware of previous incidents that made headlines, and often hesitate to introduce innovative technologies, fearing they might expose their system to new vulnerabilities as well as new ways of being attacked.



Siemens has Security Integrated components to implement cell protection concepts – these components not only have integrated communication functions but also special security functions such as firewalls and VPN.

Openness as a key to success

Siemens knows from its own experience that cyber attacks must not be taken lightly. As a global player in the automation field and operator of many factories worldwide, Siemens has therefore adopted a philosophy that actively addresses this issue – and has embedded system security into their product design, system development and services. Security integrated components represent a prime example as they not only have integrated communication functions but also special security functions such as firewalls and VPN. They also closely collaborate with their customers to openly address any vulnerability and effectively respond to any system intrusion.

The benefits of first-hand experience

For automation system providers and plant operators alike, system vulnerability is a delicate subject. Having said that, technology partners should be able to deal with this issue in an atmosphere of mutual trust and open communication. Being a global player in both discrete manufacturing and process industries. Siemens experts and solution providers can refer to a wealth of know-how gained in countless installations all around the globe – making them familiar with the specific challenges faced by a wide range of industries and customers.

Siemens also operates its own manufacturing sites in many parts of the world, leveraging its products and security integrated components to create holistic security concepts to protect its factories and automation systems. This allows Siemens to offer leading-edge solutions to its customers, based on systems and components that they have proven in their own plants and systems.

Siemens applies the Holistic Security concept in many of the factories that it owns and operates.

In addition to the crucial aspect of security, another important product attribute is that commissioning and maintenance work must be possible without requiring any on-site engineering skills. This is achieved by integrating all hardware configurations into either the engineering software or intelligent plug-ins – eliminating the need for manual configuration on site. Service technicians only have to unplug, replace and re-connect a defective component, without having to worry about configuration issues and potential errors.

Holistic approach to Industrial Security

System security goes far beyond an effective firewall. Considering the ever-present threat of cyber attacks, a holistic approach is required that extends from physically protecting facilities based on an effective access control system all the way to addressing software issues, such as frequent security patches and updates.

This is the reason that Siemens has established a hardware and software development process (secure by design) that actively integrates all relevant security issues right from the start. In all of the development projects, the responsible project manager works side by side with a dedicated security expert. This expert is responsible for a comprehensive security review of the requested features and design, and also conducts security testing prior to the release of any product on the market. The security expert is authorized to stop the release of any project if serious security breaches are identified.

The new SCALANCE SC-600 Industrial Security devices – including the secure-by-design process based on IEC 62443-4-1 along with threat and risk analysis and penetration tests.

The security process must assess and evaluate in detail all threats and risks to the industrial environments where the products will be used. In conjunction with this, it is worth mentioning that Siemens is a member of ISA 99, the standardization body of the leading international Industrial Security standard IEC 62443, and has a clear objective of fully complying with established industry standards. Siemens also actively drives the development of such standards – addressing customer demands to incorporate reliability and security aspects crucial to their factory and process automation system environments.

Security as a quality standard and open transparent incident handling

As part of the secure-by-design development process, all newly developed hardware components and software are analyzed by a team of security experts. These experts look for issues that could make the component vulnerable to external attacks, and thus compromise the security of the overall automation system. This research continues even after the product has been launched into the market.

This is why Siemens security experts collaborate closely with renowned security researchers at universities, security service providers and CERT organizations all around the globe. They are able to access the very latest security-related information. Any vulnerability that is identified is resolved in the shortest time possible by a task force drawn-up specifically for this purpose. Product updates are developed and verified – and security patches are provided to all customers that might be affected.

In other words, these hardware and software products reflect a standard of quality where the emphasis is placed on product security rather than time to market. With the objective of establishing itself as a trusted long-term partner for its customers, based on its secure-by-design development process, Siemens puts far more emphasis on launching a secure product into the market than being the first to introduce a new technology.

With defense in depth, Siemens provides a multi-faceted concept that gives plants and systems both all-round and in-depth protection. The concept is based on plant security, network security and system integrity – in-line with the recommendations of IEC 62443.

Security as a vital total cost of ownership (TCO) factor

Cyber attacks can shut down a complete process plant or manufacturing system. This not only results in substantial capital loss for the company involved, but also – depending on the industry – it can also lead to a great loss of reputation and expose the company to costly liability claims. The goods may even be blacklisted, if they are part of a public infrastructure.

As a consequence, more and more companies are willing to invest in the security of their automation systems by teaming up with a partner like Siemens who emphasizes security as an integral part of its business strategy. Although investing in hardened products will be costlier, it will greatly contribute to lower cost of ownership over the complete life cycle of the system.

Security lifetime services

"The increasing number of cyber attacks is a fact that cannot be overlooked. But this must not be a reason to forego the digitalization of industrial production. Instead, cyber security should be seen as a competitive advantage rather than a cost factor," explained Helmuth Ludwig, Chief Information Officer at Siemens.

"Industrial Security" is a strategic security concept that is designed to help pave the way to the Digital Enterprise of tomorrow. It is based on the defense-in-depth concept that is proposed in IEC 62443.

Industrial Security not only includes security-related product features, but also the design of automation systems with the help of pre-defined and security-tested software components. It also provides customers with a range of security-related services that continuously monitor automation systems and the development of preventive security measures.

Industrial cyber security is a challenge, but it can be mastered with concerted effort, open communication and dedicated services. The Plant Security Service portfolio, the Patch Management and Vulnerability Management services provide exactly the right kind of support needed here.

Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit **http://www.siemens.com/industrialsecurity**

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Germany

PDF
Technical article
FAV-390-2017-PD-PA
BR 0318 / 4 En
Produced in Germany

siemens.com/industrialsecurity