Cyber Security in Zeiten von Cyber Crime

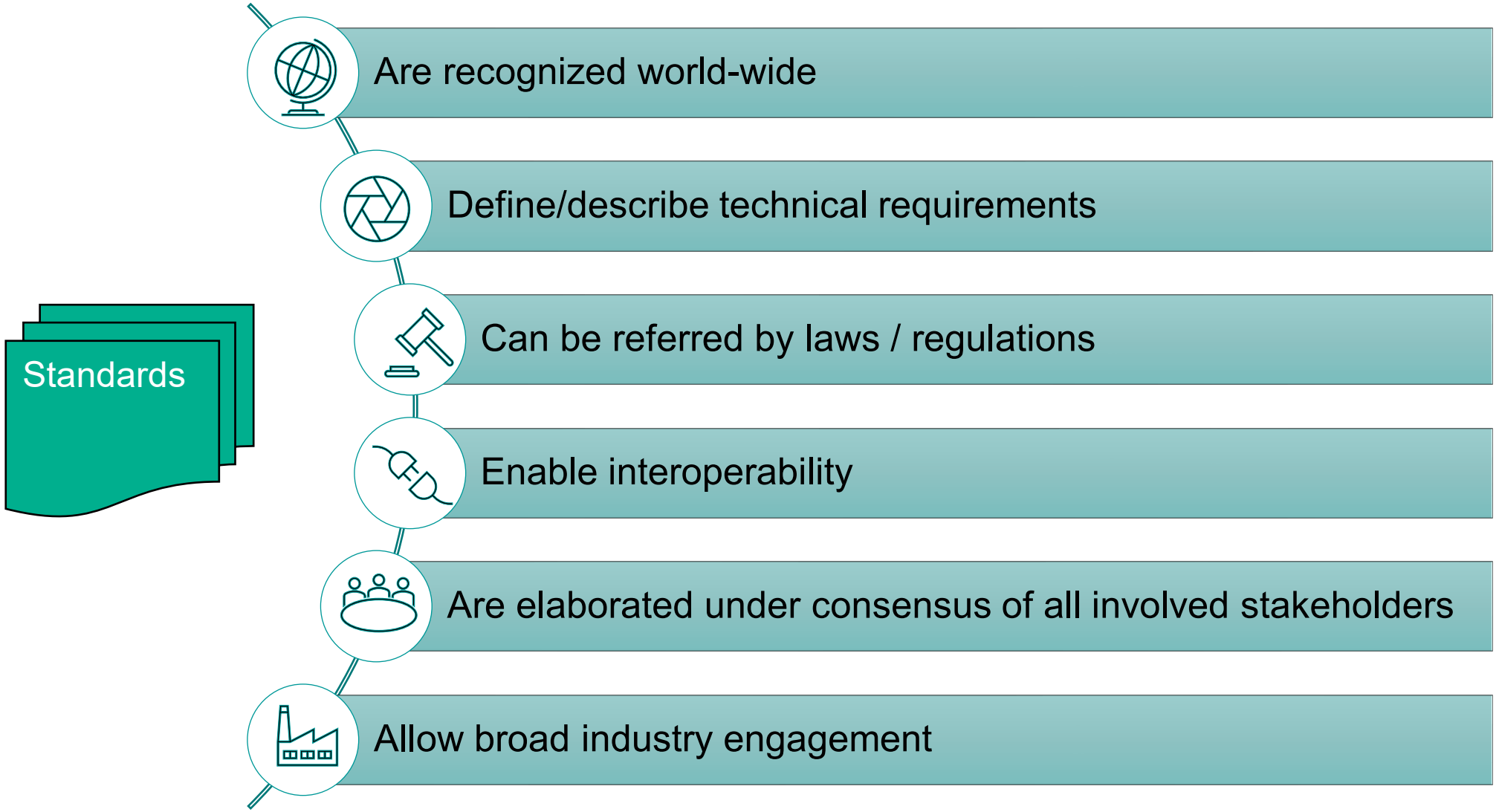
International Standards and Regulation

Dr. Ralf Rammig
Siemens AG

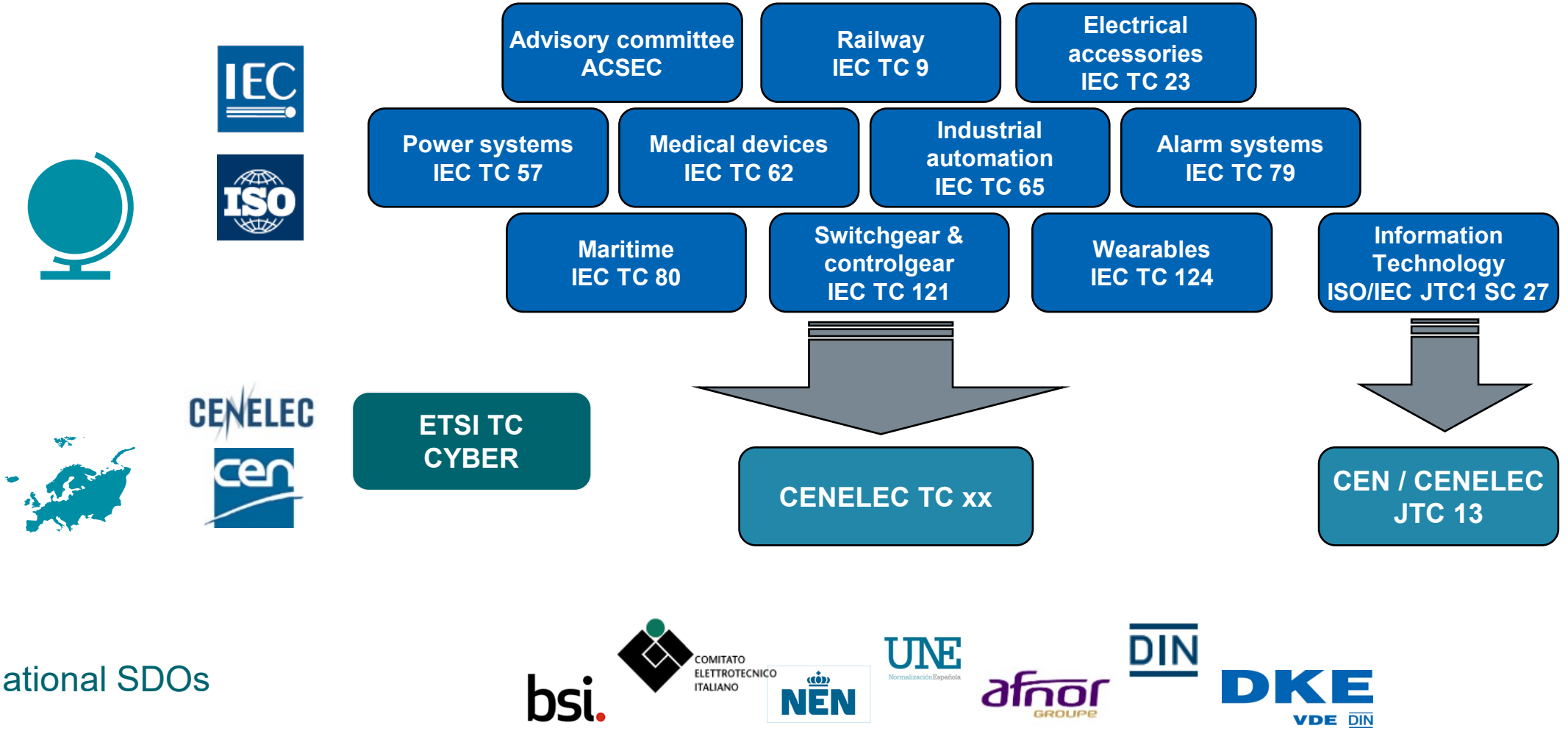
SIEMENS

Standardization

International Standards



Security Standardization Landscape
International – European – National



National SDOs

bsi. COMITATO ELETTROTECNICO ITALIANO NEN UNE Normalización Española afnor GROUPE DIN DKE VDE DIN

Germany
Cybersecurity Activities in DKE (September 2021)

Neues Projekt
< 1 Jahr

Additional Services & Projects

VDE CERT

§§§

LamA connect

- AK 225.0.9 Security aspects related to functional safety
- K 431 Niederspannungsschalt-geräte und -kombinationen
- AK 931.0.14 Smart manufacturing und Industrie 4.0
- UK 931.1 IT-Sicherheit in der Automatisierungstechnik
- UK 967.1 Elektro- und Leittechnik für kerntechnische Anlagen

- AK 901.0.115 Informationssicherheit für Elektromobilität
- AK 901.0.5 Energy Blockchain
- AK 952.0.15 IT-Sicherheit in der Netz- und Stationsleittechnik

- AK 351.0.6 IT-Sicherheit im Bahnsystem
- AK 351.1.1 Software, IT-Security
- AK 351.2.10 IT-Sicherheit in der Bahnenergieversorgung
- AK 351.3.7A Maintenance bestehende Vornormen
- AK 351.3.7B Aktuelle Themen der Rail-IT-Security in der Normung
- AK 353.0.8 Nutzerautorisierung für Ladeinfrastruktur
- GAK 353.0.11 Backend Kommunikation für Ladeinfrastruktur
- AK 353.0.12 Standardschnittstelle für Ladepunkte/Ladestationen zur Anbindung an lokales Leistungs- und Energiemanagement
- AK 355.0.5 Schutzmaßnahmen gegen nicht autorisierte Zugriffe
- AK 738.0.4 Cyber Security/ Schnittstellen

- AK 801.0.10 Adhoc Grundlagen Zertifizierung AAL-Lösungen
- AK 810.0.4 Ad-hoc-Gruppe produktbezogene Security
- AK 811.3.3 Informationssicherheit in der Medizintechnik

- AK 511.0.4 Funktionale Sicherheitsaspekte elektronischer Stromkreise und Fernwirken...
- K 713 Gefahrenmelde- und Überwachungsanlagen
- AK 713.0.22 Vernetzung
- AK 713.0.24 Remote Services
- AK 716.0.1 Normative Beschreibung eines Sicherheits-konzeptes für Energie-management im Gebäude

Austausch durch TBINK
AK IT-Sicherheit

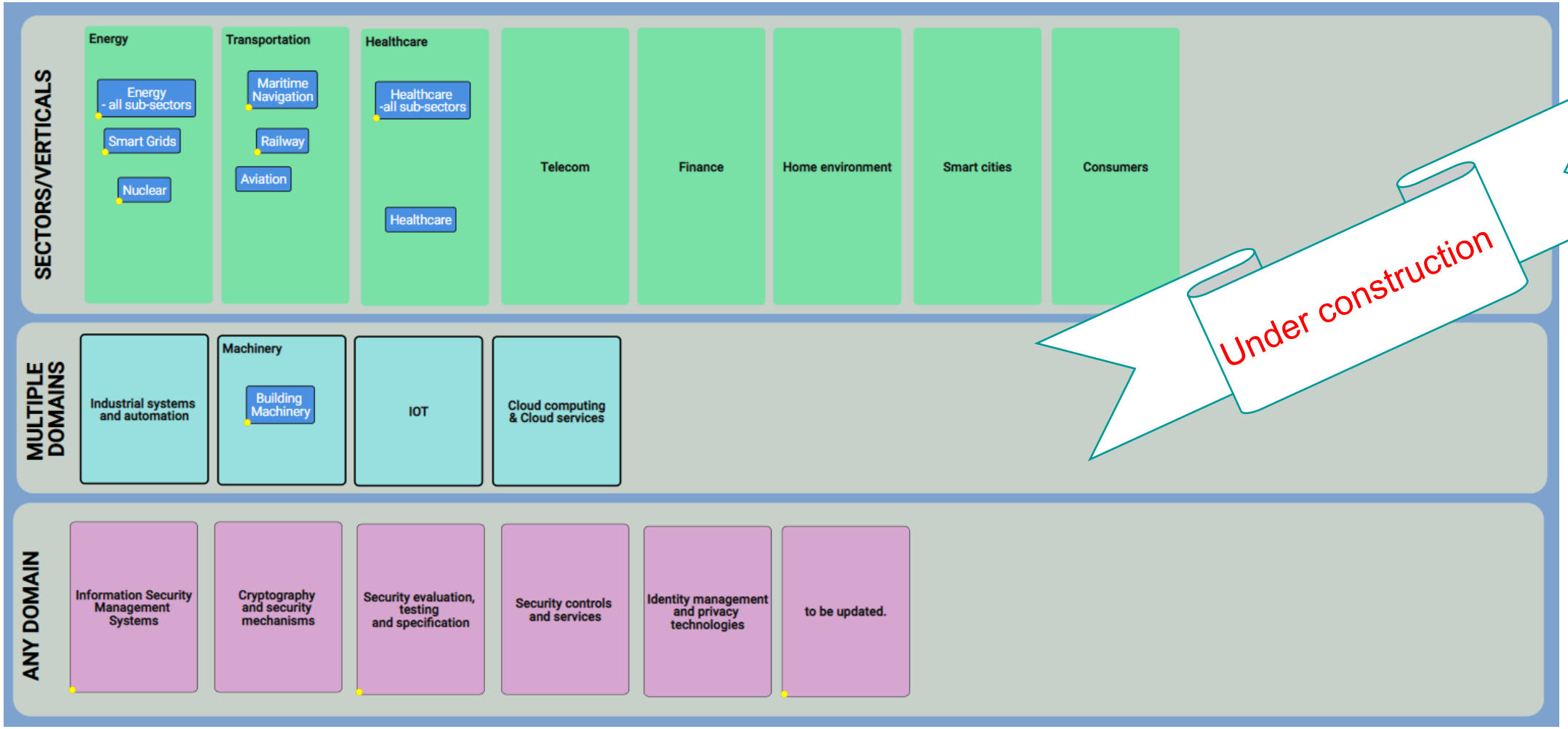
Technischer Beirat der DKE

- TB KON Cybersecurity
- TB INK AK Smart Home Cybersecurity
- TB INK AK IT-Sicherheit
- DIN/DKE Gemeinschaftsgremium Cybersecurity

DIN

- Koordinierungs-stelle IT-Sicherheit

IEC Mapping Tool
Standards Overview



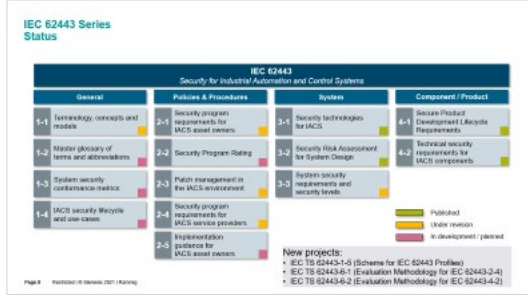
https://mapping.iec.ch/#/maps/10

SIEMENS

Security Standards Selection

1 General/horizontal standards

- IEC 62443 series — Security for Industrial Automation and Control Systems
- ISO/IEC 270xx series — Information Security Management Systems
- ISO/IEC 15408 and 18045 — Common Criteria



2 Sector-specific security standards

- IEC 62351 series — Power systems management and associated information exchange
- IEC 62645 — Nuclear power plants
- IEC 63208 — Low-voltage switchgear and control gear
- ISO/IEC 27019 — Information security controls for the energy utility industry
- EN 50159 (IEC 62280) — Safety communications in railway systems
- CLC/TS 50701 — Railway applications - Cybersecurity

SIEMENS

IEC 62443 Series Status

IEC 62443
Security for Industrial Automation and Control Systems

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Security technologies for IACS	4-1	Secure Product Development Lifecycle Requirements
1-2	Master glossary of terms and abbreviations	2-2	Security Program Rating	3-2	Security Risk Assessment for System Design	4-2	Technical security requirements for IACS components
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	System security requirements and security levels		
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers				
		2-5	Implementation guidance for IACS asset owners				

Published
Under revision
In development / planned

New projects:
- IEC TS 62443-1-5 (Scheme for IEC 62443 Profiles)
- IEC TS 62443-6-1 (Evaluation Methodology for IEC 62443-2-4)
- IEC TS 62443-6-2 (Evaluation Methodology for IEC 62443-4-2)

Hot Topics in Standardization

Standards as a basis for regulations

- Standards conformity fulfills essential requirements
- EU: RED Delegated Act
- New horizontal security directive in planning in EU

Security for Artificial Intelligence and IoT

- Billions of IoT devices connected
- AI poses new security threats
- Current risk approaches and security measures need to be adapted

Horizontal standards

- Harmonized requirements across domains
- IEC 62443 already applied by many sectors
- Horizontal function assigned to IEC TC 65

Supply chain security

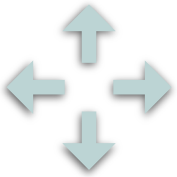
- Security needs to be ensured across multiple supplier-customer relations
- World-wide, complex supply chain poses new security challenges
- Trustworthiness is at the core

SIEMENS

Security Standardization Recommendations

Focus on international standards primarily

Regular monitoring and evaluation of standardization landscape



Adjust active participation due to priority of technical body

SIEMENS

Security Regulation

Examples

Security Regulation Landscape
Examples

European Union

- Directive (EU) 2016/1148 on Security of Network and Information Systems (“NIS Directive”)
- General Data Protection Regulation (GDPR) (REGULATION (EU) 2016/679)
- EU Cybersecurity Act (EU 2019/881) (CSA)


7.6.2019 EN Official Journal of the European Union L 151/15

REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 April 2019
on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

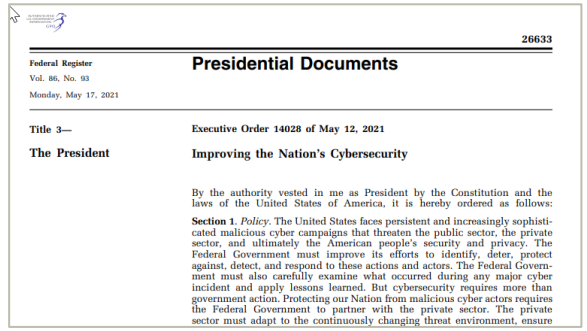
Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

USA

- Cybersecurity Improvement Act of 2017
- Executive Order 14028 (2021-05-12) on Improving the Nation’s Cybersecurity


26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

Title 3—
The President

Executive Order 14028 of May 12, 2021

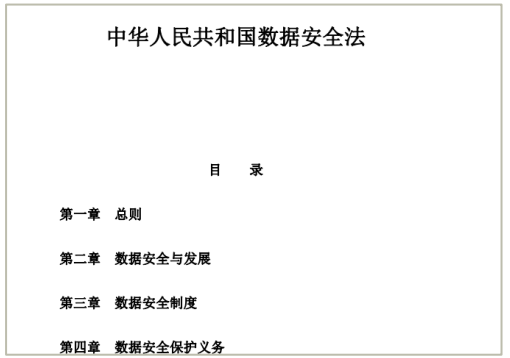
Improving the Nation’s Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy.* The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more than government action. Protecting our Nation from malicious cyber actors requires the Federal Government to partner with the private sector. The private sector must adapt to the continuously changing threat environment, ensure

China

- China Cybersecurity Law
- Data Security Law
- Personal Information Protection Law
- Regulation on Security Protection of Critical Information Infrastructure (CII)


中华人民共和国数据安全法

目　录

第一章　总则

第二章　数据安全与发展

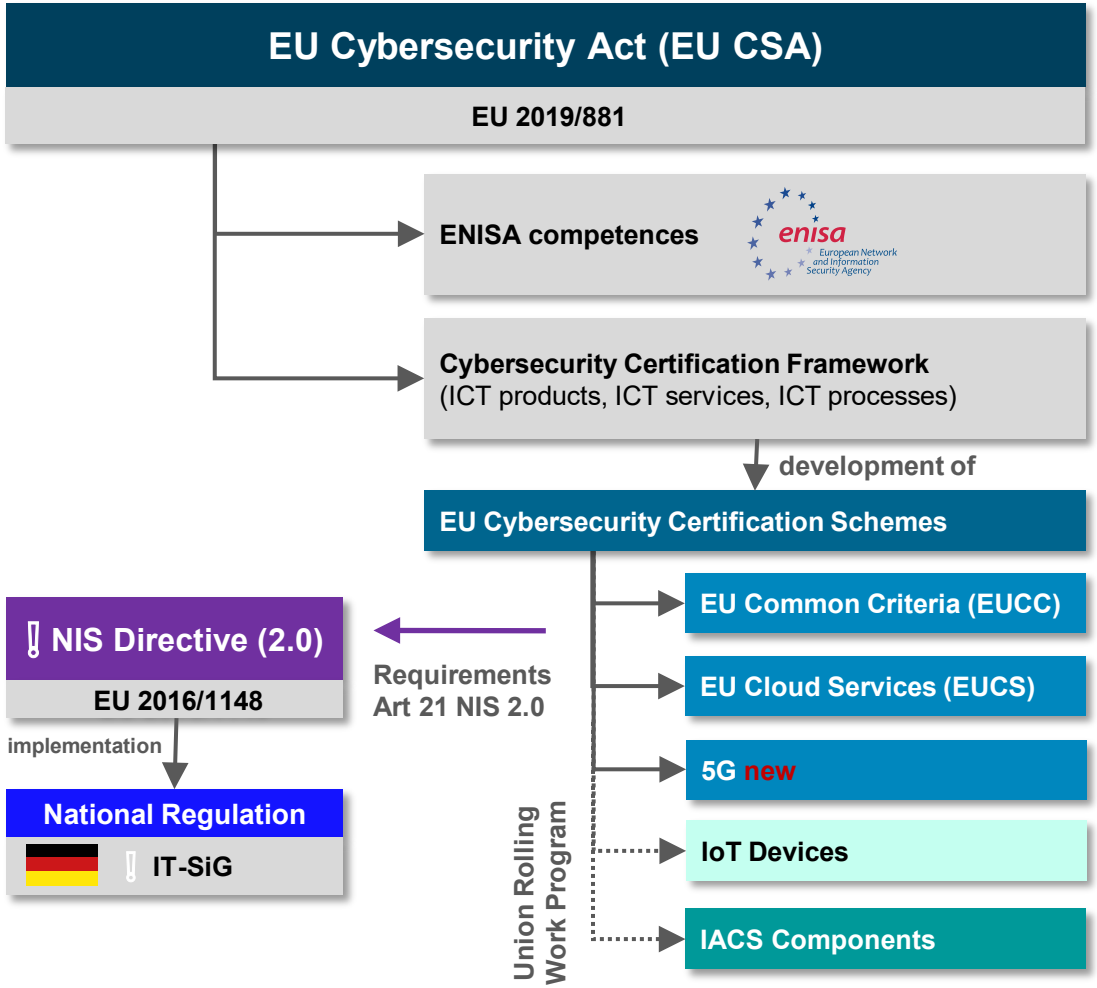
第三章　数据安全制度

第四章　数据安全保护义务

SIEMENS

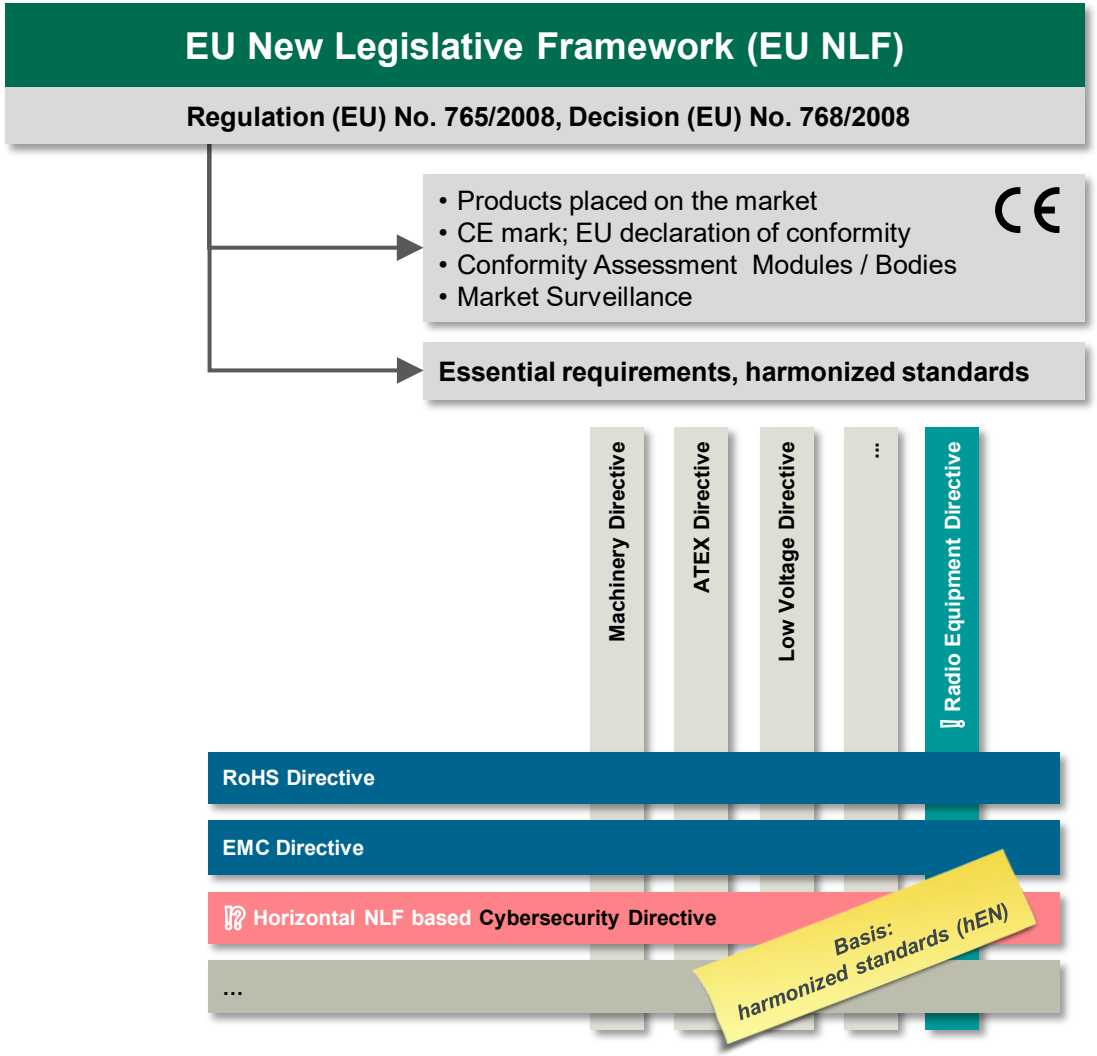
Existing EU Regulation
NIS Directive – Cybersecurity Act

- **Directive (EU) 2016/1148 on Security of Network and Information Systems ("NIS Directive")**
  - Aims to create an overall higher level of cybersecurity in the EU by handling cybersecurity breaches in a way that minimizes impact and share cyber security information EU wide
  - affects digital service providers (DSPs) and operators of essential services (OESs)
  - DSPs and OES must report major security incidents to Computer Security Incident Response Teams (CSIRT)
  - EU member states must create a NIS Directive strategy, which includes the CSIRTs, National Competent Authorities (NCAs) and Single Points of Contact (SPOCs).
- **EU Cybersecurity Act (CSA)**
  - complements the NIS Directive
  - defines the responsibilities and competences of ENISA (European Union Agency for Cybersecurity)
  - establishes an EU-wide cybersecurity certification framework for digital products, services and processes
  - ENISA develops EU cybersecurity certification schemes



SIEMENS

Proposed Horizontal EU Cybersecurity Regulation
Based on the principles of the New Legislative Framework (NLF)



„CE-Directive“ – EU harmonization of cybersecurity requirements

- Obligations of economic operators:
  when making products available on the market:
  risk assessment, design and manufacturing of compliant products, conformity assessment, …
- Formal requirements:
  CE-marking, EU-Declaration of Conformity, product marking etc.
- Essential product requirements:
  - Legally mandatory high level requirements for products and solutions
- **Harmonized standards – reflect the state of the art**
  - Essential Requirements are technically specified in (harmonized) standards and reflect the state of the art
  - developed and updated by technical experts involving all stakeholders
- Conformity assessment modules - coverage of different risk levels:
  - risk based conformity assessment modules
  - Use cases with high risk: involvement of third parties (NB)
- Market Surveillance
  - level playing field through market surveillance programs

SIEMENS

EU Cybersecurity Act (CSA)

REGULATION (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

Objective and goal:

- Part of a comprehensive package of measures to increase cybersecurity and to strengthen resilience against cyber attacks by the European Union
- complements the NIS Directive by creation of an EU framework for the IT security certification of products, services and processes

Measures:

- defines the responsibilities and competences of ENISA (European Union Agency for Cybersecurity)
- establishes an EU-wide cybersecurity certification framework for digital products, services and processes
- ENISA develops EU cybersecurity certification schemes

Status of proposed EU Cybersecurity Certification Schemes
ENISA Ad-hoc Working Groups

- **Ad-hoc WG 01: Transposition of SOGIS-MRA certification framework**
  - Common Criteria based European candidate cybersecurity certification scheme (EUCC)
  - published for comment in July 2020
- **Ad-hoc WG 02: Cloud Services Security**
  - published for comment in December 2020
- **Ad-hoc WG 03: 5G Security**
  - in planning, currently no official ENISA call

Potential further groups in planning:

- Industrial Automation Control Systems Components
- (Consumer) IoT, …

Contact

Dr. Ralf Rammig
Siemens AG
T TIM RSQ SIP
Otto-Hahn-Ring 6
81739 München, Germany

E-mail:
ralf.rammig@siemens.com

SIEMENS