As an equipment manufacturer, we measure and monitor software development processes to track performance and capabilities as a matter of course. However, ISA/IEC 62443 – focused on security for industrial automation and control systems – is the international benchmark we follow to meet appropriate cybersecurity requirements for our products, solutions and services.

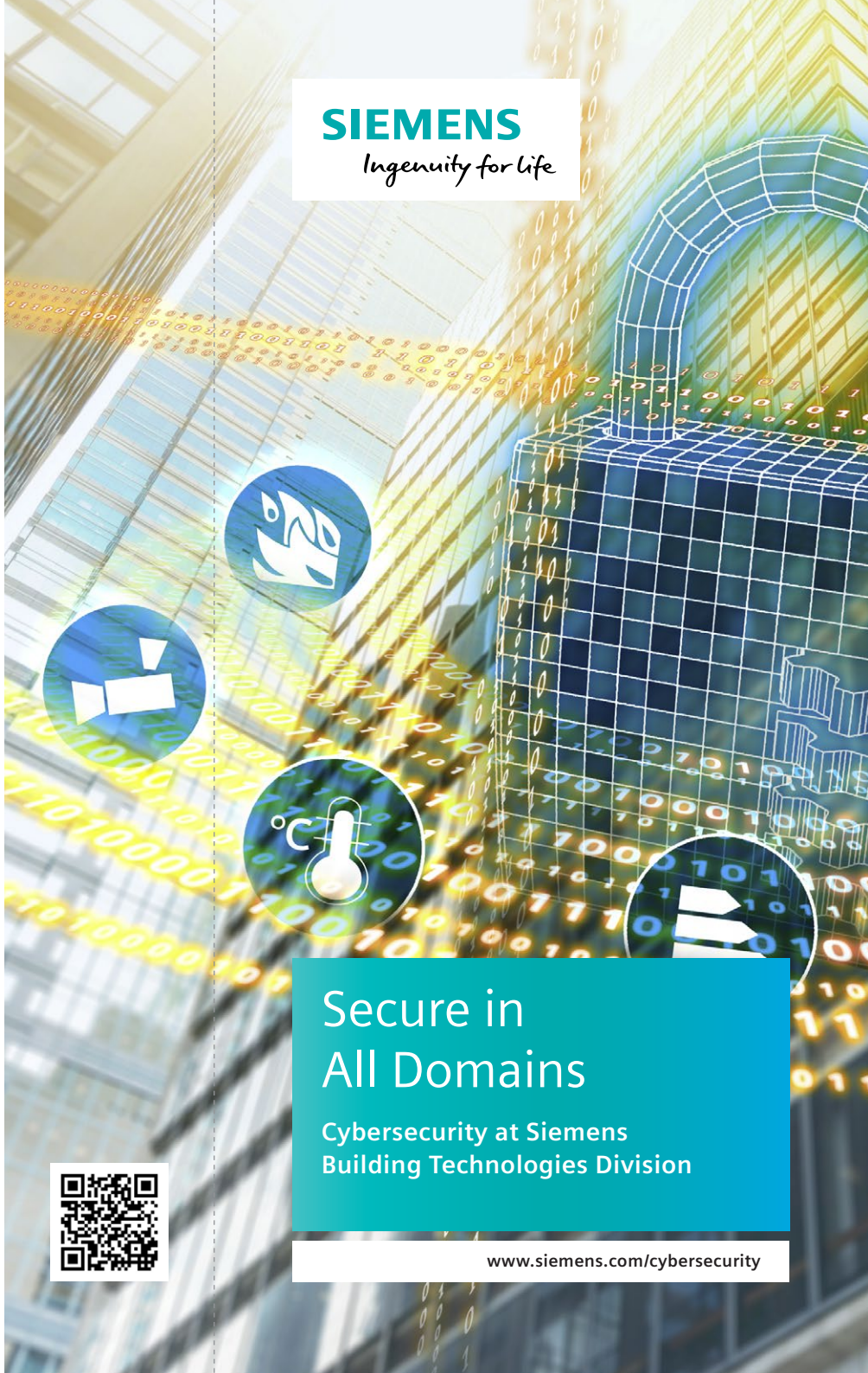
We work tirelessly to meet the highest quality levels in security and to protect your vital assets and business processes from compromise.

‘Secure in All Domains’: your trusted partner for physical and cybersecurity

Siemens Building Technologies Division is known for its extensive portfolio in physical security: Identity and access management, physical incident management and industrial command & control systems. As physical and cybersecurity has long begun to merge, we are uniquely positioned to physical and cybersecurity matters – from one single, trusted source. Rely on us to meet your security needs and protect your foundation for business continuity, brand reputation and growth.

For us, ‘Secure in All Domains’ is a necessary paradigm to minimize risk, while maintaining the integrity of our products and solutions in their intended environment. Ultimately, whether cyber or physical, we are committed to safeguarding the only thing that matters to you – security as the cornerstone of your business today.

Article no. BT_0104_EN (Status 12/2016)



Secure in All Domains

Cybersecurity at Siemens Building Technologies Division

www.siemens.com/cybersecurity

Cybersecurity at Siemens

The holistic approach to cybersecurity for our products, solutions and services at Siemens Building Technologies Division

With decades of experience in the field of building technology, Siemens understands that one of the fundamental principles of operational performance, business continuity and success for our global partners is security.

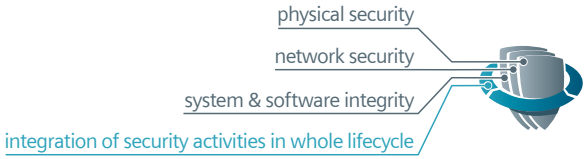
When we "think security", we follow a comprehensive approach to offering you peace of mind – a careful balance of cyber, physical and organizational security measures ensuring protection against threats faced today.

Digitalization means business requires increasing interconnectedness to thrive in a global, streamlined economy. With digital convenience comes increased cyber threat, so cybersecurity is a vital element to protect assets and prosper in the world we work in. At Siemens, we are prepared for the fact that nowadays it's not **if,** but **when** a cybersecurity breach happens. Let's take a closer look at how we integrate security into our products, solutions and services.

'Secure in All Domains' is our philosophy based on a 'Secure by Design' approach coupled with complete product lifecycle support. Not only do we base our security measures on international standards, we file over 70 cybersecurity-related patents each year. We also provide extensive secure configuration and commissioning guidelines for our products, solutions and services. And if anything were still to happen, our state-of-the-art ProductCERT team will support you on incident response matters.

Secure configuration and commissioning of products, solutions and services

As a market leader, Siemens understands what it takes to meet your cybersecurity needs today. Based on stringent internal product development activities aligned to industry standards for software developers and architects, we ensure our secure configuration and software hardening processes are cutting edge in the building technology industry.



We apply the same rigor to commissioning and installation of our products and solutions at your site. You stand to benefit from our expertise in audit-proof business processes, and compliance with the rising number of national and international regulations set to enhance cybersecurity for buildings and infrastructure.

Complete product lifecycle support

Providing you with a high degree of cybersecurity is shown through our activities integrated along the entire product lifecycle. This method minimizes our susceptibility to internal or external attacks.

Continuous threat monitoring allows us to detect and fix potential vulnerabilities in our products and solutions, thus reducing your exposure to risk. We also understand that security means every second counts so we publish security advisories and bulletins to alert you appropriately to ensure fast, streamlined communication.

Our 'Secure by Design' approach: from concept to deployment … and beyond

'Secure by Design' is a pledge to addressing comprehensive security in our development process by integrating cradle-to-grave activities. This ensures continuous enhancement to the development of our products, solutions and services:

Threat and risk analysis of our products, solutions and services starts early on in the process to identify and mitigate risk appropriately.

Secure architecture is an embedded discipline to specify and assure compliance with a wide range of security measures, requirements and implementation guidelines. To complement these activities, we validate our offerings by assuming an attacker's perspective. Secure coding focuses on standardized and secure implementation of software components fundamental to our products, solutions and services, while secure configuration looks at the hardware components – checking features and functions are secure at the default level. Where appropriate, security testing is then performed using automated and manual penetration testing tools and techniques.

'Secure in All Domains' is our philosophy based on a 'Secure by Design' approach coupled with complete product lifecycle support.

Cybersecurity is also an integral part of our secure supply chain management processes and contractual agreements to support secure supplier best practice. Adding on secure service then safeguards and maintains the security and integrity of a product or solution in your environment.

Siemens ProductCERT team

Our offerings are enhanced by the Siemens ProductCERT team who supports customers round-the-clock, whether it's to do with day-to-day business or potential disruption from critical cyber incidents. The team continuously monitors and responds to possible incidents and vulnerabilities related to Siemens products, solutions and services. Technical experts collaborate with you to help defend against potential threats, tackling security issues without delay.

Commitment to International Security Standards: ISA/IEC 62443 and ISO/IEC 27001

To stay ahead of the curve, we contribute and adhere to leading international standards which are essentially codified as best practice.

When it comes to aligning security with business need and the inevitable move towards convenience, we put a premium on cybersecurity from the outset. Siemens was one of the first companies worldwide with an Information Security Management System (ISMS) for remote services conforming to ISO/IEC 27001 – the norm followed for systematic cybersecurity management on an organizational level.