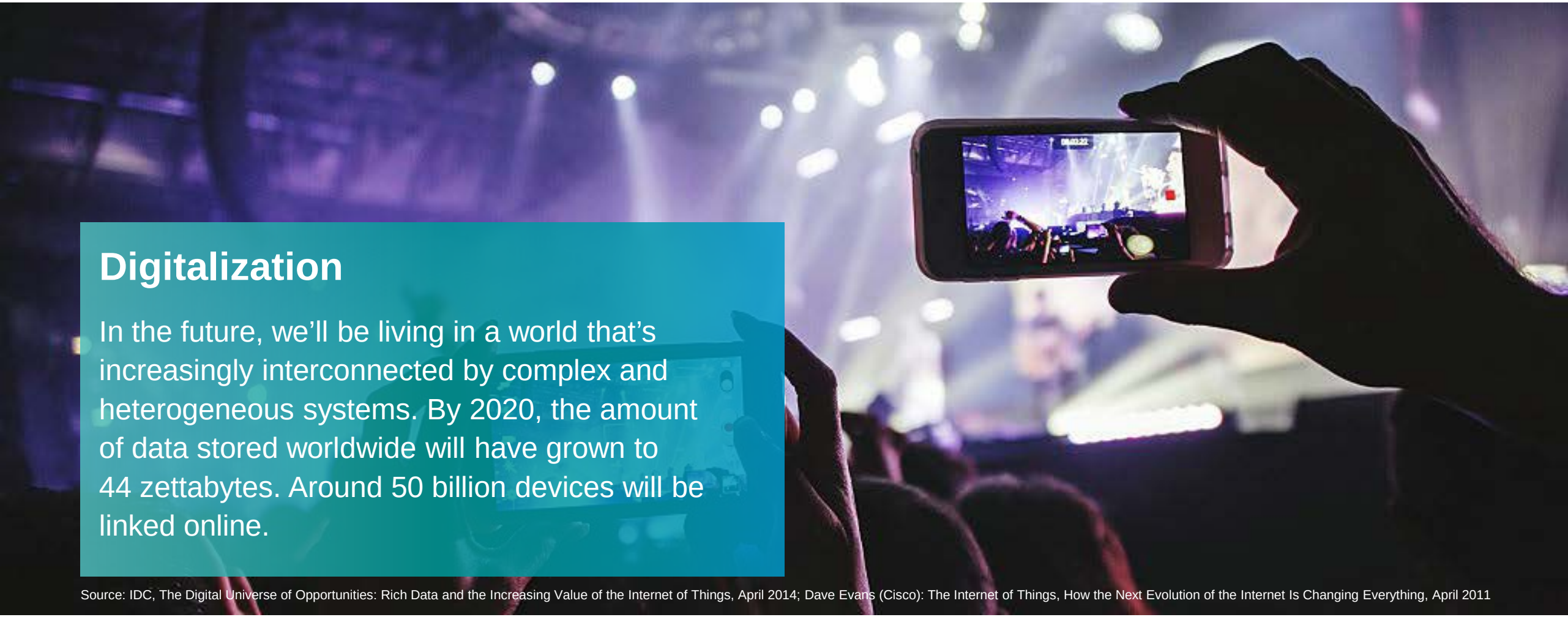
Security Standardization and Regulation

An Industry Perspective

Dr. Ralf Rammig
Siemens AG

Megatrends – Challenges that are transforming our world

SIEMENS
Ingenuity for life



Digitalization

In the future, we'll be living in a world that's increasingly interconnected by complex and heterogeneous systems. By 2020, the amount of data stored worldwide will have grown to 44 zettabytes. Around 50 billion devices will be linked online.

Source: IDC, The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things, April 2014; Dave Evans (Cisco): The Internet of Things, How the Next Evolution of the Internet Is Changing Everything, April 2011

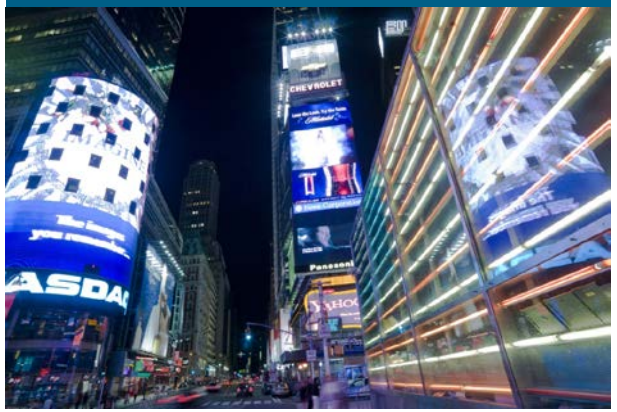
Increasing Intelligence and Open Communication Drive Security Requirements in Various Industrial Environments

SIEMENS
Ingenuity for life

Process Automation

Factory Automation

Urban Infrastructures



Building Automation

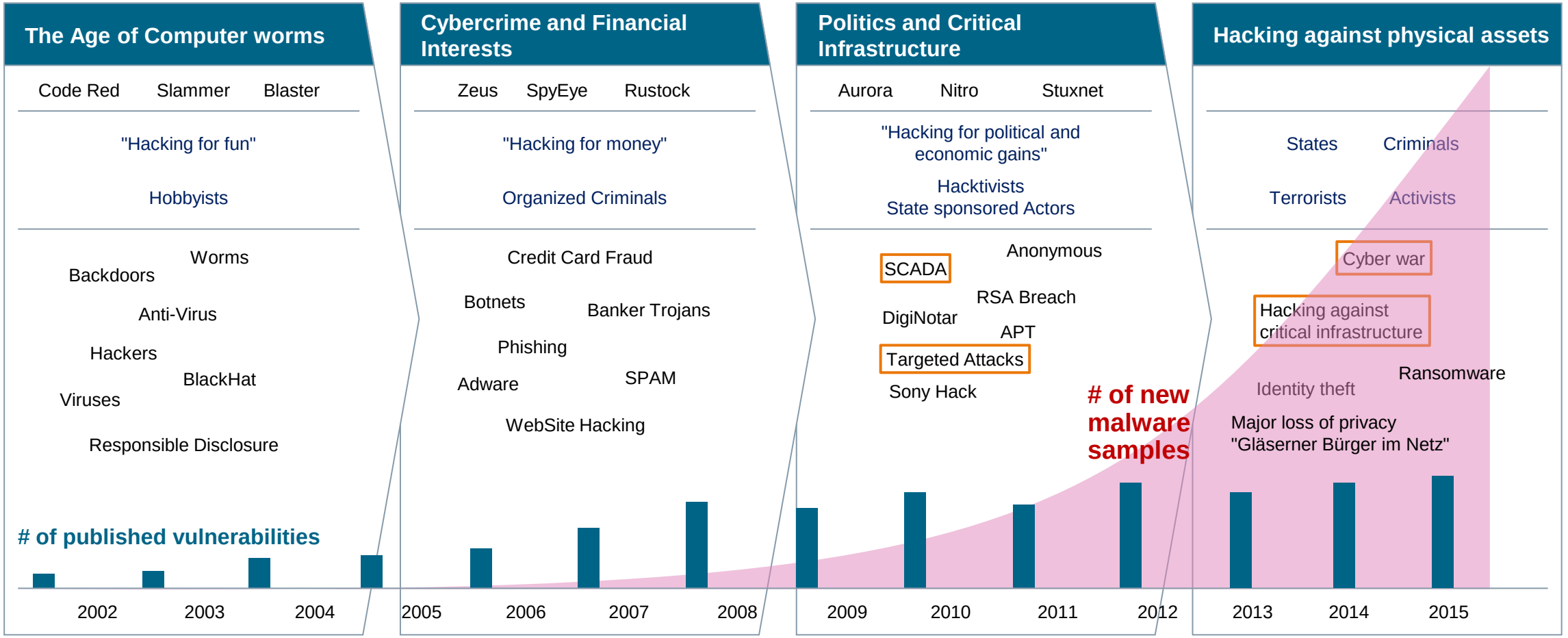
Energy Automation

Mobility Systems

The Threat Level is Rising
Attackers are Targeting Critical Infrastructures

SIEMENS
Ingenuity for life

Evolution of attacker motives, vulnerabilities and exploits

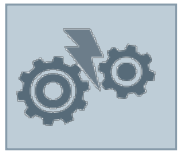


Data sources:
IBM X-Force Trend and Risk Report
HP Cyber Risk Report
Symantec Intelligence Report

Consequences of Security Issues can be far-reaching

Security incidents can affect target solution and connected (critical) assets

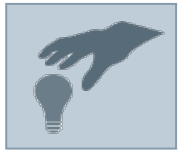
SIEMENS
Ingenuity for life



Degradation or disruption of customer business

Breaches of legal and regulatory requirements

Breaches of contractual requirements



Loss of intellectual property or license fraud

Loss of reputation, customers or market share

Safety, Privacy, Environment

Examples (since 2016):

- Maersk Previews NotPetya Impact: Up to $300 Million
- Fresh Vehicle Hack Disables Airbags, Anti-lock Brakes
- Verizon Breach: 6 Million Customer Accounts Exposed
- Ukrainian Power Grid Blackout Alert: Potential Hack Attack
- Ransomware Attack Affects 500,000 Patients
- …

Source: https://www.databreachtoday.co.uk

How can the occurrence and consequences of security incidents be reduced?

Industrial Systems and Office World have Different Characteristics & Requirements (Examples)

SIEMENS
Ingenuity for life

	Industrial Systems	Office IT
Protection target for security	Production resources, incl. logistics	IT- Infrastructure
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real-time requirement	Can be critical	Delays accepted
Security Standards	Under development	Focus on ISO/IEC 27000 series
Application of patches	Controlled / limited due to availability	Regular / scheduled
Anti-virus	Uncommon, hard to deploy, white listing	Common / widely used

“Office“ security concepts and solutions are not directly applicable for industrial systems

Characterization of Different Scenarios

SIEMENS
Ingenuity for life

	Product supplier	System Integrator, Operator, Service Provider, Asset Owner	Recommendations for regulation
B2C	• Products are connected to the Internet • Products with basic state-of-the-art security features	• User has limited expertise • Updates are deployed automatically or under user control	• Basic requirements as legal requirements according to state-of-the-art on product level (NLF)
B2B / B2Critis	• Focus on the intended use and operational environment of the products and solutions • Products with intended use specific security features	• Cyber Security expertise on the user's side (operator, integrator, service provider) • Updates are deployed in a controlled manner	• Regulation of operators depending on criticality • Entry level by self-declaration • Regulation gives preference on process requirements rather than product certifications

A Combination of Technical Measures and Processes is needed!

SIEMENS
Ingenuity for life

		Consequence Category		
		A	B	C
Likelihood	High	High-risk	High-risk	Medium-risk
	Medium	High-risk	Medium-risk	Low-risk
	Low	Medium-risk	Low-risk	Low-risk

Risk Assessment

e.g. IEC TC 65
IEC 62443-3-2

Security measures

Technical measures

Process measures

Security for products

Security for solutions

Rules & procedures

People, Training

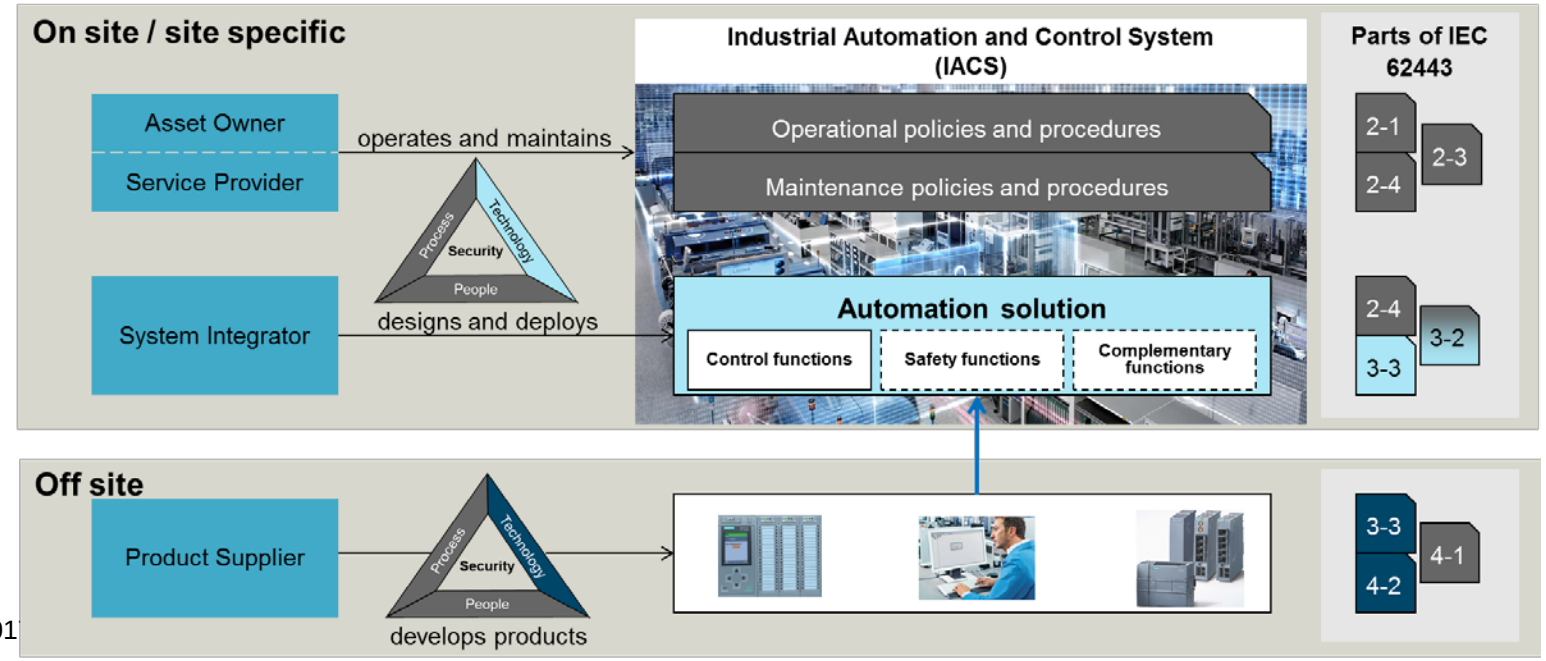
Committees / Standards (example)
IEC TC 57 IEC 62351-3, 4…
IEC TC 65 IEC 62443-3-3
ISO/IEC JTC1/SC 27 ISO/IEC 27019
ISO TC 292 WG4 ISO 12931, ISO 16678

IEC 62443 Standards Series
A Holistic Security Approach

SIEMENS
Ingenuity for life

IEC 62443

- defines organizational and technical requirements for all stakeholders involved (manufacturer, integrator, operator)
- targets people, processes, systems, solutions and components/products
- applies to all types of plants, facilities and systems in all industries
- supports purpose fit security solutions by supporting security features with different strength
- used for certification of security processes and security capabilities of the solution



How could regulation support security?

Managing Cyber Security in Critical Environments through Standards and Regulations (Examples)

SIEMENS
Ingenuity for life

- IEC 62351-1 … -14
  Power systems management and associated information exchange – Data and communications security
- IEC 62443-1-1 … -4-2
  Industrial communication networks - Network and system security
- ISO/IEC 15118
  Road vehicles -- Vehicle to grid communication interface

- ISO 27001 – Information technology - Security techniques - Requirements
- ISO 27002 – Code of Practice for information security management
- ISO 27019 – Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002

- IEEE 1588 – Precision Clock Synchronization
- IEEE C37.238 – Profile for Use of IEEE 1588 PTP in Power System Applications
- IEEE 1686 – Intelligent Electronic Devices Cyber Security Capabilities

- Critical Infrastructure Protection CIP 001-014
- Executive Order EO 13636 improving Critical Infrastructure Cyber Security
- IoT Cybersecurity Improvement Act 2017

- IT Security Act
- B3S Standards
- BNetzA Security Catalogue
- German Energy Act

- Network Information Security Directive

- Critical Infrastructure Protection
- Certification and Key Measures

- Cyber Essential Scheme
- Direct adaptation of European NIS Directive and GDPR (General Data Protection Regulation

Note: the stated organizations and standards are just examples and are not complete

Guiding Principles for Implementing Industrial Security (1)

SIEMENS
Ingenuity for life

- Security-by-Design shall follow a risk-based approach
- Product and solution security has to consider the intended use and operational environment
- Distinction of roles and responsibilities is recommended according to the stakeholders involved
- Process-related certifications are better suited to address cybersecurity than product- or solution-related certifications

Guiding Principles for Implementing Industrial Security (2)

SIEMENS
Ingenuity for life

- Any regulation should refer to international standards and specifications
- Regulation supported by standards should be preferred over tight (national) frameworks or issuing of quality/security labels
- Security regulations should be independent from other regulations like safety regulations or privacy regulations
- Manufacturer's self-declaration in accordance to international standards is the preferred means to demonstrate conformity with security requirements

What should a potential future European Security Certification Framework consider?

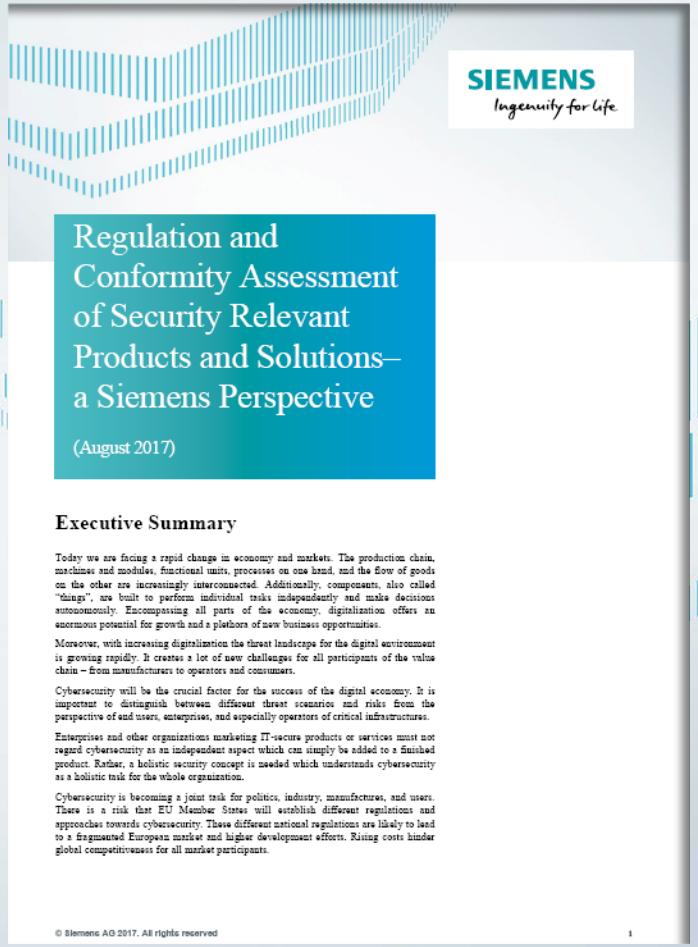
Application of Guiding Principles
Envisioned main characteristic of a European certification framework

SIEMENS
Ingenuity for life

- Targeting global acceptance of the intended European certification framework
- Based on internationally acknowledged industry standards
- Reference to technical requirements, i.e., no specific solution or component should be preferred.
- Preference for clearly formulated conformity assessment framework at European level, inspired by the conformity assessment modules contained in decision 768/2008/EG
- Allow manufacturer’s self-declarations
- Dependence of security measures on the target operational environment
- Independence of security certifications or regulations from those in the areas of safety or privacy.

Contact

SIEMENS
Ingenuity for life



SIEMENS
Ingenuity for life

Regulation and Conformity Assessment of Security Relevant Products and Solutions– a Siemens Perspective

(August 2017)

Executive Summary

Today we are facing a rapid change in economy and markets. The production chain, machines and modules, functional units, processes on one hand, and the flow of goods on the other are increasingly interconnected. Additionally, components, also called "things", are built to perform individual tasks independently and make decisions autonomously. Encompassing all parts of the economy, digitalization offers an enormous potential for growth and a plethora of new business opportunities.

Moreover, with increasing digitalization the threat landscape for the digital environment is growing rapidly. It creates a lot of new challenges for all participants of the value chain – from manufacturers to operators and consumers.

Cybersecurity will be the crucial factor for the success of the digital economy. It is important to distinguish between different threat scenarios and risks from the perspective of end users, enterprises, and especially operators of critical infrastructures.

Enterprises and other organizations marketing IT-secure products or services must not regard cybersecurity as an independent aspect which can simply be added to a finished product. Rather, a holistic security concept is needed which understands cybersecurity as a holistic task for the whole organization.

Cybersecurity is becoming a joint task for politics, industry, manufacturers, and users. There is a risk that EU Member States will establish different regulations and approaches towards cybersecurity. These different national regulations are likely to lead to a fragmented European market and higher development efforts. Rising costs hinder global competitiveness for all market participants.

© Siemens AG 2017. All rights reserved 1

Dr. Ralf Rammig
Standards and Innovation
Siemens AG
Corporate Technology

E-mail:
ralf.rammig@siemens.com

Internet
siemens.com/corporate-technology