

Presenter: Dr. Hans-Joachim Herrmann, Energy Automation, Nuremberg

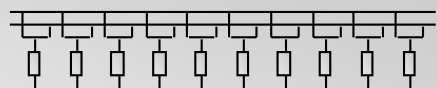
Security Management for Substation Automation and Protection

Substation Automation and Protection of Today

1st generation:
Standard cabling

Ancient past

Mimic board

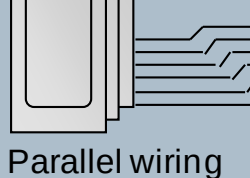


Fault recorder
Protection



Parallel wiring

Bay



2nd generation:
Point-to-point connections
since 1985

Recent past



Substation
controller

Other bays

Serial connection

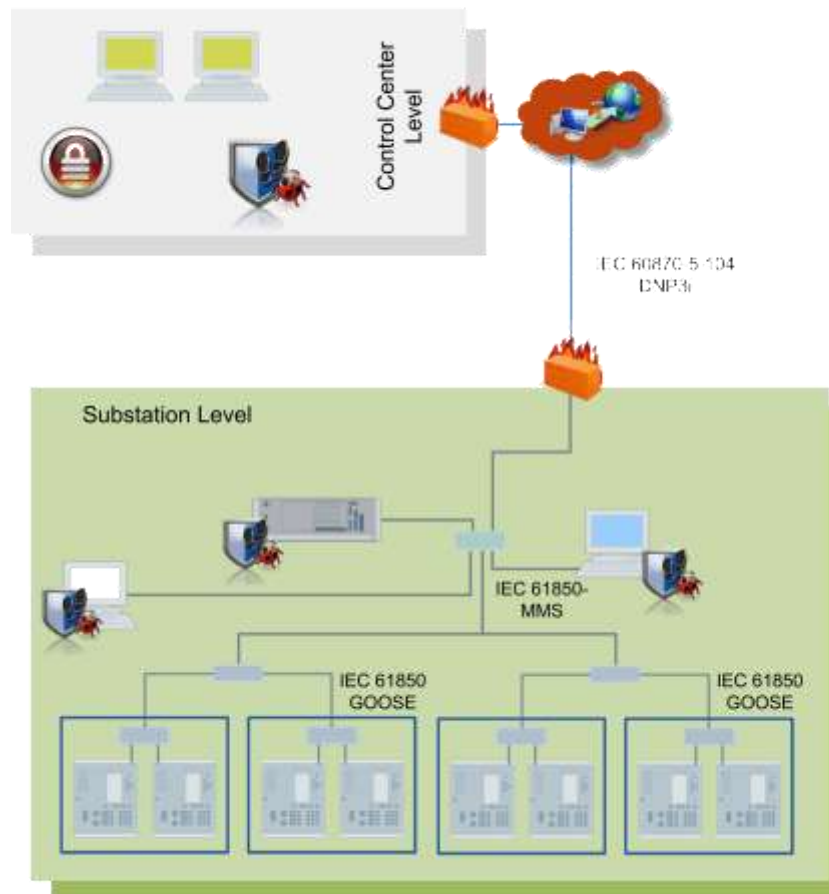


Parallel wiring

Bay



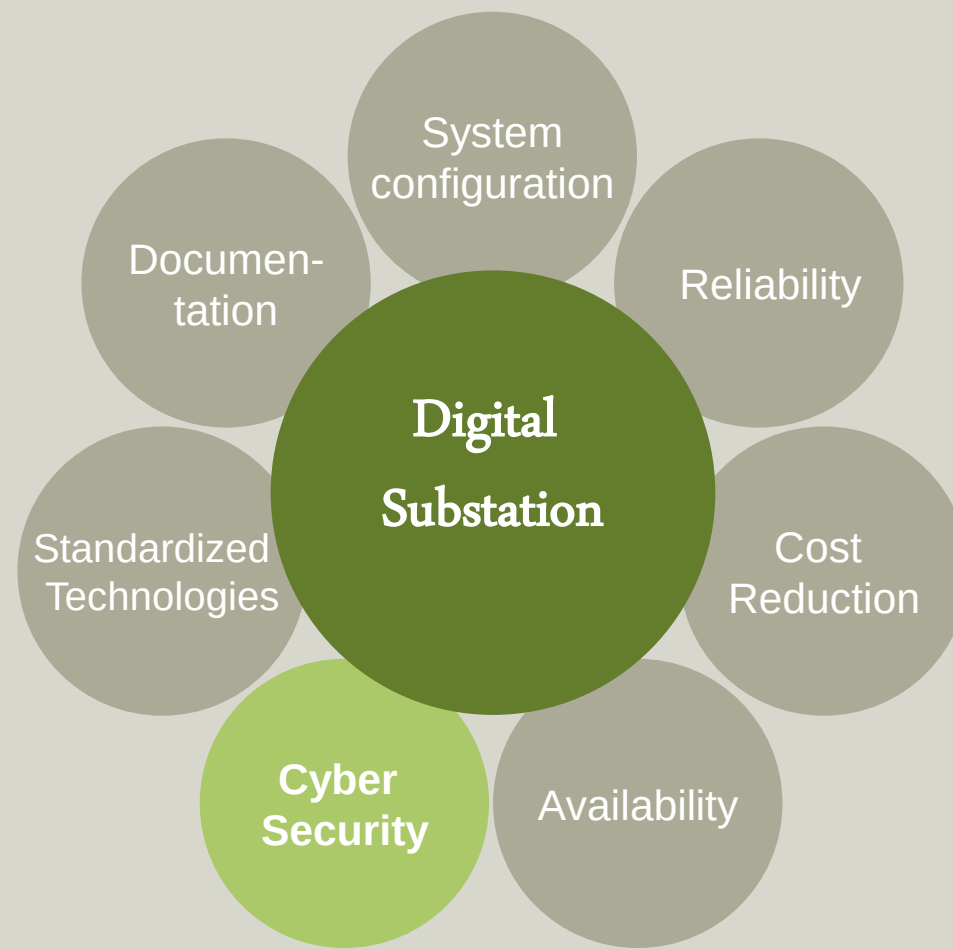
3rd Generation: Digital Substations



- Account Management
- Malware Protection
- Virtual Private Network (VPN)
- Firewall with n-ports
- Untrusted network
- Trusted Zone
- Switch
- Protection Device Field Device
- Substation Controller
- Local HMI
- Engineering PC

Digital Substation: One Goal many Aspects

Aspects of the Digital Substation



Security Threats

Critical Infrastructure Operators have Good Reasons to Fear

SIEMENS

'Night Dragon' Attacks Threaten Major Energy Firms

New advanced persistent threat (APT) attack combines a variety of vectors, seeks to steal sensitive data, McAfee researchers say

Feb 11, 2011 | 12:13 AM |

By Tim Wilson

September 29, 2010

Reports: SCADA-Attacking Worm Infects Computers at Iran Nuclear Reactor

POWERnews



Sandworm Zero Day Used to Target CIMPLICITY SCADA Systems

October 17, 2014

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries: default password - Finds results with "default password" in the banner; the named defaults might work!

'Nitro' Attacks: China-Based Hacker Targeted Chemical Firms, Symantec Reports

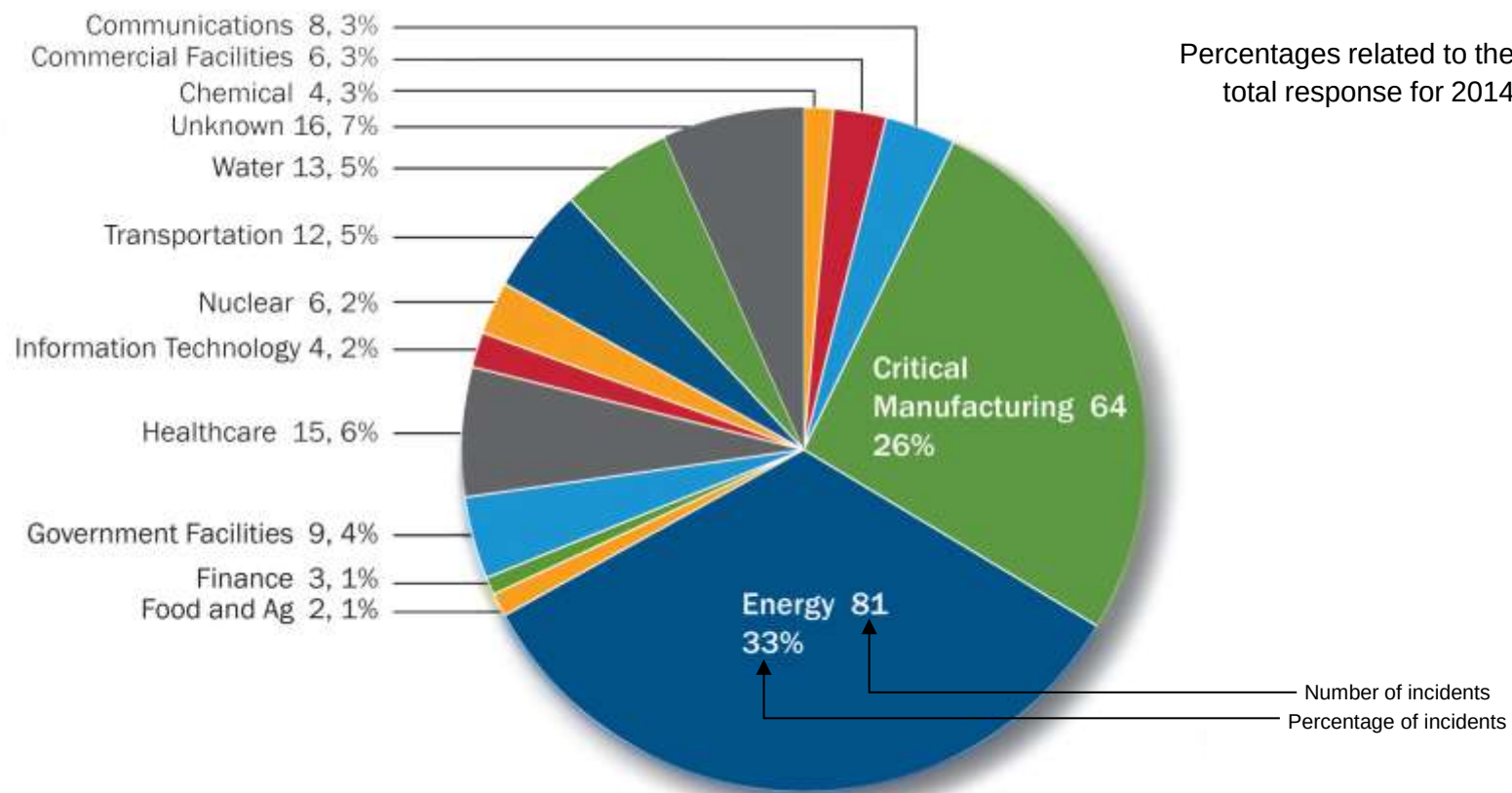


First Posted: 10/31/11 04:59 PM ET | Updated: 10/31/11 04:59 PM ET

Security Threats

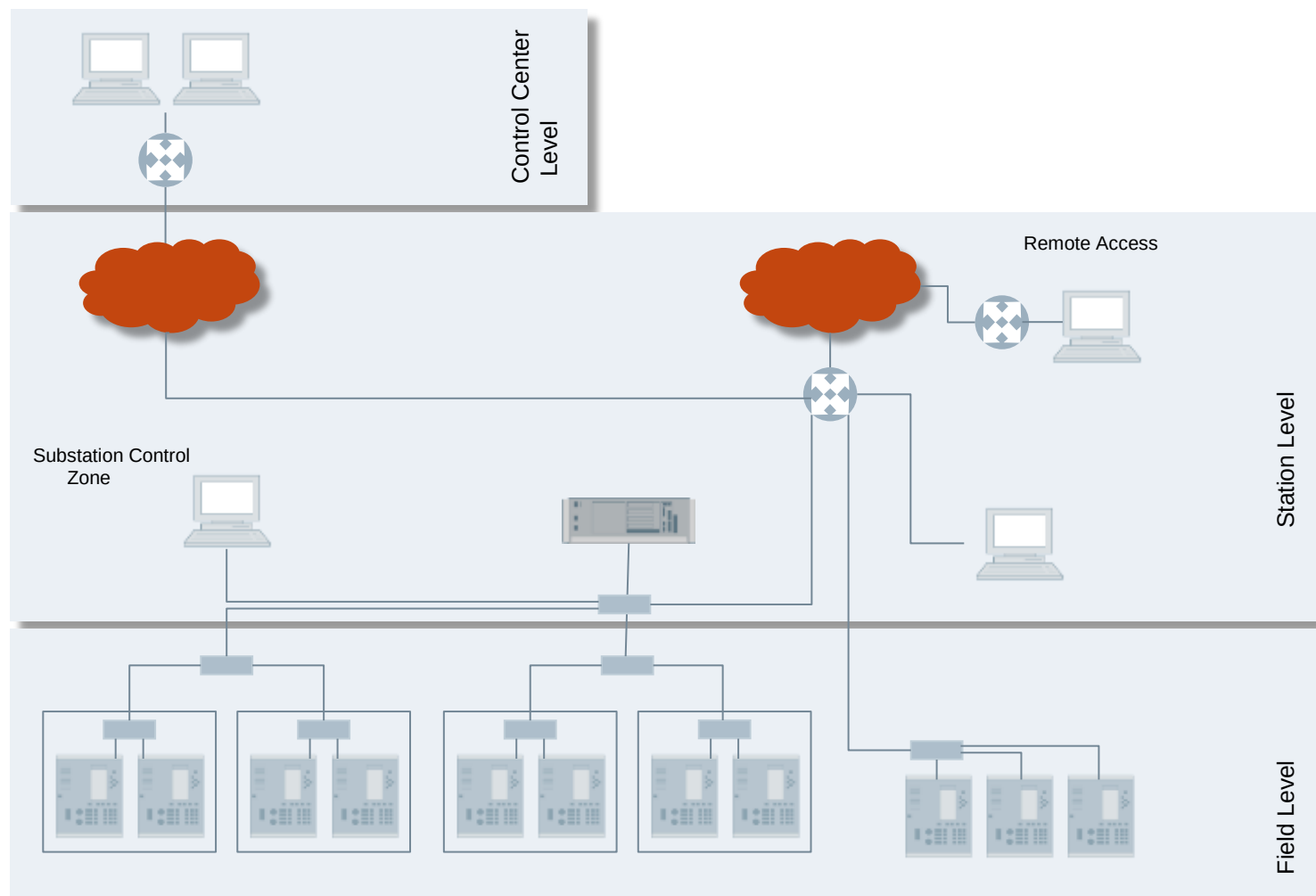
The Energy Sector is a Prime Target

ICS-CERT Responses to sector specific cyber security threats across the critical infrastructure sectors in the U.S. in 2014



Digital Substations are vulnerable to Cyber Attacks

Context of a Digital Substation



Context:

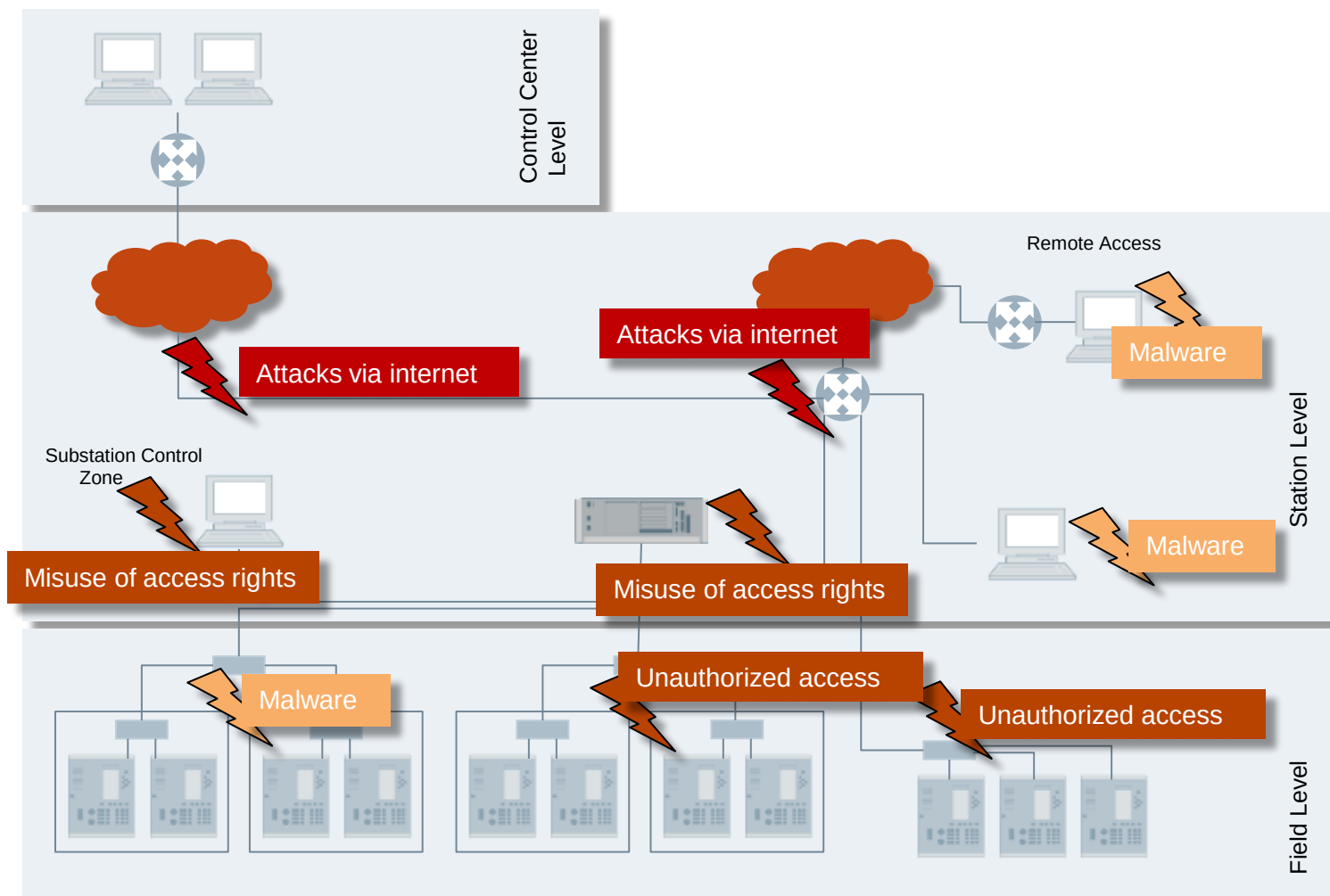
- Critical infrastructure
- 24h/7days Operational availability
- Interfaces to unsecure networks
- Interfaces to office networks
- Legacy components
- Mix of components from different vendors with different technologies

Digital Substations are vulnerable to Cyber Attacks

Possible Threats and Attackers

Possible Attackers:

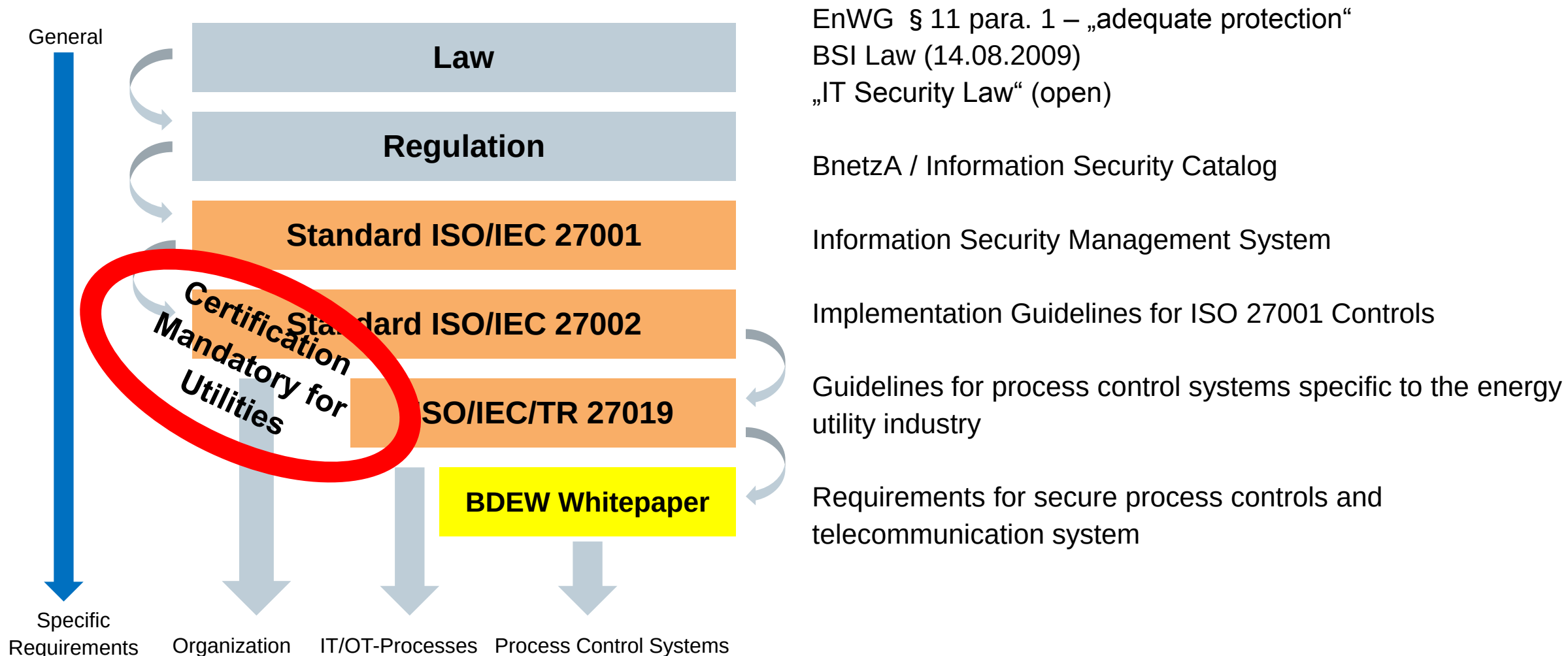
- States
- Criminal organizations
- Script kiddies
- Insider



Cyber Regulations & Standards

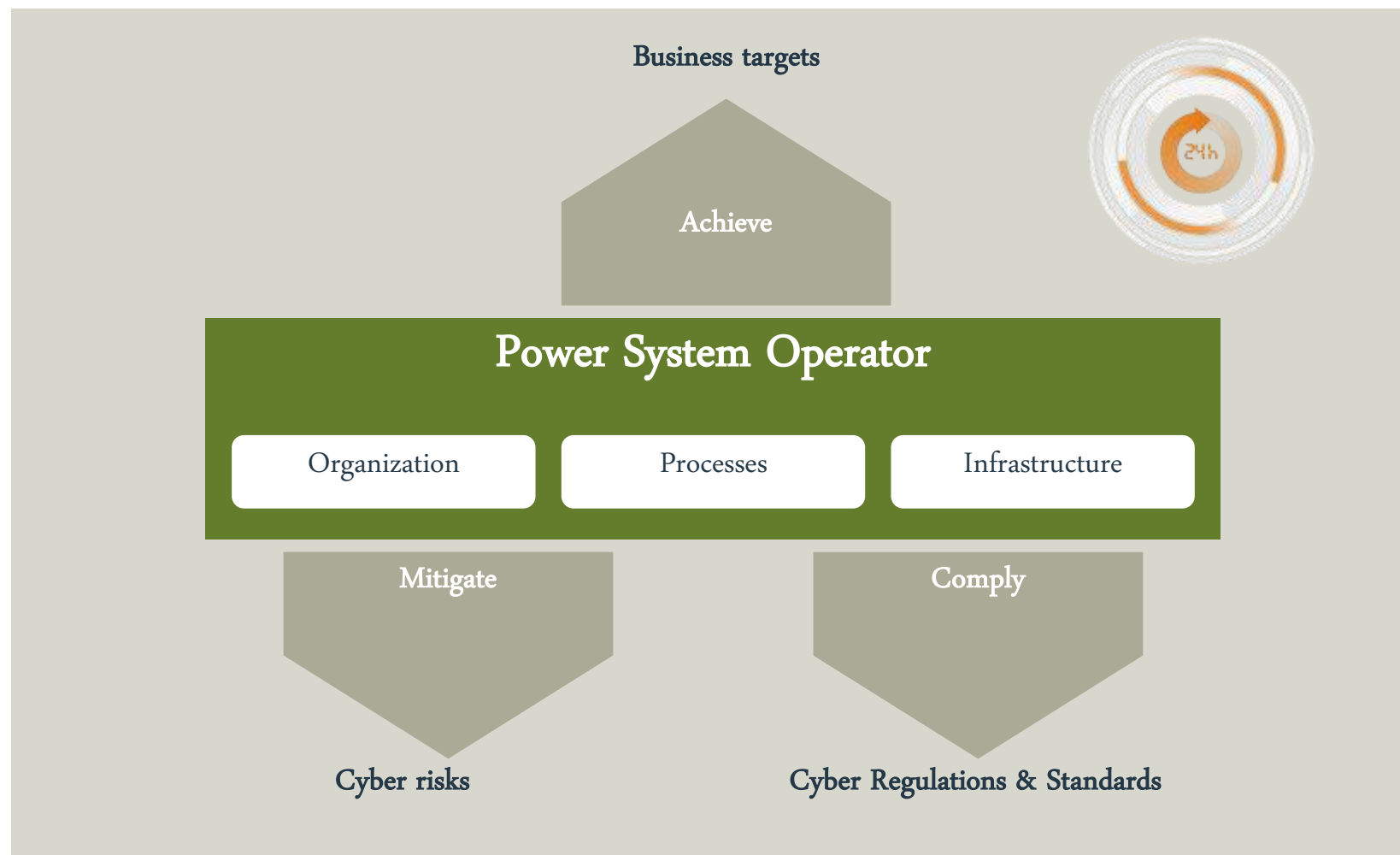
Regulation makes implementation of ISMS mandatory

Example of Cyber Regulation from Germany



Security is a must for Digital Substations

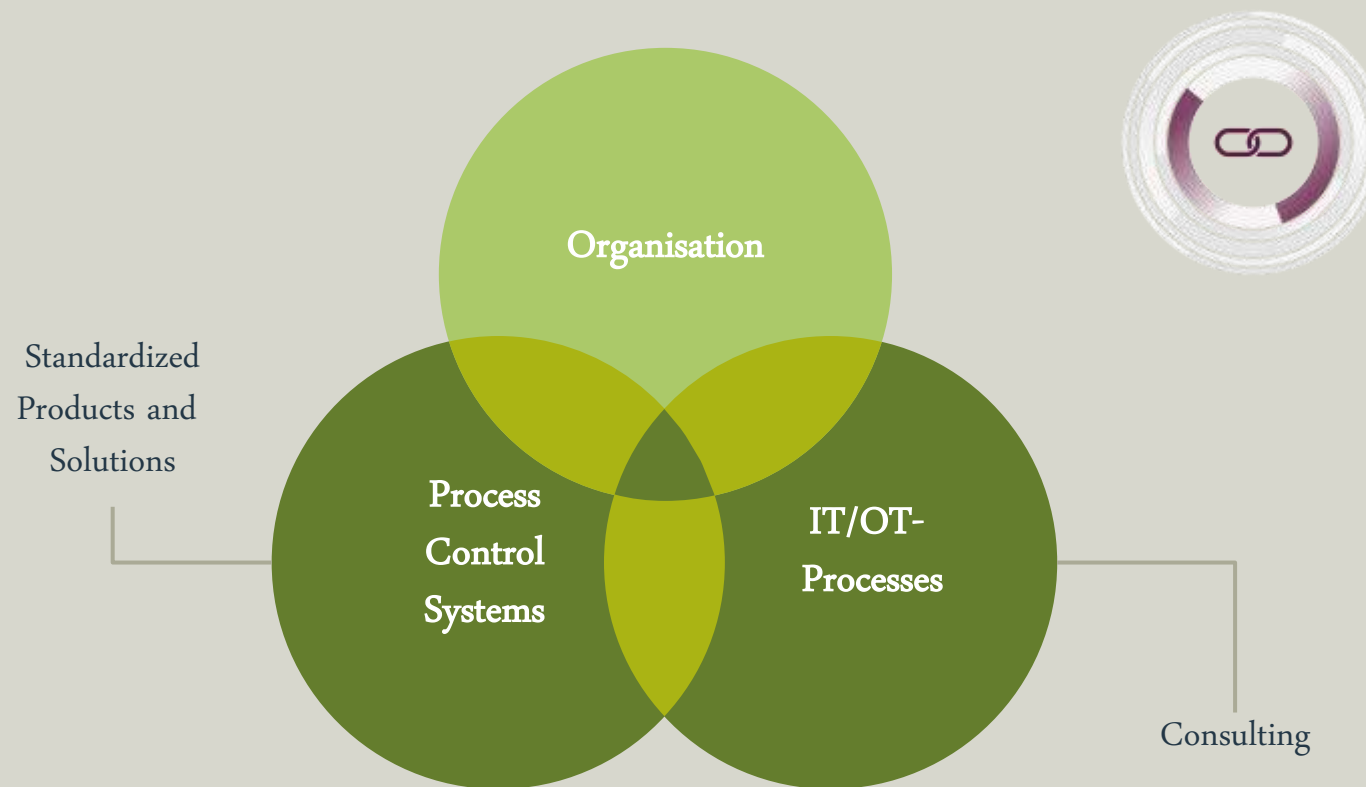
Are you prepared
for Cyber Security?



Security is a must for Digital Substations

Regulatory Compliance is a must for Operators

Operators need trustworthy
and competent partners —
who deliver secure products
and solutions



Vendors play an important role in enabling operators to achieve their cyber security goals

Equipping Digital Substations with Cyber Security

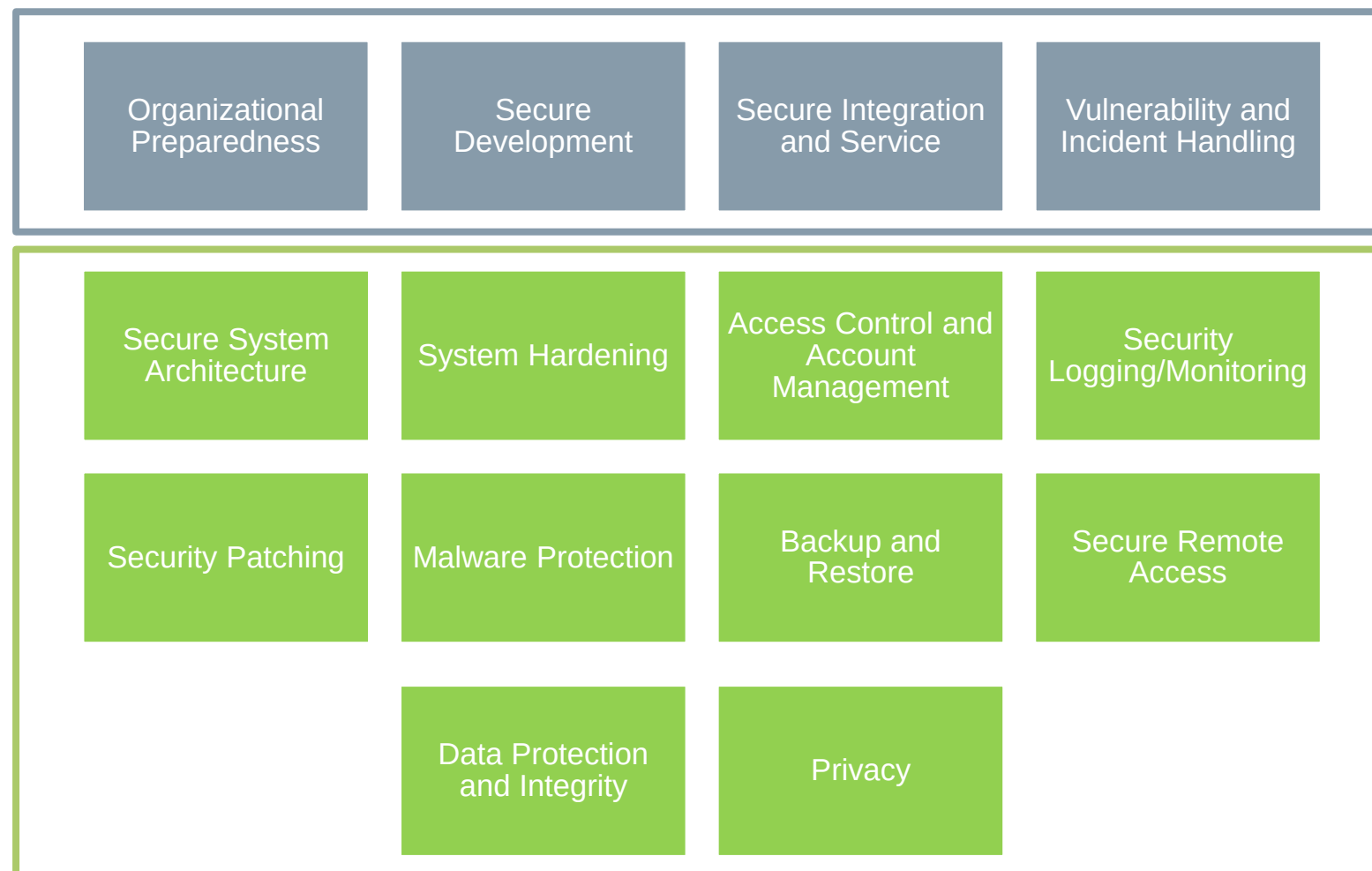
Substation Automation & Protection Vendor Responsibilities

Policies, Processes and Procedures

- Organizational security, secure development and integration, vulnerability and incident handling

Security Technologies

- Common security technologies need to be implemented and contribute to the overall secure system architecture



Equipping Digital Substations with Cyber Security

Secure Products as a Basis for Secure Substations

Encryption of the communication line
between DIGSI 5 and the SIPROTEC 5 device

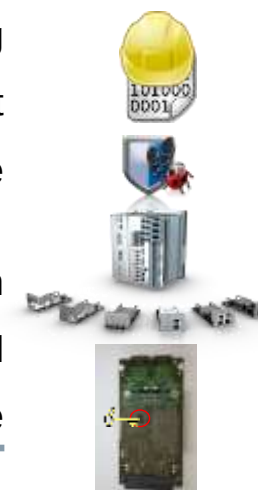
Connection password according to
Regulations and Standards

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

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



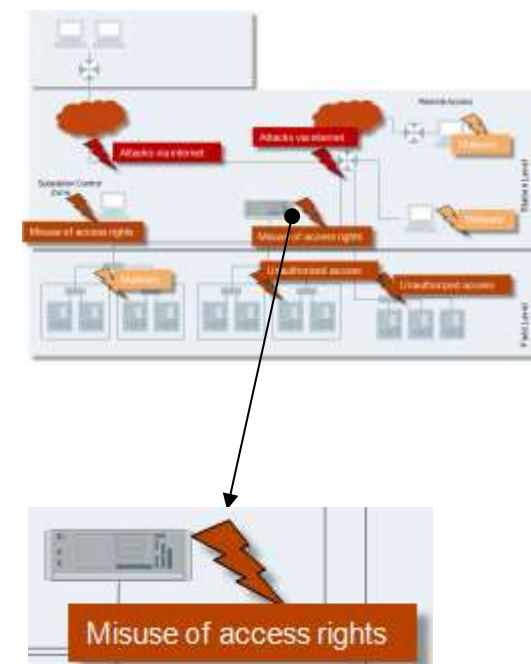
Equipping Digital Substations with Cyber Security

Secure Products as a Basis for Secure Substations

Restrictive Control of User Administration in Substation Automation using SICAM PAS/PQS

- Role to rights assignment for configuration and operation tasks

User Group	Manage Access Rights	Read Configuration	Write Configuration	View Operations	Manage Operations
Administrator	✓	✓	✓	✓	✓
System Engineer		✓	✓	✓	✓
Data Engineer		✓	✓	✓	
Switch Operator		✓		✓	✓
Guest		✓		✓	

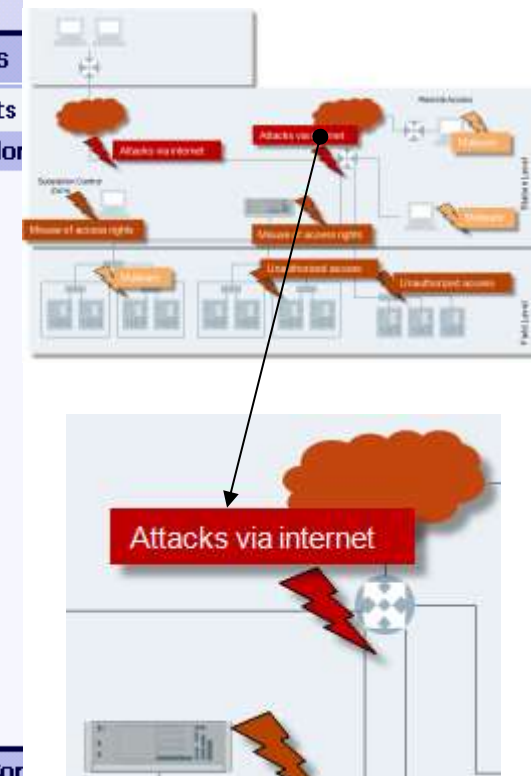
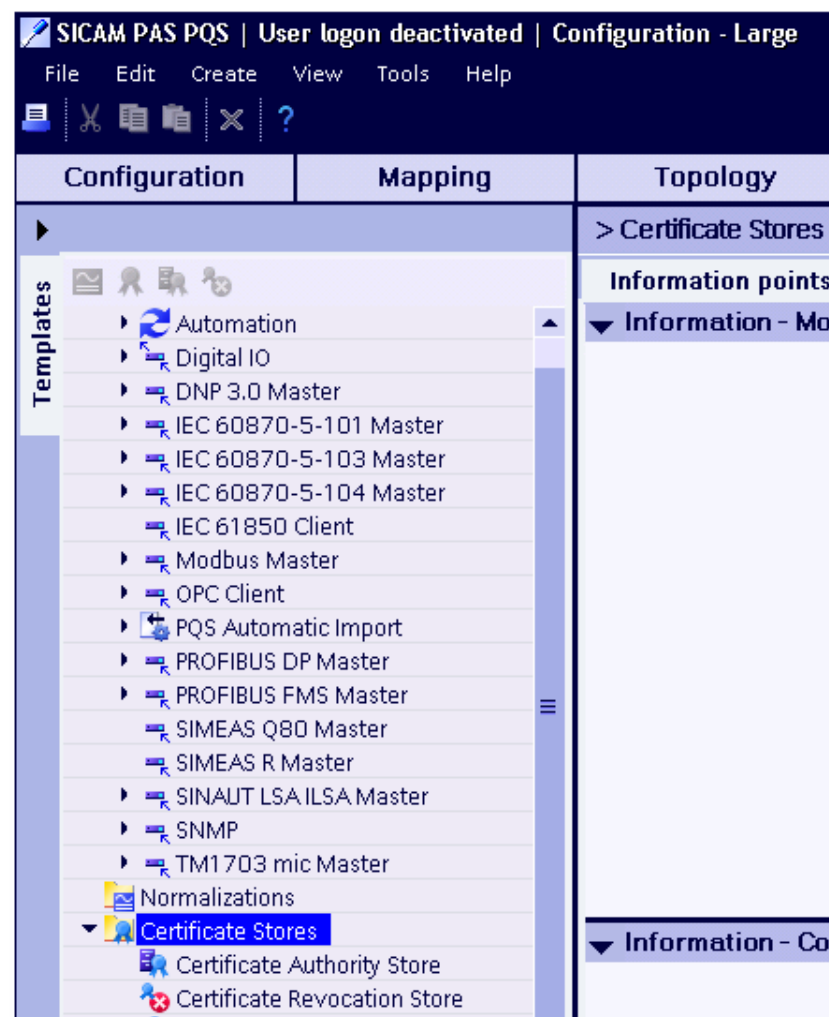


Equipping Digital Substations with Cyber Security

Secure Products as a Basis for Secure Substations

Secure Communication in SICAM PAS

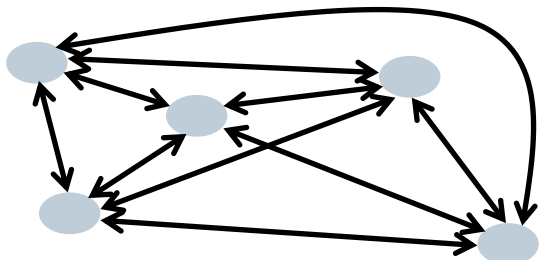
- Certificate management for Transport Layer Security (TLS) based communication
- IEC 62351-5 conformance
- Secure IEC 104 master/slave
- Secure DNP 3.0i master/slave with authentication



Managing Security in Substations

Migration Path to X.509 Certificates

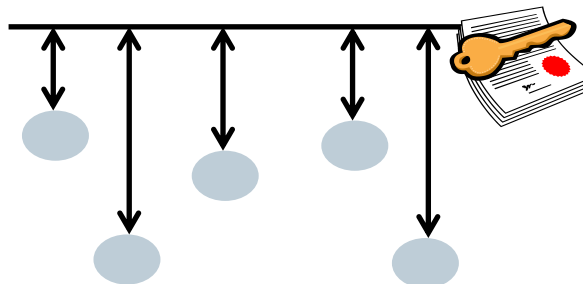
Shared Secrets



Keys needed for n nodes:
 $n * (n-1) / 2$

- Limited scalability
- Trust relation based on mutually shared secrets
- Mutually secrets to be managed on all nodes
- **High administrative effort**
 (manual exchange of shared secrets, typically bad practise)

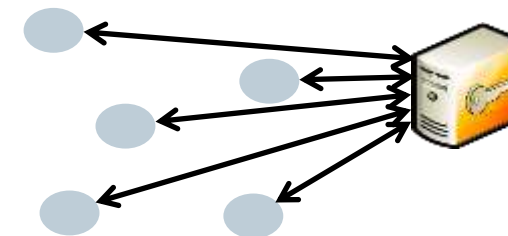
Self-signed Certificates



Keys needed for n nodes:
 $n + \text{White List}$

- Improved scalability
- **Trust based on peer certificates (locally generated) and white list**
- White list managed on all nodes
- Secrets are node local
- **X.509 standard applied**
- Medium administrative effort (manual list adaptations, node related updates)

PKI

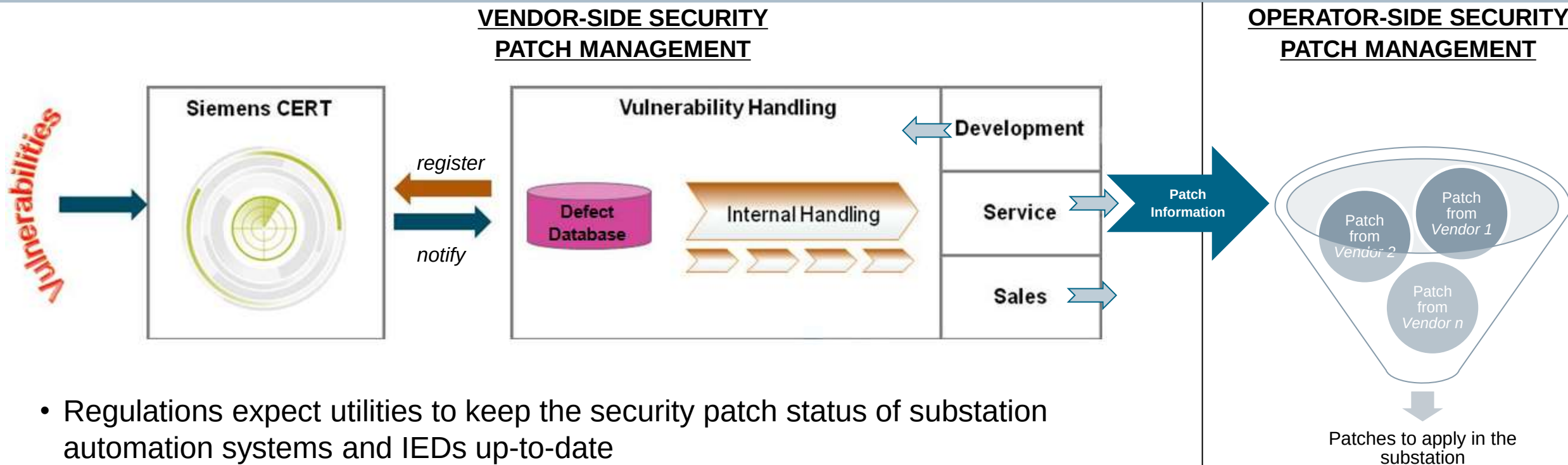


Keys needed for n nodes:
 $n + \text{Root Certificate}$

- Improved scalability
- **Trust based on peer certificates (centrally generated) and root certificates**
- Root certificate managed on all nodes
- Secrets are peer local
- **X.509 standard applied**
- **Low operative administrative effort**
 (automated certificate handling, centralized updates)

Security Patch Management

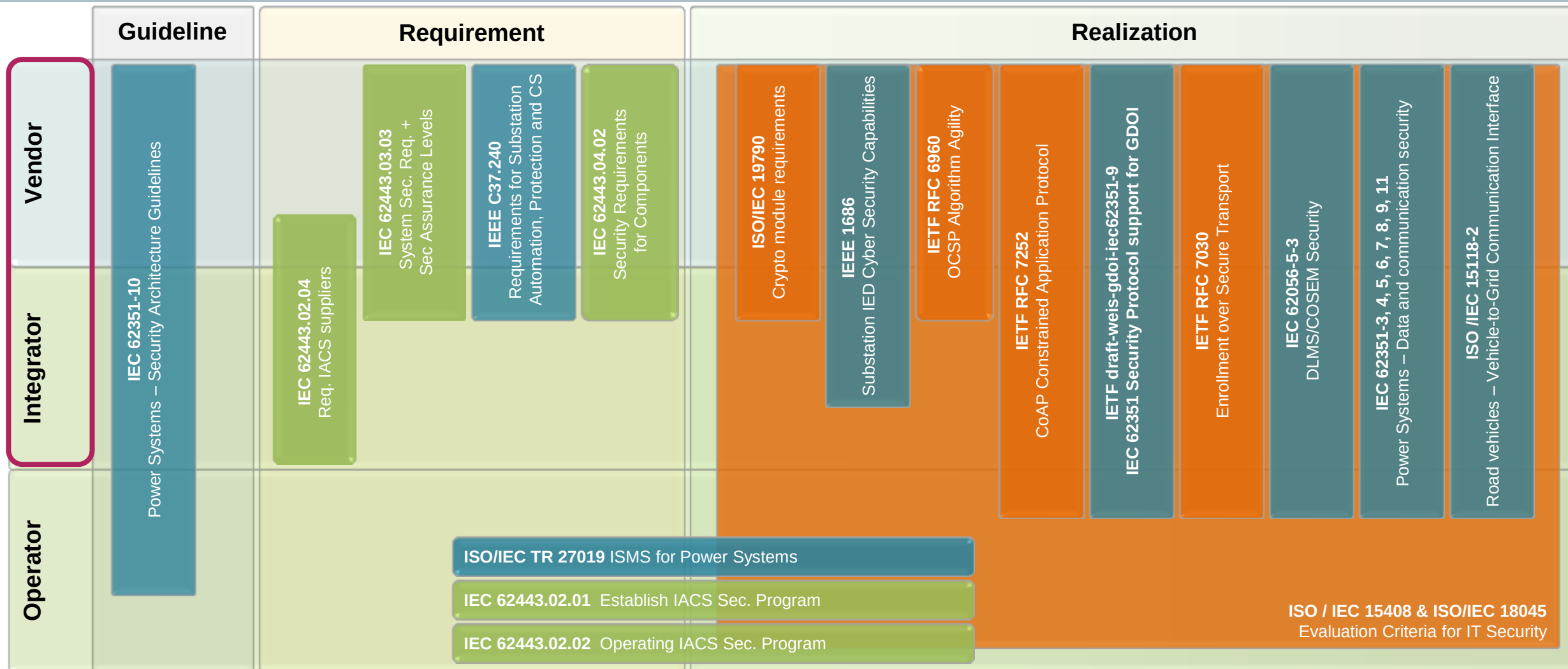
Keeping the Substation Secure & Up-to-date



- Regulations expect utilities to keep the security patch status of substation automation systems and IEDs up-to-date
- Requirements for high availability, reliability and safeguarding primary equipment makes security patching in substations challenging
- Patch Management of an operational environment needs a scalable, secure and cost-efficient solution
- **Automation can help to support the key requirements**

Managing Security Through Standardization

Interoperability Through Security Standards for the Power Utility Ecosystem



Unrestricted © Siemens AG 2015. All rights reserved.

Focus: Power Systems

Focus: Information Systems

Focus: Industrial Automation

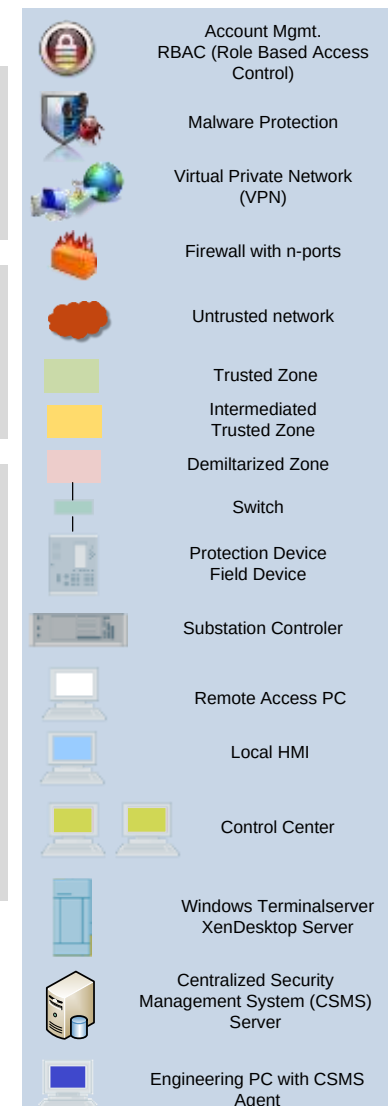
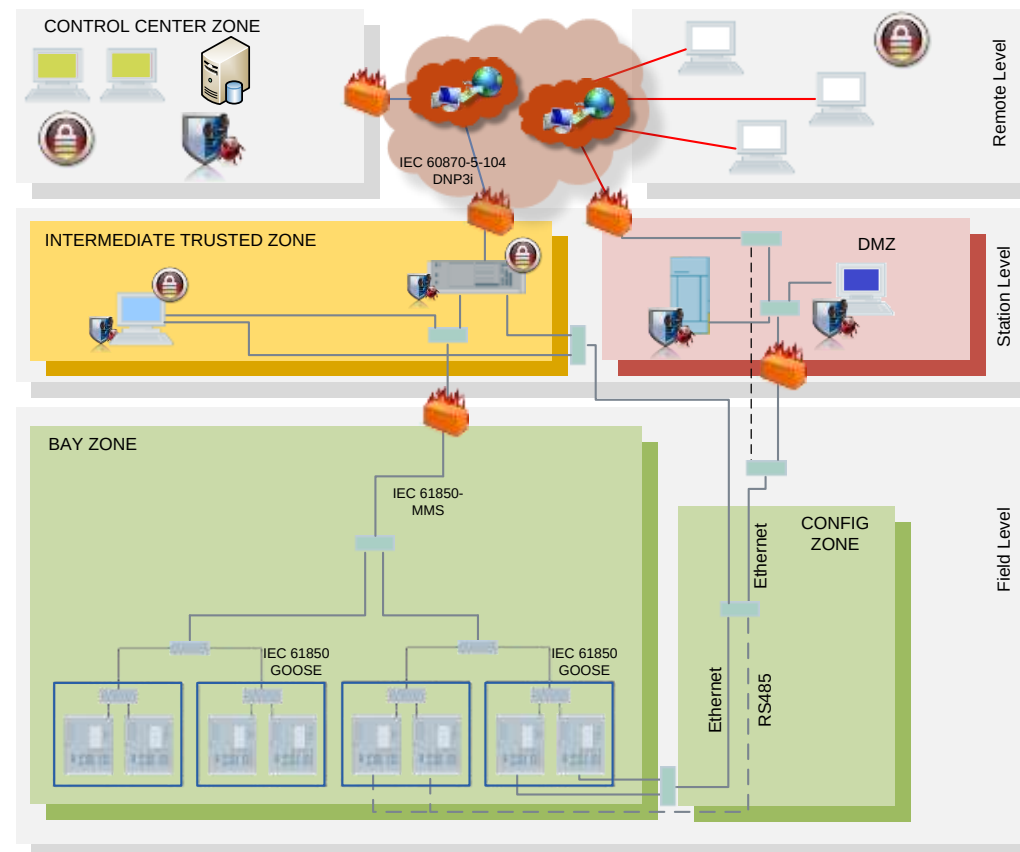
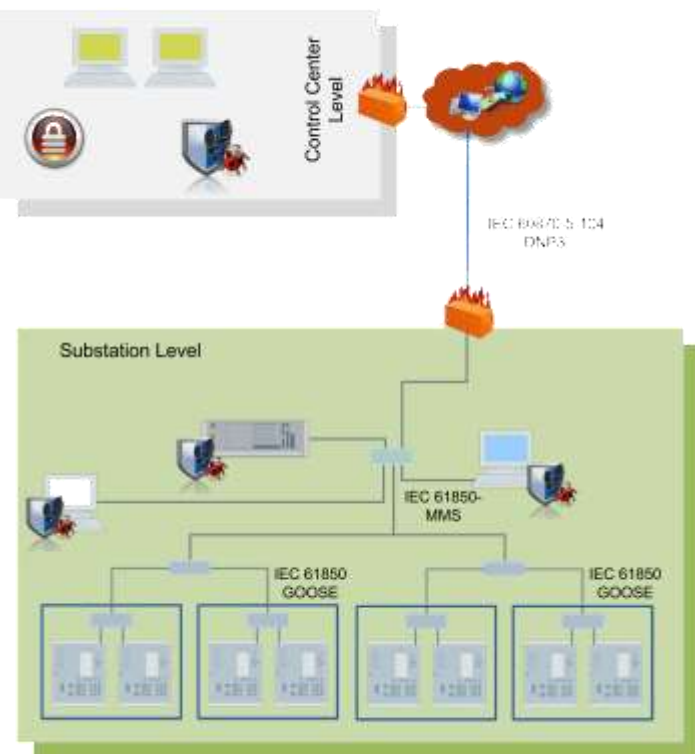
Secure Substation

Multiple Aspects Considered

DIGITAL SUBSTATION



SECURE DIGITAL SUBSTATION



- **out-of-band maintenance channel**
- **network segmentation** for defense in depth
- **centralized management** of DSAS configuration software in DMZ

DMZ: Demilitarized Zone

Thank you for your attention!



Chaitanya Bisale

**Product Lifecycle Manager
Cyber Security & Substation Automation
EM EA PRO LM2**

**Humboldtstr. 59
90459 Nuremberg
Phone: +49 (911) 433 5546
Mobile: +49 (172) 7345783
E-mail: chaitanya.b@siemens.com**

siemens.com/gridsecurity