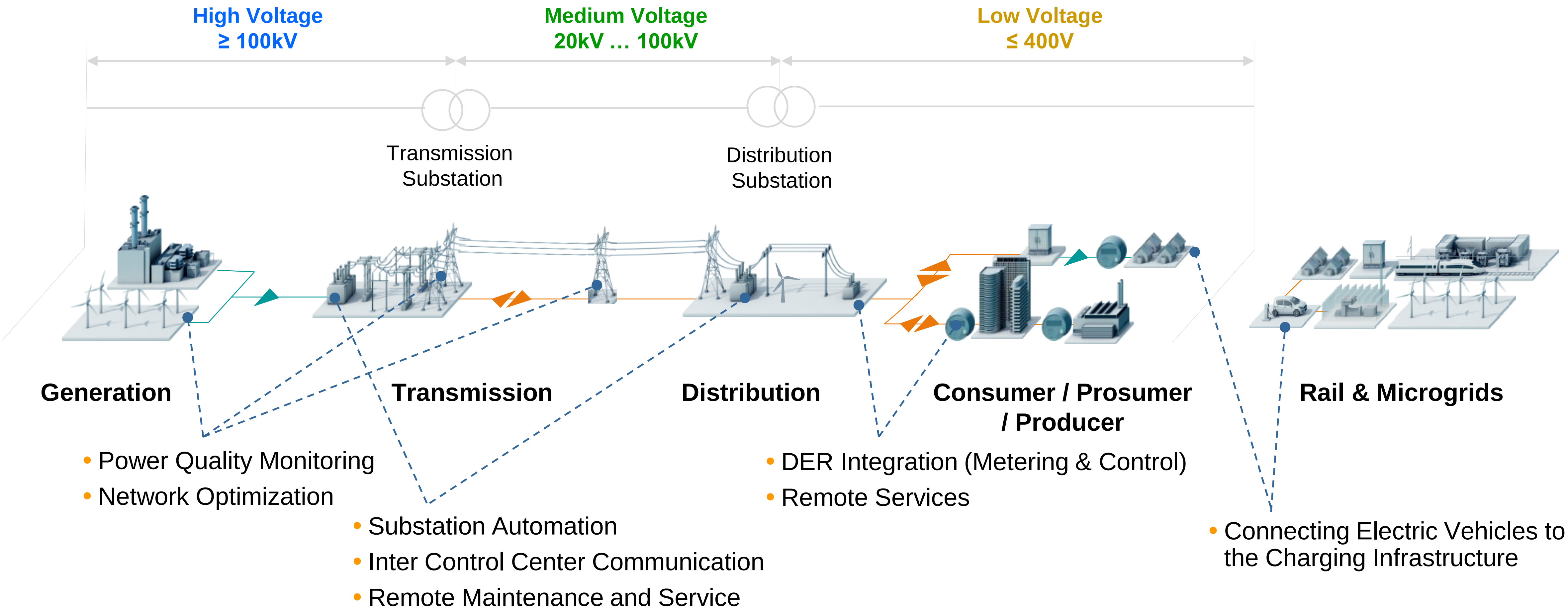
X.509 Applications in Power Systems

Steffen Fries, Siemens, T CST

May 09, 2022

Digital Power Grid – a critical infrastructure

Power system value chain and use case examples



High Voltage
≥ 100kV

Medium Voltage
20kV … 100kV

Low Voltage
≤ 400V

Transmission
Substation

Distribution
Substation

Generation

Transmission

Distribution

Consumer / Prosumer / Producer

Rail & Microgrids

- Power Quality Monitoring
- Network Optimization

- Substation Automation
- Inter Control Center Communication
- Remote Maintenance and Service

- DER Integration (Metering & Control)
- Remote Services

- Connecting Electric Vehicles to the Charging Infrastructure

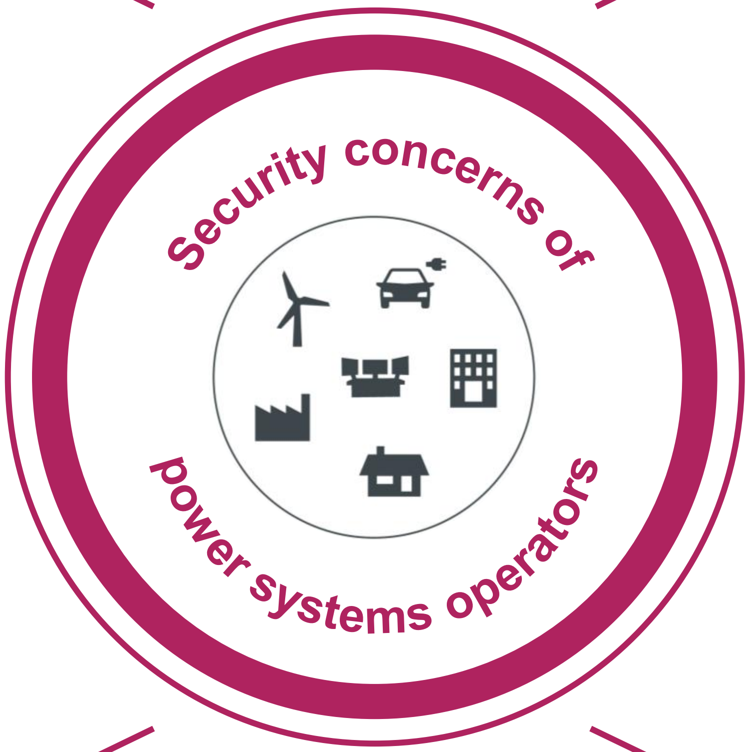
Cybersecurity for Power Systems

Challenges of Securing Digitalized Power Systems

Who and what are the entities in my digital grid? (relates to personal but also to devices)

Who and what has access to my OT? (may differ based on, e.g., location)

Can I trust my OT network?



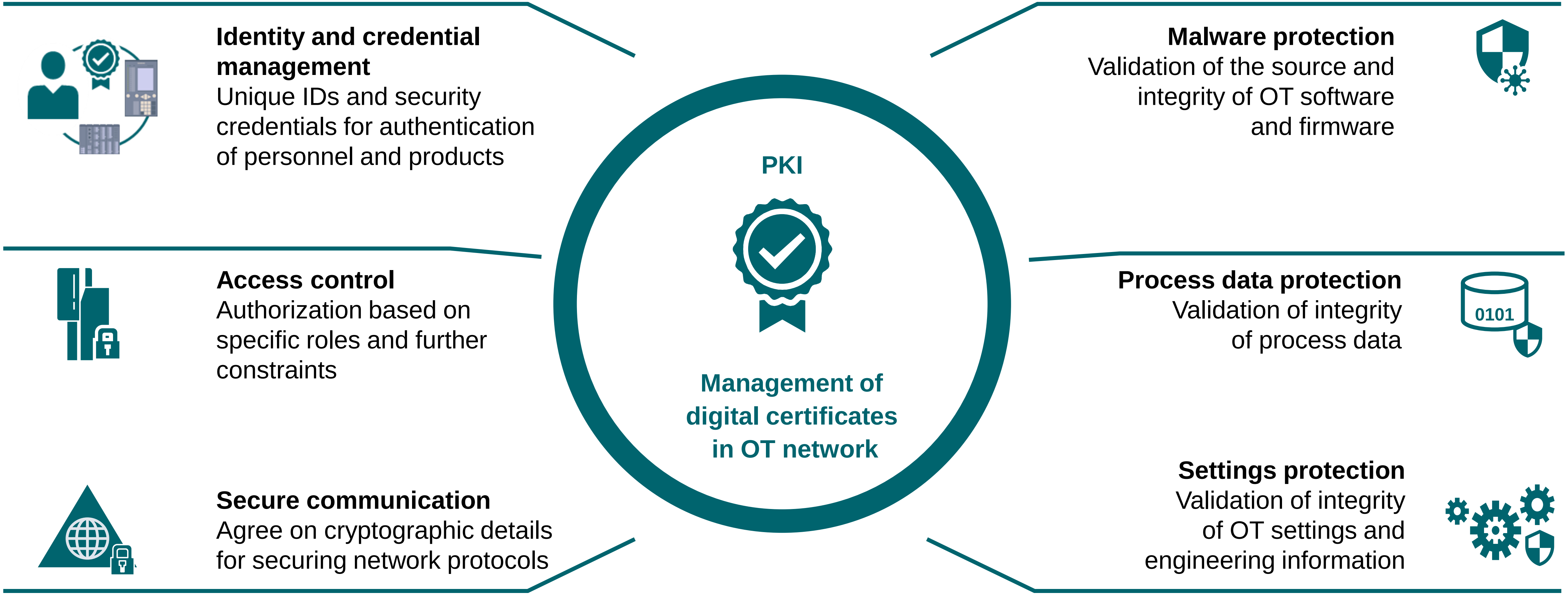
Can I trust the software and firmware running in my OT? (relates to device integrity)

Can I depend on my process data? (relates to data integrity)

Are my critical operational settings intact? (relates to data integrity)

Cybersecurity for Power Systems

X.509 Certificates make Security Controls Manageable



Identity and credential management
Unique IDs and security credentials for authentication of personnel and products

Access control
Authorization based on specific roles and further constraints

Secure communication
Agree on cryptographic details for securing network protocols

PKI

Management of digital certificates in OT network

Malware protection
Validation of the source and integrity of OT software and firmware

Process data protection
Validation of integrity of process data

Settings protection
Validation of integrity of OT settings and engineering information

[1] PKI: Public Key Infrastructure

Core Communication Standards for Digital Grids

IEC TC57 Reference Architecture with domain-specific Cybersecurity

Scope

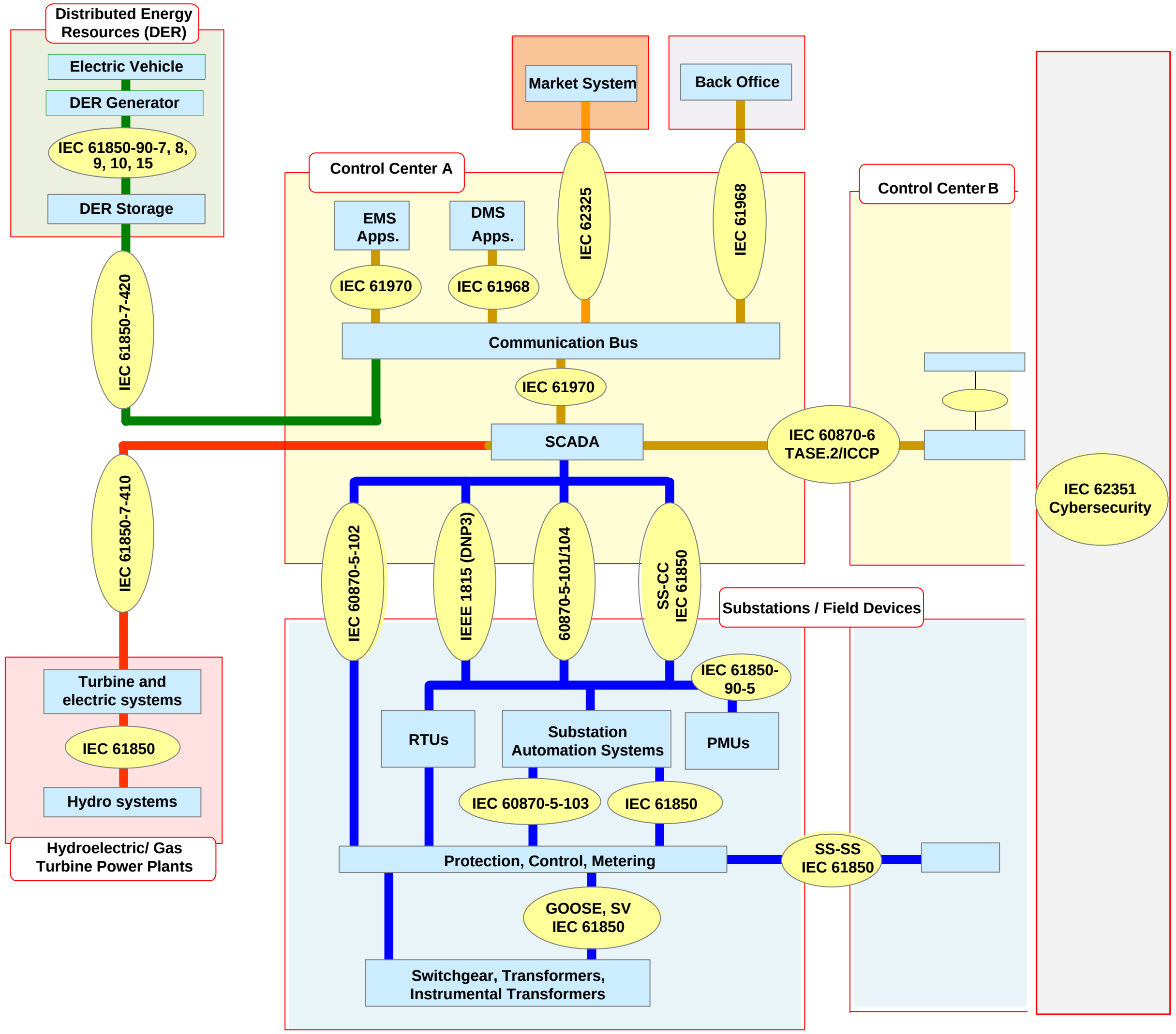
- Development of IEC 62351 to secure communication protocols defined by IEC TC 57, specifically
  - IEC 60870-5 and IEC 60870-6 series,
  - IEC 61850 series,
  - IEC 61968 & IEC 61970 series.

IEC 62351 defines means for

- Authentication and authorization (RBAC[1])
- Secure IP-based and serial communication
- Secure application level exchanges
- Security monitoring and event logging
- Testing defined approaches
- Guidelines for applying specific security measures

by utilizing or profiling

- existing standards and recommendations



[1] RBAC = Role-based Access Control

X.509 supports addressing the Security Challenges in Power System

Application and Enhancements in IEC 62351 (I)

- Identification and authentication
  - Application of X.509 public key certificates to identify and authenticate user and devices
  - Used in the context of communication protocols to protect the session parameter negotiation

- Authorization
  - Application of IEC 62351 defined extensions in *public-key certificates* and *attribute certificates* to support role-based access control taking domain specifics into account.

```
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 (SIZE(0..23)),
   -- optional fields to be used within IEEE 1815 and IEC60870-5
   operation        Operation OPTIONAL,
   statusChangeSequenceNumber INTEGER (0..4294967295) OPTIONAL,
}
```

  - Specifically attribute certificates provide support for short validity assignments of roles.

X.509 supports addressing the Security Challenges in Power System

Application and Enhancements in IEC 62351 (II)

- Authorization (cont.)
  - Authorization validation lists (AVL) have been introduced in IEC 62351 to address requirements for fine granular acceptance of certificates either issued from a CA or even self-signed certificates.
  - The general concept has been taken over into ITU-T X.509 (2019) as `CertAVL`
  - IEC 62351-9 defines extensions to the `CertAVL` to further restrict the usage of certificates, e.g., to a specific scope (area of responsibility) or to selected domain specific protocols.

- Communication security
  - IEC 62351 relies on mutual authentication and protection of the handshake using X.509 in protocols like TLS[1], group key distribution using GDOI[2], and also domain specific telecontrol protocols like IEC 60870-5 or IEC 61850

[1] TLS = Transport Layer Security, IETF RFC 8446
[2] GDOI = Group Domain of Interpretation, IETF RFC 6407

X.509 supports addressing the Security Challenges in Power System

Application and Enhancements in IEC 62351 (III)

- Process data security
  - IEC 62351 further specifies application of XML security means for data containerized in XML based on X.509 credentials. This approach is intended to secure data exchanged between utilities.
  - Besides the processing of data, also the monitoring and security event handling is important, to get early information about potential deviations from the expected system behavior. Here, X.509 is employed in the key management to secure the logging data (syslog-over-TLS).
- X.509 credential management
  - IEC 62351 relies on the availability of a PKI, which supports online and offline operation from a central location. Therefore specific PKI functionality needs to be available on site, e.g., in a substation.
  - IEC 62351 strongly recommends the usage of X.509 credentials for devices in the complete lifecycle starting from the manufacturer for initial credentials to the operator for providing and maintaining operational credentials. For this it relies on IETF standardized protocols for enrollment (EST, SCEP), revocation handling (CRL, OCSP) and trust anchor handling (TAMP).

[1] GDOI = Group Domain of Interpretation, RFC 6407

X.509 application example

X.509 contributes to secure power system communication in various ways

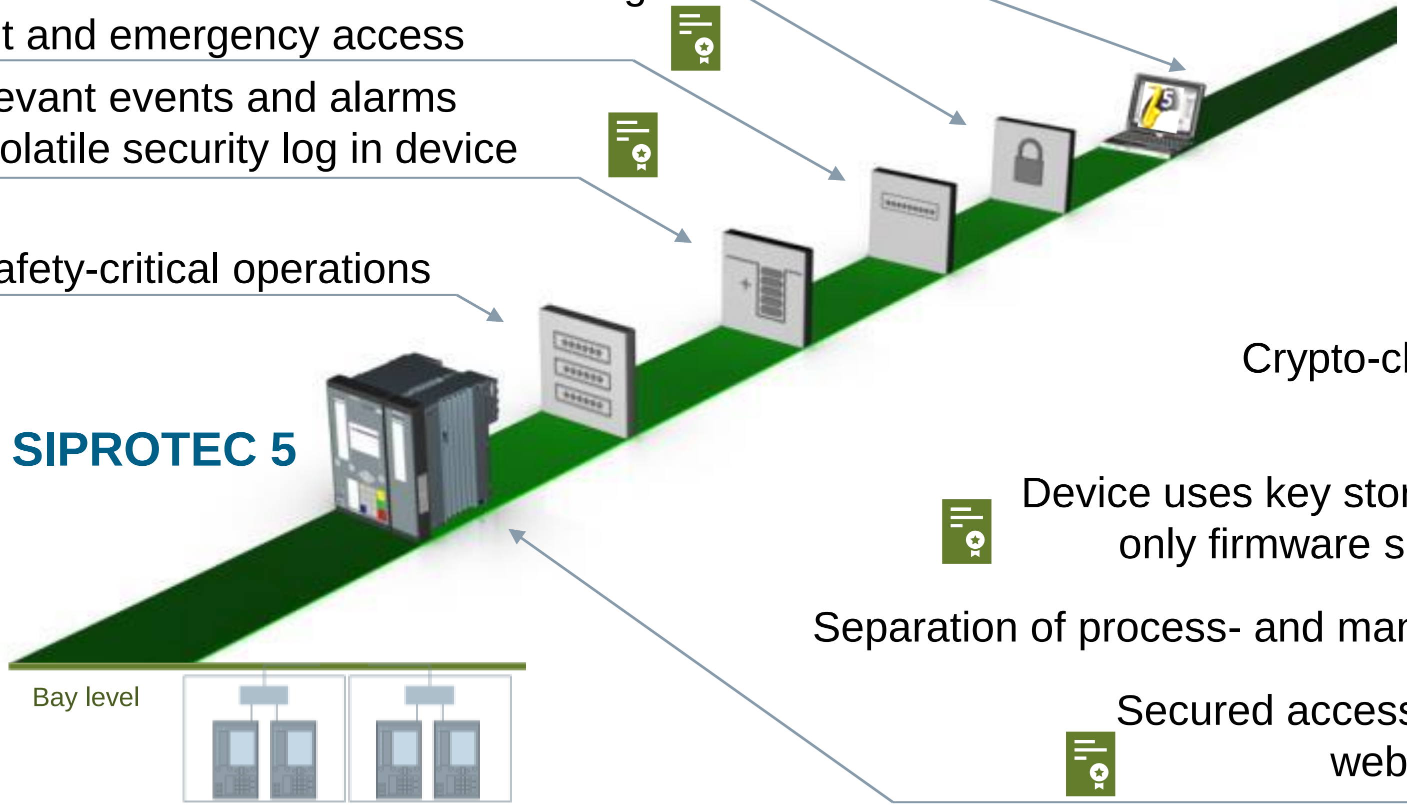
Technical Measures according to IEC 62351

Mutually authenticated and encrypted communication line for operational protocols and engineering

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

Virus protection

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

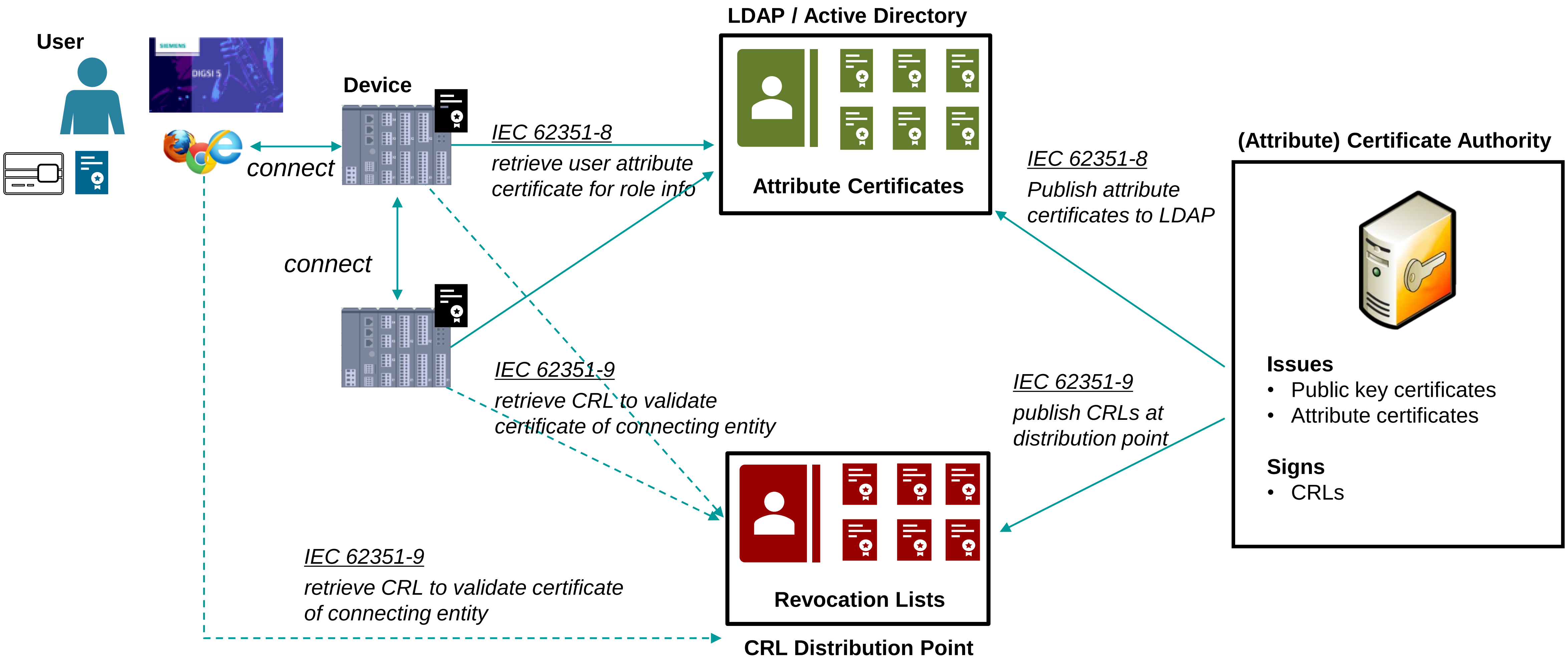
Secured access for HMI interactions and web-based device monitoring

Measures for product lifecycle supported by requirements from IEC 62443

X.509 Application

X.509 application example

IEC 62351 Workflow for RBAC based on X.509 attribute certificates



User

connect

Device

connect

IEC 62351-8
retrieve user attribute certificate for role info

LDAP / Active Directory

Attribute Certificates

IEC 62351-8
Publish attribute certificates to LDAP

(Attribute) Certificate Authority

Issues
- Public key certificates
- Attribute certificates

Signs
- CRLs

IEC 62351-9
retrieve CRL to validate certificate of connecting entity

IEC 62351-9
publish CRLs at distribution point

IEC 62351-9
retrieve CRL to validate certificate of connecting entity

Revocation Lists

CRL Distribution Point

Entity certificate

Attribute certificate

X.509 application example

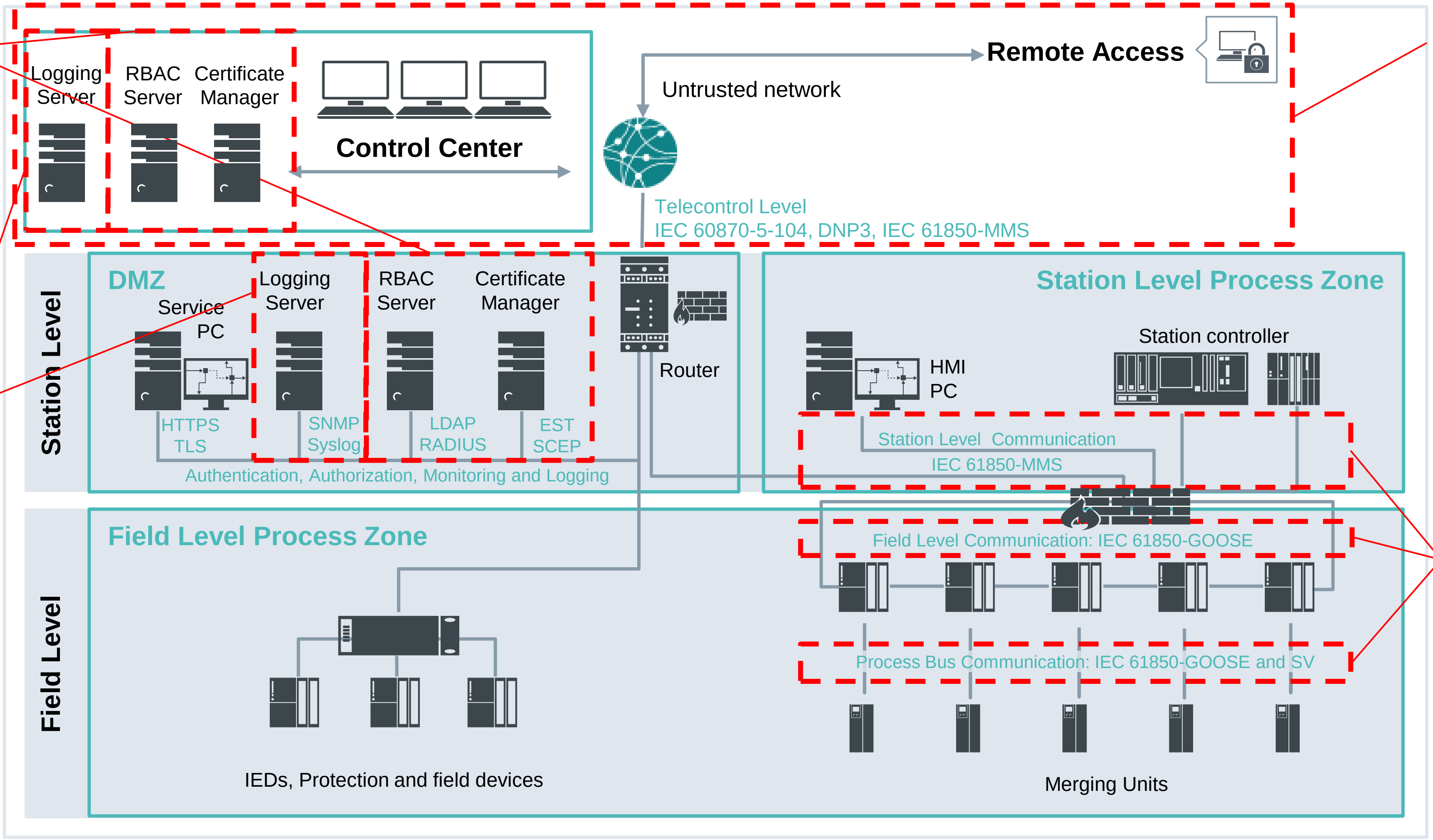
Substations incorporate PKI components to maintain X.509 credentials

Specification of technical solutions for an infrastructure supporting certificate based authentication and authorization (PKI, RBAC)

IEC 62351-8/9

Monitoring & Audit Adaptation and enhancement of existing infrastructures and technologies for network management using SNMP and syslog

IEC 62351-7/14



Securing telecontrol and control center communication using TLS and / or security measures on application level

IEC 62351-3/4/5/9

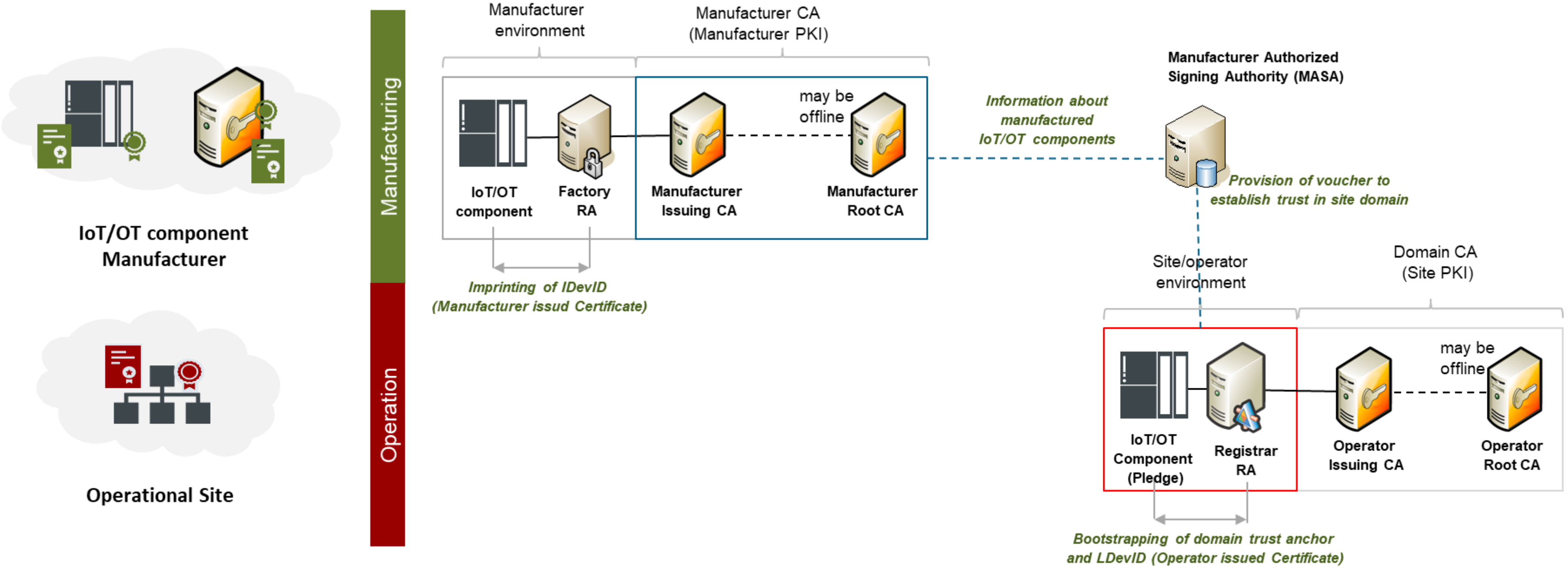
Protection of process level and field level communication with real-time constraints using appropriate security measures

IEC 62351-3/4/5/6/9

Outlook for further X.509 application in Power System

Automation of security credential bootstrapping

- Bootstrapping of security credentials typically increases the effort for service technicians during installation. Automated bootstrapping makes it transparent to the technician.
- Zero touch onboarding approaches currently defined in the IETF leverage the existence of device certificates and utilizes a *provisional accept* of X.509 domain certificates to establish trust. Provisional accept = preliminary acceptance of a peer certificate, until root certificate is provided in an automated and trustful way to enable peer certificate verification.
- Example approach from Bootstrapping of Remote Secure Key Infrastructures (BRSKI, IETF RFC 8995).



IoT/OT component Manufacturer
Operational Site
Manufacturing
Operation
Manufacturer environment
Manufacture CA (Manufacturer PKI)
IoT/OT component
Factory RA
Manufacturer Issuing CA
may be offline
Manufacturer Root CA
Imprinting of IDevID (Manufacturer issud Certificate)
Information about manufactured IoT/OT components
Manufacturer Authorized Signing Authority (MASA)
Provision of voucher to establish trust in site domain
Site/operator environment
Domain CA (Site PKI)
IoT/OT Component (Pledge)
Registrar RA
Operator Issuing CA
may be offline
Operator Root CA
Bootstrapping of domain trust anchor and LDevID (Operator issued Certificate)

Contact

Steffen Fries
Principal Key Expert

Technology – Cybersecurity & Trust
Otto-Hahn-Ring 6
81739 Muenchen, Germany
Mobile: +49 (89) 7805-22928
E-mail: steffen.fries@siemens.com