

Cybersecurity in Industrial Environments

From requirements to solutions on the example of Digital Grid

Steffen Fries, Siemens AG, CT RDA CST
October 27th, 2019

1

Introduction and motivation

2

Determination of security requirements

3

Cyber security implications for the Digital Grid

4

Technology examples

- Security credential management
- Securing the substation process bus (GOOSE)

5

Application examples & Conclusions

Our industrial society confesses a growing demand for IT-Security

IT Security trends are determined by drivers such as

- Changes in industrial infrastructures (Digitalization)
- Increasing use of networked embedded systems
- Increasing device-to-device communication
- Need to manage intellectual property

and changing boundary conditions

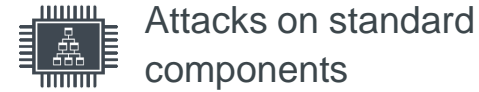
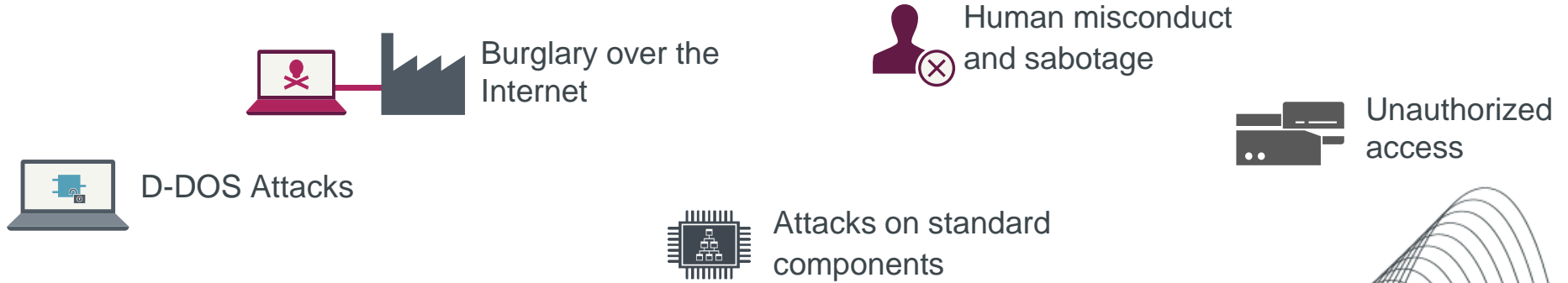
- Increasing international organized crime
- Privacy
- Compliance enforcement
- Cyber war fare
- Cloud/Virtualization
- Data mining and smart data analytics
- Smart mobile devices
-



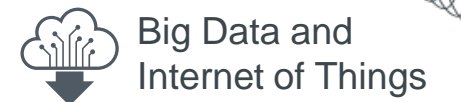
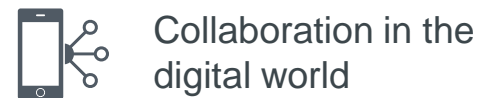
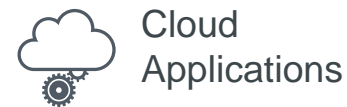
Security must be (continuously) adopted to the changing threat and vulnerability landscape



Changing threat landscape*



Changing infrastructure and processes



Cyber Security is the most important enabler for Digitalization

Design & Engineering

Automation & Operation

Maintenance & Utilization

Siemens Software



Siemens Digital Services



MindSphere

The cloud-based, open IoT operating system
Platform as a Service

Enabler: Infrastructure as a Service (storage, processing power, provider agnostic)

Digitally enhanced Electrification and Automation



Holistic IT security concept

Industrial systems like the Digital Grid systems vs. Office IT Protection targets for security

Digital Grid Systems:
Protection of generation, transmission, and distribution



Lifetime up to 20 years and more

Office IT:
Protection of IT-Infrastructure



Lifetime 3-5 years

Critical infrastructures have an influence on safety

Security-by-Design is different from Safety-by-Design

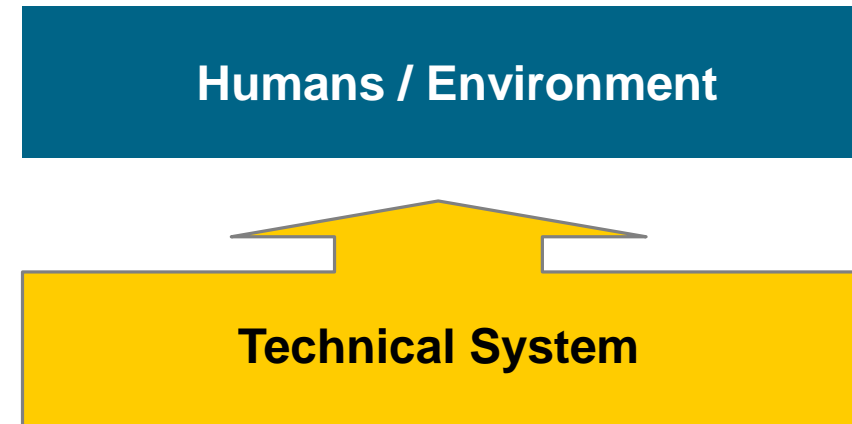
IT Security

Prevention of consequences of threats to a system (intentionally) caused by humans and/or environment



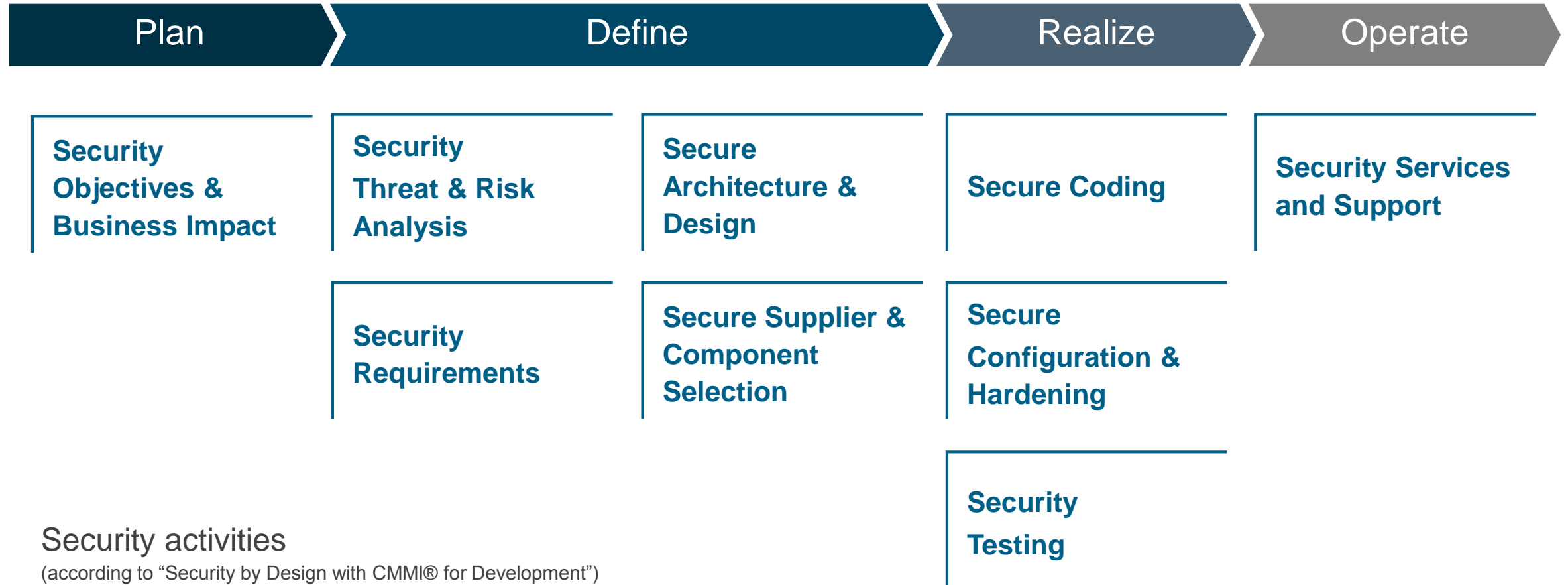
Safety

Prevention of threats to humans and environment caused by technical systems



Despite different design goals, the interrelationship between of IT-security and safety, needs to be obeyed during system design to prevent consequences of accidental and intentional threats.

Defining & Maintaining secure products and solutions requires an accompanying lifecycle process



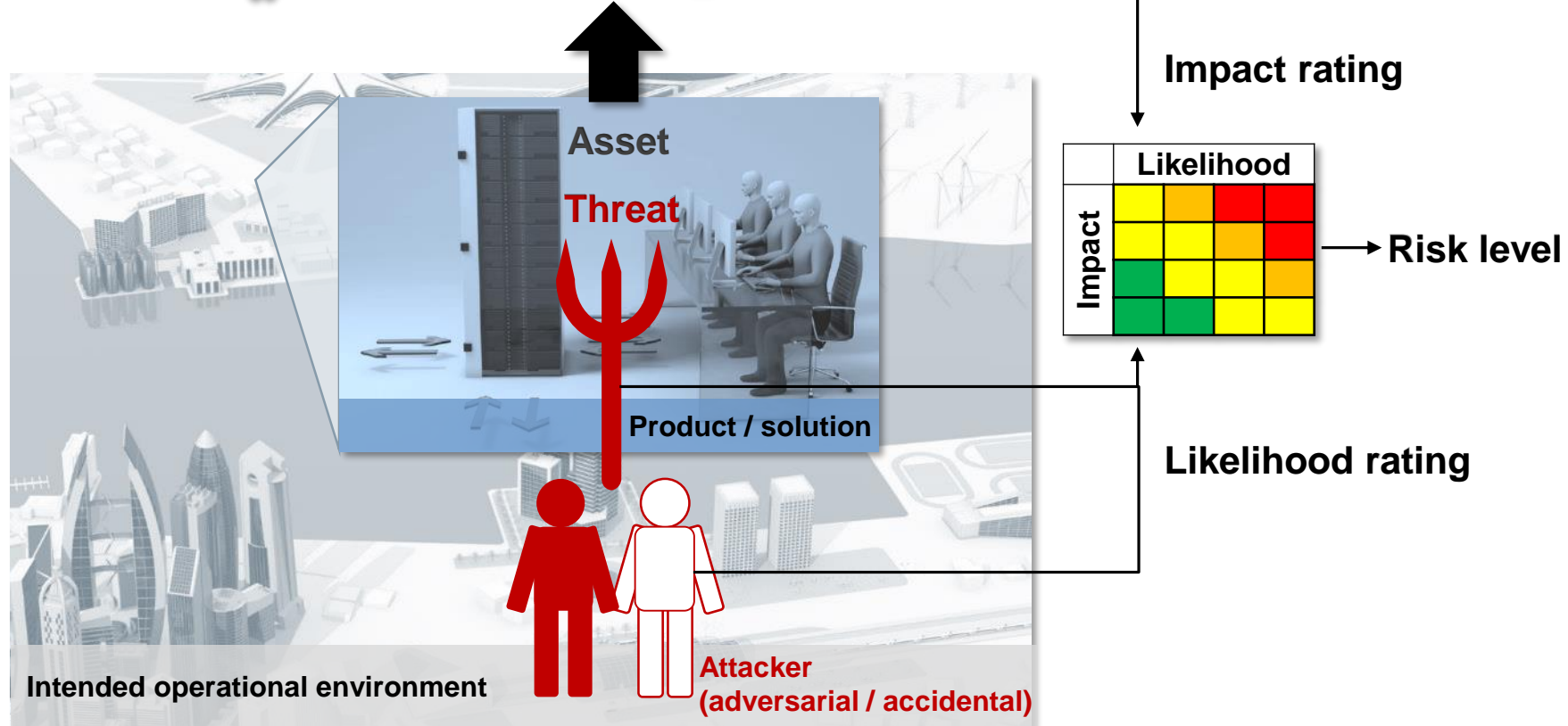
Security activities

(according to "Security by Design with CMMI® for Development")

Evaluation of risk from security threats to products, solutions or services as one starting point for the derivation of security requirements

- Threat and risk analysis to
 - identify security weaknesses and vulnerabilities
 - analyze threats that might exploit these weaknesses or vulnerabilities
 - evaluate of resulting risks.


Safety, Availability, Legal and Contractual Requirements , Intellectual Property, Reputation



- Supports
- derivation of counter measures
 - check the effectiveness of planned or implemented counter measures.

- Different methods exists, e.g.,
 - [SGIS Toolbox](#)
 - [NIST Guide for Risk Assessments](#)
 - [Cyber Security Capability Model](#)
 - [German BSI-Standard 100-3 Risikoanalyse](#)

Digital Grid as critical infrastructure is addressed through standards and regulative requirements (examples, global view)

- IEC 62351 – Power systems management and associated information exchange – Data and communications security
- IEC 62443 – Security for industrial automation and control systems
- ISO/IEC 15118 – Road vehicles -- Vehicle to grid communication interface

- ISO/IEC 27001 – Information technology - Security techniques - Requirements
- ISO/IEC 27002 – Code of Practice for information security management
- ISO/IEC 27019 – Information security controls for the energy utility industry

- IEEE 1588 – Precision Clock Synchronization
- IEEE 1686 – Intelligent Electronic Devices Cyber Security Capabilities

- RFC 4301 – Security Architecture for the Internet Protocol
- RFC 5246 – Transport Layer Security TLS v1.2
- RFC 8446 – Transport Layer Security TLS v1.3

- 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)

Standards and Regulation

NERC Critical Infrastructure Protection (CIP)



- Series of Standards of North American Electric Reliability Council (NERC), Mandatory by Energy Policy Act of 2005 (EPACT)
- Applies to **operators of Bulk Electric Systems** in the US (also Canada and parts of Mexico)
- Auditable compliance to CIP required

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009	CIP-010	CIP-011
BES cyber system categorization	Security management controls	Personnel and training	Electronic security perimeter	Physical security	Systems security management	Incident reporting and response planning	Recovery plans	Configuration change management, vulnerability assessment	Information protection
1. Asset impact classification 2. Regular classification review 3. Regular management approval	1. Cyber security policy 2. Leadership 3. Cyber security plan for low impact systems	1. Security awareness program 2. Security training program 3. Personnel risk assessment 4. Access Management 5. Access Revocation	1. Electronic security perimeter 2. Interactive remote access management	1. Physical security plan 2. Visitor control program 3. Physical access control system maintenance and testing program	1. Ports and services 2. Security patch management 3. Malicious code protection 4. Security event monitoring 5. System access control	1. Incident response plan specification 2. Implementation and testing 3. Review, update and communication	1. Recovery Plan Specifications 2. Implementation and testing 3. Review, update and communication	1. Configuration change management 2. Configuration monitoring 3. Vulnerability assessment	1. Information protection 2. Cyber asset reuse and disposal



NERC-CIP: Enforcement through FERC



Enforcement with fines for non-compliance

Enforcement Actions 2019

Enforcement Actions 2019

Date	Regulatory Authority	Regulatory Filing ID	Region	Registered Entity	NCR ID	Total Penalty (\$)	NERC Violation ID	Reliability Standard	Requirement	Violation Risk Factors
9/26/2019	FERC	NP19-18-000 View Filing View A-1 Spreadsheet >> View A-2 Spreadsheet >>	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information
8/29/2019	FERC	NP19-17-000 View Filing View A-1 Spreadsheet >> View A-2 Spreadsheet >> View Notice >>	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information
8/29/2019	FERC	NP19-16-000 View Filing View Notice >>	WECC	Unidentified Registered Entity	NCRXXXXX	\$2,100,000	WECC2018019480 WECC2017017880 WECC2017017881 WECC2017017882 WECC2018019481 WECC2017017883 WECC2017017884	CIP-007-1 CIP-007-1 CIP-007-1 CIP-007-1 CIP-010-2 CIP-010-2	R2 R3 R5 R1 R1 R2	
7/31/2019	FERC	NP19-15-000 View Filing View A-1 Spreadsheet >> View A-2 Spreadsheet >> View Notice >>	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information	See Spreadsheets and NOP for Spreadsheet NOP Information
							SERC2016015954 SERC2017018136 SERC2017018279 SERC2017018774 SERC2016016548	CIP-002-5.1 CIP-004-6 CIP-004-6 CIP-005-5 CIP-005-5	R1 R5 R5 R1 R2	



NERC Notice of Penalty
The Entity
August 29, 2019
Page 2

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

The Entity agreed to the **two million, one hundred thousand dollars (\$2,100,000) penalty**, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and the Entity. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations,⁵ NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on these violations is set forth in the Settlement Agreement and herein.

Target Group

Operator of critical infrastructures
 ("KRITIS-Betreiber")

Sectors (1.Basket)

- Energy
- Information Technology and Telecommunications
- Water
- Food

Sectors (2.Basket)

- Transport and Traffic
- Health
- Finance and Insurance

Manufacturer of IT-Products and Systems

Obligations

Adherence to a minimum set of technical and organizational IT-Security Measures

- Minimum set have been developed per domain
- For the sectors Energy, Information Technology and Telecommunications, Water and Food, respective measures must generally be implemented until May 2018 at the latest
- Adherence to minimum security must be shown every 2 years against German BSI (e.g., security audits, certification, etc.)
- Penalties in case of non-compliance up to 100,000 EUR

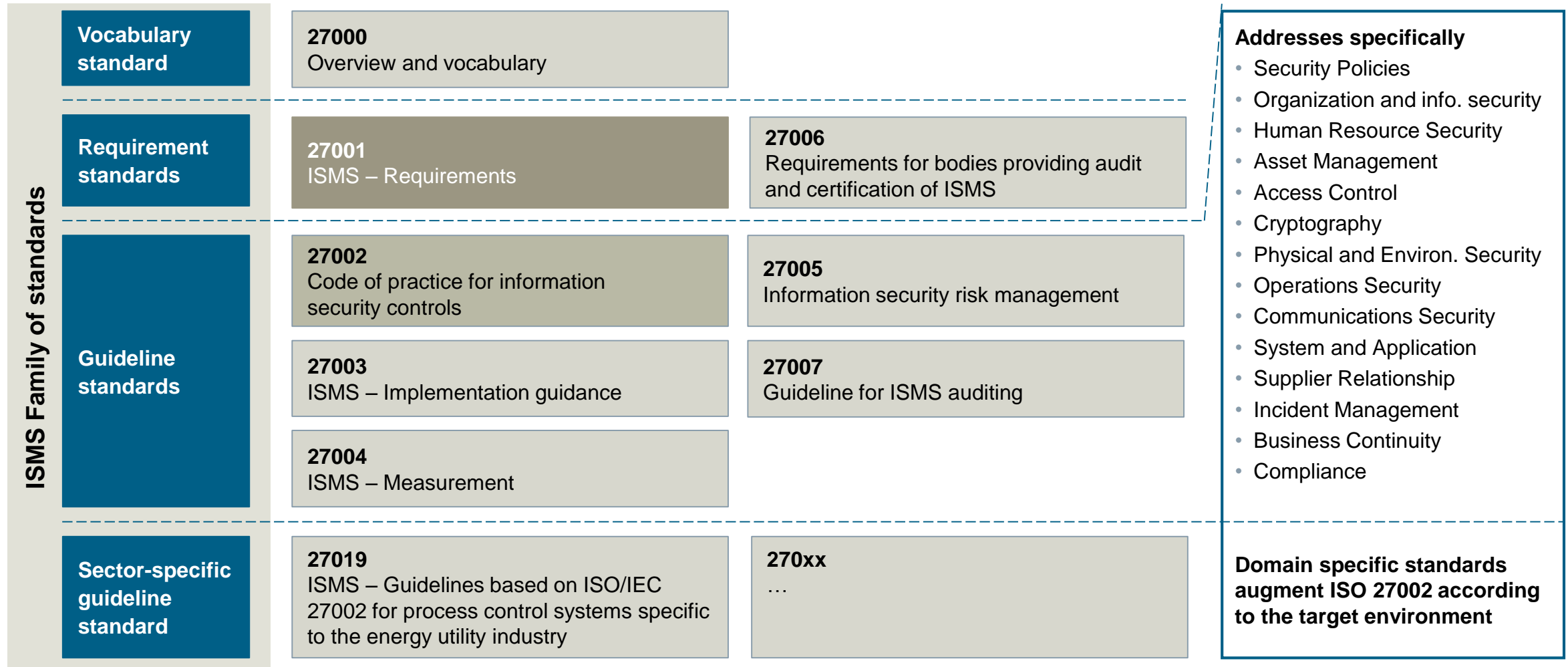
Notification Requirements in case of security breaches (at German BSI)

- Establishment of a contact point to the German BSI
- Transition period: 6 months after enactment
- In case of failures to notify penalties up to 50,000 EUR possible (without damage claims)

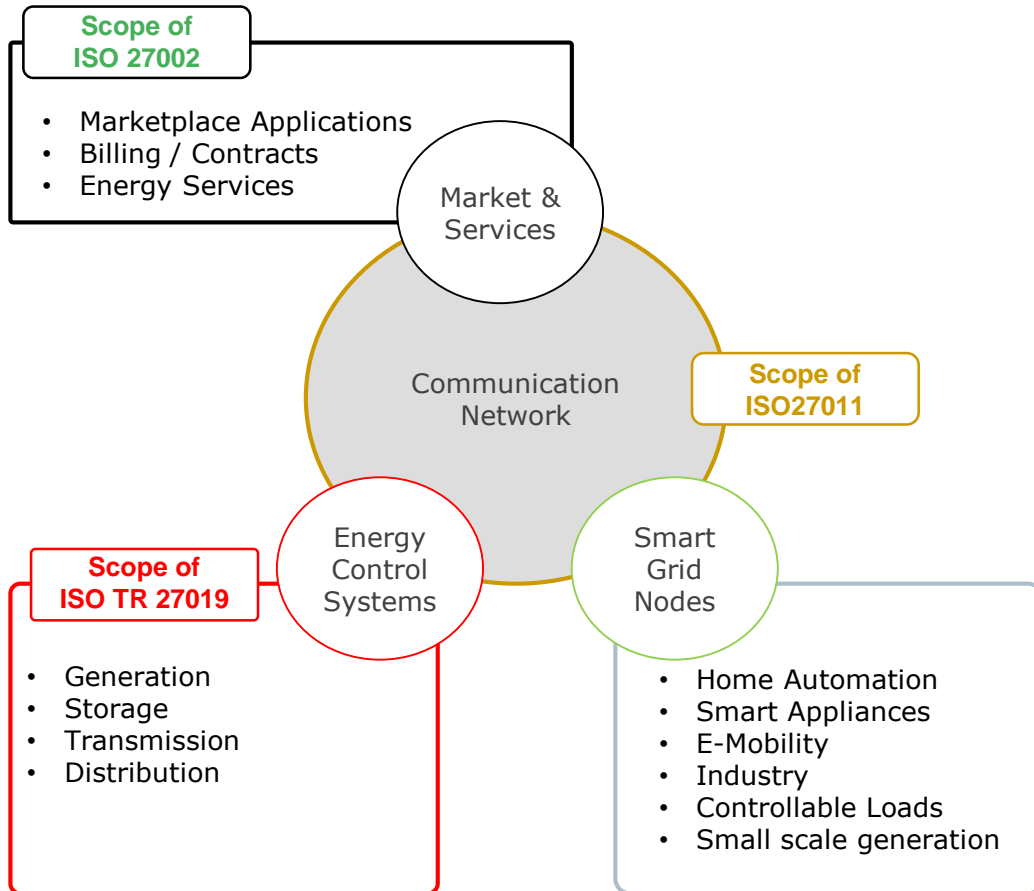
On request of the German BSI: **obligations to support** during the handling or avoidance of disturbances for KRITIS-Operators (e.g., Security Update provisioning)

Standards and Regulations

ISO/IEC 270xx Series – Information Security Management System (ISMS)



Information Security Management – Application of the ISO 270xx series targets Digital Grid specific security controls in ISO 27019



• ISO 27019 targets

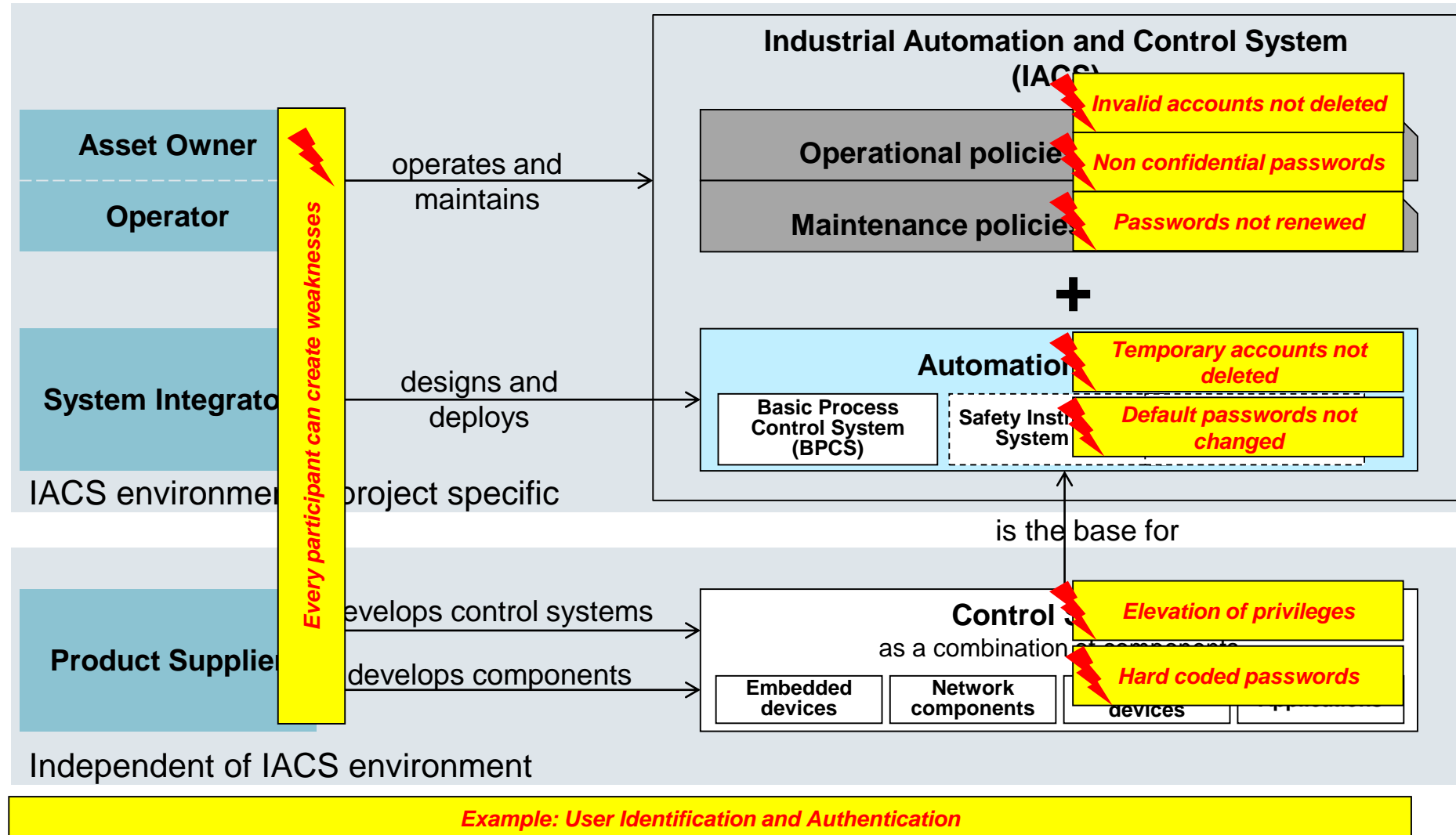
- Process control systems [...] for controlling and monitoring the generation, transmission, storage and distribution of electric power, gas and heat in combination with the control of supporting processes

• Augments ISO 27002, examples:

- Physical security
 - Control centers and PCS equipment rooms
 - Peripheral sites, e.g. substations or distributed storage and generation sites
- Communications and operations management
 - Treatment of potential insecure legacy systems
 - Malware protection and patch management for critical systems
 - Securing process control data communication
- Access control
 - Special requirements for group accounts, session timeouts etc.

IEC 62443 a 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
- Used for certification of security processes and security capabilities of the solution



IEC 62443 addresses the complete value chain from product to service

- Addresses
 - Operator
 - Integrator
 - Product Supplier
- in terms of
 - processes and
 - security capabilities
- and allows for
 - certification

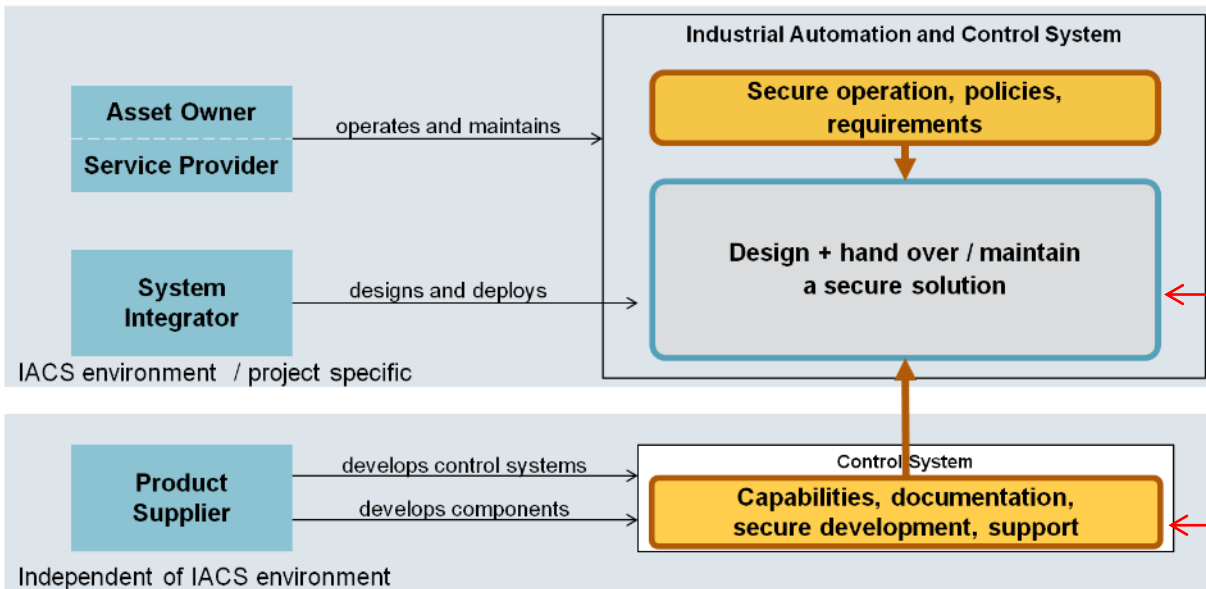
General	Policies and Procedures	System	Component
1-1 Terminology, concepts and models IS 2009	2-1 Requirements for an IACS security management system Ed.2.0 Profile of ISO 27001 / 27002 CD 2Q18 Cert Procedural	3-1 Security technologies for IACS TR 2009	4-1 Product development requirements IS 1Q18 Cert Procedural
1-2 Master glossary of terms and abbreviations In Progress	2-2 IACS protection levels NP 3Q18 Procedural	3-2 Security risk assessment and system design CDV 1Q/18 Procedural Functional	4-2 Technical security requirements for IACS products IS 1Q19 Cert Functional
1-3 System security compliance metrics Rejected	2-3 Patch management in the IACS environment TR 06/2015 Procedural	3-3 System security requirements and security levels IS 08/2013 Cert Functional	
1-4 IACS Security Life Cycle and Use Cases Planned	2-4 Requirements for IACS solution suppliers IS 06/2015 Cert Procedural		
Definitions and Metrics	Requirements for Organizations	Requirements for Systems	Requirements for Components
IS 2015 = Status		Cert = Certification relevance	Procedural / Functional = Scope

*DC: Draft for Comment
*CDV: Committee Draft for Vote

*IS: International Standard
*FDIS: Final Draft International Standard

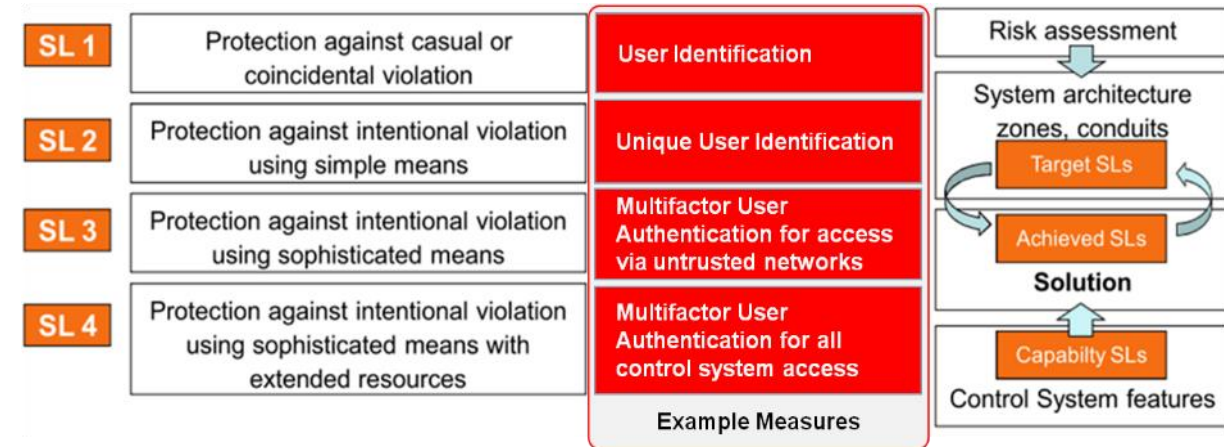
*NP: New Proposal
*TR: Technical Report

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



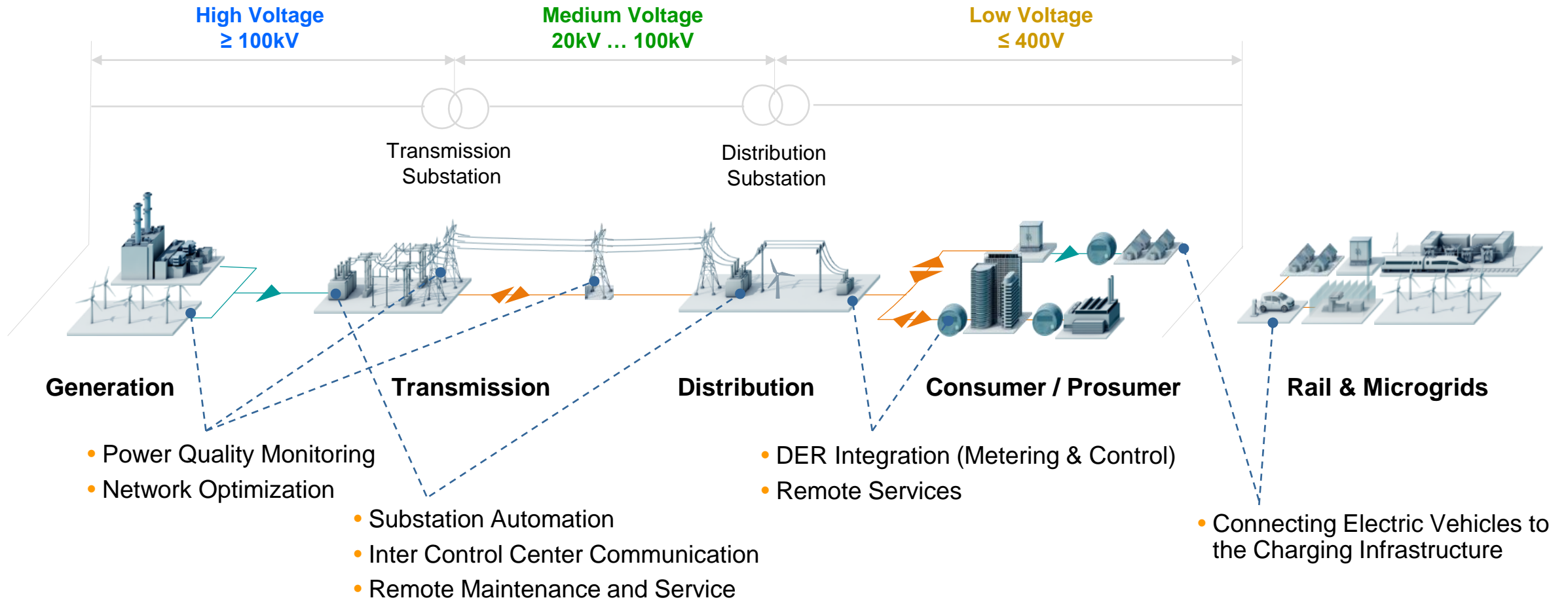
General	Policies and Procedures	System	Component
1-1 Terminology, concepts and models IS 2006	2-1 Requirements for an IACS security management system Ed.2.0 Profile of ISO 27001 / 27002 CDV 1017 Cert Procedural	3-1 Security technologies for IACS TR 2009	4-1 Product development requirements CDV 2016 Cert Procedural
1-2 Master glossary of terms and abbreviations In Progress	2-2 Implementation Guidance for an IACS Security Management System Planned Procedural	3-2 Security risk assessment and system design NP 4015 Cert Functional	4-2 Technical security requirements for IACS products CDV 1017 Cert Functional
1-3 System security compliance metrics Rejected	2-3 Patch management in the IACS environment TR 2015 Procedural	3-3 System Security Req.	
1-4 IACS Security Life Cycle and Use Cases Planned	2-4 Req. for IACS Supplier		
Definitions and Metrics	Requirements for Organizations	Requirements for Systems	Requirements for Components

IS 2015 = Status Cert = Certification relevance
DC: Draft for Comment
 CDV: Committee Draft for Vote
 IS: International Standard
 TR: Technical Report
 Procedural / Functional = Scope
 NP: New Proposal



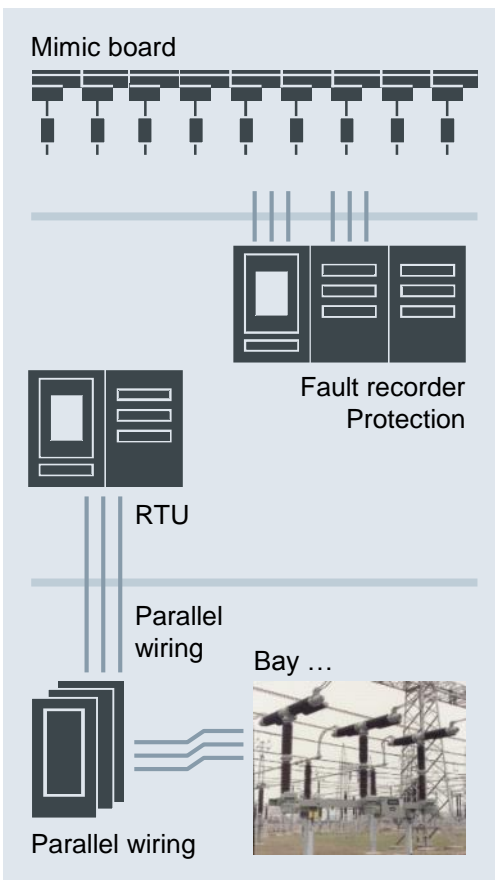
Digital Grid – a critical infrastructure

Power system value chain and use case examples

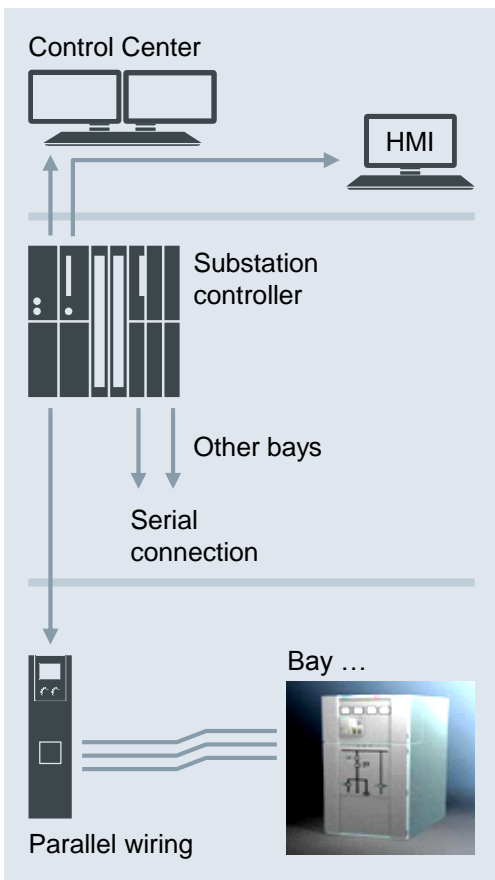


Architecture evolution in substation automation

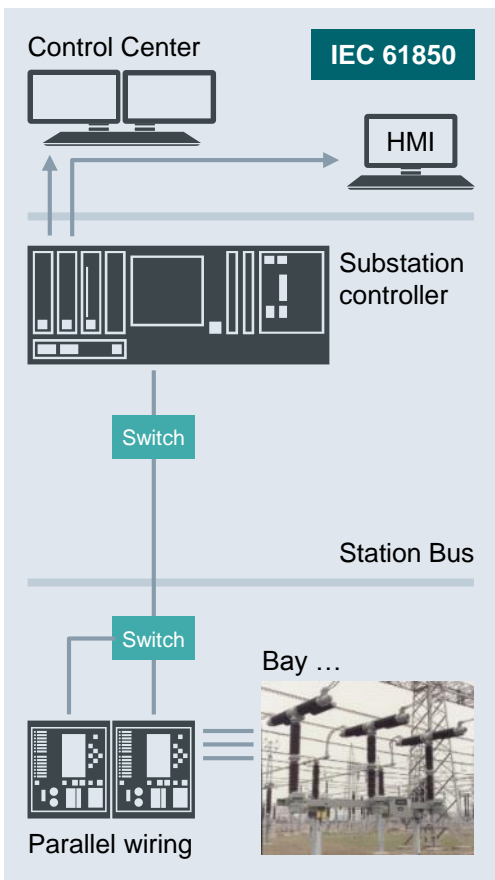
1st generation – Standard cabling



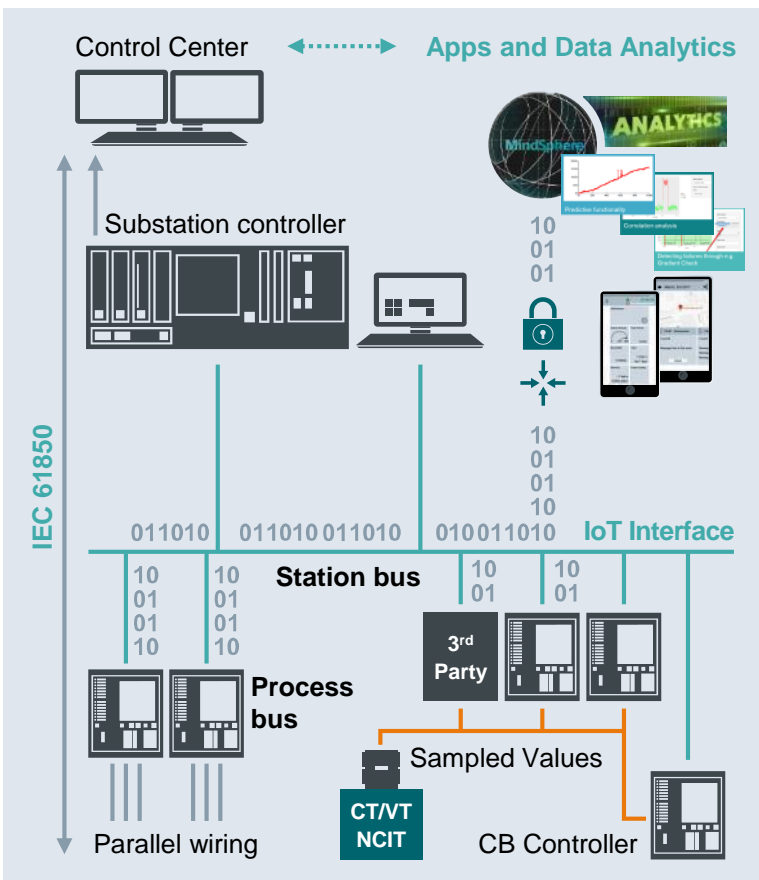
2nd generation – Point- to-point connections since 1985 ...



3rd generation – Digital Station Bus since 2004 ...



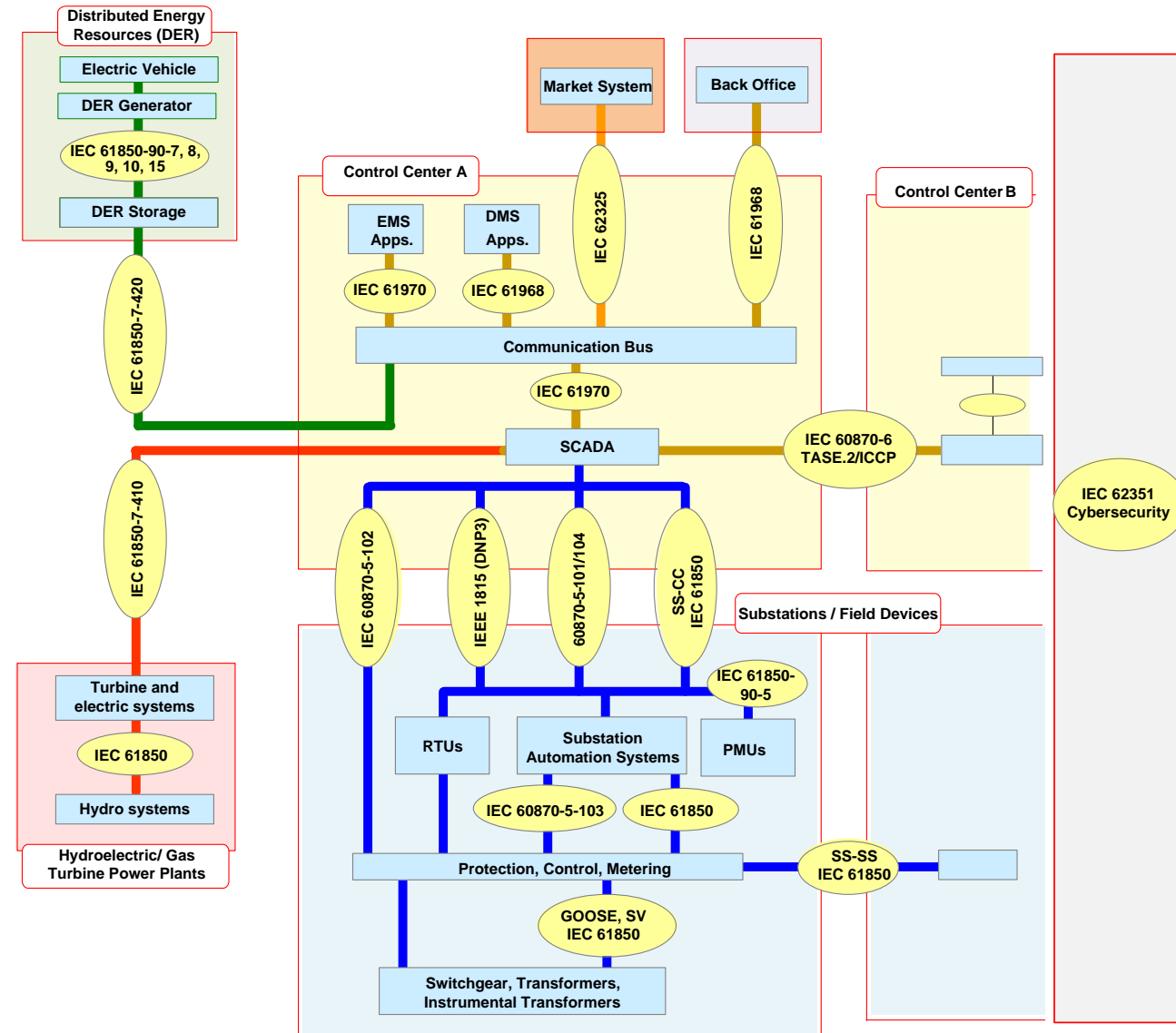
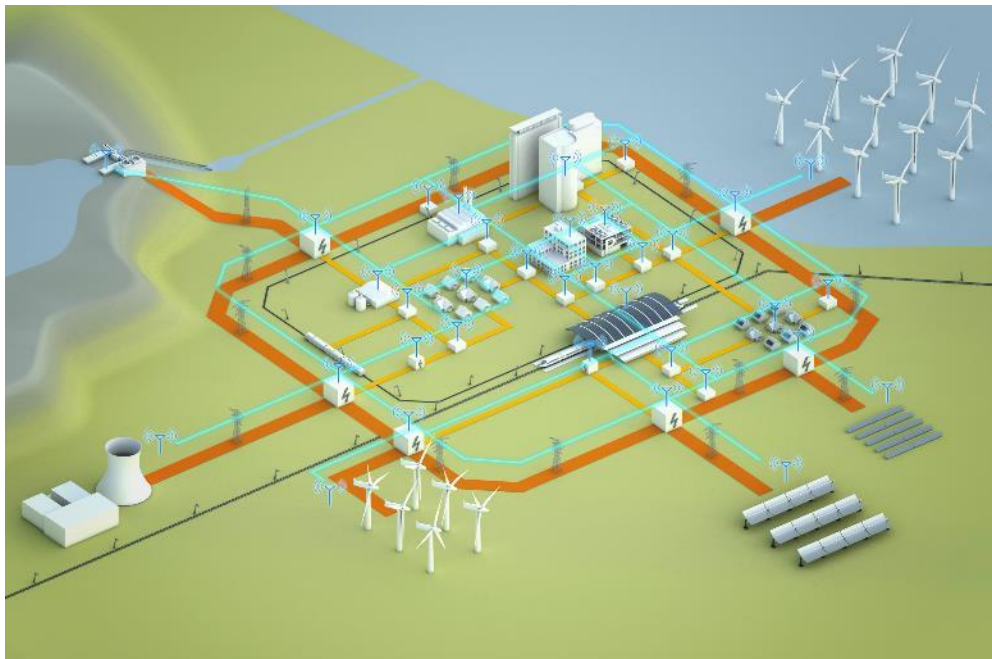
Digital Substation 4.0



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



Typical data exchanged in Digital Grid applications and their security impact



Information asset	Description, potential content	Security relation to
Customer ID and location data	Customer name, identification number, schedule information, location data	customer privacy
Meter Data	Meter readings that allow calculation of the quantity of electricity consumed or supplied over a time period and may be used for controlling energy loads but also for interactions with an electricity market.	system control and billing
Control Commands and Measurements	Actions requested by one component of other components via control commands. These commands may also include Inquiries, Alarms, Events, and Notifications.	system stability and reliability and also safety
Configuration Data	Configuration data (system operational settings and security credentials but also thresholds for alarms, task schedules, policies, grouping information, etc.) influence the behavior of a component and may need to be updated remotely.	system stability and reliability and also safety
Time, Clock Setting	Time is used in records sent to other entities. Phasor measurement directly relates to system control actions. Moreover, time is also needed to use tariff information optimally. It is also used in security protocols, e.g., when verifying the validity of using certificates.	system control (stability and reliability and also safety) and billing
Access Control Policies	Components need to determine whether a communication partner is entitled to send and receive commands and data. Such policies may consist of lists of permitted communication partners, their credentials, and their roles.	system control and influences system stability, reliability, and also safety
Firmware, Software, and Drivers	Software packages installed in components may be updated remotely. Updates may be provided by the utility (e.g., for charge spot firmware), the car manufacturer, or another OEM. Their correctness is critical for the functioning of these components.	system stability and reliability and also safety
Tariff Data	Utilities or other energy providers may inform consumers of new or temporary tariffs as a basis for purchase decisions.	customer privacy and also competition

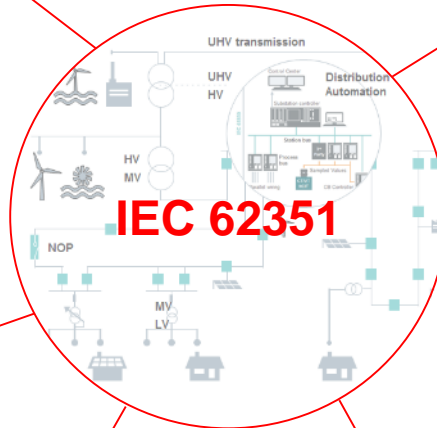
Cyber security is addressed in power system automation with IEC 62351 building on state of the art security technology



IAM – Authentication, Identification
Authorization (RBAC) of Users/Devices
Focus: Usage of X.509 certificates

Key management of long term and session keys
Focus: Application of established certificate management (EST, SCEP) and key management (GDOI) protocols

Secure communication between different actors (Ethernet, IP, serial)
Focus: Profiling of existing standards (e.g., TLS) and definition of security enhancements if necessary

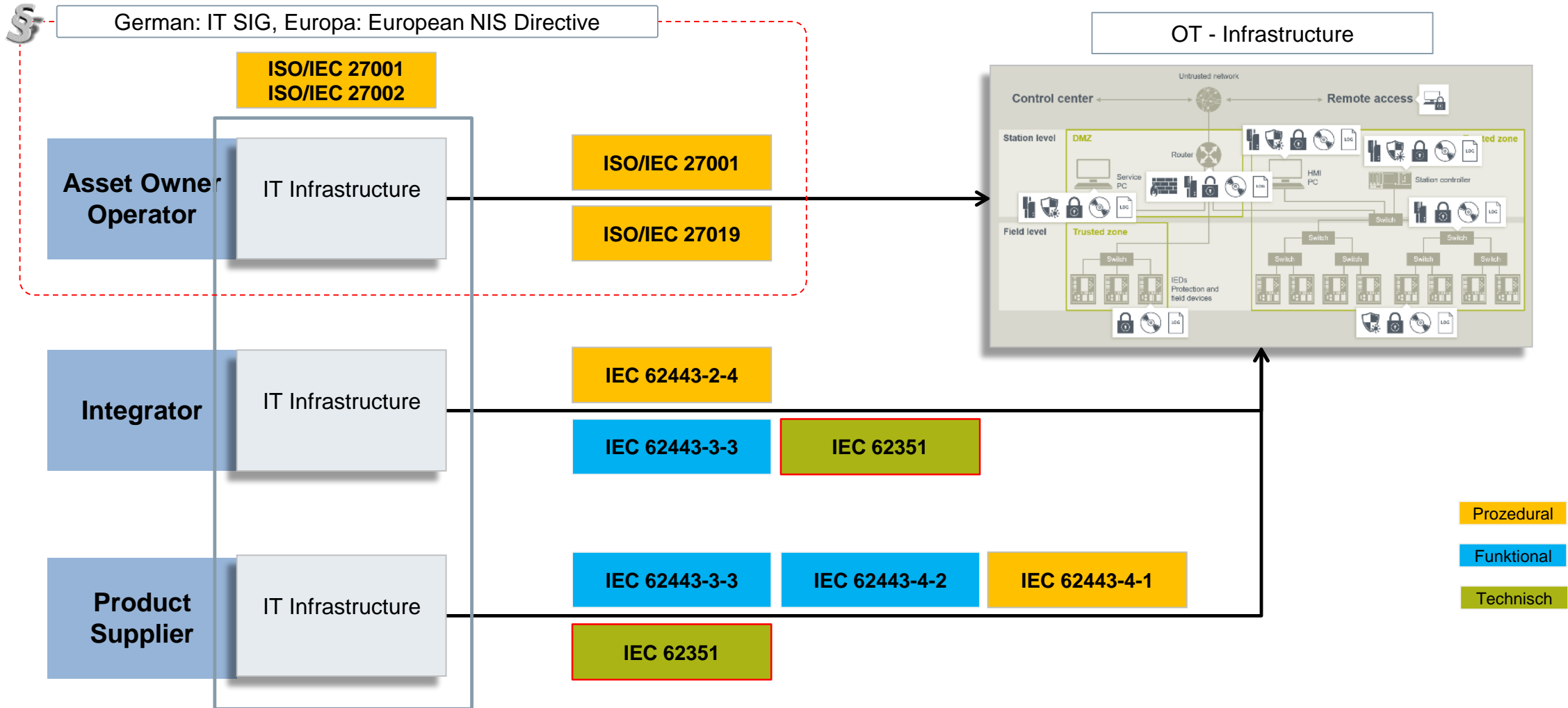


Test case description for the specified security measures in the different parts of IEC 62351
Focus: Specification of conformity test cases

Monitoring and audit of security relevant events
Focus: Application of established standards like syslog and SNMP

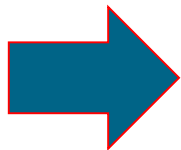
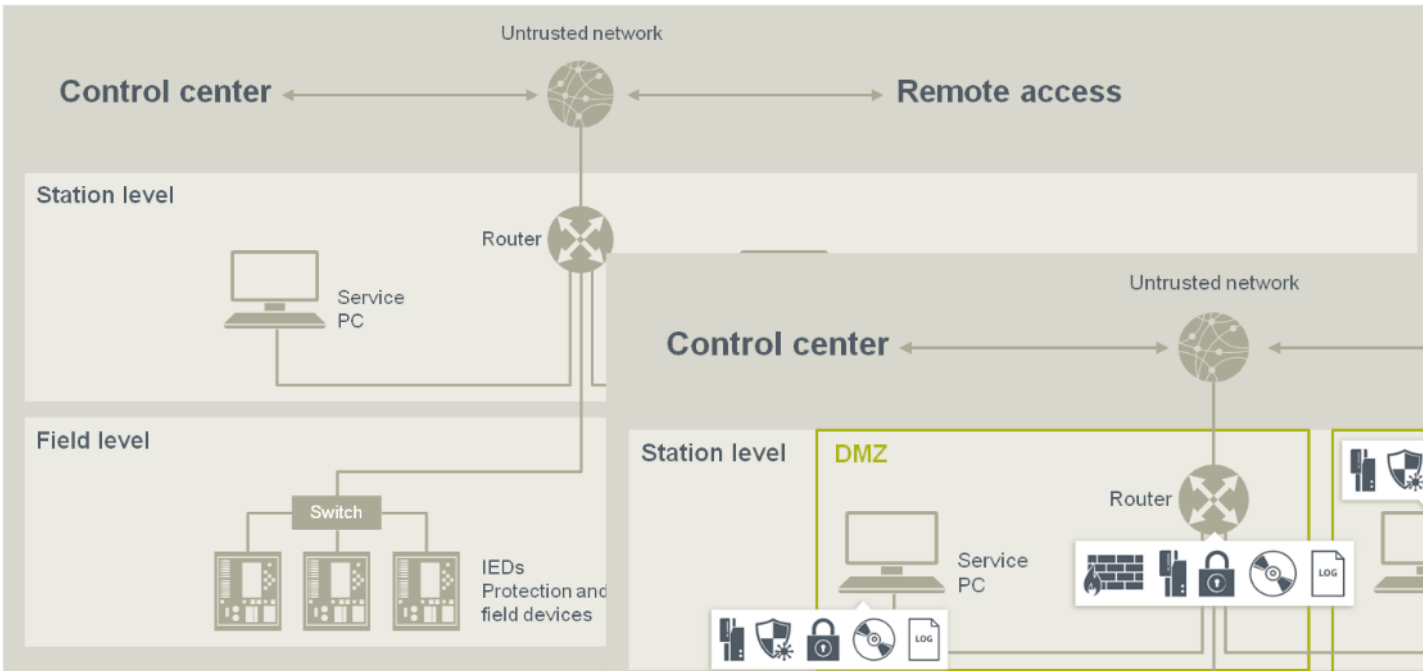
Guidance and support for securing power system
Examples comprise role based access control (RBAC), Monitoring of communication connections, ...

Cyber Security for Power System Automation – The Interplay of ISO/IEC 27001 / IEC 62443 / Domain Specific Standards

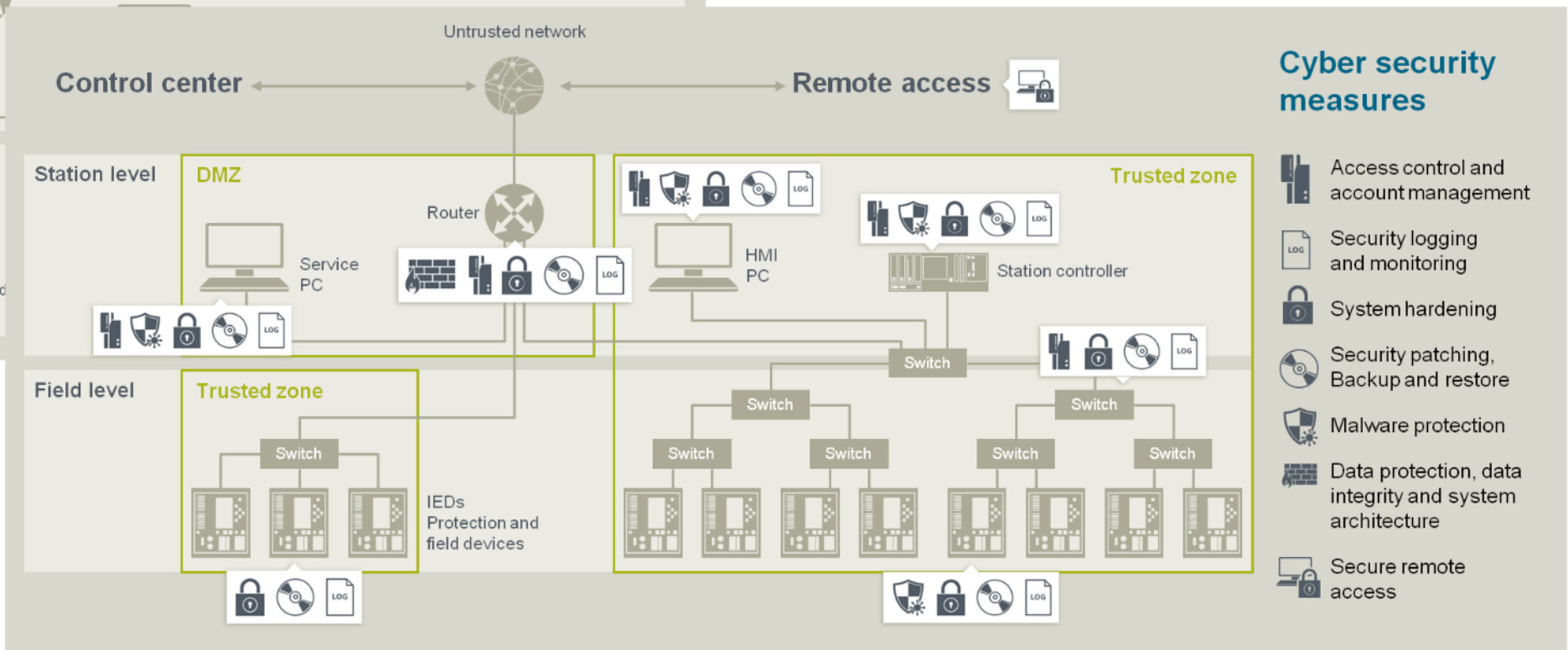


Application of standards and guidelines: The transition from digital substations to secure digital substation addresses multiple aspects

Substation



Secure Substation



Cyber security measures

- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, Backup and restore
- Malware protection
- Data protection, data integrity and system architecture
- Secure remote access

Security has to be suitable for the addressed environment



Awareness and Acceptance

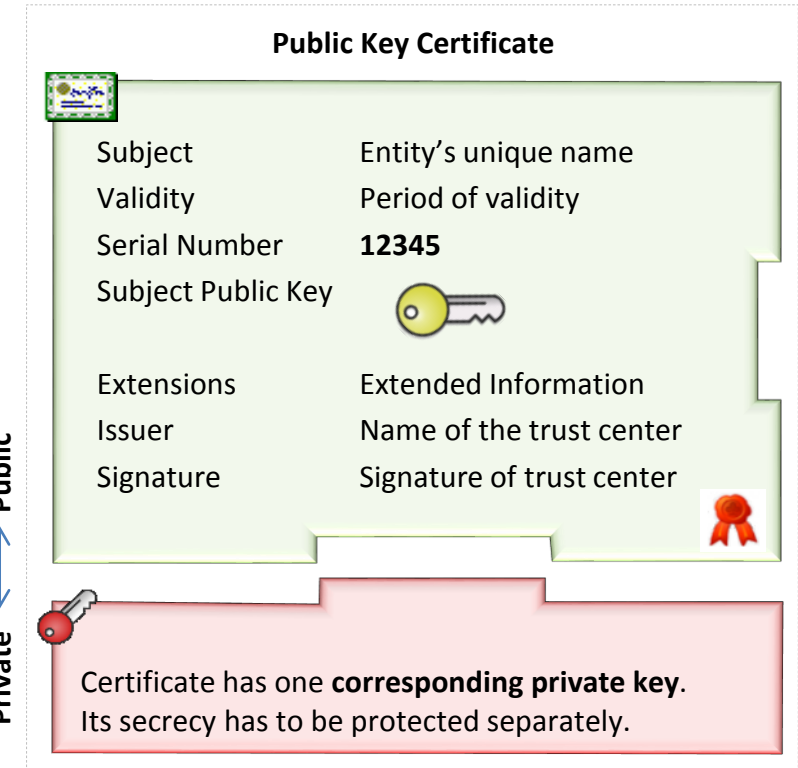
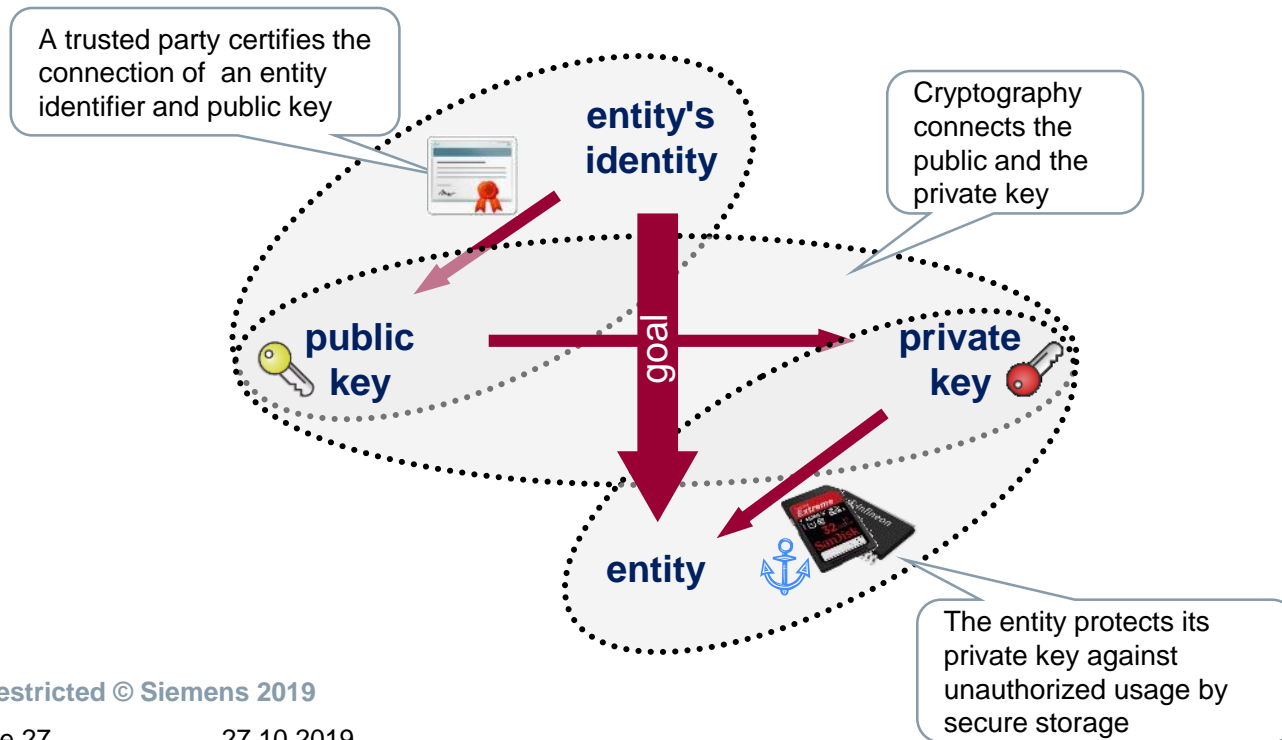
Since security is not just a technical solution, which can be incorporated transparently, we need to consider how humans can get along with this issue.

This needs, especially for automation environments, actions for:

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

Mutual trust based on X.509 key material – A key element in power system security

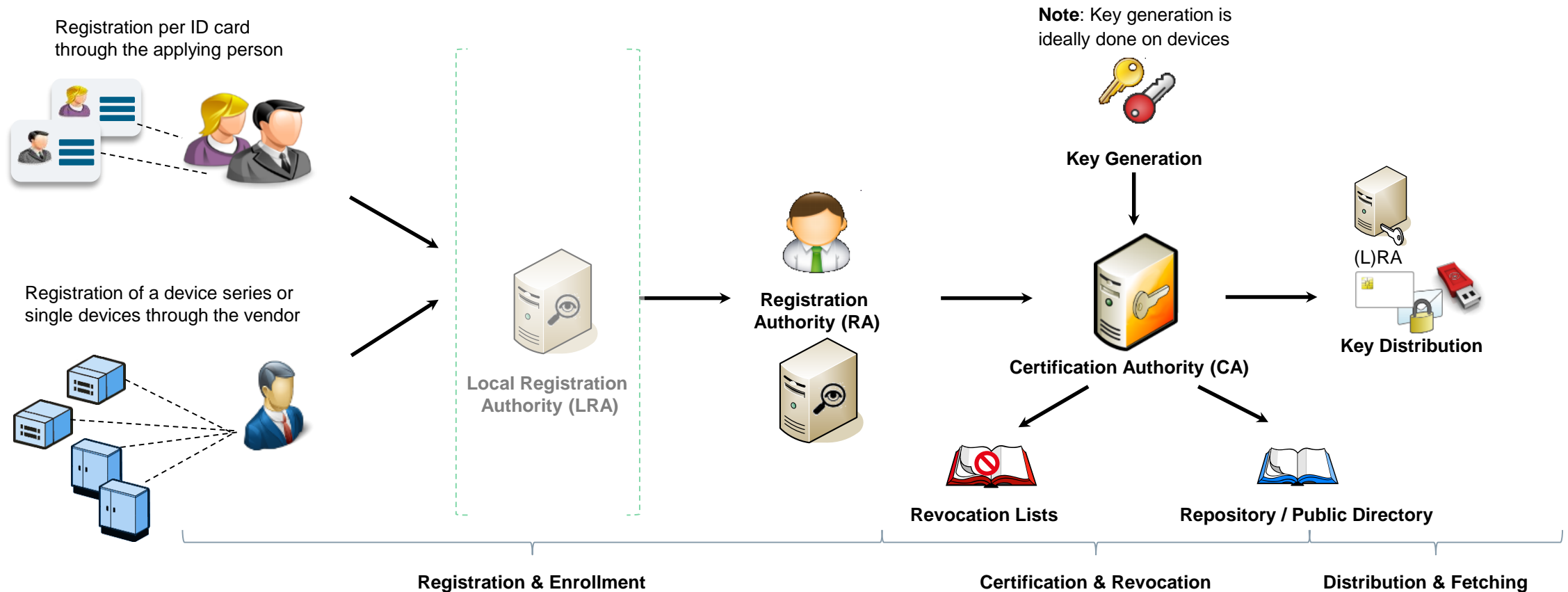
- Key material in terms of certificates and corresponding private keys as well as the managing infrastructure has been standardized by the ITU-T in X.509. It was also published by the IETF as RFC 5280.
- Bases on a key pair, for which the public key has been certified by a trusted third party.
- The certificate binds the identity of the owner to the public key.
- A certificate has a limited lifetime.



Comparable with :



Handling of X.509 key material through a Public Key Infrastructure (PKI)



Realization examples	Enrollment	Revocation	Fetching
	<ul style="list-style-type: none"> • manual • automated (SCEP, EST, CMP, CMC) 	<ul style="list-style-type: none"> • manual (CRL) • automated (CRL, OCSP, SCVP) 	<ul style="list-style-type: none"> • manual (configuration) • automated (LDAP, HTTP)

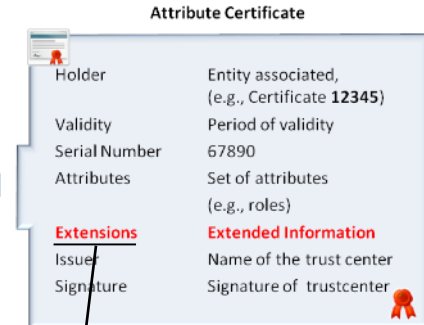
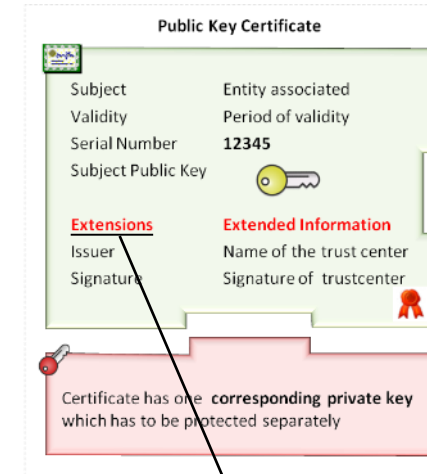
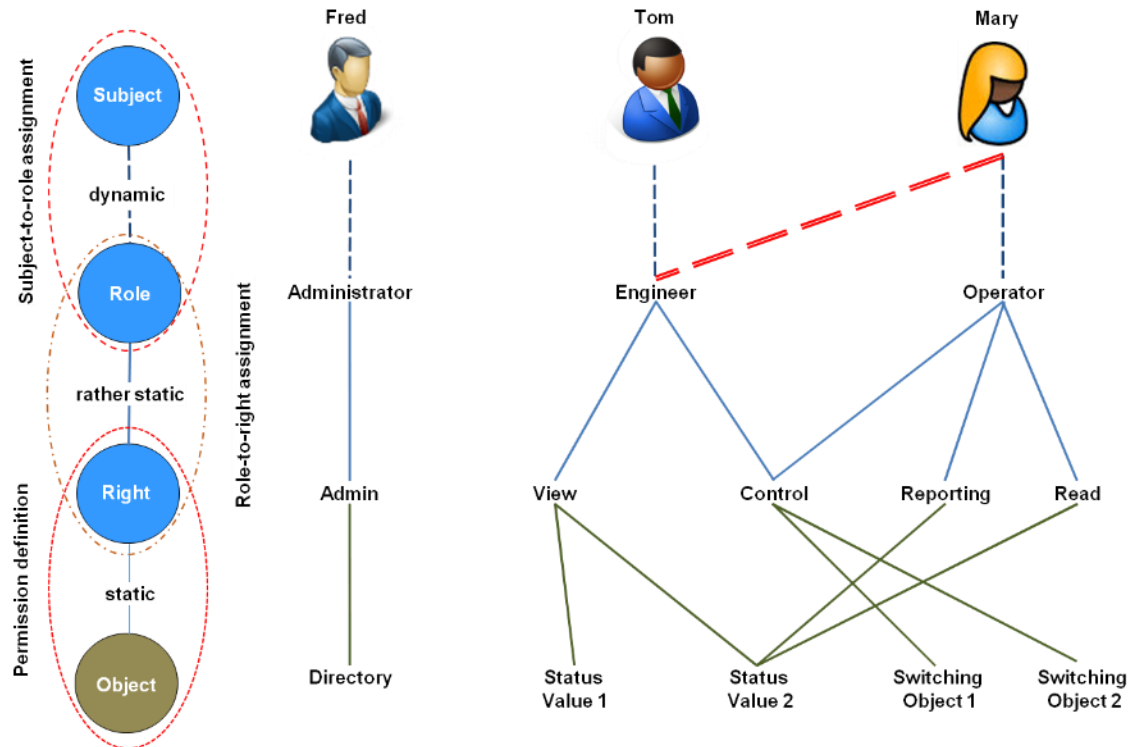
Application of certificates on the example of Role Based Access Control (RBAC) for operator and maintainer in power system management



IEC 62351-8 Role-based access control for power system management

There are two mappings to be configured by an administrator:

- Subject-to-role
- Role-to-right



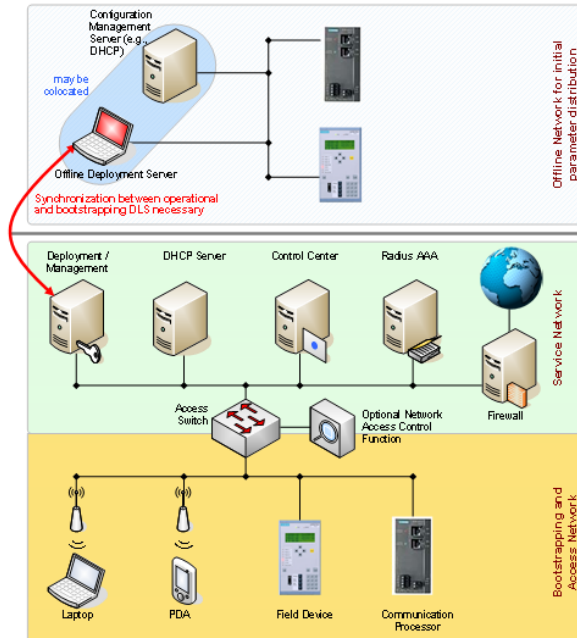
```

id-IEC62351 OBJECT_IDENTIFIER ::= { 1 2 840 10070 }
id-IECuserRoles OBJECT_IDENTIFIER ::= id-IEC62351 { 8 1 }
IECuserRoles ::= SEQUENCE OF UserRoleInfo
UserRoleInfo ::= SEQUENCE { -- contains the role information blob
-- IEC62351 specific parameter
userRole          SEQUENCE SIZE (1..MAX) OF RoleID
aor                UTF8String (SIZE(1..64)),
revision           INTEGER (0..255),
roleDefinition     UTF8String (0..23) OPTIONAL,
-- optional fields to be used within IEEE 1815 and IEC60870-5
operation          Operation OPTIONAL,
statusChangeSequenceNumber INTEGER (0..4294967295) OPTIONAL,
}
RoleId ::= INTEGER (-32768..32767)
Operation ::= ENUMERATED { Add (1), Delete (2), Change (3) }
    
```

Security bootstrapping requires procedural and technical means and needs to be considered during product design and commissioning

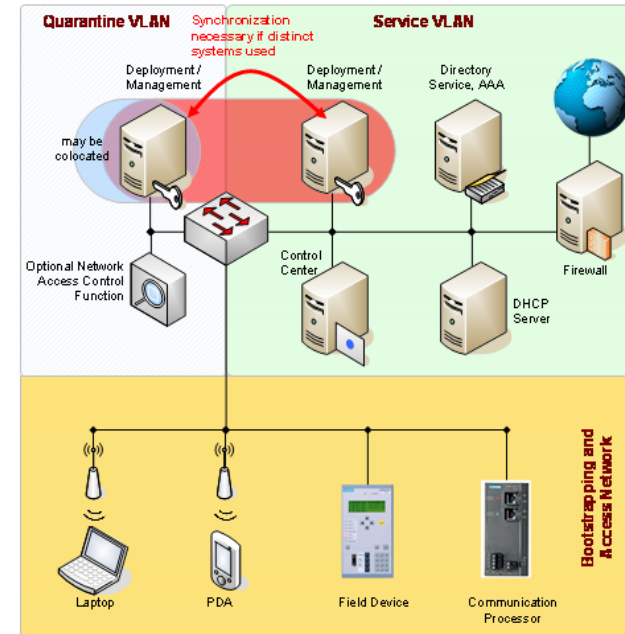
Security parameters are the basis to ensure appropriate protection of communication between different entities as well as services like licensing or anti counterfeiting.

Setting up security parameters securely is crucial!



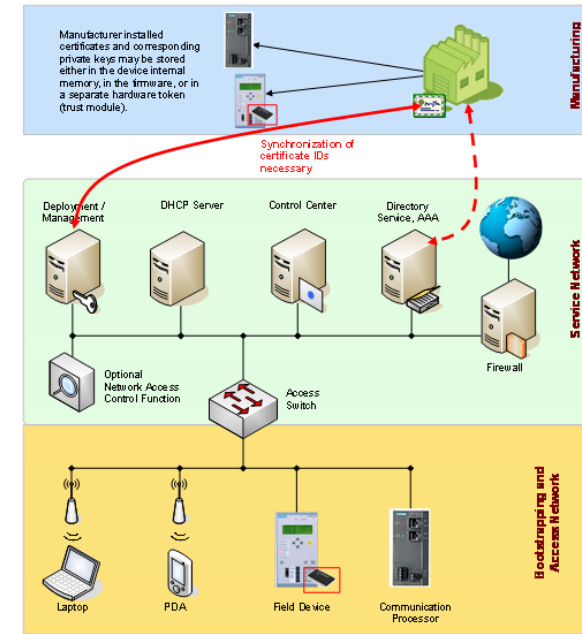
Offline parameter distribution

Engineering tools with security parameters sets directly connected to the device or via a separate network



Out-of-band parameter distribution

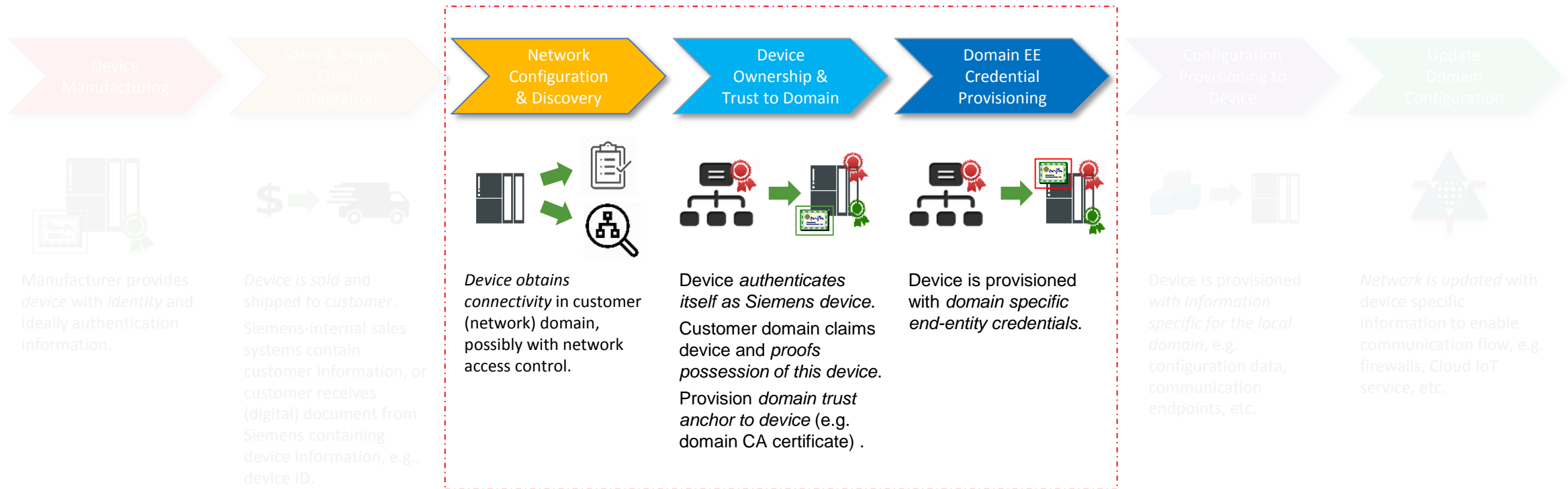
Separate logical communication channel used to configure security parameters. Devices may already possess a cryptographic credential, which can be provided by the device manufacturer.



In-band parameter distribution

Distribution using the same communication channels as used during regular operation, based on pre-configured device identifiers, manufacturer installed security credentials or even liaison devices.

Zero Touch Onboarding (ZTO) – enabling automated mutual trust establishment in the field



Mutually trustworthy establishment of operational security credentials (LDevID) based on manufacturer provided security credentials (IDevID). This is typically done in these phases of Zero Touch Onboarding (ZTO). Technically, this is supported e.g., by the IETF work on Bootstrapping Remote Secure Key Infrastructures (BRSKI) to allow for automated onboarding.

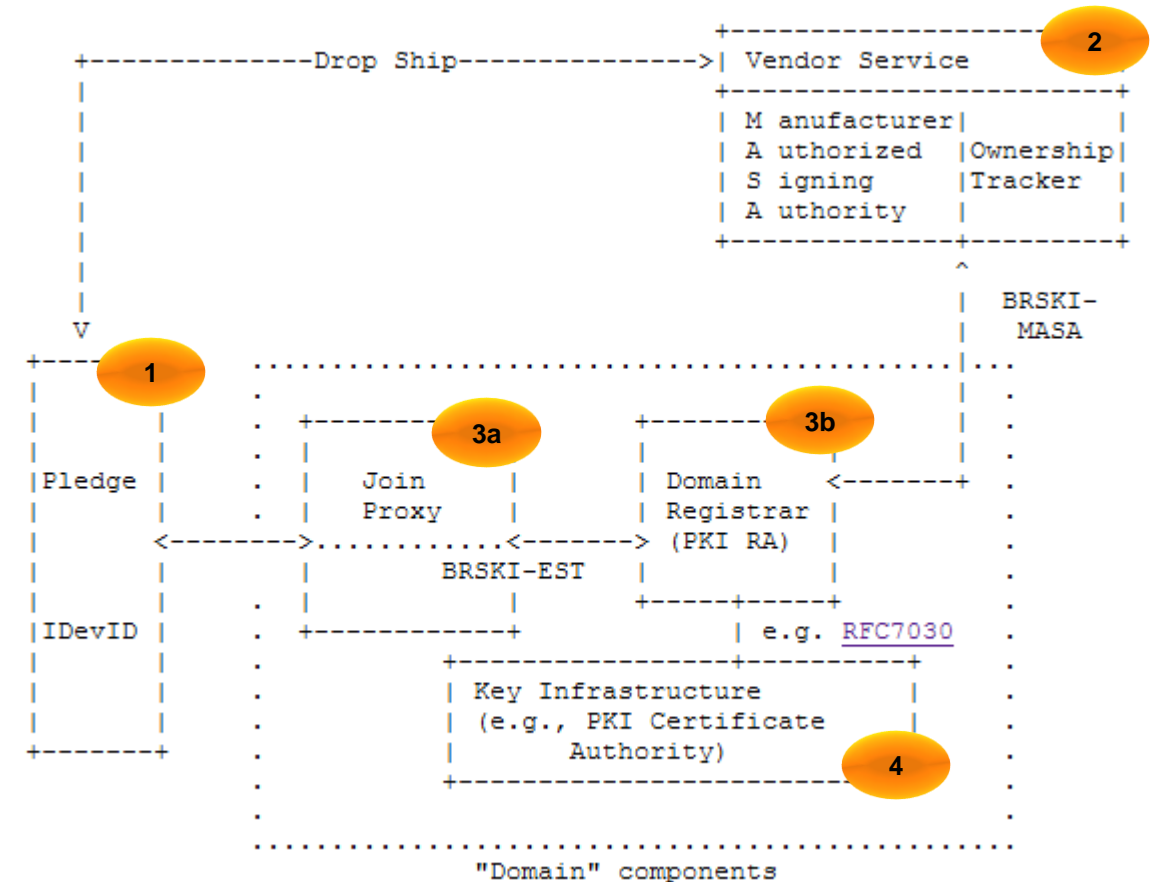
Example: Bootstrapping Remote Secure Key Infrastructures (BRSKI)

BRSKI is an IETF draft, to become RFC status soon

Components

1. **Device attempting to join the domain.**
Pledge possesses IDevID (EE Cert + Prov. Key, CA Cert)
2. **Manufacturer Service (MASA)**
Signing a voucher for manufacturer's pledges containing the target domains certificate.
3. **On-site services supporting the onboarding process.**
 - a. **Join proxy** facilitates the https connectivity between the pledge and the Domain Registrar by forwarding the packets back and forth.
 - b. **Domain registrar** interacts with BRSKI-MASA to retrieve the voucher and also with the RA/CA to get a site related certificate (LDevID) for the pledge.
4. **Public Key infrastructure** issues certificates for the target domain.

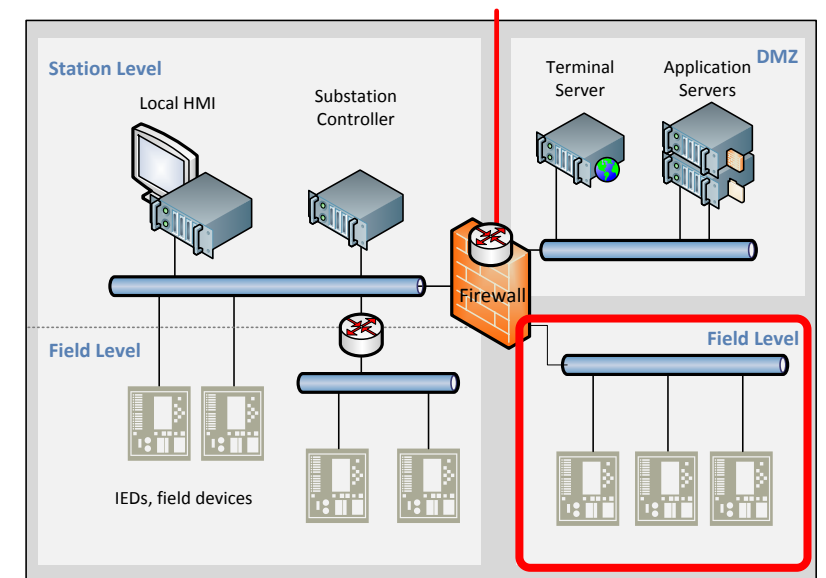
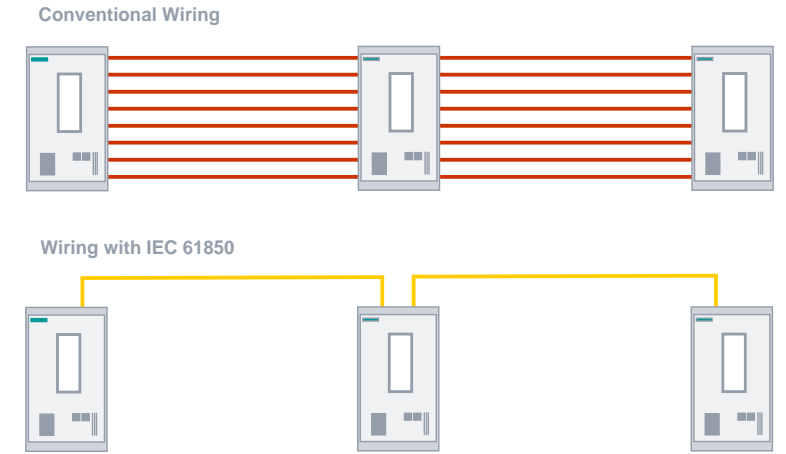
Interaction



Note the distribution of services on-site and off-site is use case specific.

Considering the embedding environment during the design of security measures is essential – Example (Substation) GOOSE

- Conventional wiring is replaced by Ethernet based communication using IEC 61850 with Generic Object Oriented Substation Events (GOOSE) and Sample Values (SV)
- Control model mechanism in which any format of data (status, value) is grouped into a data set and transmitted as set of substation events, such as commands, alarms, or indications.
- Usage of multicast transfer (device local subscription for events)
- Security requirement: source authentication and message integrity
- Initial solution approach
 - Digital signatures of the messages by the sender
 - Verification at subscriber / receiver site
- BUT
 - High performance requirements, e.g., sample rate of 80 samples per cycle → sums up to 4000 packets per second for the common frequency of 50 Hz
 - Field test have shown that the performance of typical field devices does not cope with the signature generation and verification

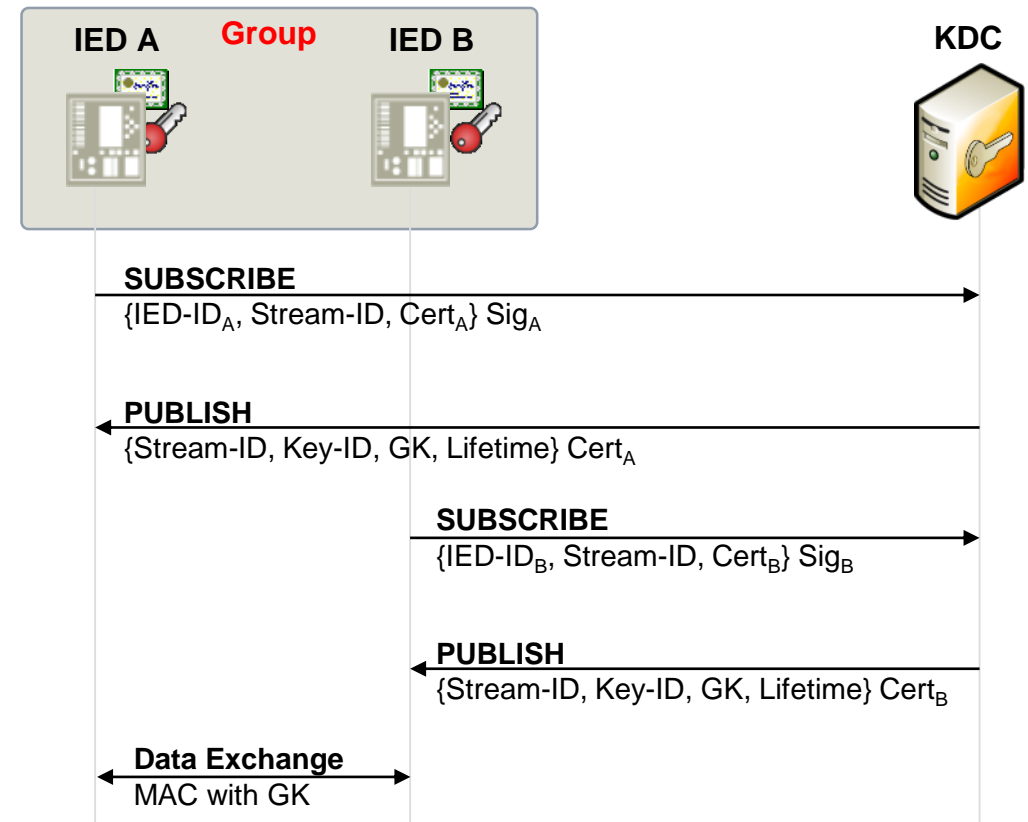


Considering the embedding environment during the design of security measures is essential – Example GOOSE (cont.)

- Alternative security approach: Group security
 - Rely on entity certificates and digital signatures for the initial key management and utilize symmetric key for integrity protection in operational phase
 - Key Management based on Group Domain of Interpretation (GDOI (RFC 6407) and additions in RFC 8052)
 - IED authenticate towards KDC using IED specific certificates and corresponding private keys
 - Integrity protection by using keyed hashes or symmetric algorithms in MAC mode (e.g., AES-GMAC)
- Results in
 - meeting performance requirements
 - source authentication during KDC subscription phase
 - communication failures/attacks cannot traced back to an individual IED

Key Distribution Center (KDC)

- configured data stream related IED access list
- generates data stream related (group) keys GK
- may be collocated with a distinct IED



Application of standards and guidelines

Enhancing IEDs in digital substations with cyber security

Mutually authenticated and encrypted communication line between DIGSI 5 and the SIPROTEC 5 device

Device-side support for role-based access control including central user management and emergency access

Recording of security-relevant events and alarms over Syslog and in non-volatile security log in device

Confirmation codes for safety-critical operations

Secure development
Patch management
Antivirus compatibility

Product hardening

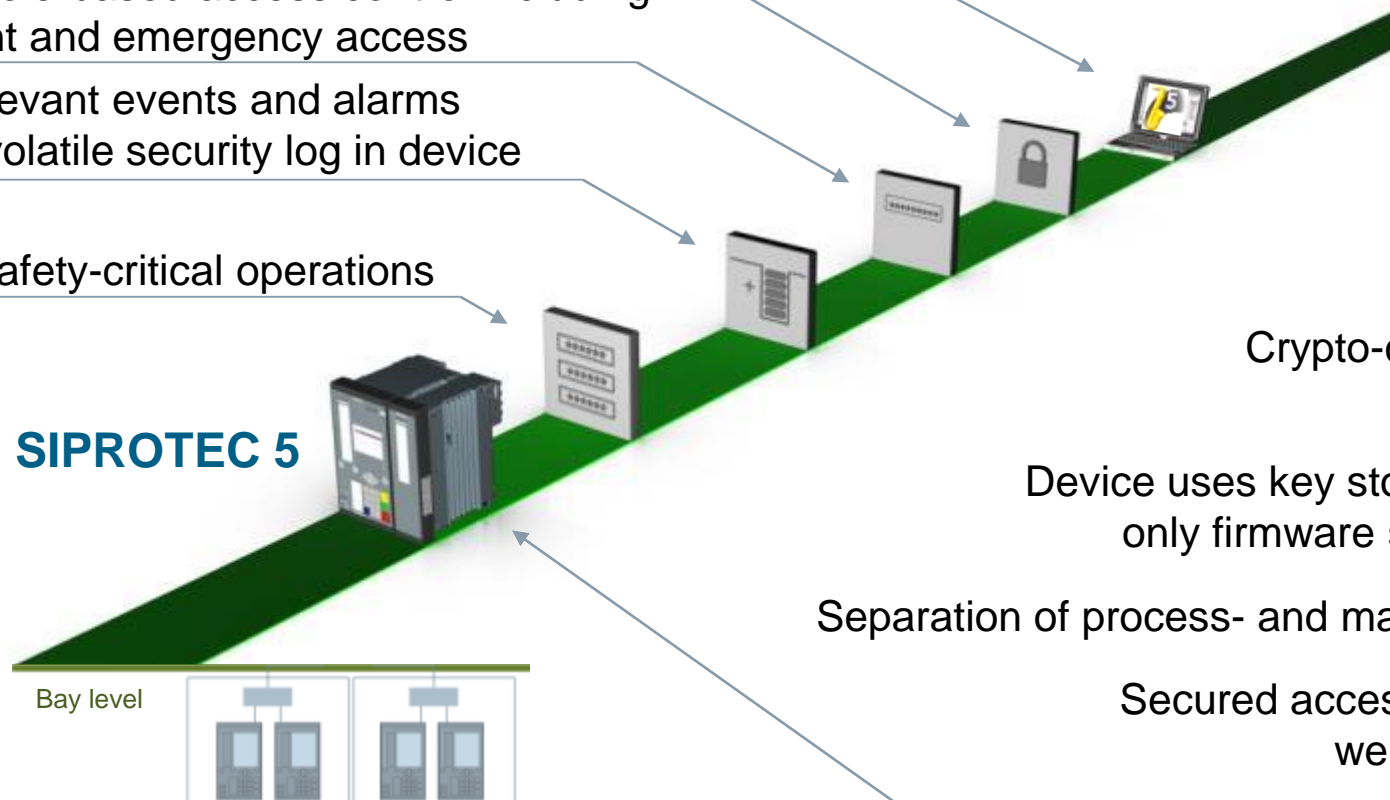
Independent testing

Crypto-chip for secure information storage and transmission

Device uses key stored in crypto-chip to allow only firmware signed by Siemens to load

Separation of process- and management communication

Secured access for HMI interactions and web-based device monitoring



SIPROTEC 5

Bay level

Siemens Cyber Security Framework – Defined security measures covering all security aspects

Organizational Security & Processes
People, Policies, Processes, Governance

- Organizational Preparedness
- Secure Development
- Secure Integration and Service
- Vulnerability and Incident Handling

Products & Systems
Common security technologies need to be implemented and contribute to the overall secure architecture

- Secure System Architecture
- System Hardening
- Access Control and Account Management
- Security Logging & Monitoring
- Data Protection and Integrity
- Security Patch Management
- Malware Protection
- Backup and Restore
- Secure Remote Access
- Privacy

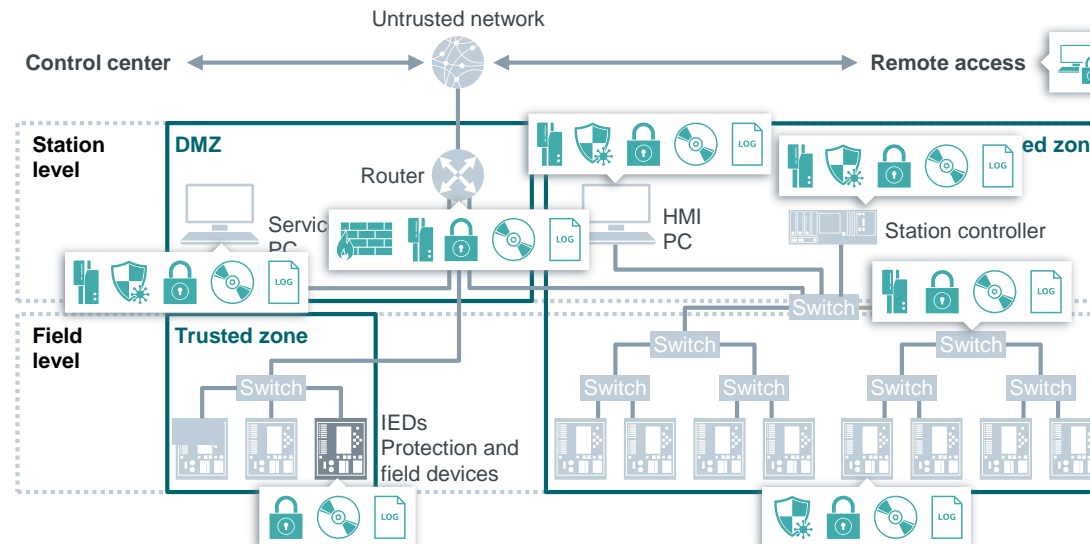
Energy Management uses these security measures to define security controls based on identified risks

Protecting Primary Substations Secure Substation Blueprint – Conforming to Standards



Siemens Digital Grid: ISO/IEC 27001
 • Information Security Management System

Cybersecurity for substations
 • IEC 62443-2-4: Integrator Process
 • IEC 62443-3-3 : Cybersecurity measures

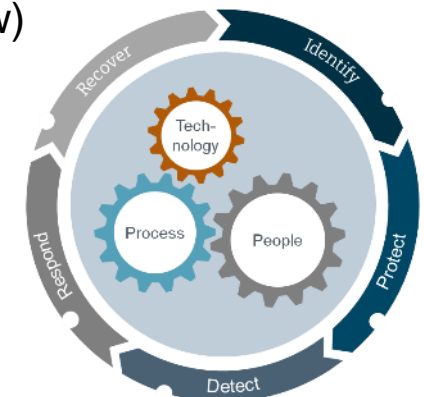


Cybersecurity Measures

- Access control and account management
- Security audit trail and monitoring
- System hardening
- Security patches, Backup und recovery
- Malware protection
- Data protection, data integrity, secure architecture
- Secured remote access

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 and requires appropriate means
- 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 (e.g., German IT-Security Law)
- Security-by-Design is essential to provide appropriate security features from the ground
- Cyber security needs a holistic approach – collaboration between vendors, integrators and operators; taking into account people, processes, and products in the specific domain
- Still, some challenges remain, like the migration from existing more closed environment to an open environment featuring appropriate cyber security measures



Contact Information



Siemens AG

Steffen Fries

Principal Key Expert

CT RDA CST

Otto-Hahn-Ring 6

81739 Munich

Germany

E-mail

steffen.fries@siemens.com

Internet

[siemens.com/corporate-technology](https://www.siemens.com/corporate-technology)

Siemens – Cyber Security

[siemens.com/digitalization/cyber-security.html](https://www.siemens.com/digitalization/cyber-security.html)