SIEMENS
Ingenuity for life

Cyber security for digital substations

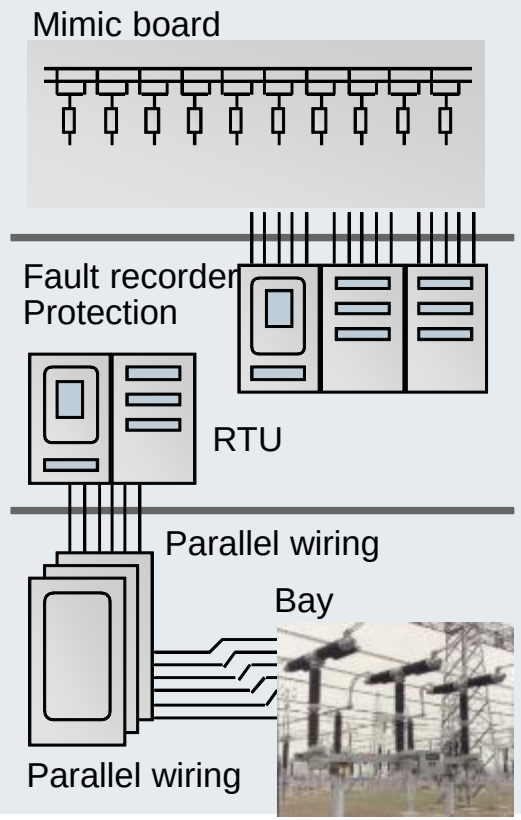
IEC 61850 Europe Conference 2017

siemens.com/gridsecurity

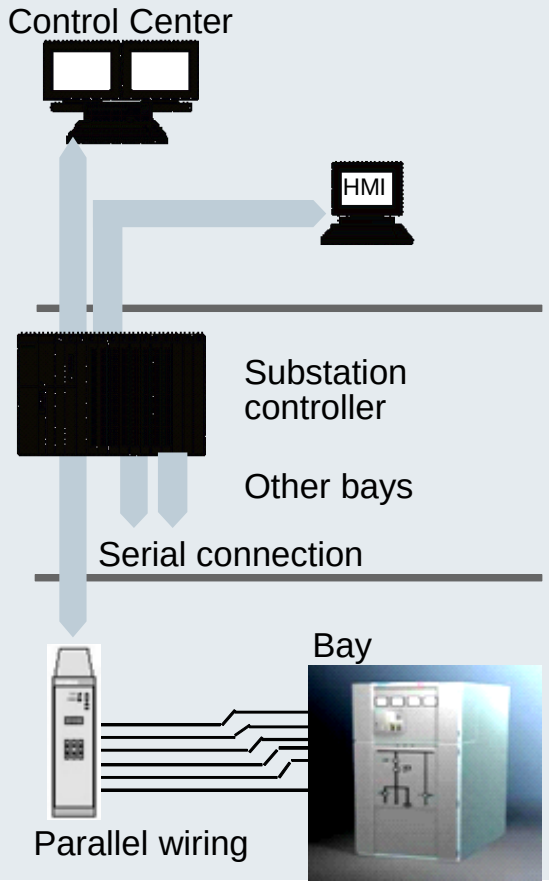
Substation Digitalization process – From security via simplicity…

SIEMENS
Ingenuity for life

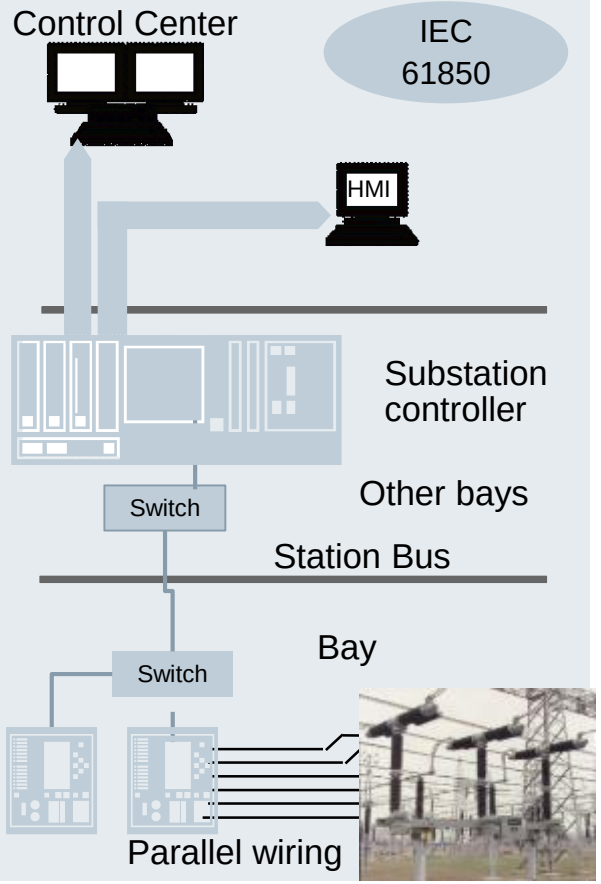
1st generation: Standard cabling



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

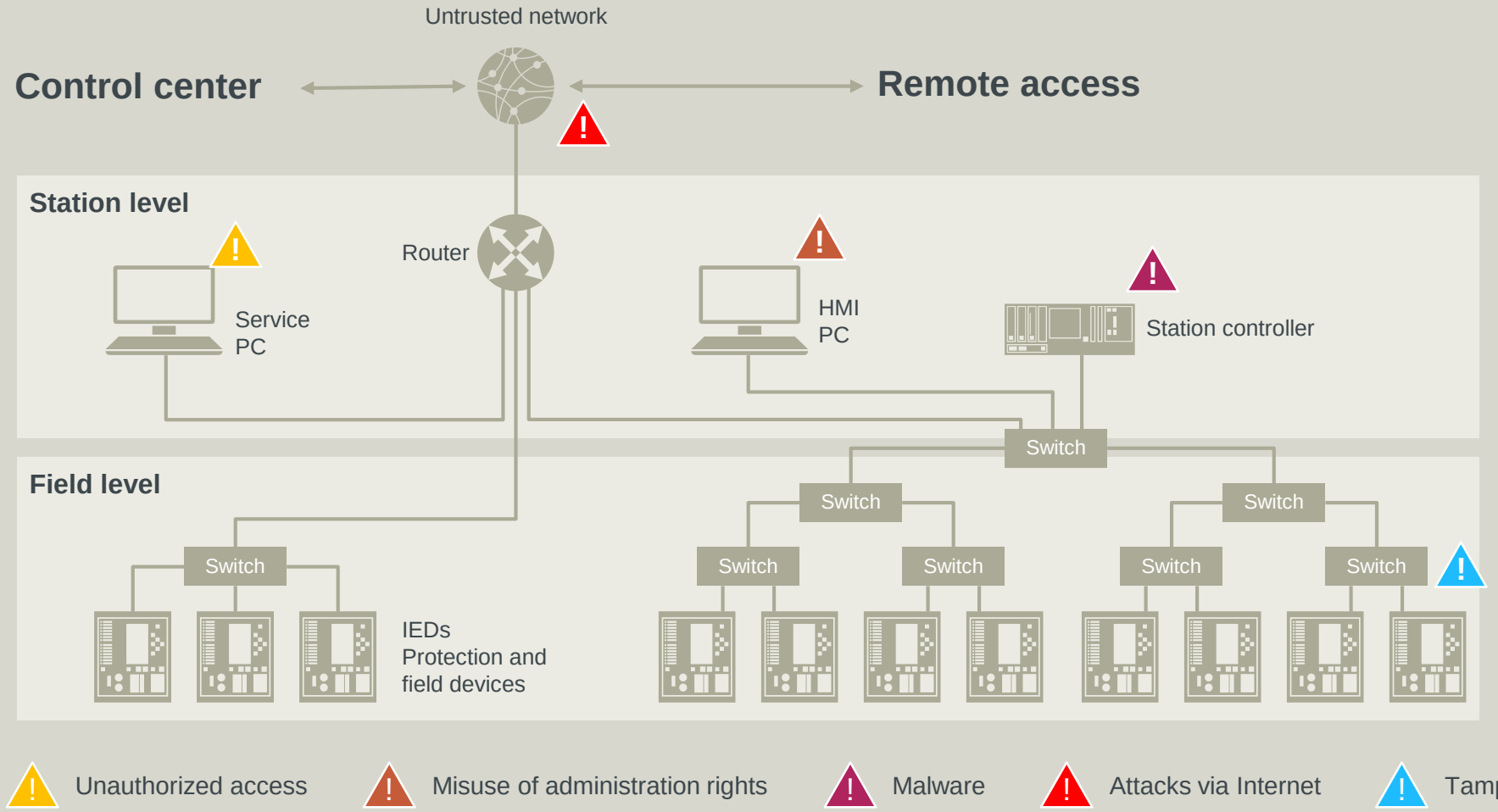


3rd generation: Digital Station Bus since 2004 .....



… to Cyber Security
Possible Threats and Challenges

SIEMENS
Ingenuity for life



Special operational conditions in a substation

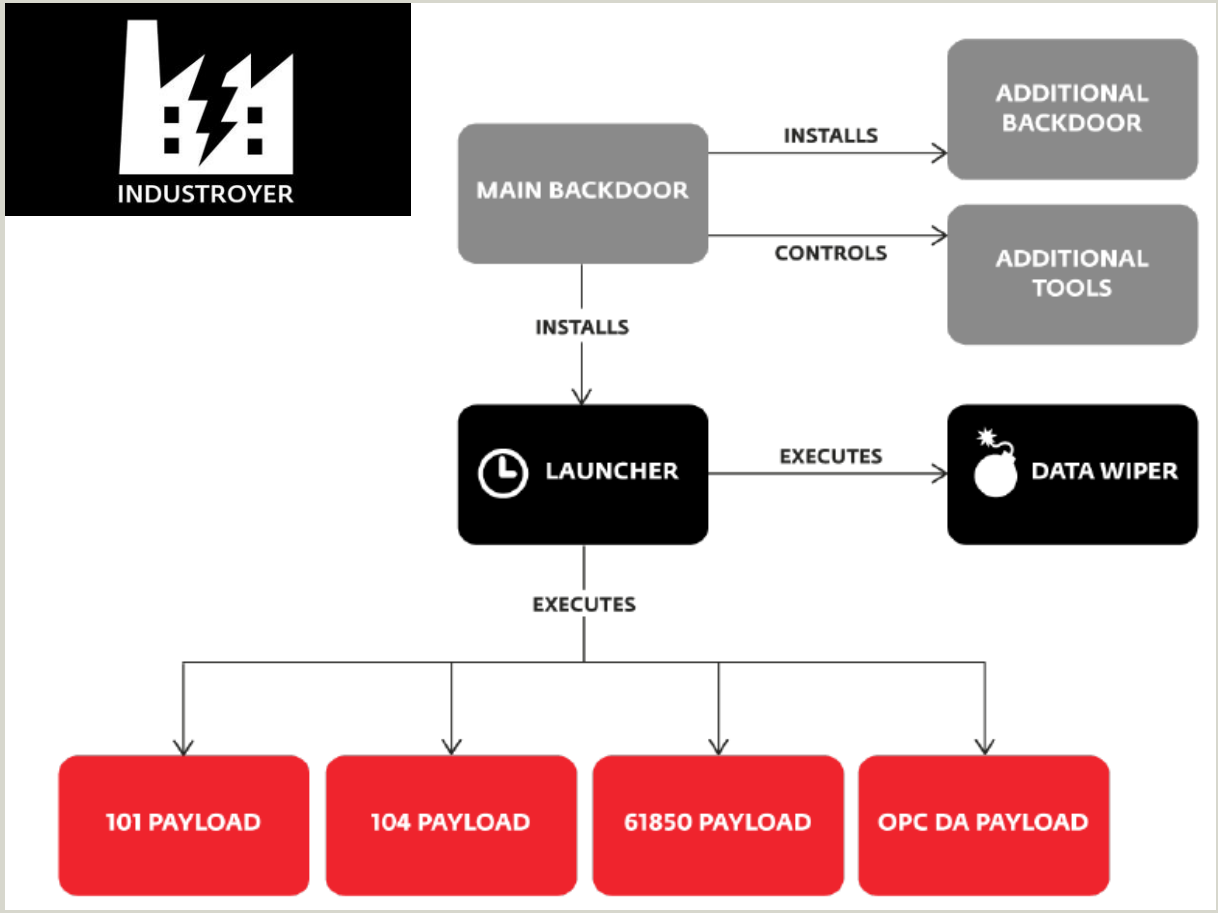
- 24/7 operation
- Components from different vendors
- Interfaces to unsecure networks
- Standard operating systems components
- Proprietary technology

A real risk with an IEC 61850 malware - Industroyer used during Ukraine Attack in December 2016

SIEMENS
Ingenuity for life

attack
in Ukraine power grid

- A vendor independent malware
- Additional targeting of some vendor products



Source: ESET

Standards and Regulations
Cyber Security Framework in a Nutshell

SIEMENS
Ingenuity for life

Following Key-Guidelines
Describing 'What' should be done

NERC CIP

NIST Cyber Security Framework

bdew white paper

Compliant with Key-Standards
Describing 'How' should it be done

ISO/IEC 62443 (System Security)

ISO/IEC 62351 (Communication Security)

ISO/IEC 27001/27019 (Security Mgmt)

Conform to regulatory requirements
Describing what 'must' be done

Bundesministerium des Innern
IT Security Law

Bundesnetzagentur
Security Catalogue

Bundesamt für Sicherheit in der Informationstechnik
Protection Profile

- Follow industry standard, i.e. bdew
- Report on incidents
- Implementation and Certification of an Information Security Management System (ISMS)
- Cryptographic requirements for Smart Metering

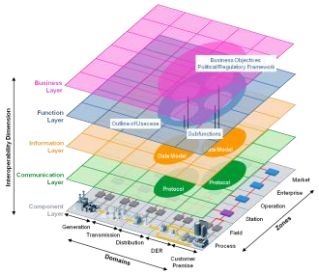
- Assessment and certification of ICS systems

- Auditable compliance (NERC) is required for bulk power systems (since 2010)

Standards and Regulations
Holistic approach is necessary

SIEMENS
Ingenuity for life

Smart Grid Coordination Group / Smart Grid Information Security Mandate M/490



Focus: Power Systems
Focus: Information Systems
Focus: Industrial Automation

Design Details / Technical Aspects

IEC 62443

IEC 62351

ISO/IEC TR 27019

ISO/IEC 27001/2

Details for Operations

Relevance for Products

Completeness / Governance & Policy Aspects

Key Standards

- IEC 62443 (System Security)
- IEC 62351 (Communication Security)
- ISO/IEC 27001/27019 (Security Mgmt)

Managing Cyber security risks –
Secure products as a basis for secure digital substations

SIEMENS
Ingenuity for life

Secured Communication

- Secured with SSL/TLS/IPsec (IEC 62351-3)
- Client/server authentication (IEC 62351-4/6)

Operational Security

- Signed software/firmware (IEC 62351-10)
- Malware protection
- ProductCERT – Vulnerability handling

Access Control

- Centralized account management
- Centralized password management (IEC 62351-8)

Security Monitoring

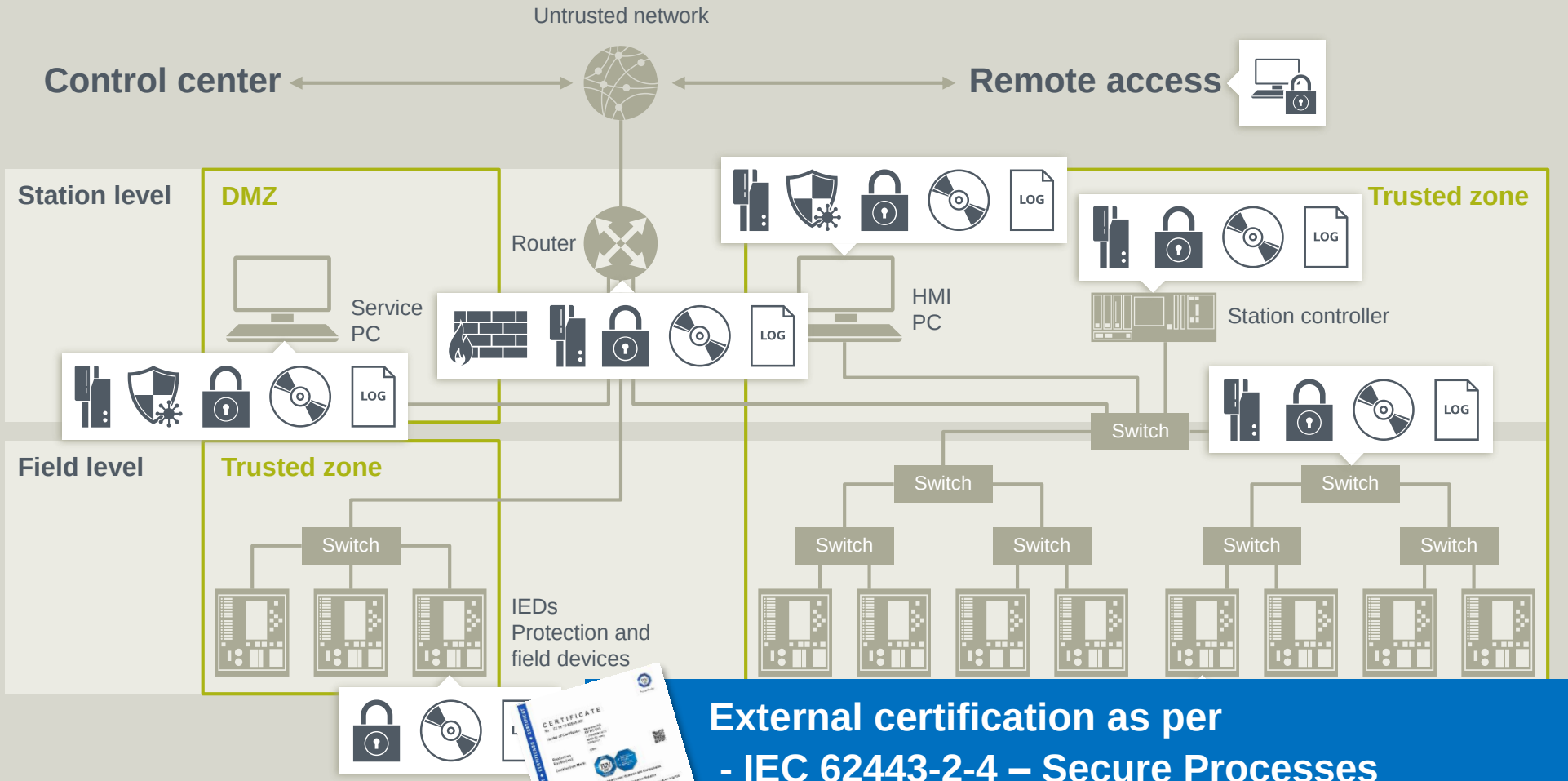
- Centralized event logging (IEC 62351-14)
- Installed base monitoring (IEC 62351-7)

Future Readiness

- Ready for PKI (IEC 62351-9)
- Modularity for tomorrow

Managing Cyber security risks - Implementation of a Secure Substation

SIEMENS
Ingenuity for life



Cyber security measures

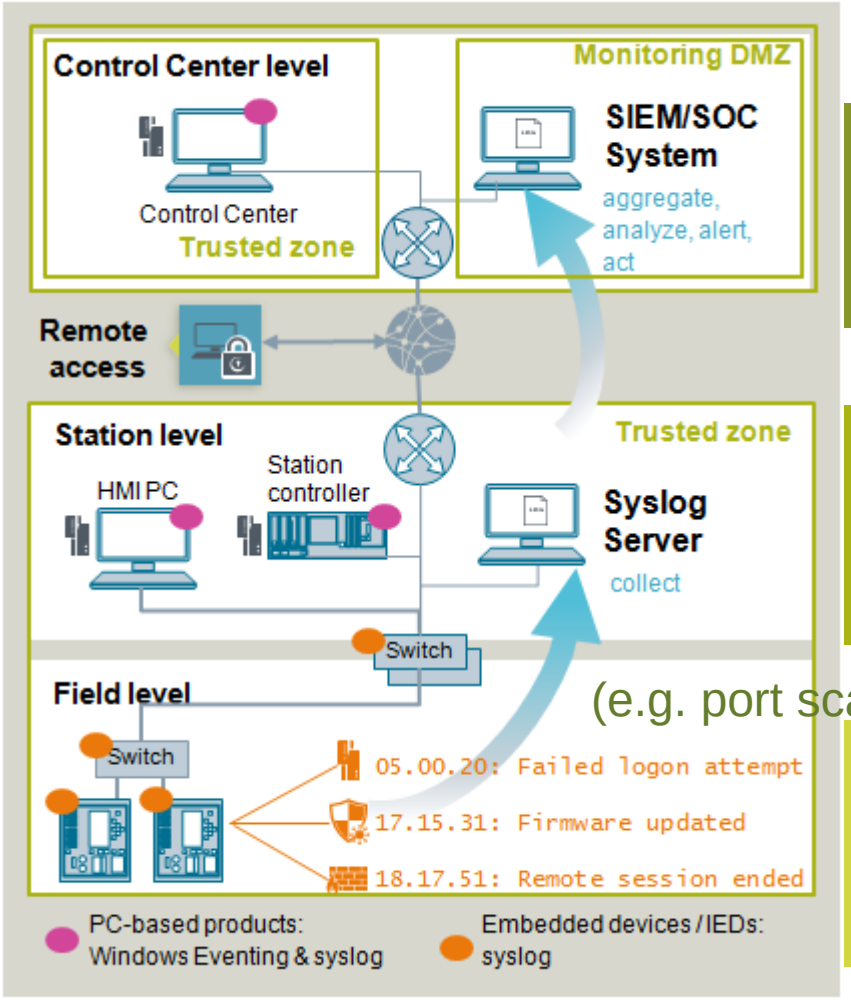
- Access control and account management
- Security logging and monitoring
- System hardening
- Security patching, Backup and restore
- Malware protection
- Data protection, data integrity and system architecture
- Secure remote access

External certification as per
- IEC 62443-2-4 – Secure Processes
- IEC 62443-3-3 – Technical security controls

Managing Cyber security risks - Host-based / network-based Intrusion detection

SIEMENS
Ingenuity for life

	Security Monitoring
Central level	Central monitoring on premise with analysis and alarming functionalities
Station level	Central Log server collecting all security events/alarms from IEDs and substation automation systems
Bay level	IEDs providing security event/alarm data



Timeline for Industroyer
Security patch management in practice

SIEMENS
Ingenuity for life

Vulnerability Handling
EN100 FW Update and advisory to address security researcher findings: SSA-732541 [1]

Patch management service offering and IEC 62443 certification for secure substation blueprint

Siemens reemphasizes systematic patch management to customers worldwide

Mid 2015

Autumn 2016

12th June 2017

Mid 2016

„Spear Phishing“ emails assumed to be used to deploy malware to gain network information at Ukraine utility

Dec. 2016

„Industroyer“: 2nd cyber attack at Ukraine utilities in 2 years

Analysis Reports claim [2]: “Industroyer” can attack SIPROTEC 4 devices by addressing known vulnerability [1]

[1] https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-732541.pdf
[2] https://dragos.com/blog/crashoverride/

Managing Cyber security risks – Security Patch Management

SIEMENS
Ingenuity for life

Vendor side

Single point of contact

Siemens ProductCERT

Central Database

Responsible Disclosure process

Monitoring and Information

Monitoring

Security Researchers

- Pentesters
- Free-time Hackers
- IT-Security Contractors

CERT network

- US ICS-CERT
- BSI
- ...

3rd Party Vendors, OSS

Microsoft
ORACLE
Adobe
...

Notification

Siemens Digital Grid Products

- Service
- Sales
- R&D

Defect Database

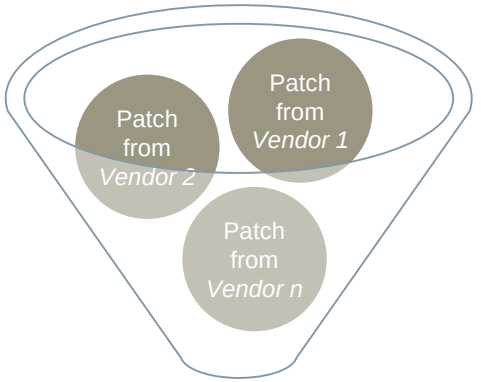
Security Advisories

Security Newsletter

Service Contract

Operator side

Asset Owner's Patch Management Process

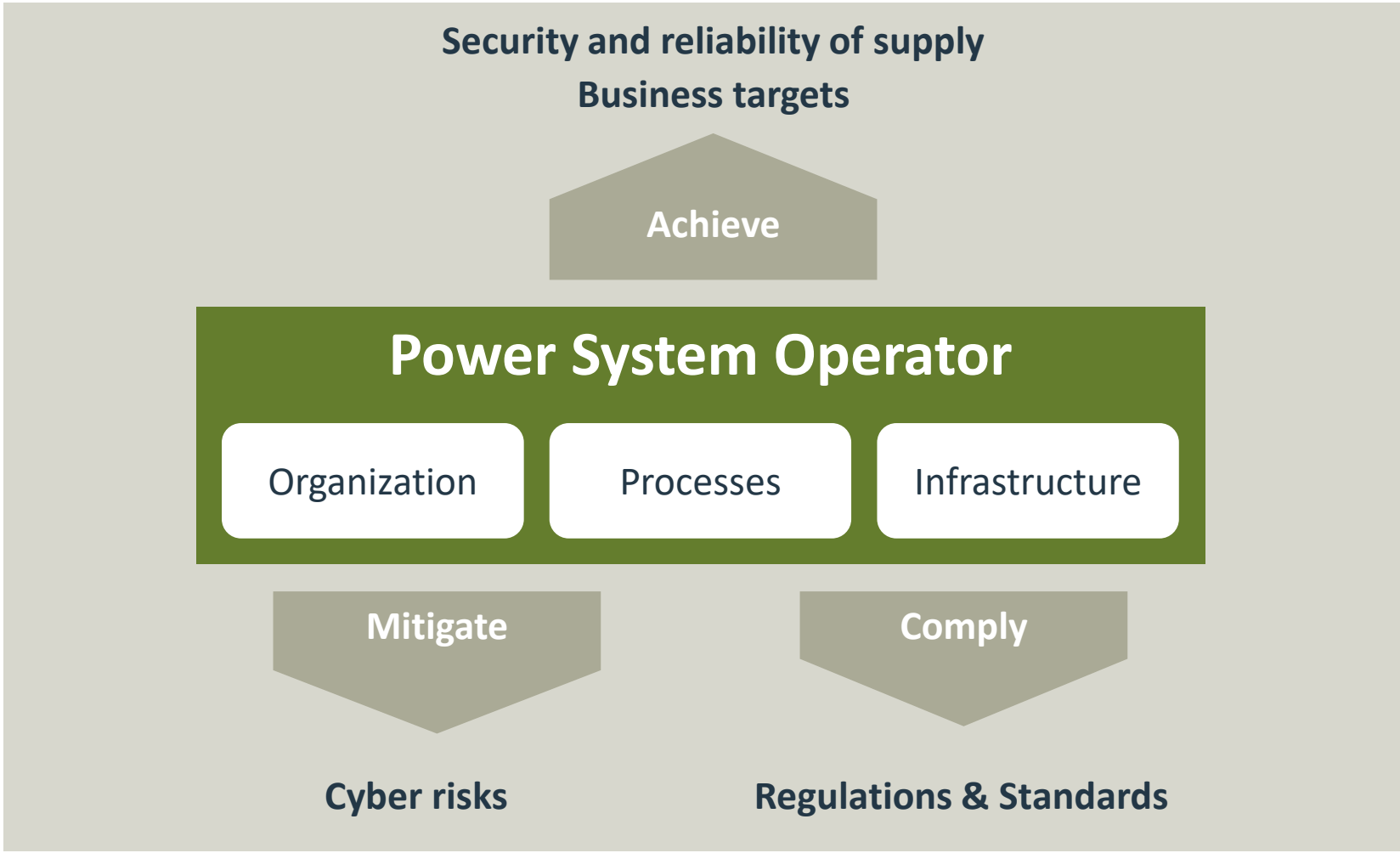


Patch qualification/testing/ deployment

Cyber security conclusion, a pre-requisite for digital substations
A multi-level approach with multi-level responsabilities

SIEMENS
Ingenuity for life

- Secure products → manufacturers
- Secure systems → system integrators
- Secure operations→ operator



Thank You!

SIEMENS
Ingenuity for life

Cédric Harispuru
Product Lifecycle Manager IEC 61850 & Communication protocols
E-mail: cedric.harispuru@siemens.com

Chaitanya Bisale
Product Lifecycle Manager, Senior Key Expert Cyber Security
E-mail: chaitanya.b@siemens.com

Siemens Energy Management

siemens.com/gridsecurity