Energy | 2016

Cyber Security –

An industrial View on the Interplay of Standards, Regulations, and Guidelines on the Example of Digital Grid

Lisbon, June 30th, 2016

Siemens Corporate Technology

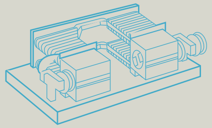
Outline

Our milestones –
Across 170 years of history

SIEMENS

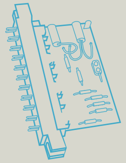
1816-1892

Company founder, visionary and inventor



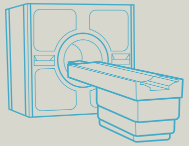
1866

Dynamo



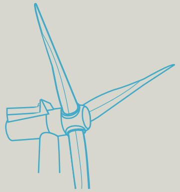
1959

SIMATIC controller



1983

Magnetic resonance tomograph



2012

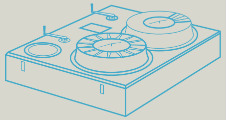
Field testing of world's largest rotor at an offshore wind farm

Werner von Siemens

Siemens innovations over 168 years

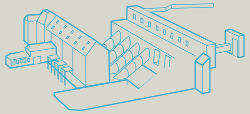
1847

Pointer telegraph



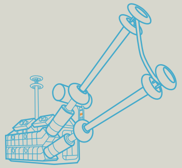
1925

Electrification of Ireland with hydropower



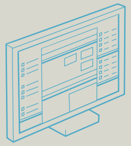
1975

High-voltage direct-current (HVDC) transmission



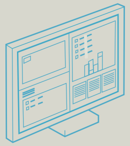
2010

TIA Portal for automation



2015

Sinalytics



Our innovative power in figures – Siemens as a whole and Corporate Technology

SIEMENS

Expenditures for research and development

€4.5 billion
Expenditures for R&D in fiscal 2015

32,100
R&D employees[1]

Inventions and patents – securing our future

7,650
inventions[1]

3,700
patent applications

University cooperations – our knowledge edge

9
CKI universities[2]

16
principal partner universities

1 In fiscal 2015
2 Centers of Knowledge Interchange

Corporate Technology – our competence center for innovation and business excellence[3]

7,800
employees worldwide

5,300
software developers

1,600
researchers

400
patent experts

3 Employee figures: Status September 30, 2015

Our organization – Corporate Technology at a glance

SIEMENS

Corporate Technology (CT)

CTO – Prof. Dr. Siegfried Russwurm

Business Excellence, Quality Management, *top*⁺

- Business excellence
- Quality management
- Internal process and production consulting

Corporate Intellectual Property

- Protection, use and defense of intellectual property
- Patent and brand protection law

Development and Digital Platforms

- Competence center for horizontal and vertical product-and-system integration as well as software, firmware, and hardware engineering

Innovative Ventures

- Access to external innovations
- Start-up foundation
- Commercialization of innovations

Research in Digitalization and Automation

- Research activities covering all relevant areas in digitalization and automation for Siemens

Research in Energy and Electronics

- Research activities relating to energy and electrification, electronic, new materials and innovative manufacturing methods

Technology and Innovation Management

- Siemens' technology and innovation agenda
- Standardization, positioning regarding research policy
- Provision of publications relating to R&D

University Relations

- Global access to the academic world
- Top positioning in terms of university cooperations

Increasing intelligence and open communication drive security requirements in various industrial environments

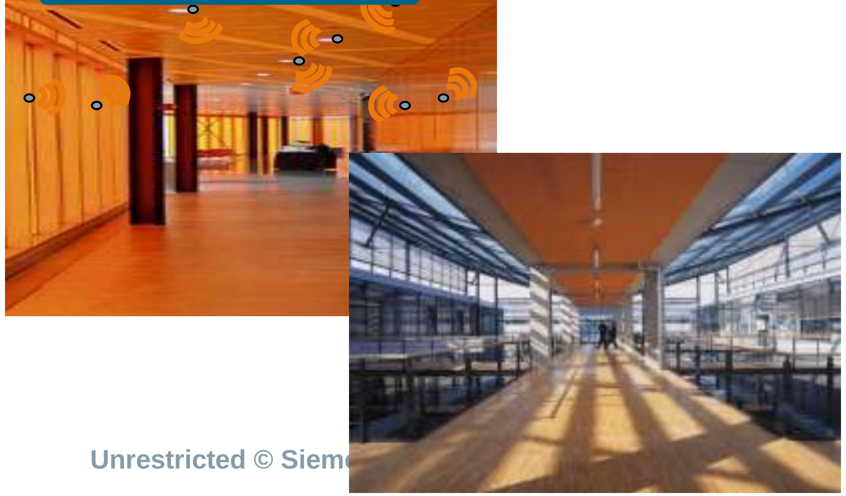
SIEMENS

Process Automation

Factory Automation

Urban Infrastructures

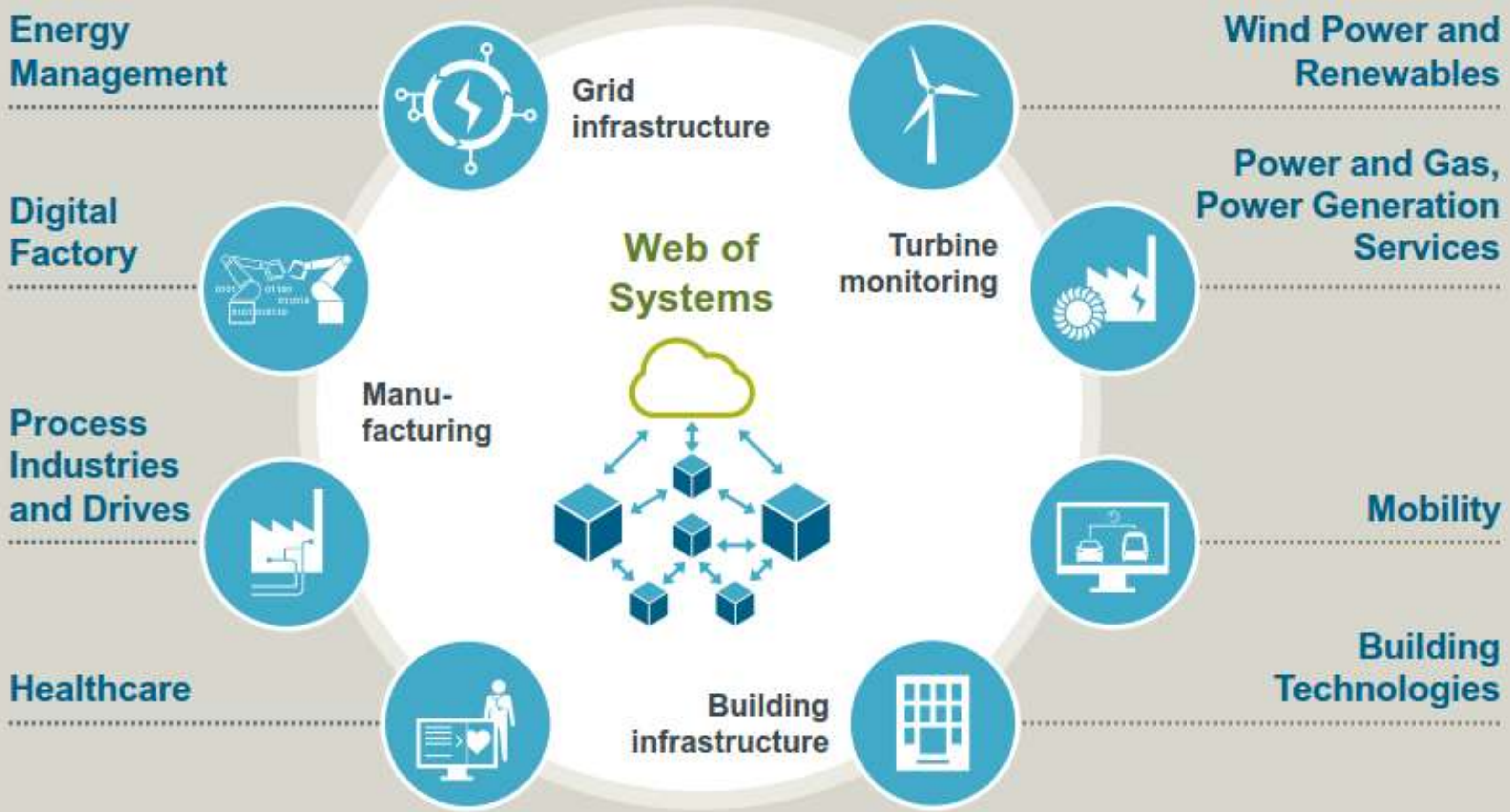
Building Automation



Energy Generation / Automation / Distribution

Mobility Systems

Concept for the industrial application of the Internet of Things – The Web of Systems provides security for critical infrastructures

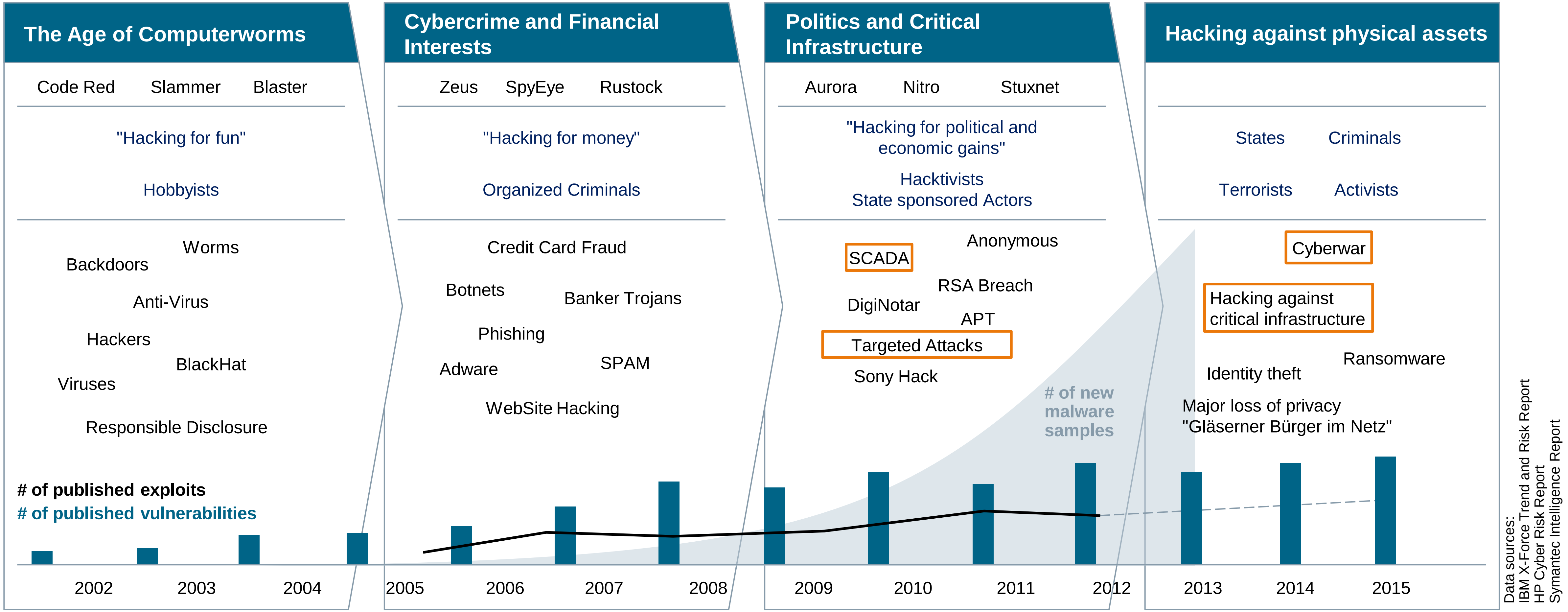


- Siemens believes the Internet of Things has tremendous potential
- In critical infrastructure, customers have much higher requirements regarding reliability, service life and data protection
- For this reason, in a Web of Systems the data is processed locally
- This ensures that the knowledge and the intellectual property of our customers remain protected
- Siemens is already using this technology in many projects today

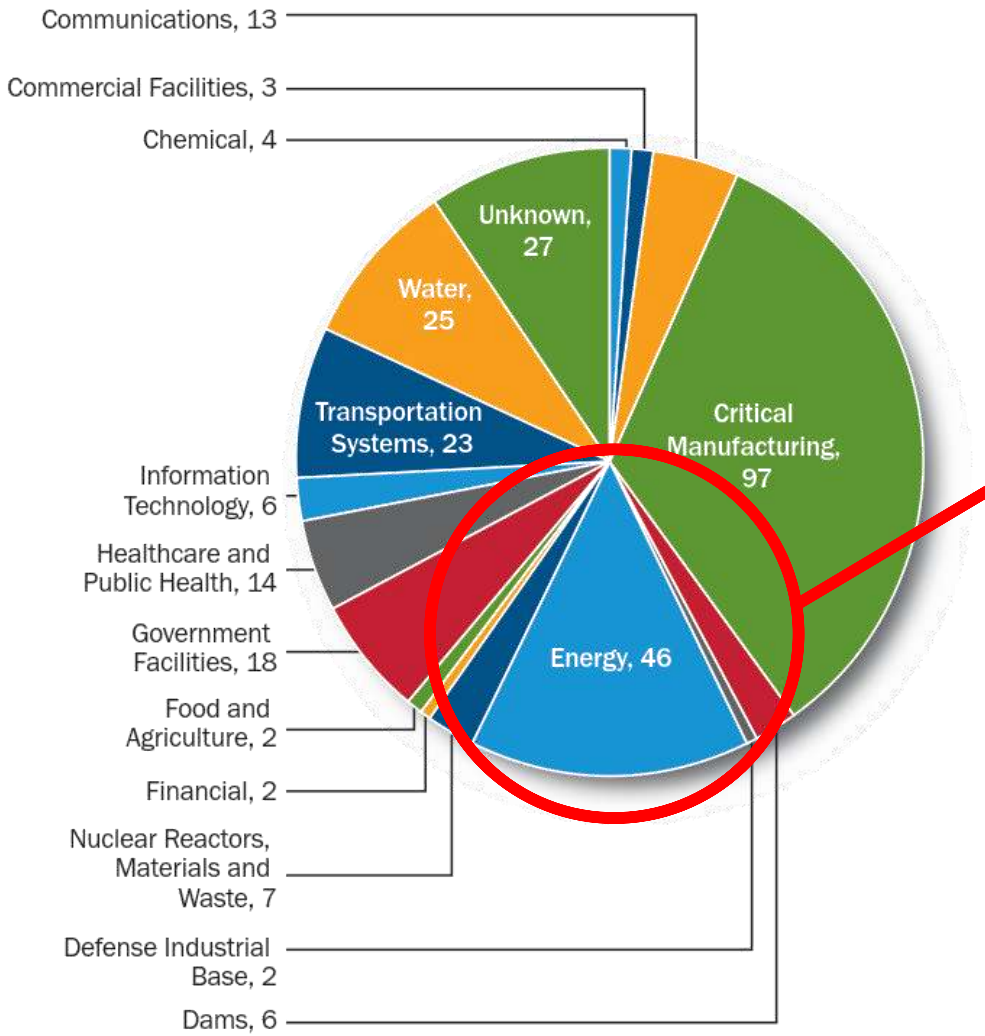
The threat level is rising – Attackers are targeting critical infrastructures

SIEMENS

Evolution of attacker motives, vulnerabilities and exploits



What makes security in the Digital Grid so important?



Source: ICS Report: Year in review 2015
Numbers represent responses out of 295 participants.

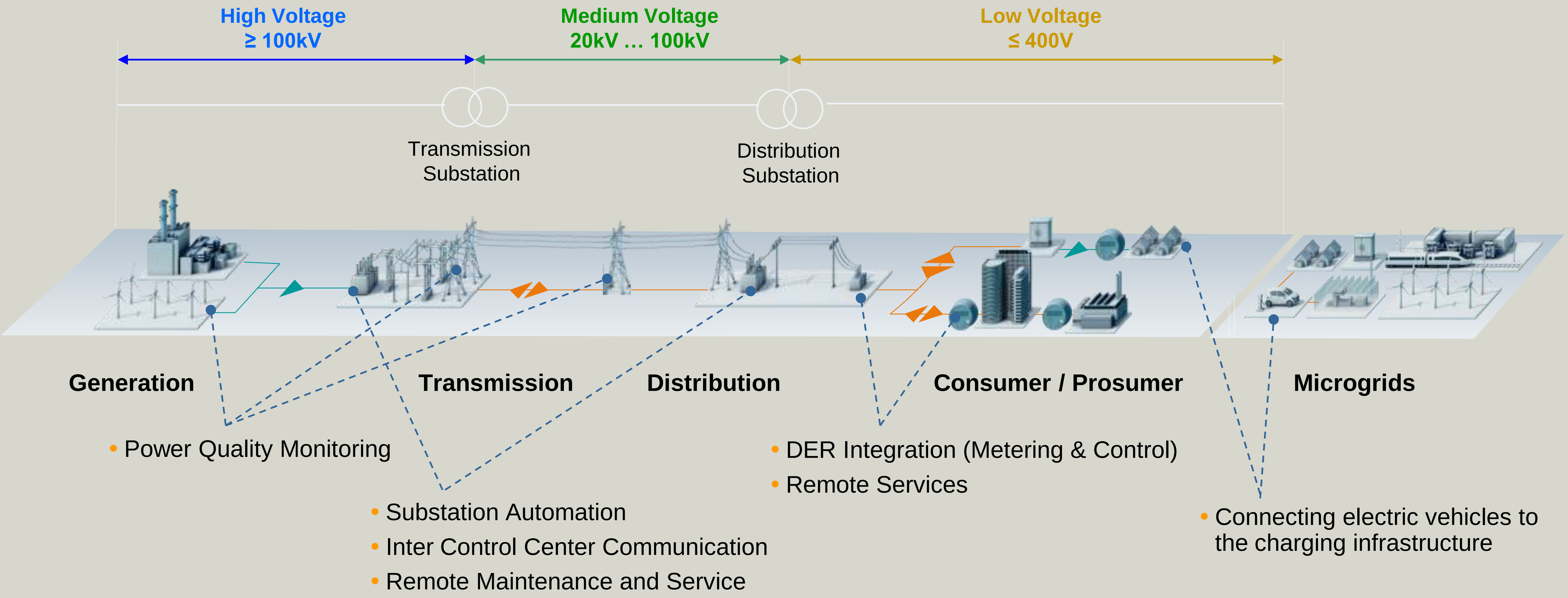
The Energy Sector is a Prime Target.

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

- Performance degradation
- Loss of system availability & control
- Loss of privacy
- Capturing, modification or loss of data
- Reputation (company image)
- Environmental impact
- Financial loss
- Loss of health/life

Cyber Security ensures reliable operation of critical infrastructures like the Digital Grid

Critical infrastructures
Power system value chain and use case examples



Digital Grid Masterplan Architecture

SIEMENS

Digitalization

Cloud enabled Applications

Enterprise IT

IVR | GIS | Network planning | Asset management | WMS/mobile | Weather | Forecasting | Web portals | CIS/CRM | Billing

Enterprise Service Bus

Grid control applications

CIM

Market driven applications

Global Interoperability: IEC 61850 & 60870, DNP3, OpenADR, DLMS, …

Automation

Electrification

Smart transmission

01100
011010
010110

Smart distribution

01100
011010
010110

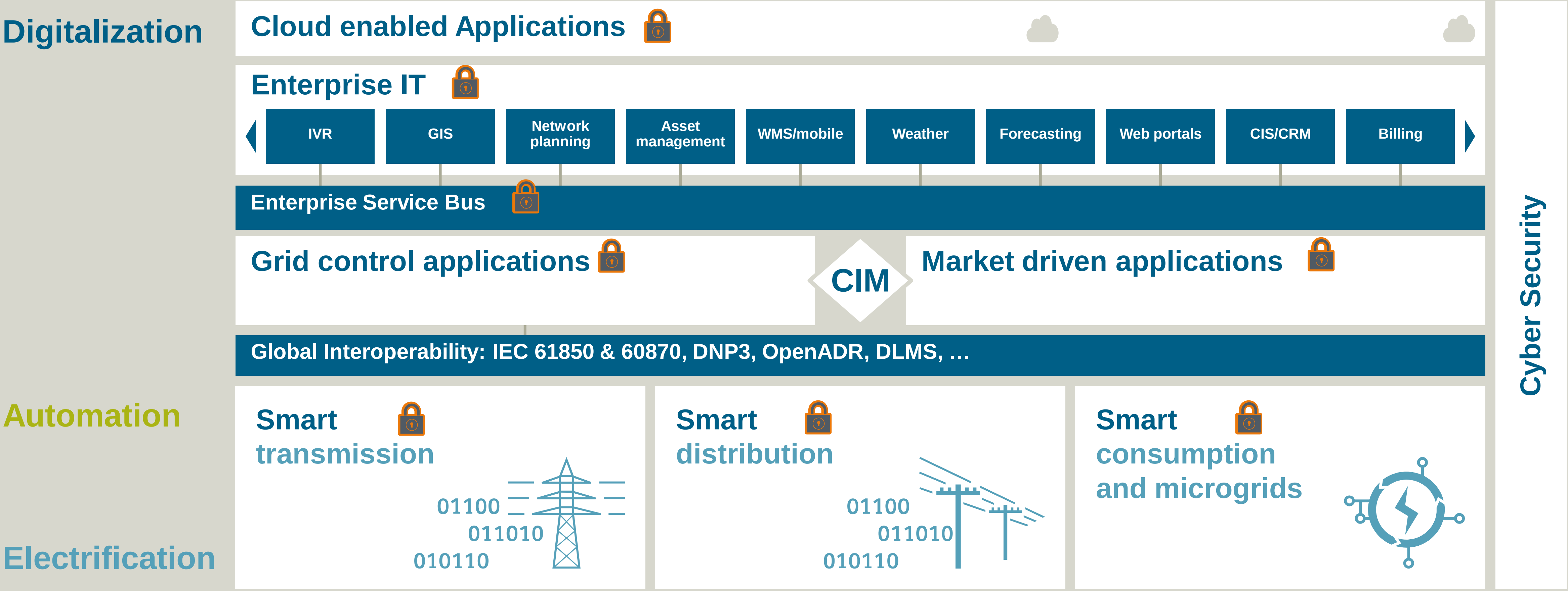
Smart consumption and microgrids

Cyber Security

CIM – Common Information Model (IEC 61970)

Cyber Security is a an integral part of Digital Grids to ensure reliable operation

SIEMENS



CIM – Common Information Model (IEC 61970)

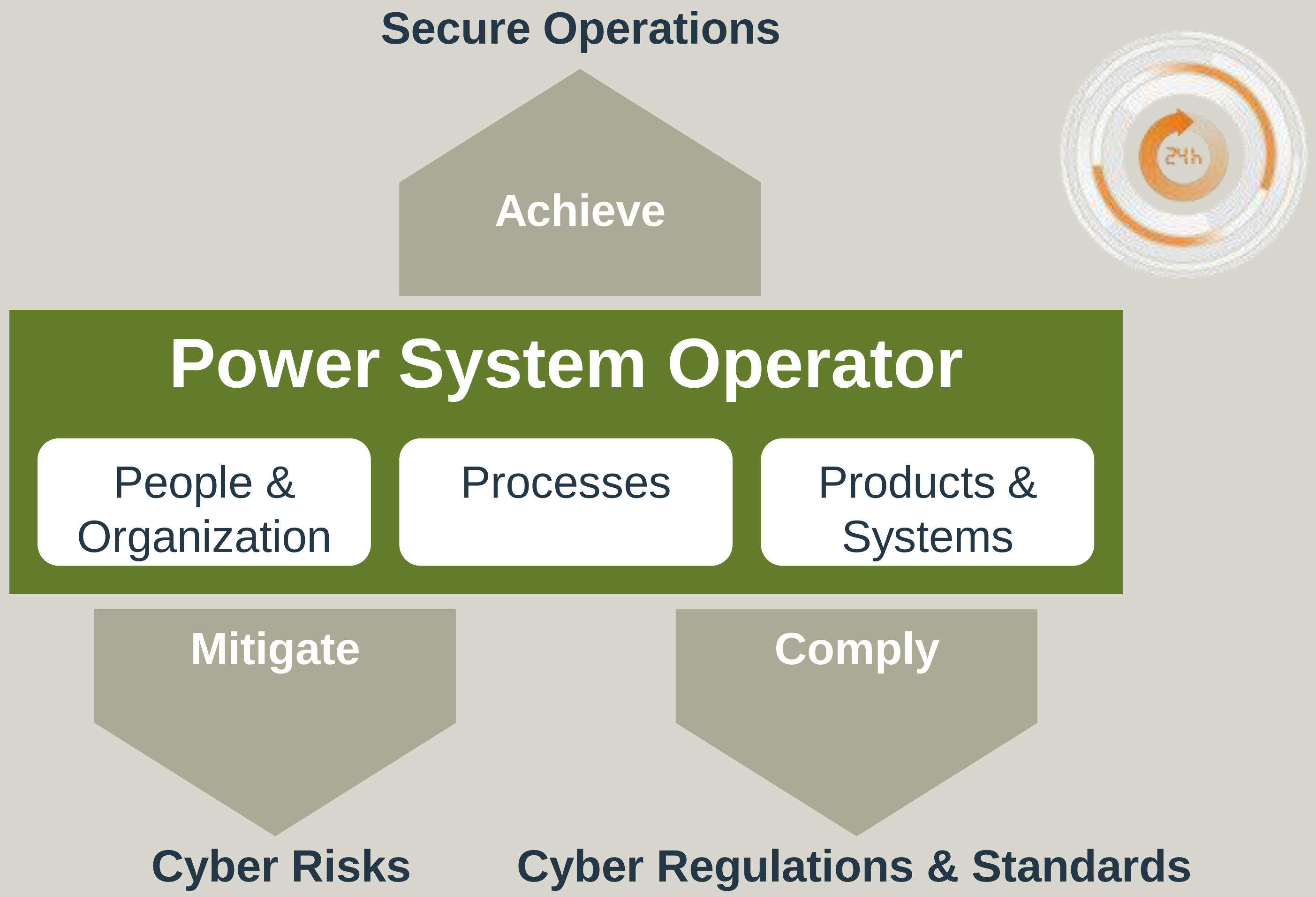
Appropriate security

Cyber security targets for a power system operator

SIEMENS

Security Targets

- Security of Supply
- Data Protection & Privacy (considering Availability, Integrity, Confidentiality)



Cyber security needs a holistic methodology

SIEMENS

Recover

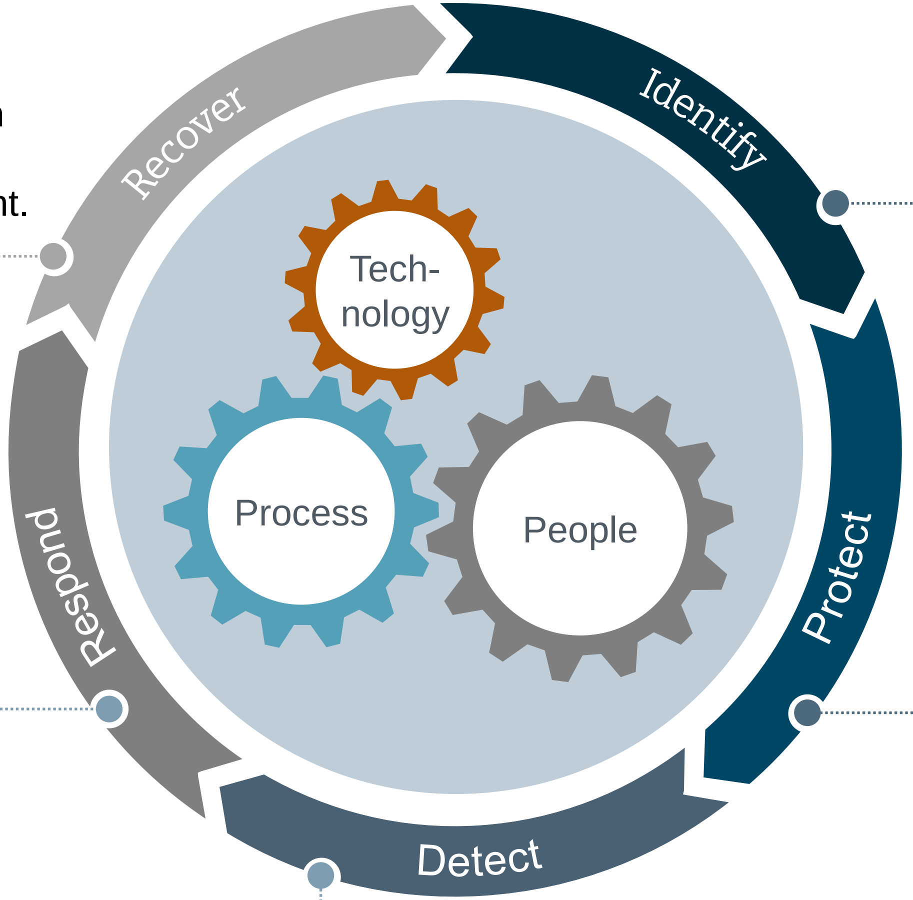
Creating plans for resilience and **restoration** of any capabilities or services that were impaired due to a cyber security related event.

Respond

Taking action against detected cyber security related events. Supports the ability to contain the impact of a potential event.

Detect

Rapid **identification** of the occurrence of a cyber security related event.



Identify

Understanding the business context, the resources that support critical functions and the related cyber security risks.

Protect

Protection of critical infrastructure service, e.g., energy supply by safeguarding the overall system.

NIST National Institute of Standards and Technology U.S. Department of Commerce

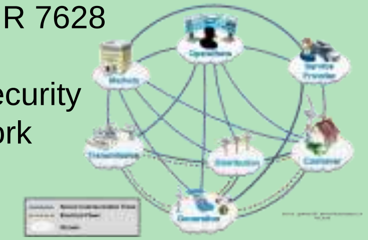
Based on NIST Cyber Security Framework

Managing cyber security in Digital Grids through
Guidelines / Standards / Regulation

SIEMENS

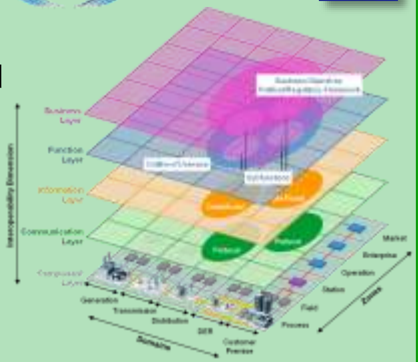
Smart Grid Interoperability Panel, Cyber Security WG
→ NIST IR 7628

Cyber Security Framework



SGAM – Smart Grid Architecture Model

→ SG-CG (M.490)
→ SEG-CG (successor)



BDEW White Paper Requirements for Secure Control and Telecommunication Systems

- IEC TC 57 – Power systems management and associated information exchange
  → IEC 62351-1 … -14
- IEC TC 65 – Industrial Process Measurement, Control and Automation
  → IEC 62443-1 … -4
- ISO/TC 022/SC 03 & IEC/TC 69 JWG 01 – Vehicle-to-Grid Interface
  → Security integral part of ISO/IEC 15118

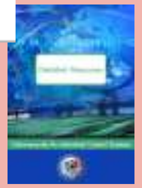
- ISO 27001 – Information technology - Security techniques - Requirements
- ISO 27002 – Code of Practice for information security management
- ISO 27019 – Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002

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

- Critical Infrastructure Protection CIP 001-014
- Executive Order EO 13636 Improving Critical

Bundesamt für Sicherheit in der Informationstechnik

- IT Security Law
- German Energy Act req. SM GW

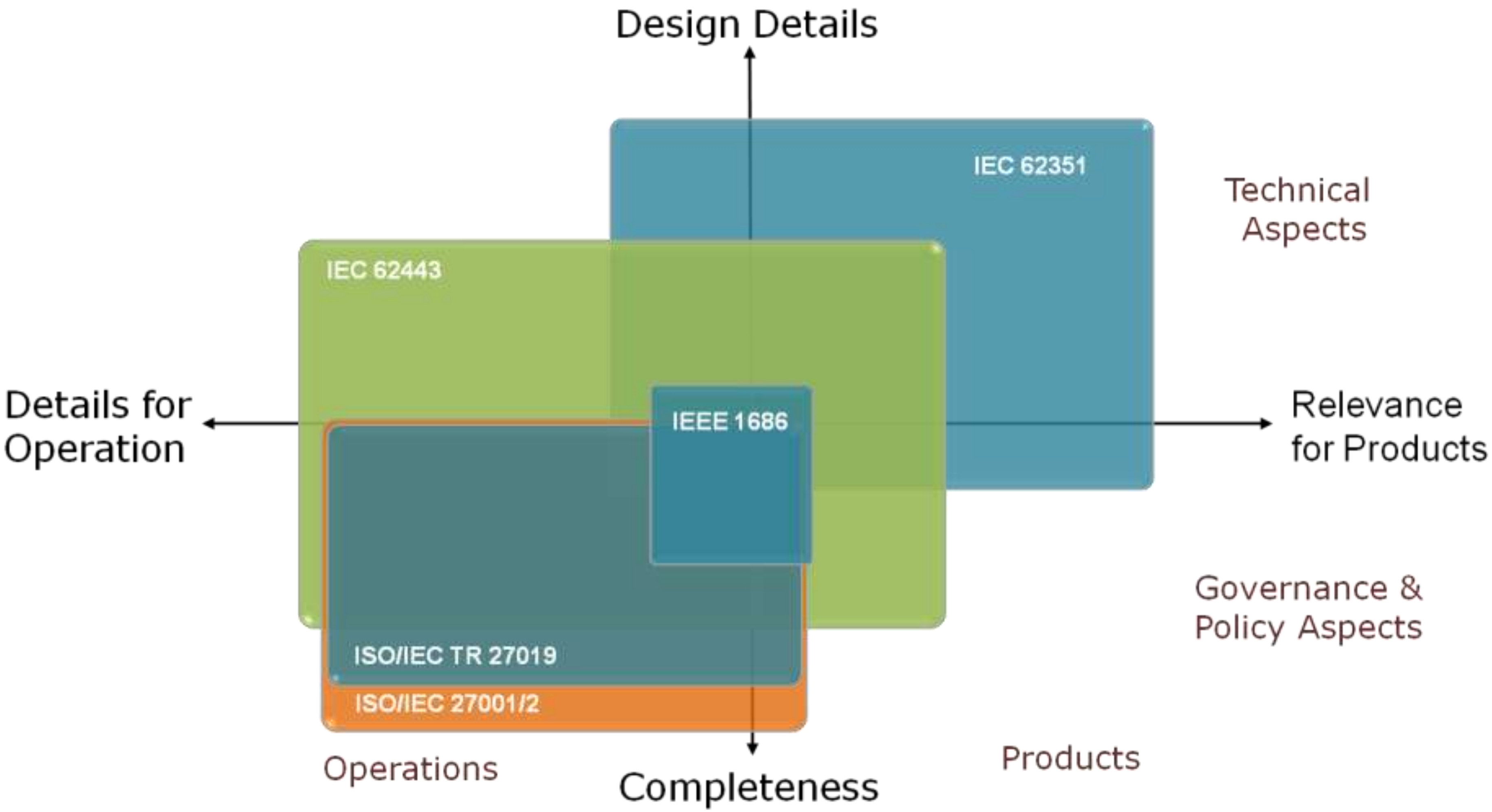


- Critical Infrastructure Protection, Certification and Key Measures

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

Interoperability through security standards for the power utility ecosystem involves vendors, integrators, operators

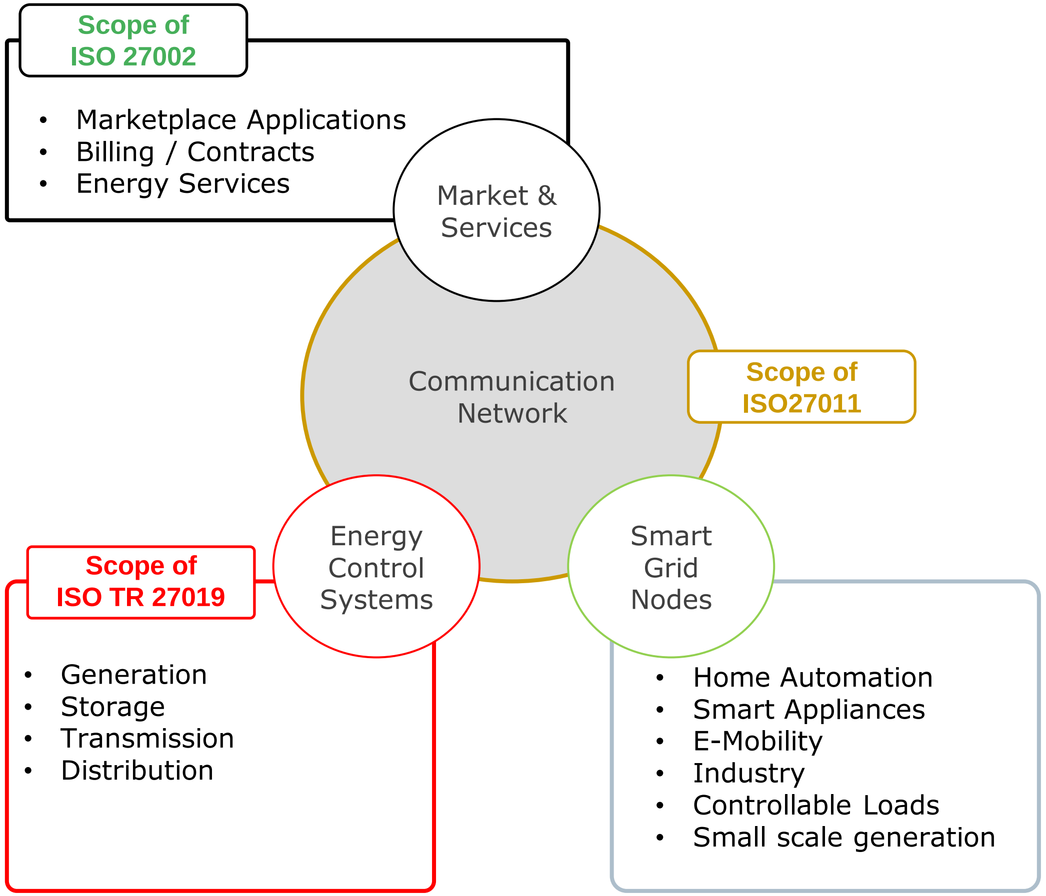
SIEMENS



- **Standards have different importance for**
  - Vendor
  - Integrator
  - Operator

  as they target
  - specific technical means ensuring interoperability
  - procedural requirements
  - addressing risk based security requirements
  - auditablity of actions

Information Security Management – Application of the ISO 270xx series targets Digital Grid specific security controls

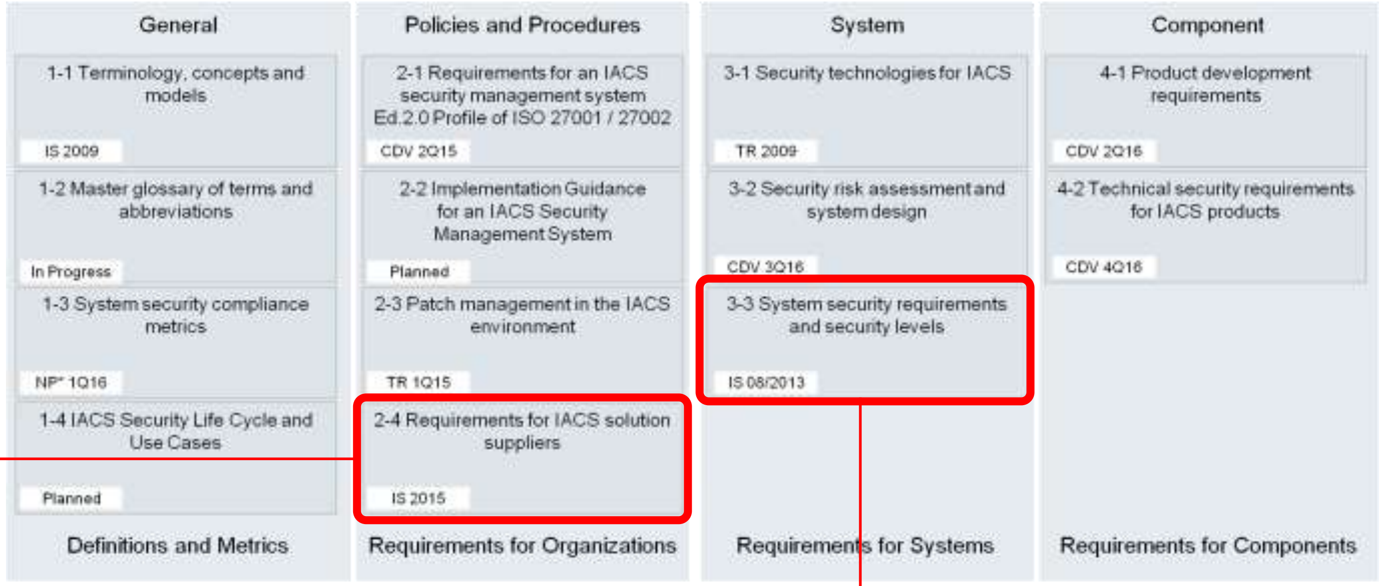


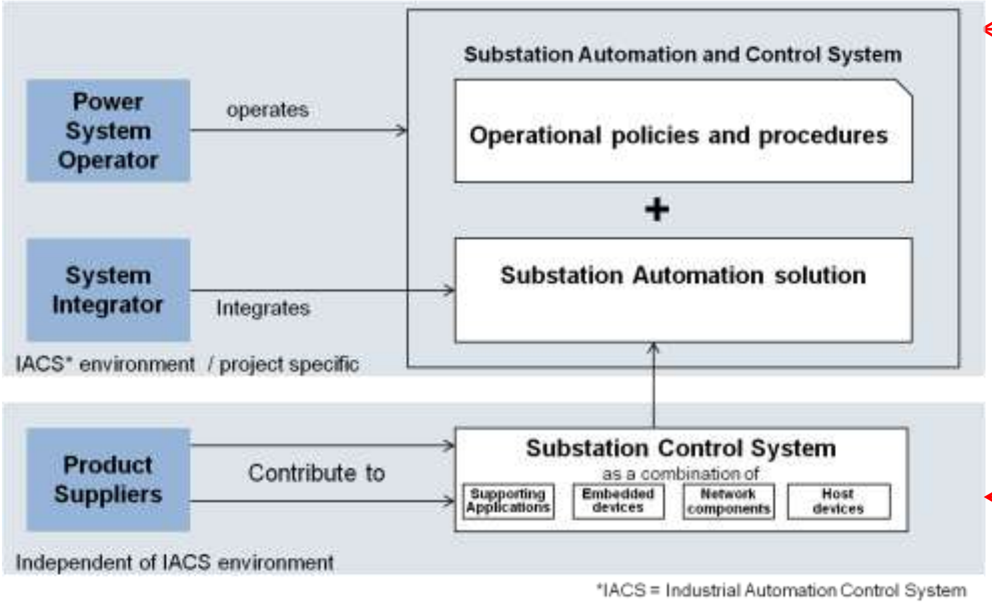
- **ISO 27001/2** provide security requirements and implementation guidance that target ISMS (Information Security Management Systems) at the most generic level
- Extended through domain / sector-specific specifications, e.g.
  - 27011: Telecommunication,
  - 27015: Finance sector,
  - 27017 / 27018: Cloud Computing,
  - 27019: Energy utilities
- **ISO TR 27019**
  - *Process control systems [..] for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes*

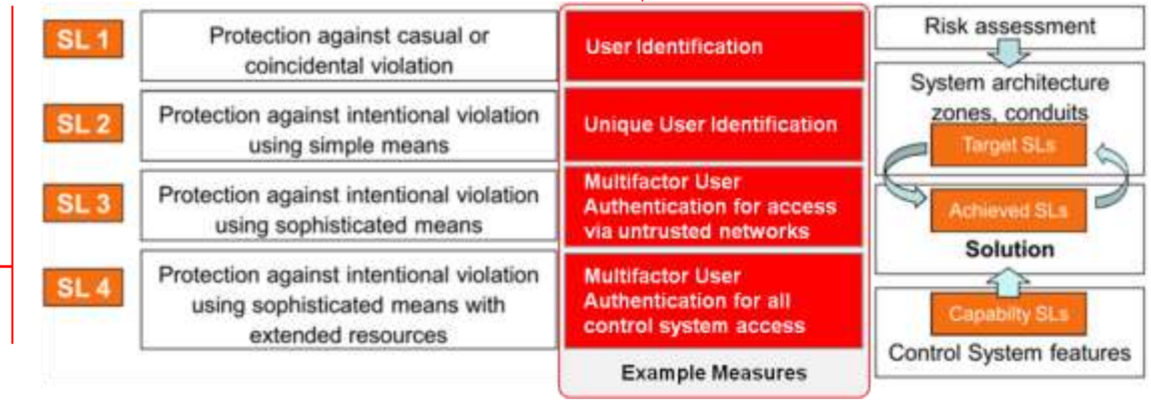
IEC / ISA-62443 as standard for industrial security enables a graded security approach to achieve appropriate protection

SIEMENS

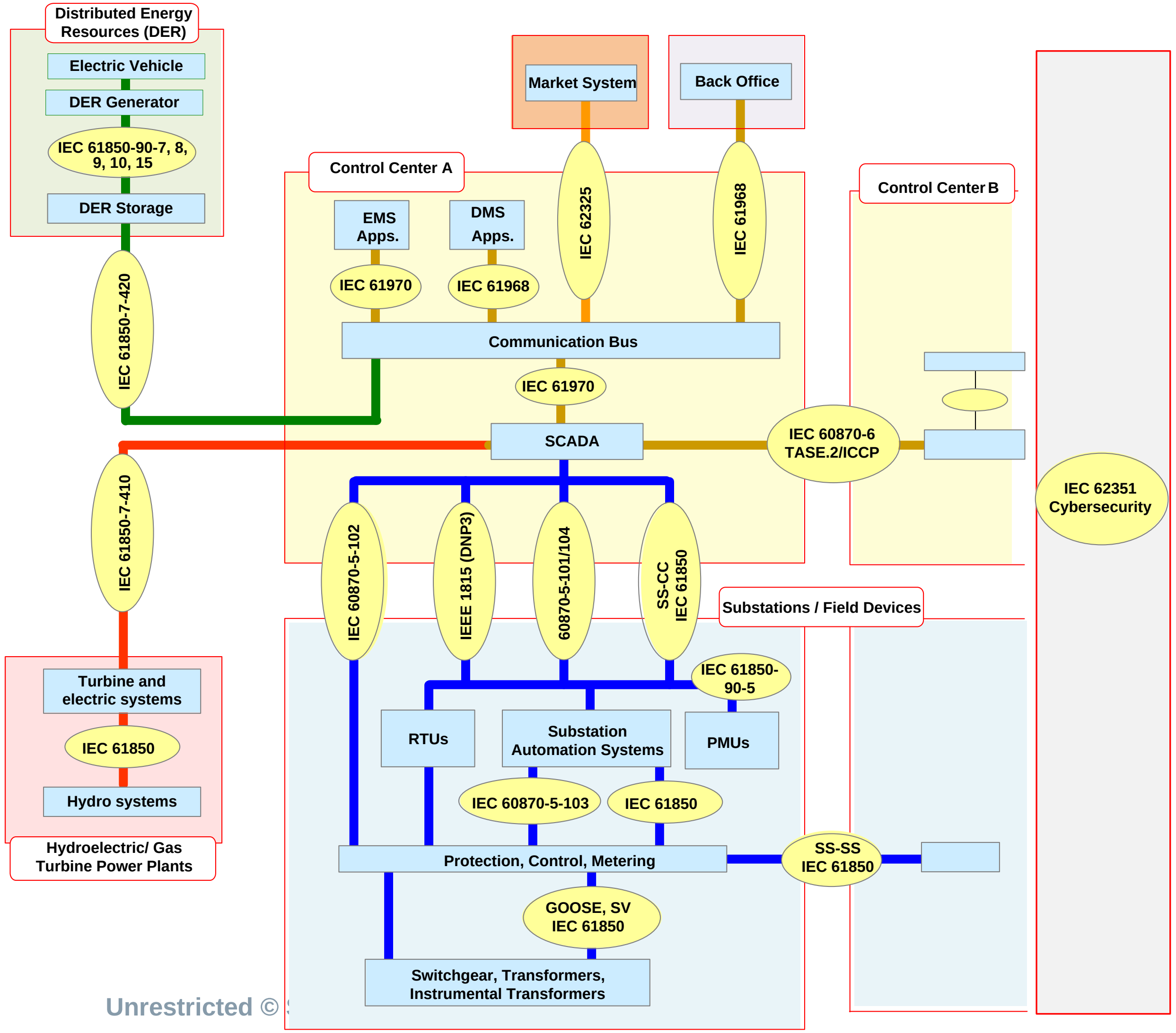
- IEC 62443 – Framework specifying security requirements for industrial automation control systems (IACS)
- Addresses organizational and technical requirements
- Supports purpose fit security solutions by supporting security features with different strength



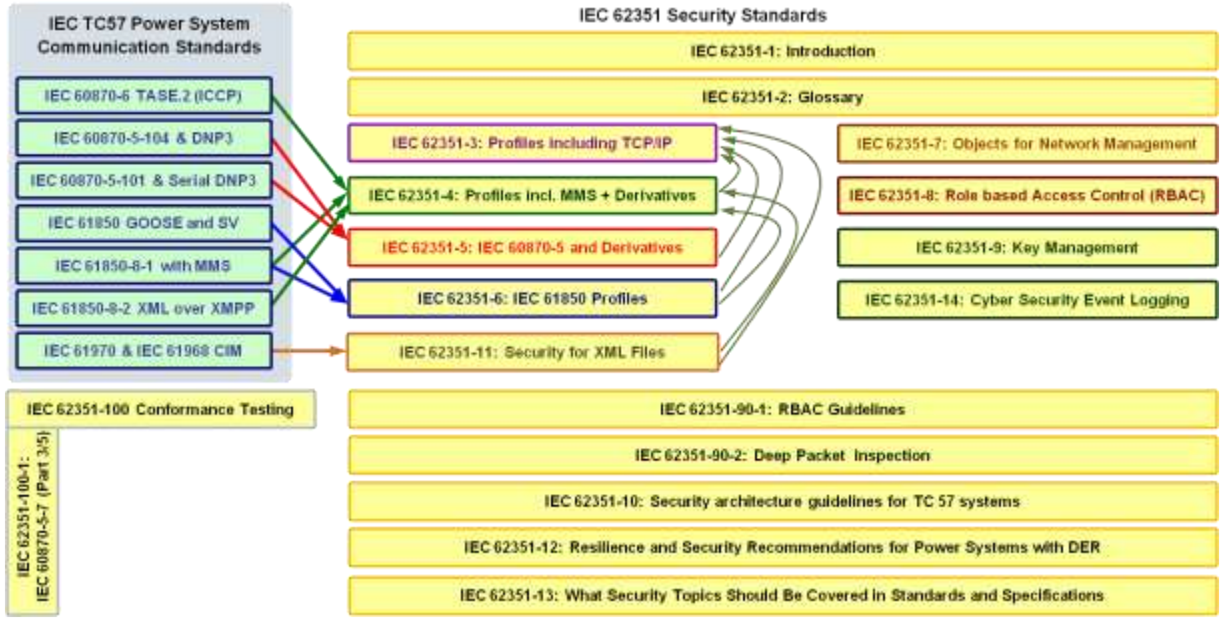




Core communication standards for Digital Grids
IEC TC57 reference architecture with domain-specific cyber security



- **IEC 61970 / 61968** Common Information Model (CIM)
- **IEC 62325** Market Communication using CIM
- **IEC 61850** Substation, Distribution, DER Automation
- **IEC 60870** Telecontrol Protocols (serial/TCP)
- **IEC 62351** Security for Power Systems enables end-to-end security

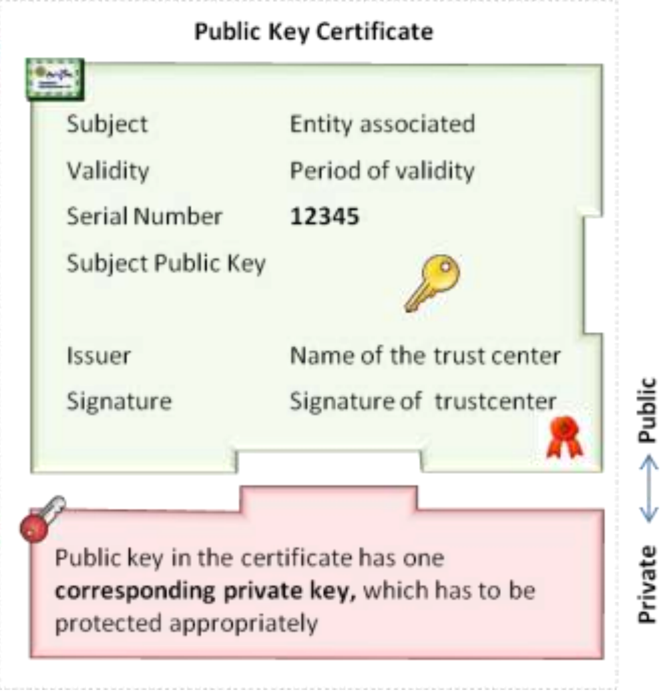


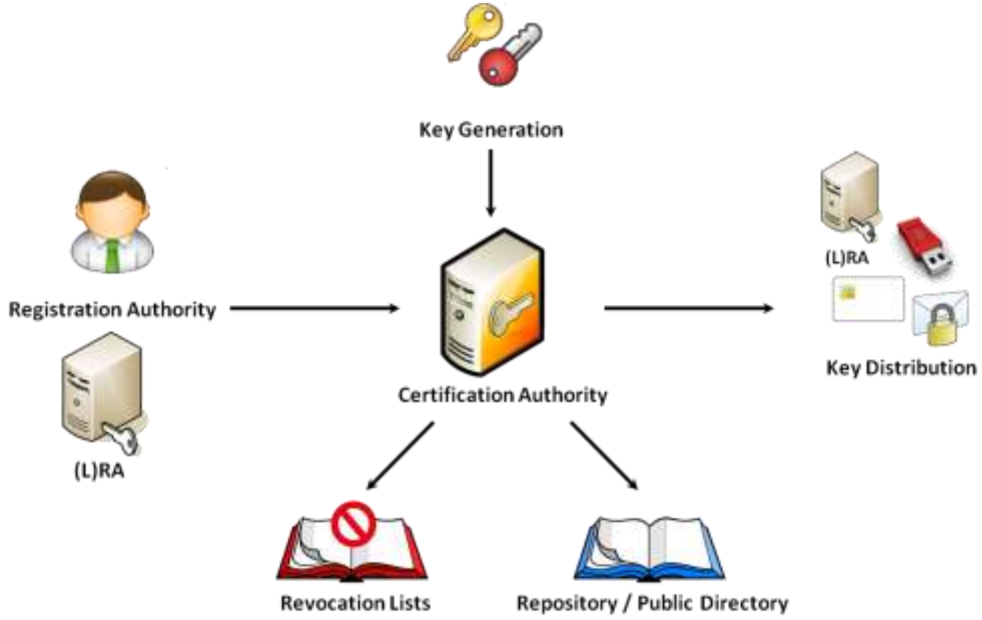
Mutual trust based on X.509 certificates – A key element in IEC 62351 based power system security

What is a certificate ?

- Data structure binding a public key to a subject
- Public key has a corresponding private key
- Limited lifetime
- Binding through certification authority (CA)

  → Comparable with passport or ID





Certificate management is achieved through a PKI

- Enrollment (manual or automatic)
- Key generation
- Certificate issuing
- Certificate distribution
- Certificate revocation

Application of standards and guidelines
Enhancing IEDs in digital substations with cyber security

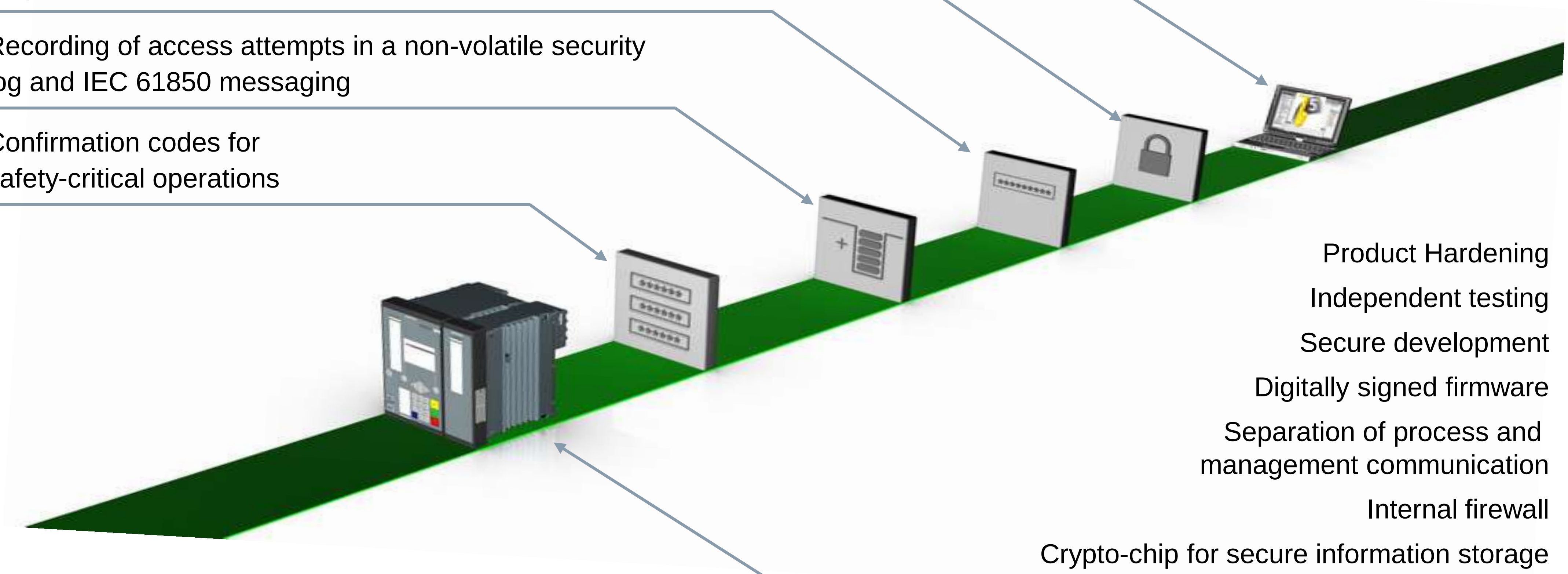
Secure communication (mutual authentication and encryption) between Engineering (DIGSI5) and the IED (SIPROTEC 5)

Connection password according to Regulations and Standards

Recording of access attempts in a non-volatile security log and IEC 61850 messaging

Confirmation codes for safety-critical operations

Secure development
Patch management
Antivirus compatibility

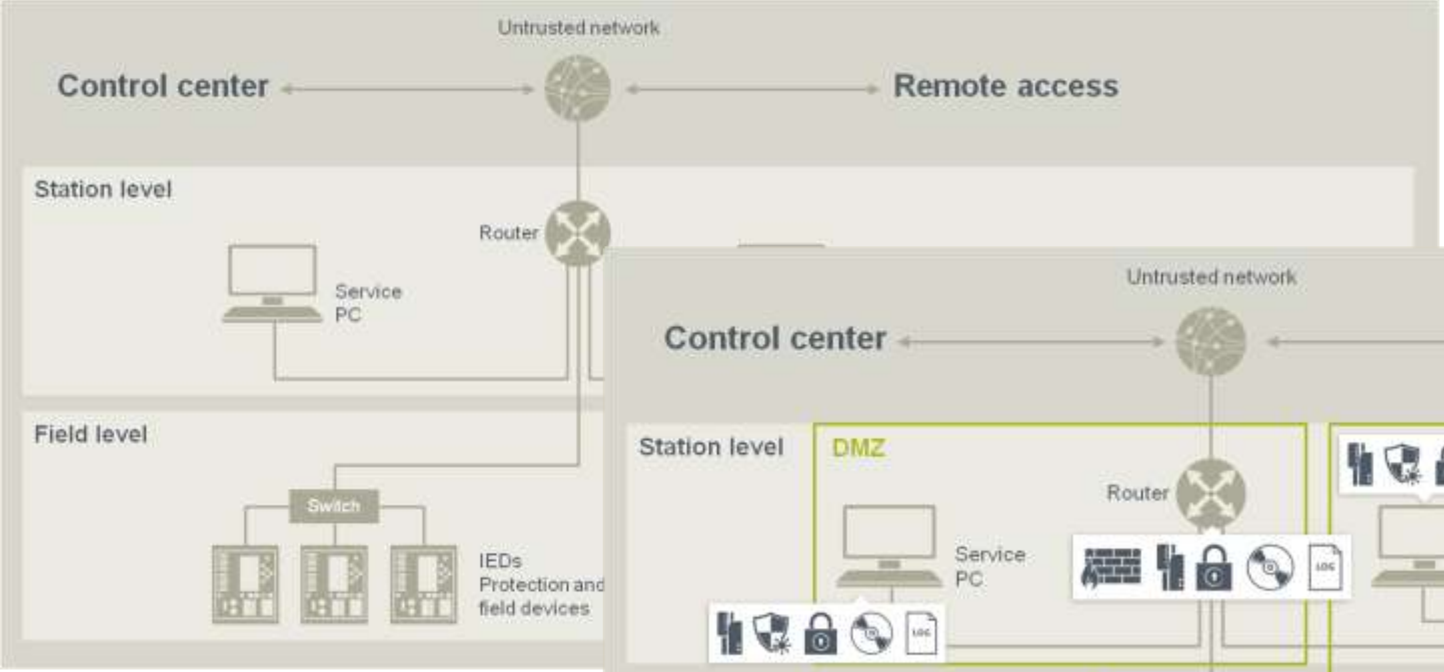


Product Hardening
Independent testing
Secure development
Digitally signed firmware
Separation of process and management communication
Internal firewall
Crypto-chip for secure information storage

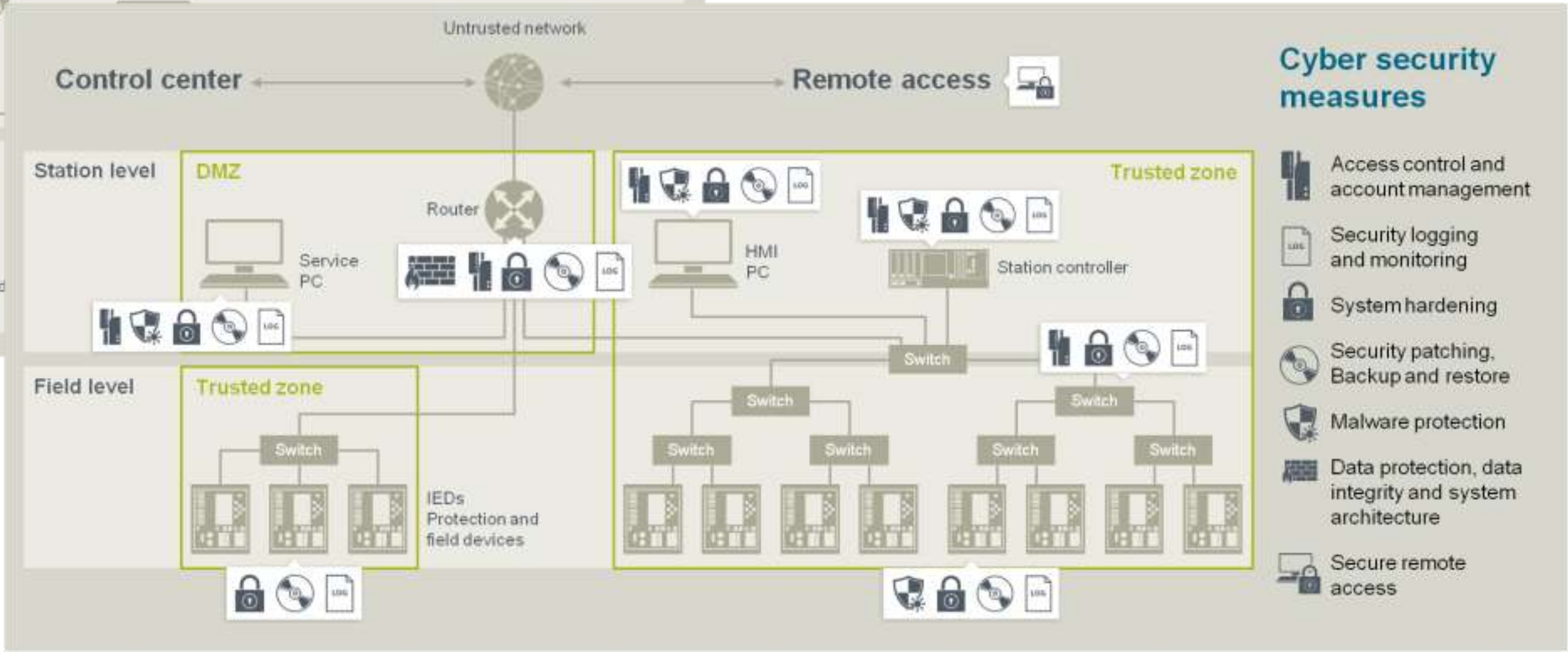
Application of standards and guidelines: The transition from digital substations to secure digital substation addresses multiple aspects

SIEMENS

Digital Substation



Secure Digital Substation



Security has to be suitable for the addressed environment

Awareness and Acceptance

Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue.

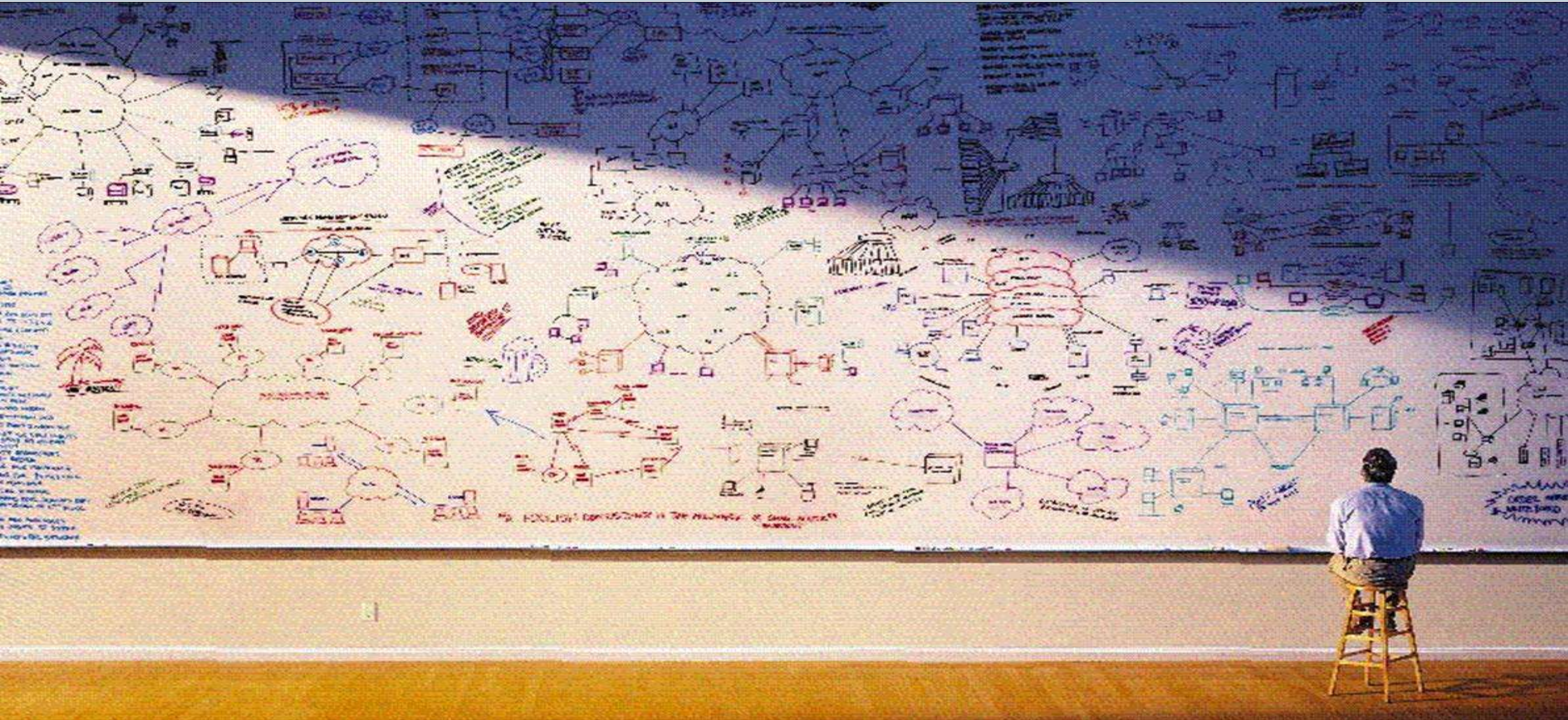
This needs, especially for automation environments, actions for:

- awareness trainings
- help people to understand security measures and processes
- provide user friendly interfaces and processes

Conclusions

- Machine-2-Machine connectivity down to field devices is a major driver for the Digital Grid
- The threat level for critical infrastructures like the Digital Grid is rising
- Cyber security has been acknowledged as prerequisite for limiting risks in and to support a reliable Digital Grid
- Standardization and guideline activities support the alignment of approaches and supports interoperability
- Regulation fosters adoption of security by domain specific requirements (through laws)
- Cyber security needs a holistic approach – collaboration between vendors, integrators and operators; taking into account people, processes and products
- Still, some challenges remain, like the migration from existing environment to an environment featuring appropriate cyber security measures

Thank you for the attention! Questions?



Contact Information

Siemens AG

Steffen Fries

Principal Key Expert

CT RDA ITS
Otto-Hahn-Ring 6
81739 Munich
Germany

E-mail
steffen.fries@siemens.com

Internet
siemens.com/corporate-technology

Digital Grid
siemens.com/digitalgrid