Cybersecurity in low-voltage power distribution

Planning and implementation of a cyber-secure low-voltage power distribution

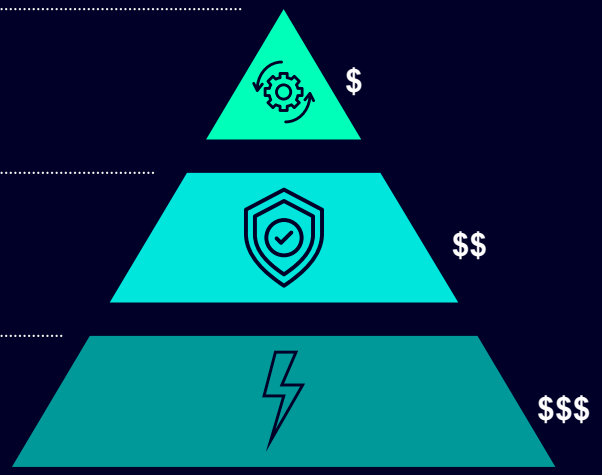
SIEMENS

Digitalization in Electrical Power System

Digitalization plays a key role in solving problems and meeting basic needs

Problem	Improvement through digitalization	Added value
	Induction measurements due to consumption transparency	Reduction of energy costs
	Control and increased use of renewable energies	Reduction of CO_2 emissions
	Increase in reliability of the power supply	Reduction in outage times
	Prevention of malfunctions and outages of plants	Increase in process reliability

Basic needs

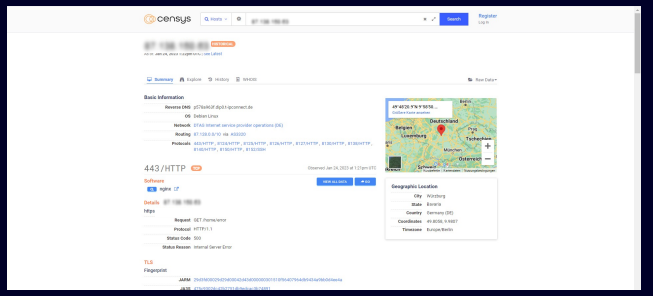


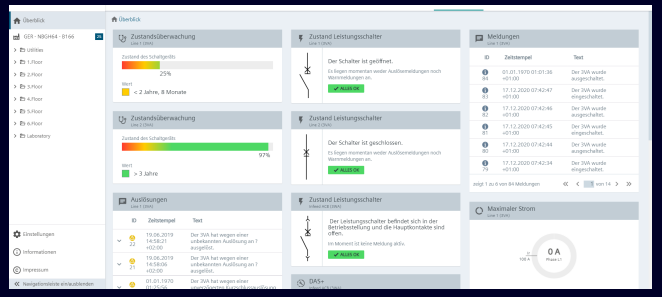
But it also poses risks of cyberattacks

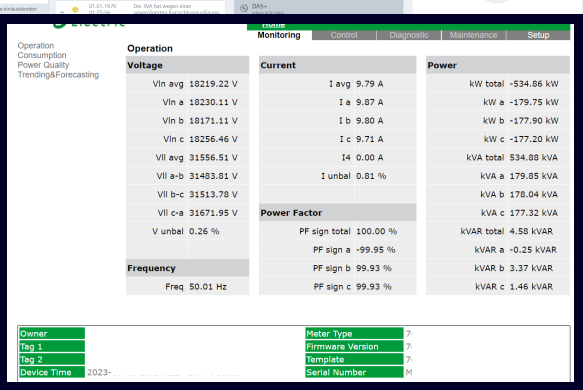
SIEMENS

Cybersecurity and low voltage?!

LIVE DEMO







Low-voltage installations can provide a way in for attackers if they are connected directly to the Internet

SIEMENS

Habits in OT and their effects on protection of power distribution systems

Habits in operative technology

- **Systems are seldom checked** if there is no specific need
- **Focus on convenience** and easy access to be able to respond quickly if a technical problem occurs
- Operating functions and data acquisition are often performed by **different people**

"As long as it works, you don't need to touch it!"

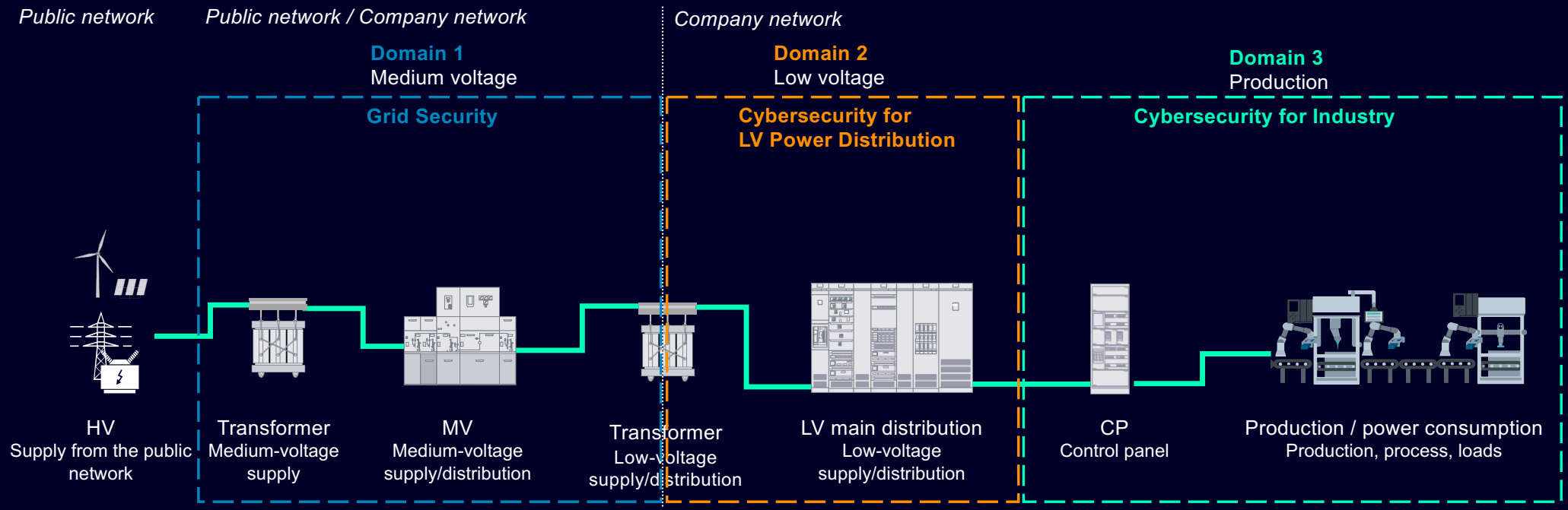
Vulnerabilities of many power distribution systems

- **No patch management**
- **Low access barriers**
- Use of **standard passwords**
- No logging
- Long operating periods

A networked low-voltage switchboard combined with a relaxed approach to cybersecurity create opportunities for cyberattacks.

SIEMENS

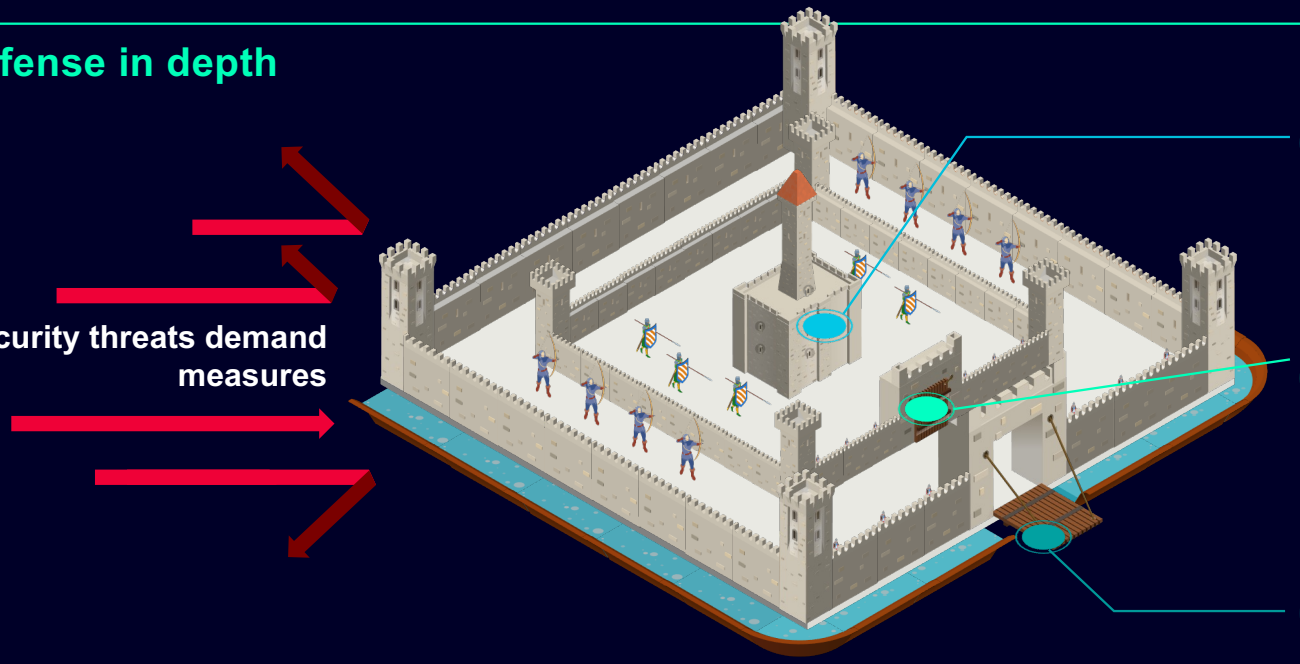
Cybersecurity along the power distribution



SIEMENS

The "defense in depth" strategy provides comprehensive cybersecurity

Defense in depth



System integrity
Field devices (hardening)

Network security
Various parts of a network (e.g. VLAN, subnetting)

Plant security
Physical access (e.g. access control, doors)

"Defense in depth" is the approach for defending the system against a certain attack using several independent methods.

SIEMENS

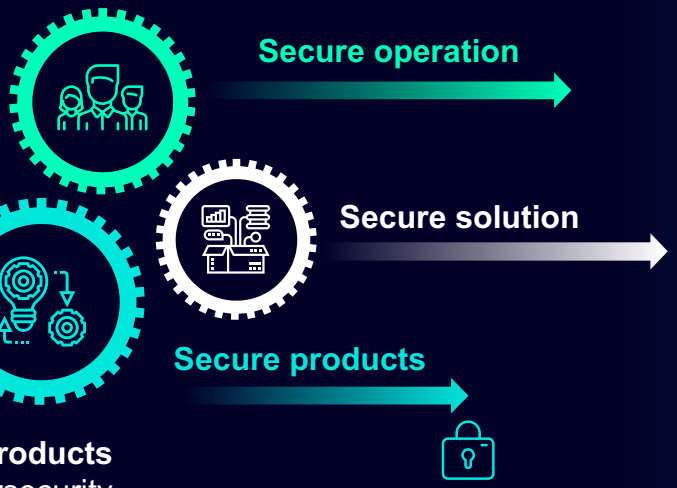
A holistic approach is required to ensure cybersecurity in low-voltage power distribution

System security IEC 62443

Persons (organization)
Awareness and understanding of cybersecurity.

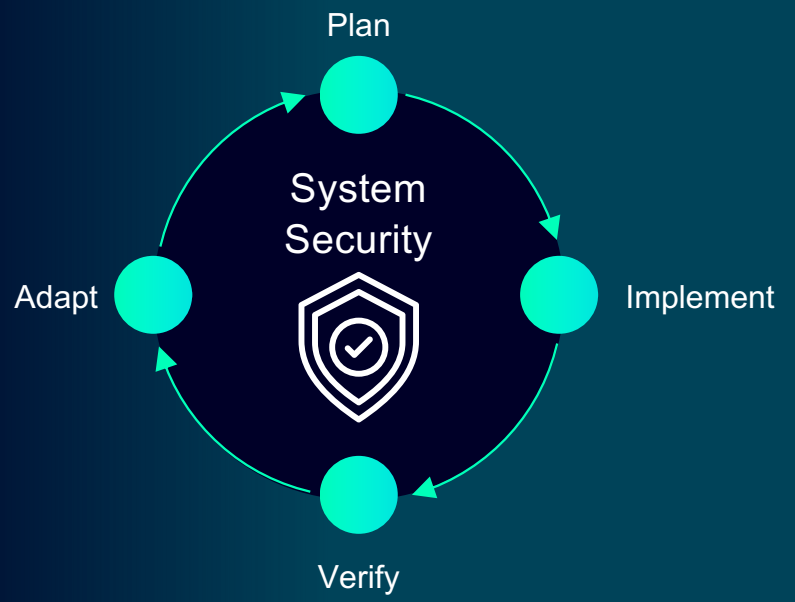
Processes
Covers the complete life cycle
Supports the technical solution and operation.

Products
Supports the cybersecurity protection objectives (availability, integrity, confidentiality).



Security management ISO 27001

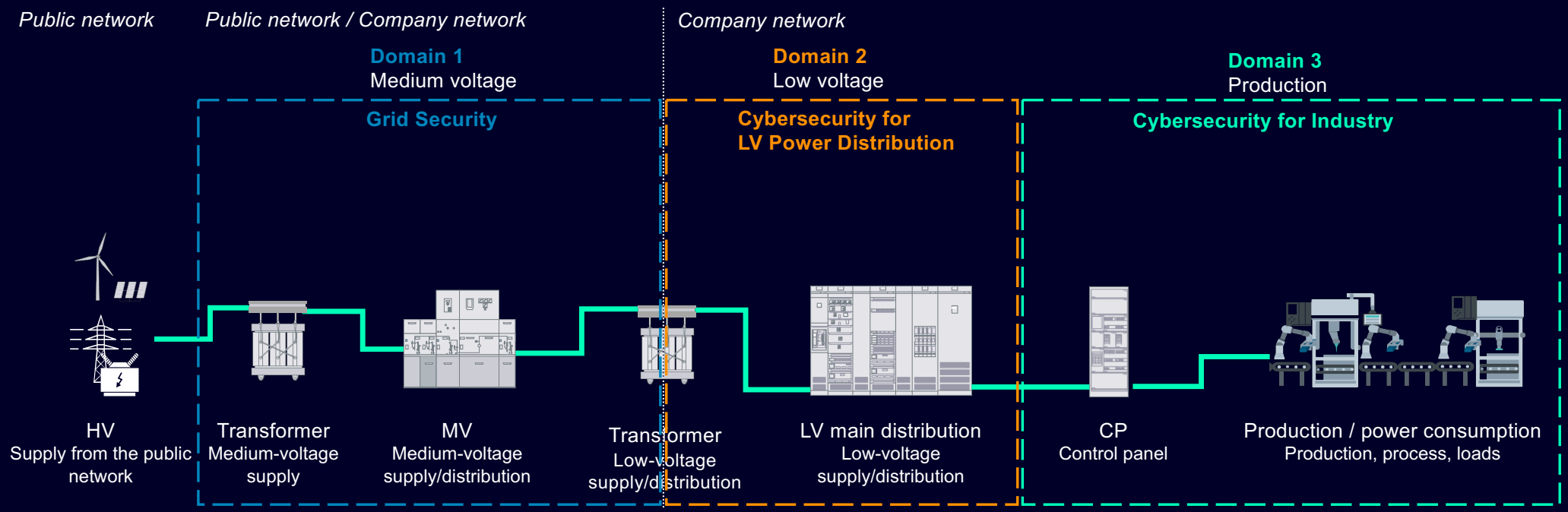
Information security management system (ISMS)



SIEMENS

System approach according to IEC 62443

- Each domain has its special aspects and System approaches (blueprints) should be designed/planned individually for each domain.
- At the corporate level, the individual domains must be grouped together to form a holistic security concept.



SIEMENS

Cybersecurity in Manufacturer

Corporate Technology ProductCERT

For our customers

Computer **E**mergency **R**esponse **T**eam
SIEMENS CERT & ProductCERT

- Advice
- Testing device/app cybersecurity
- Siemens Security Advisories (SSA)

Product and Solution Security Initiative

For ourselves

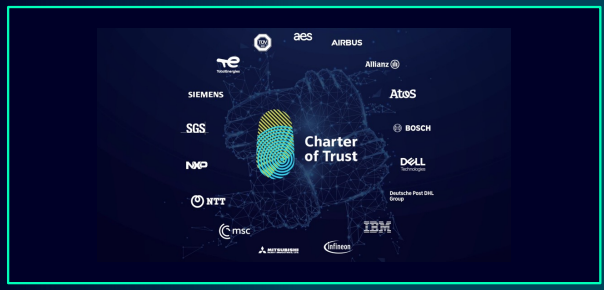
PSS Initiative

Product &
Solution **S**ecurity

- Organization
- Sharing information and knowledge
- Training courses

Charter of Trust

For society



Charter **o**f **T**rust

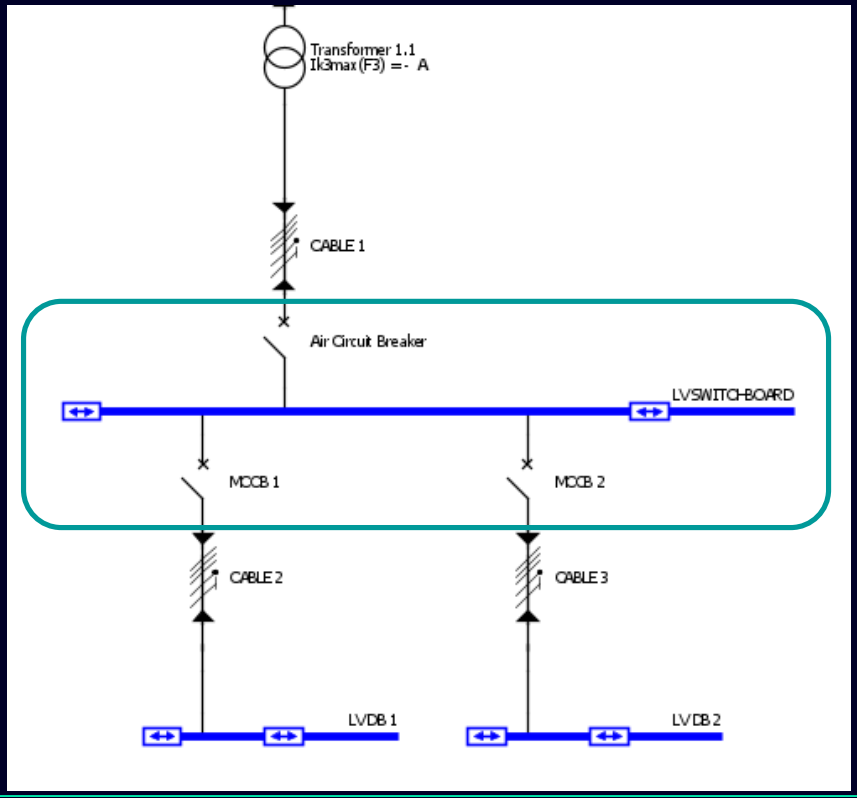
1. Protection of the data of individuals and companies
2. Prevention of damage to people, companies, and infrastructures
3. Creation of a reliable basis on which trust in a networked, digital world can grow

Central website: **www.siemens.com/cybersecurity**

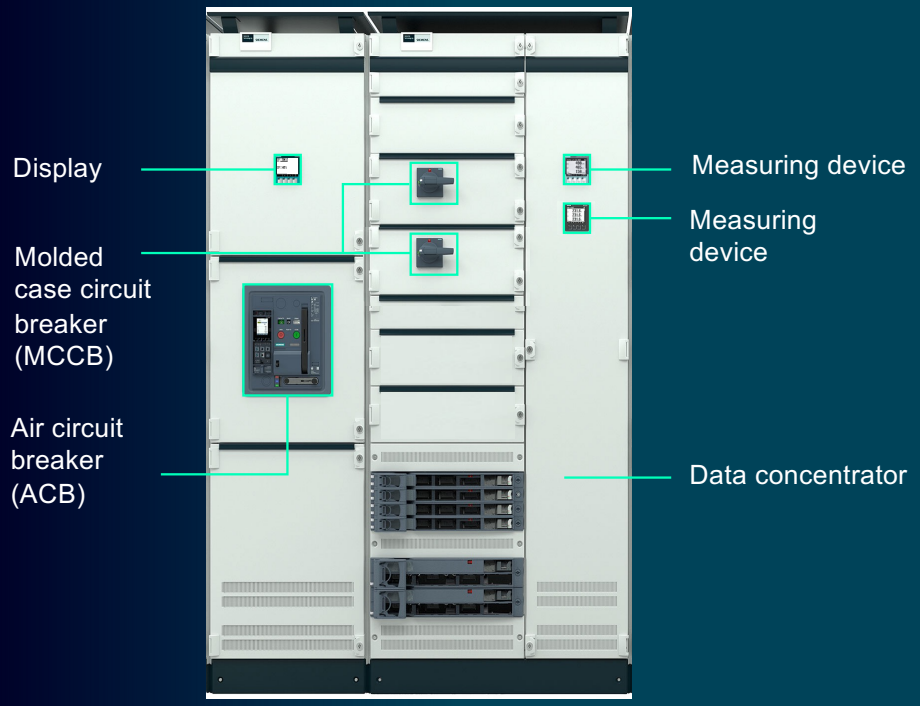
SIEMENS

Low-voltage main distribution – system approach

Single line diagram



Physical structure

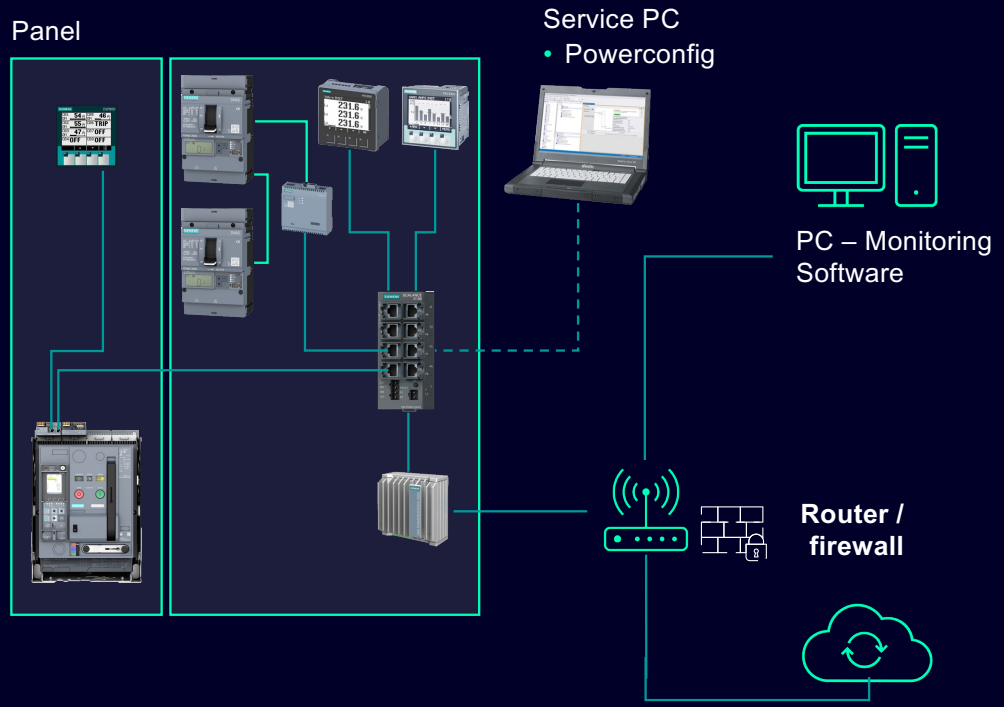


SIEMENS

Low-voltage main distribution – system approach

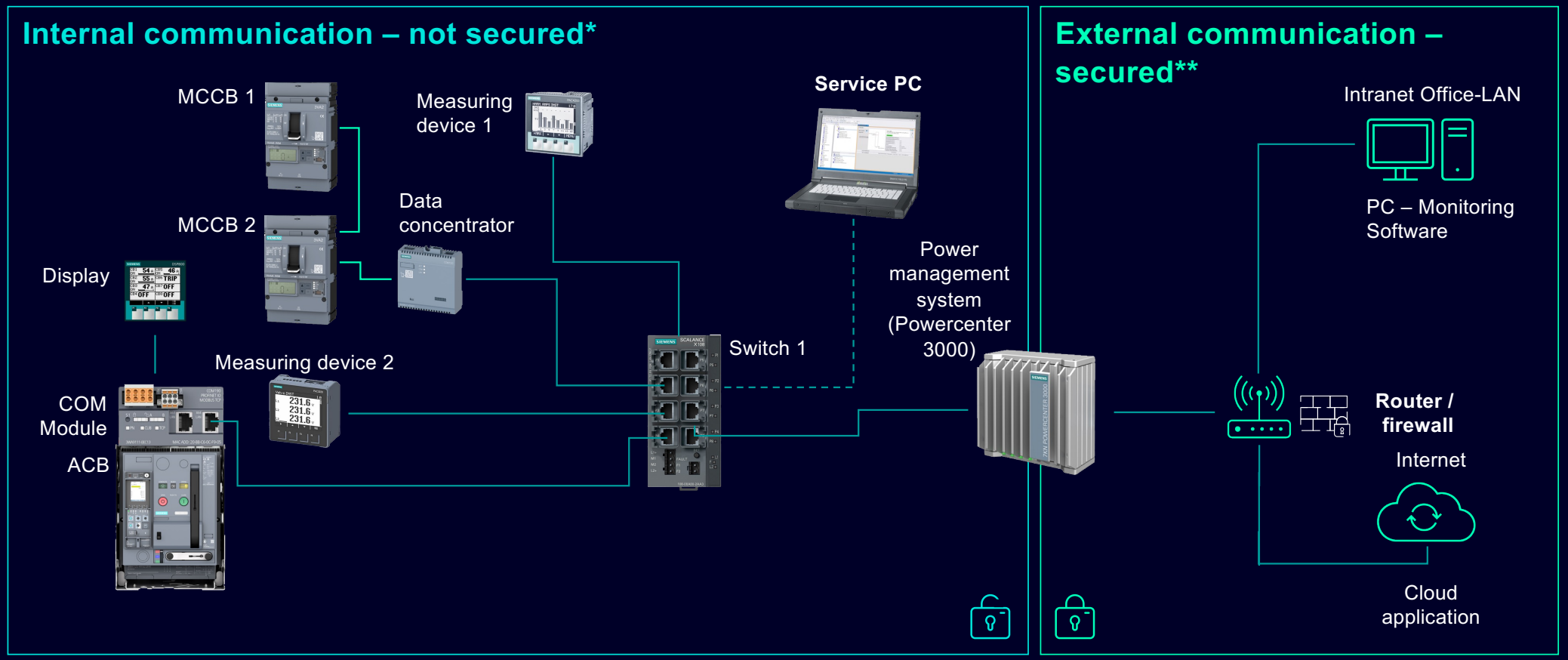
Physical structure

Network topology



SIEMENS

System approach – simplified topological representation



* LV MDB internal communication e.g. via Modbus TCP, sNTP, http ** LV MDB external communication – secured e.g. via https via TLS, MQTT via TLS

SIEMENS

Summary – What you should do to improve your Security

Cybersecurity is more than a functionality within a product!

1. Never ever directly connect the power distribution to the internet!
2. Combine secure products into a secure system. (use Blueprints)
3. Use a multi layer security concept. (Defense in Depth)
4. Create awareness for the topic of cybersecurity among your organisation and define processes and policies.
5. Check your system regularly for vulnerabilities and close them promptly.

SIEMENS

Thank you!

Chen Zhao

Specification Manager (Electrical Products)

Siemens Plc
Smart Infrastructure Division

Cellphone: +44 7808823606
mailto:zhao.chen@siemens.com

Connect with me on LinkedIn: LinkedIn Chen Zhao

SIEMENS

Smart Infrastructure
A broad offering

Electrical Products

- Protection devices, e.g. air circuit breakers, molded case circuit breakers, miniature circuit breakers, motor starter protectors
- Switching devices, e.g. soft-starters, contactors
- Measuring devices, e.g. PAC-meters[1], SEM3[2] measuring device modules
- Monitoring devices, e.g. function relays, motor management systems
- Safety devices, e.g., safety relays and safety starters
- Software, e.g. SENTRON powermanager, Control Panel Designer
- Low-voltage distribution boards and systems
- Wiring accessories

Building Products

- Building and room automation, lighting control, HVAC[3] OEM automation
- Sensors, valves and actuators
- Fire safety
- Building management software for automation, fire safety, security and 3rd-party integrations
- Security software
- Cloud applications for smart buildings]

Electrification and Automation

- Medium-voltage primary and secondary switchgear, vacuum circuit-breakers, contactors and interrupters
- Low-voltage distribution boards, motor control centers, and busbar trunking systems
- Distribution solutions
- Digital & Classical services for full portfolio of distribution systems
- Photovoltaics inverter systems
- Substation automation, protection, power quality, and communications

Regional Solutions and Services

- Vertical markets specific offerings (e.g. for data centers, life science, smart offices) leveraging cloud and on-premise software
- Solutions and services for building automation, fire safety, security, energy and performance services, workplace experience and other domains
- Distributed Energy Systems
- Digital services

Grid Software

- Grid operations software and Grid control software
- Grid planning software and Grid simulation software
- Power system consulting and energy business advisory
- Meter data management software
- Grid resilience software
- Grid edge software

eMobility

- AC & DC charging infrastructure
- Connected services
- Digital charging software & services
- Smart charging & fleet management
- Managed charging operations for fleets
- Ship-to-Shore power supply

1 PAC: Power Analysis and Control | **2** SEM3: Siemens Embedded Micro Metering Module | | **3** HVAC: heating, ventilation and air conditioning

SIEMENS