FHI INDUSTRIËLE AUTOMATISERING

Is uw productienetwerk net zo veilig als uw kantoornetwerk?

Industrial Ethernet

26 maart 2024 | De Basiliek, Veenendaal

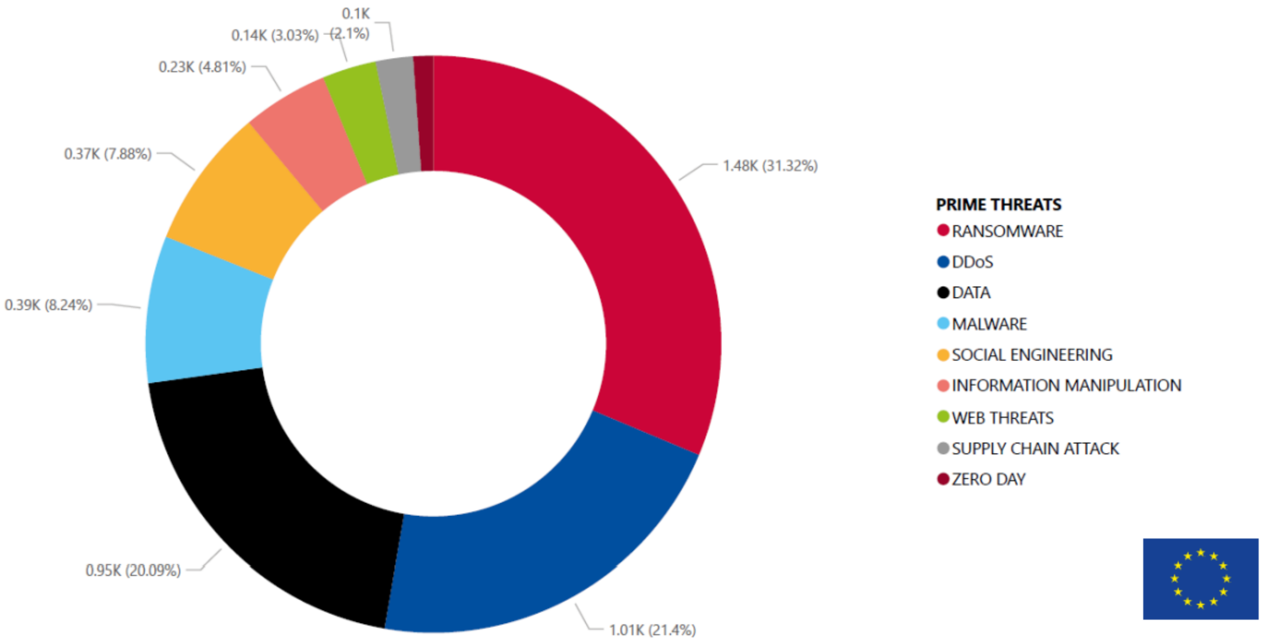
Agenda

- Overview Security Regulations
- Defense in Depth as "onion skin" model
- Practical tips to get started already

ENISA

Threat Landscape:

Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

New Security Regulation for operating companies

EU - NIS2

EU critical infrastructures + more sectors, companies.

National law liability at:
Oct. 2024

US - SEC

USA public listed companies.
SEC Securities and Exchange Commission

Liability at:
Dec. 2023

IACS UR-E26/27

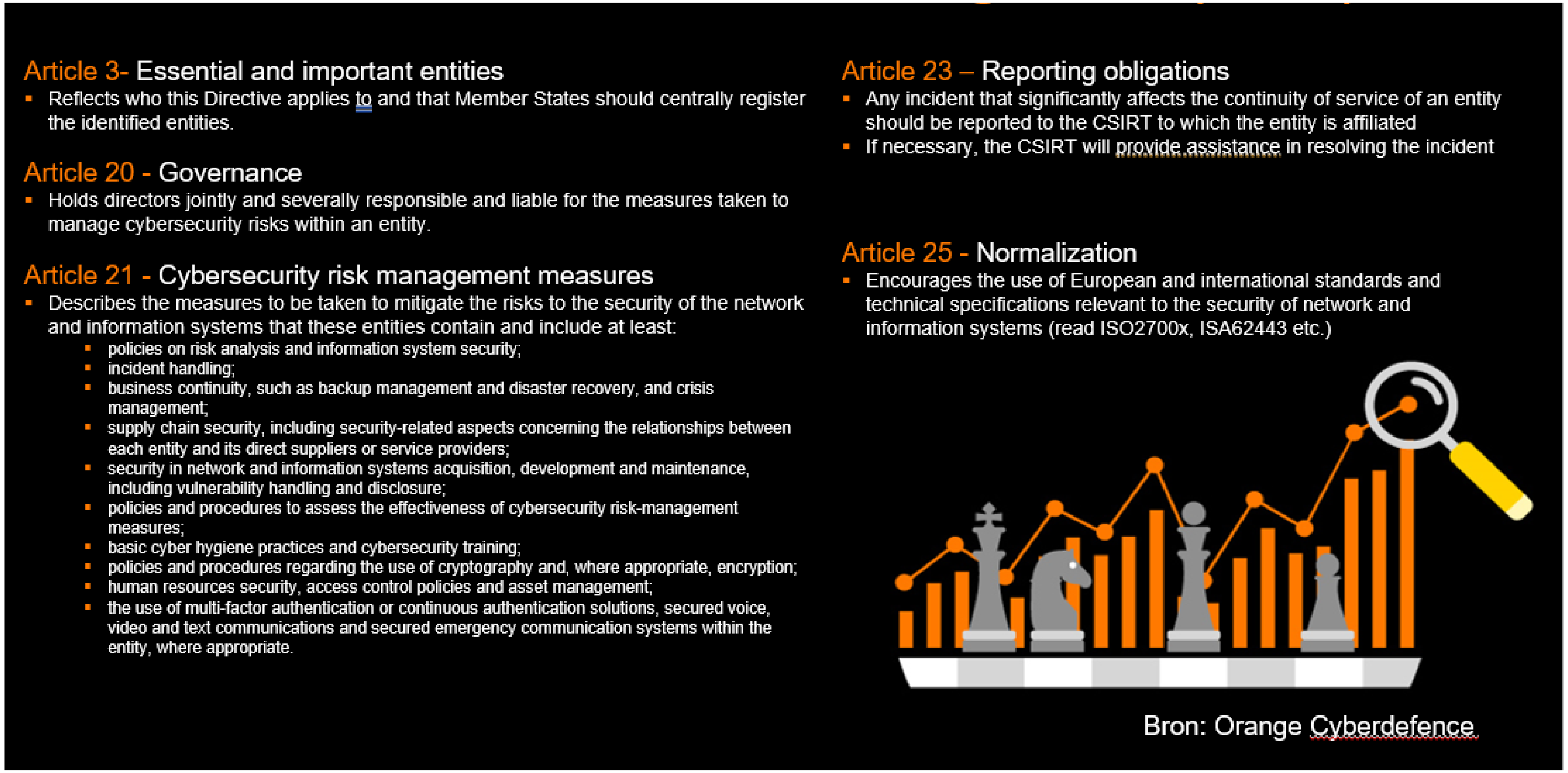
International shipbuilding standards. Base for test companies like DNV, …

Liability for new ship contracts at:
Aug. 2024

New Security Regulation for Products

EU – RED DA	EU – Machinery Act	EU-Cyber Resiliance Act
EU extended RED regulations for wireless devices with network interfaces to the internet.	EU new Machinery Regulation with security requirements.	All products with digital elements and network interfaces.
CE liability at: **Aug. 2025**	CE liability at: **Jan. 2027**	CE liability at: **Q3 2027**

There is a new law based on an EU regulation (NIS-2)



Article 3- Essential and important entities

- Reflects who this Directive applies to and that Member States should centrally register the identified entities.

Article 20 - Governance

- Holds directors jointly and severally responsible and liable for the measures taken to manage cybersecurity risks within an entity.

Article 21 - Cybersecurity risk management measures

- Describes the measures to be taken to mitigate the risks to the security of the network and information systems that these entities contain and include at least:
  - policies on risk analysis and information system security;
  - incident handling;
  - business continuity, such as backup management and disaster recovery, and crisis management;
  - supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
  - security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
  - policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
  - basic cyber hygiene practices and cybersecurity training;
  - policies and procedures regarding the use of cryptography and, where appropriate, encryption;
  - human resources security, access control policies and asset management;
  - the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Article 23 – Reporting obligations

- Any incident that significantly affects the continuity of service of an entity should be reported to the CSIRT to which the entity is affiliated
- If necessary, the CSIRT will provide assistance in resolving the incident

Article 25 - Normalization

- Encourages the use of European and international standards and technical specifications relevant to the security of network and information systems (read ISO2700x, ISA62443 etc.)

Bron: Orange Cyberdefence

NIS2 Sector classification (article 3)

Sectors of high criticality

- Energy (Electricity, Oil, Gas, Hydrogen, District heating and cooling)
- Transport (Air, Rail, Water, Road)
- Water (Drink, Waste)
- Banking, Financial market infrastructure
- Health, Space
- Digital infrastructure(Cloud comp. provider, ….)
- ICT service management (business to business)
- …

Other critical sectors

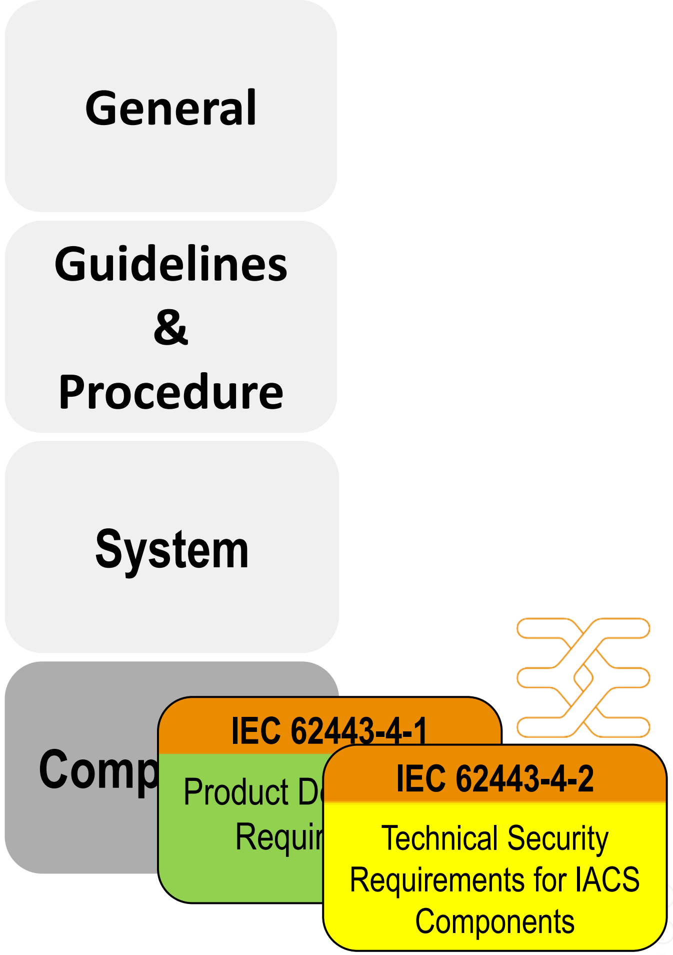
- Postal and courier services
- Waste management
- Chemical companies, Food companies
- Product manufacturer of
  a) Medical device
  b) Computer, electronic or optical
  c) Electrical equipment
  d) Machinery
  e) Motor vehicles, trailers, Transport equipment
- Digital providers (marketplaces, search, social)

Use of Security Management Systems

ISO 27001

IEC 62443

- Main scope IT environment
- *Computer, Printer, Server, Cloud…*



General

Guidelines & Procedure

System

Comp

IEC 62443-4-1

Product D

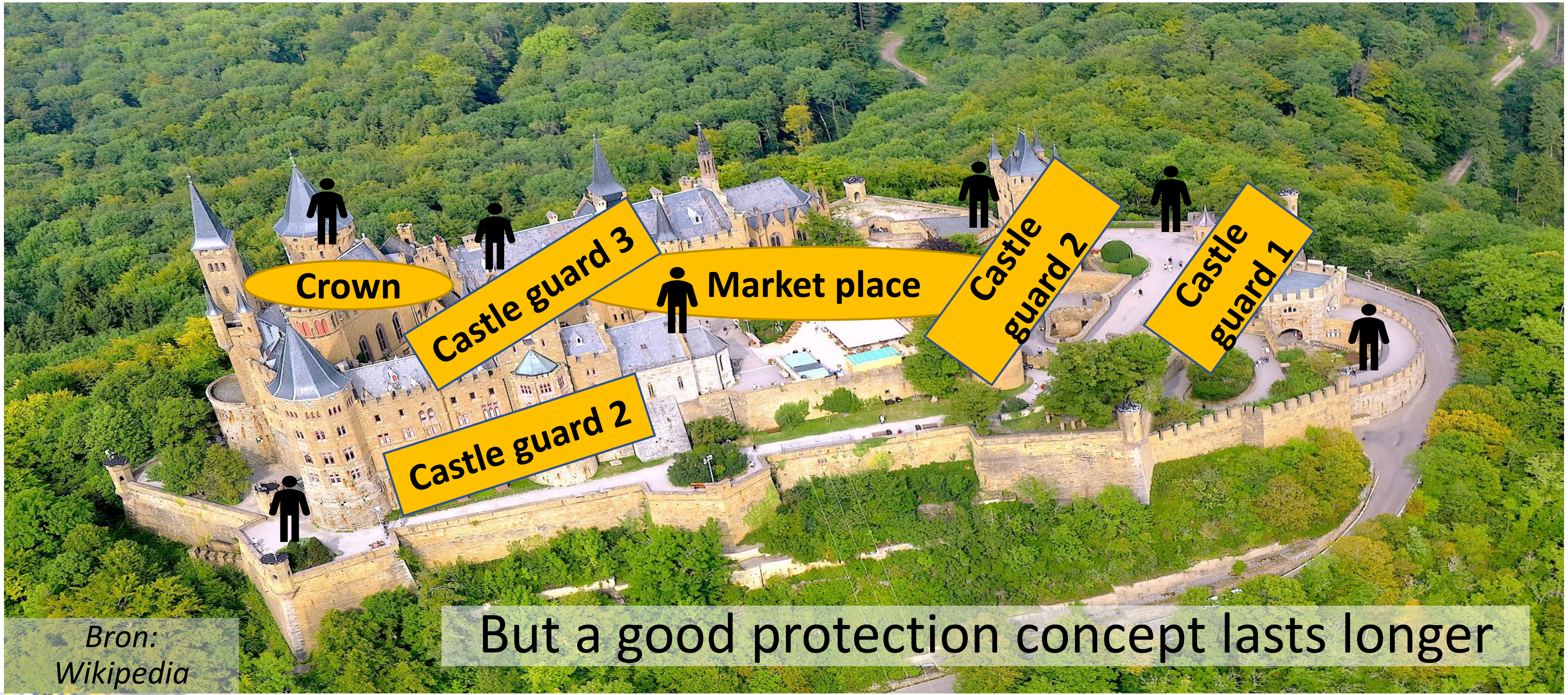
Requir

IEC 62443-4-2

Technical Security Requirements for IACS Components

Defence in Depth in the past

The bitter truth: there is no 100% protection

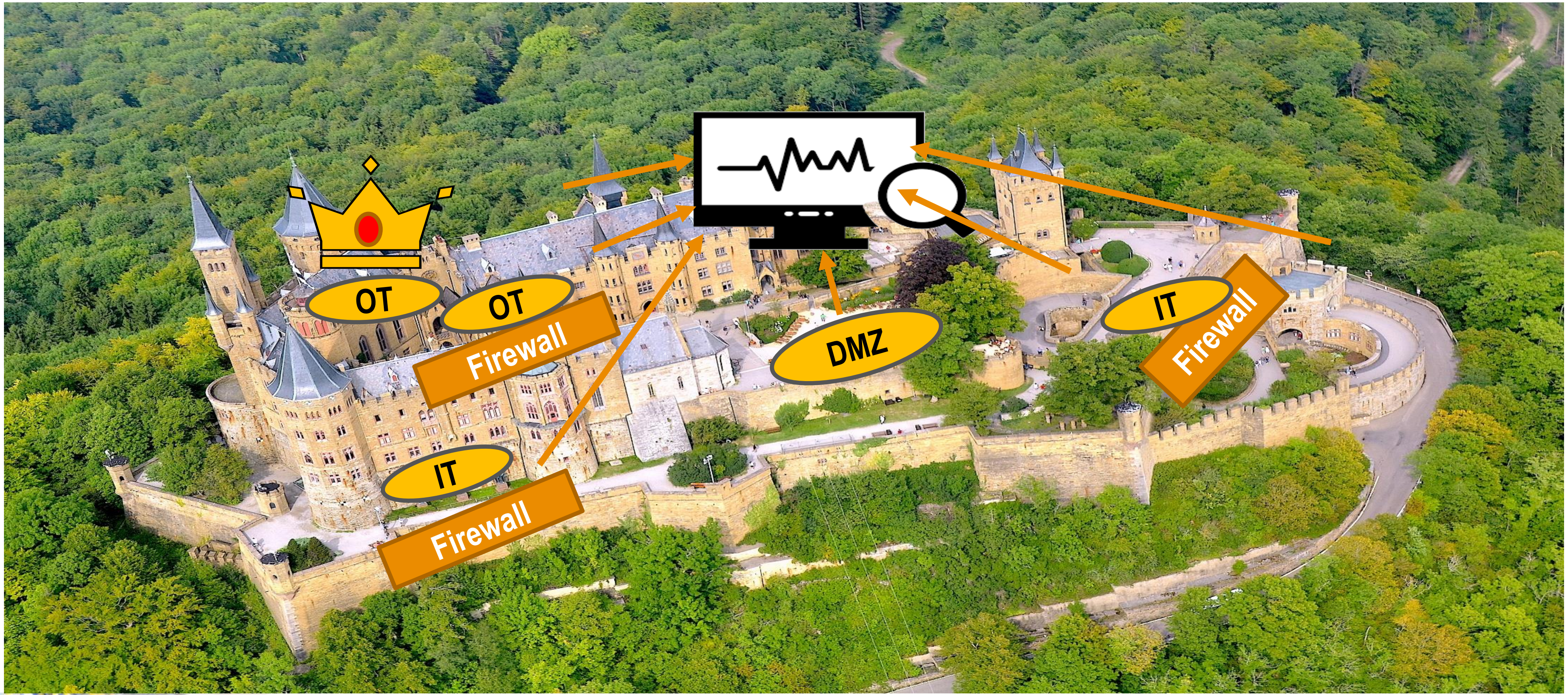


Bron: Wikipedia

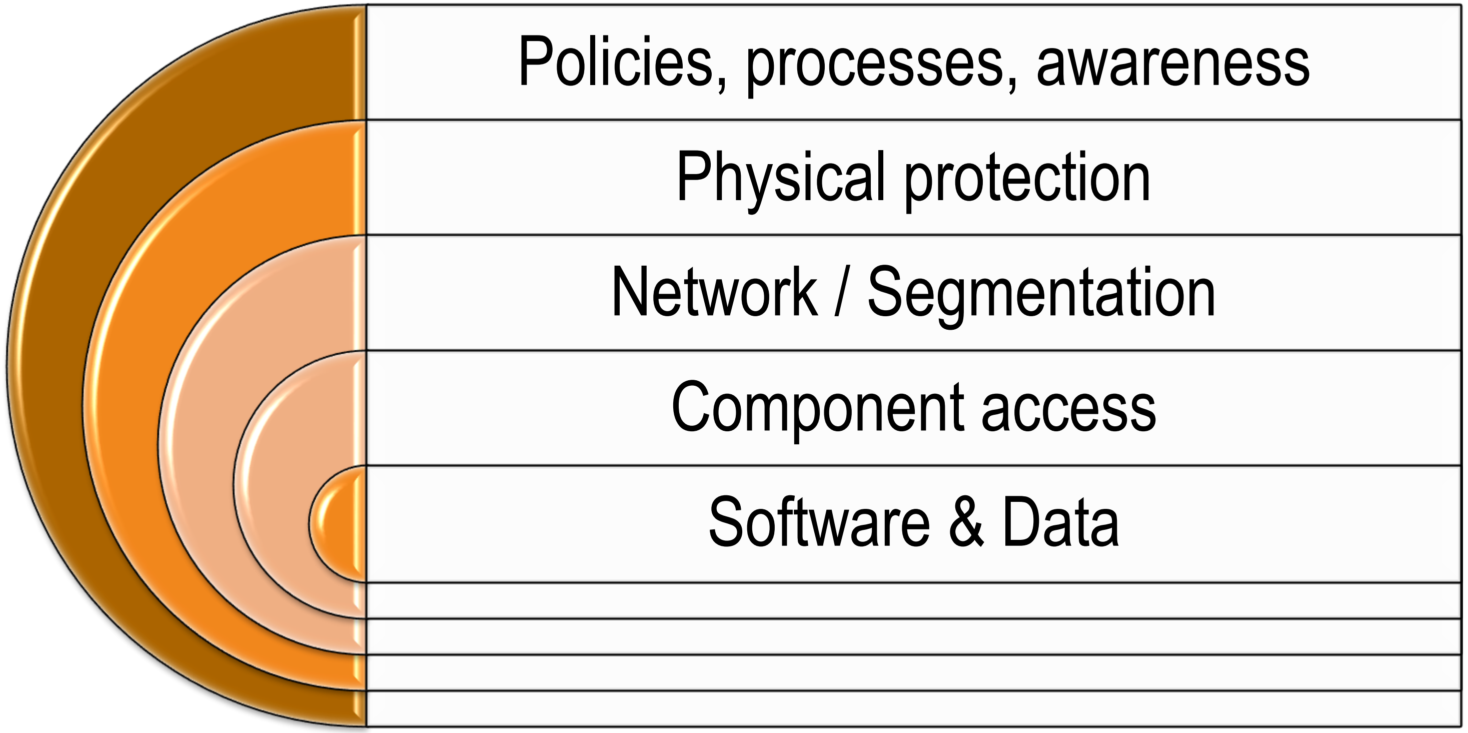
But a good protection concept lasts longer

Defence in Depth today (IT/ OT)

Still no 100% protection…



Defense in Depth as an "onion skin" model



Policies, processes, awareness

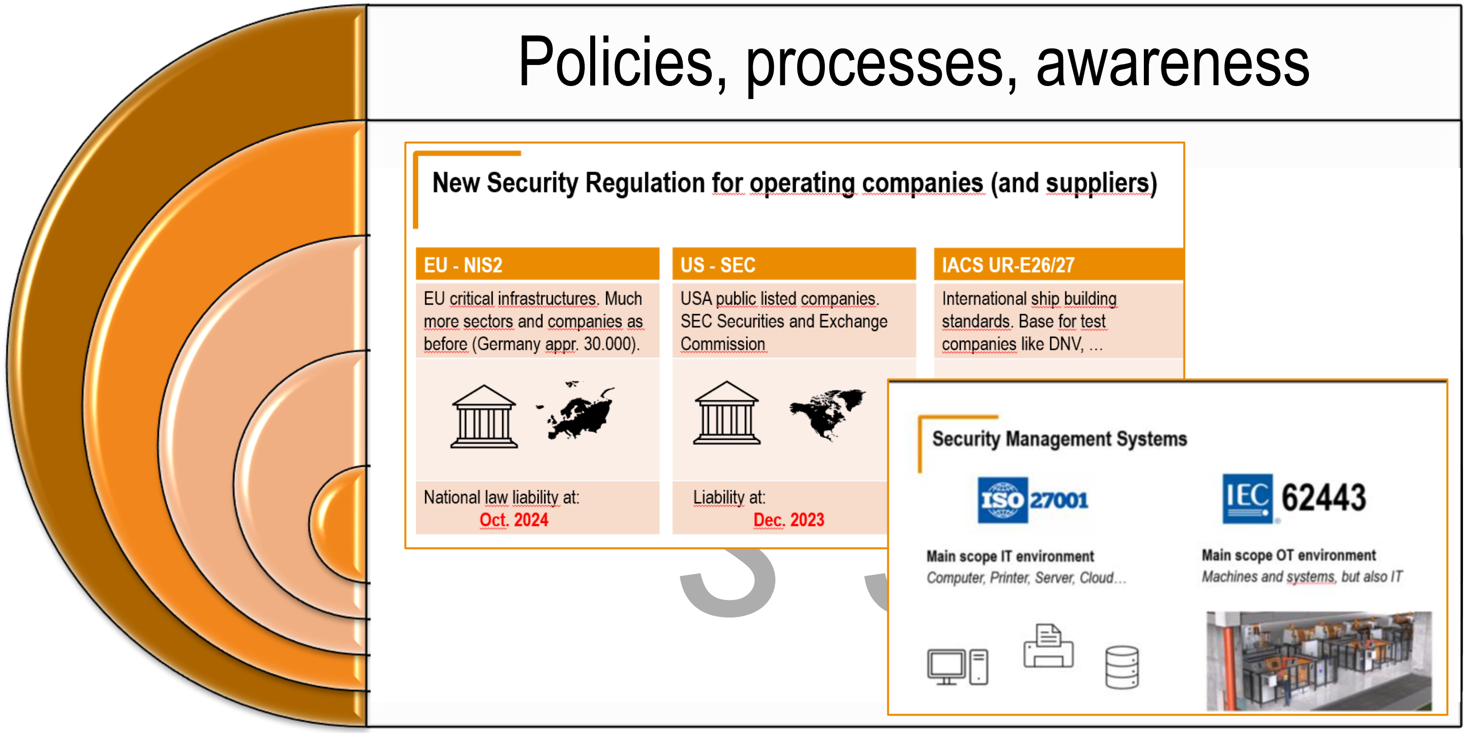
Physical protection

Network / Segmentation

Component access

Software & Data

Defense in Depth as an "onion skin" model



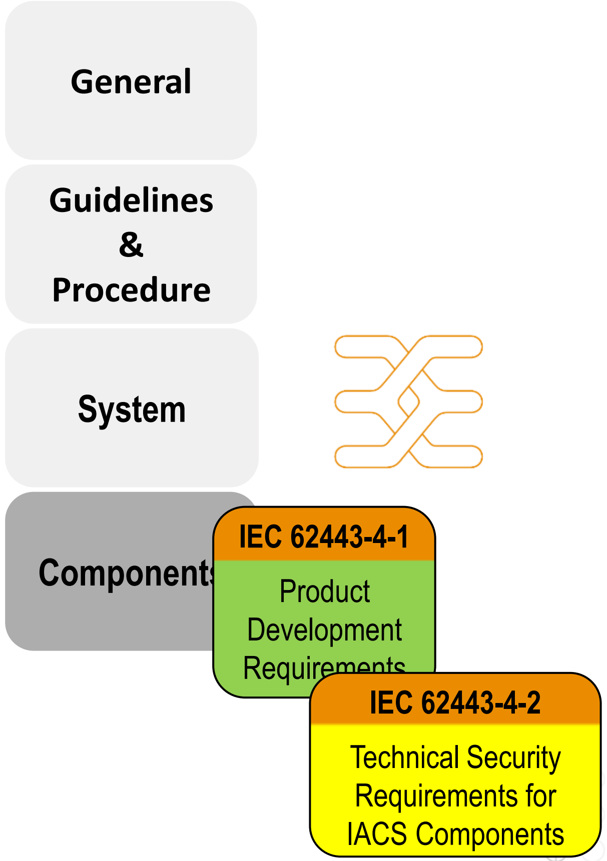
Policies, processes, awareness

New Security Regulation for operating companies (and suppliers)

EU - NIS2	US - SEC	IACS UR-E26/27
EU critical infrastructures. Much more sectors and companies as before (Germany appr. 30.000).	USA public listed companies. SEC Securities and Exchange Commission	International ship building standards. Base for test companies like DNV, …
National law liability at: Oct. 2024	Liability at: Dec. 2023	

Security Management Systems

ISO 27001	IEC 62443
Main scope IT environment *Computer, Printer, Server, Cloud…*	Main scope OT environment *Machines and systems, but also IT*



General

Guidelines & Procedure

System

Components

IEC 62443-4-1

Product Development Requirements

IEC 62443-4-2

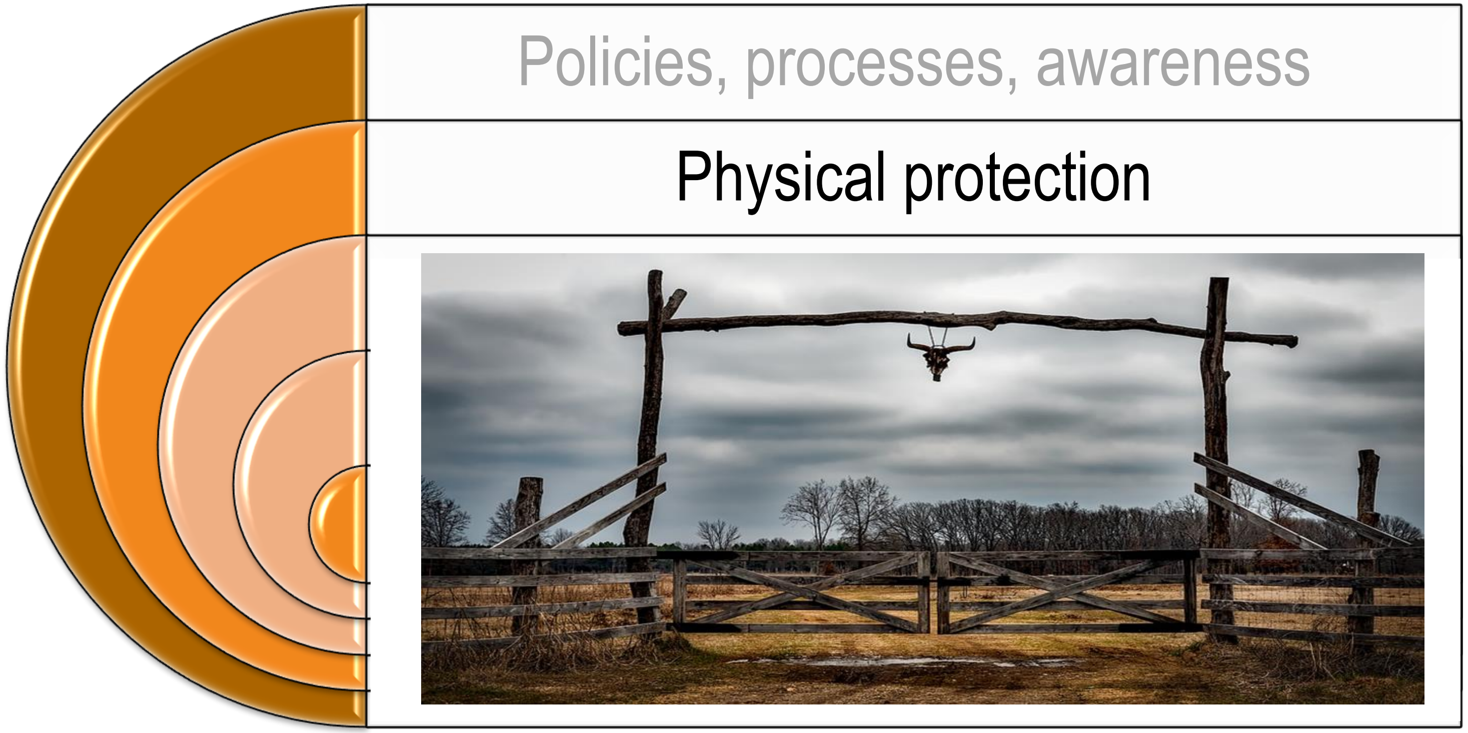
Technical Security Requirements for IACS Components

Defense in Depth

Topics for policies, processes, awareness acc. to IEC 62443

- Awareness and training of personnel
- Definition/review of responsibilities of plant users
- Definition/review of (user) roles
- Definition/review user access rights
- Regulations of physical access
- Implementation of an incident response plan.
- Definition of a patch management system for rolling out security patches

Defense in Depth

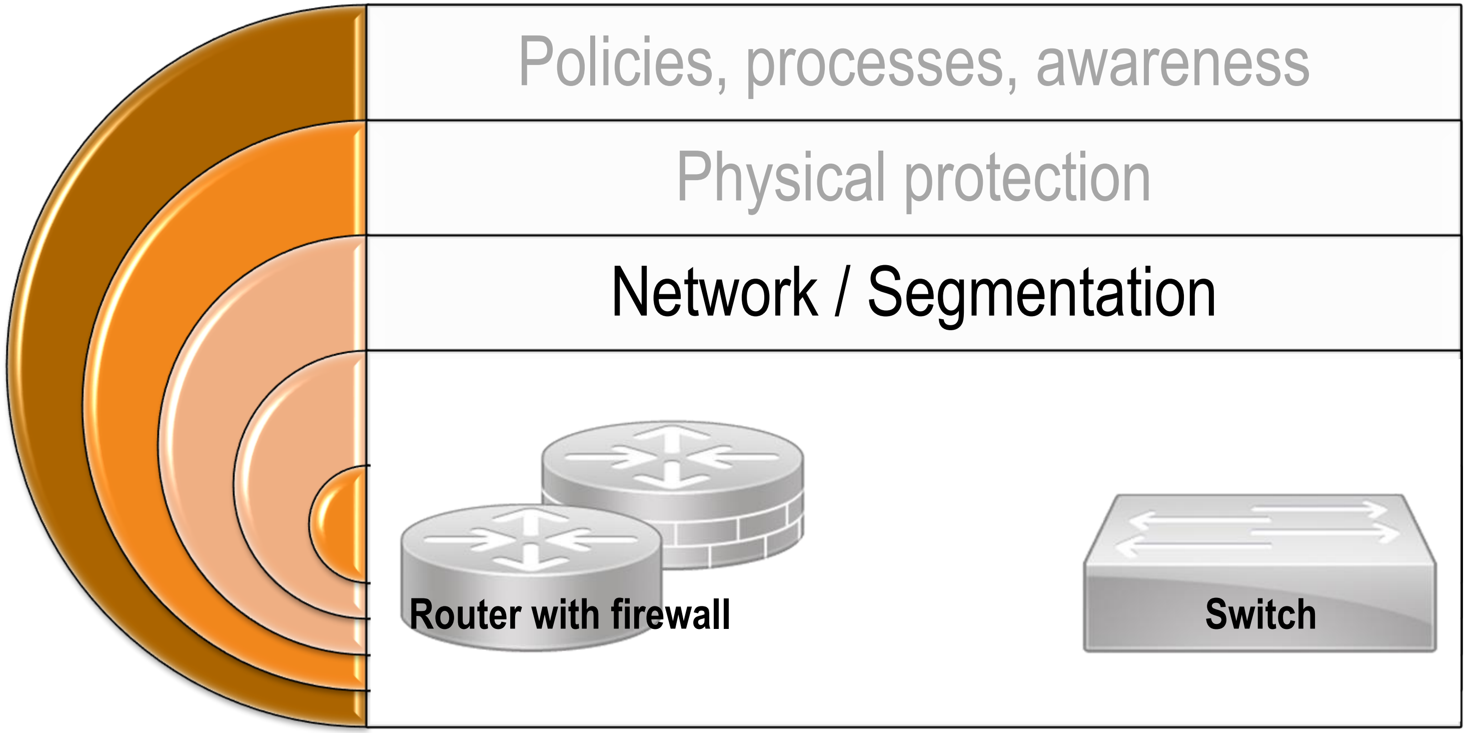


General Access Control

Cabinet lock with key

Lockable Service Interfaces

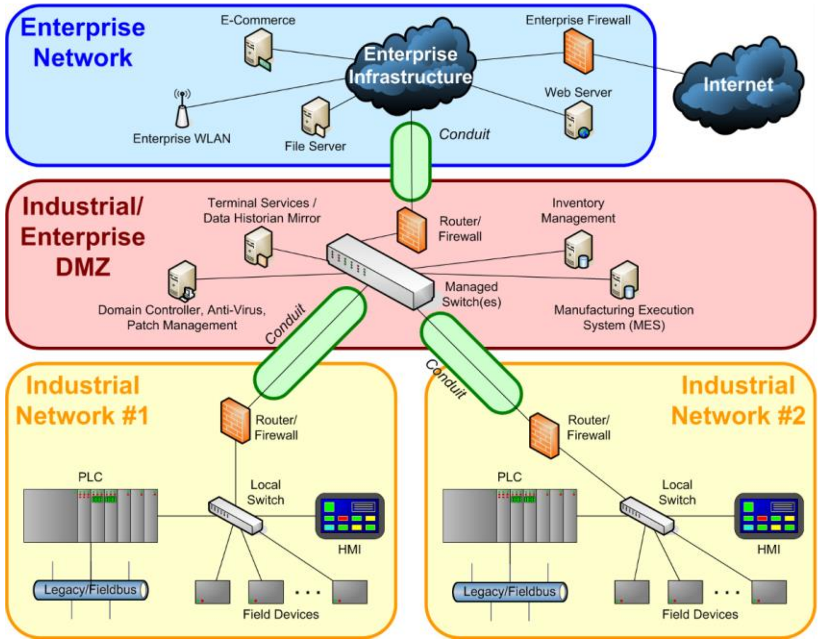
Defense in Depth: Physical access control



Policies, processes, awareness

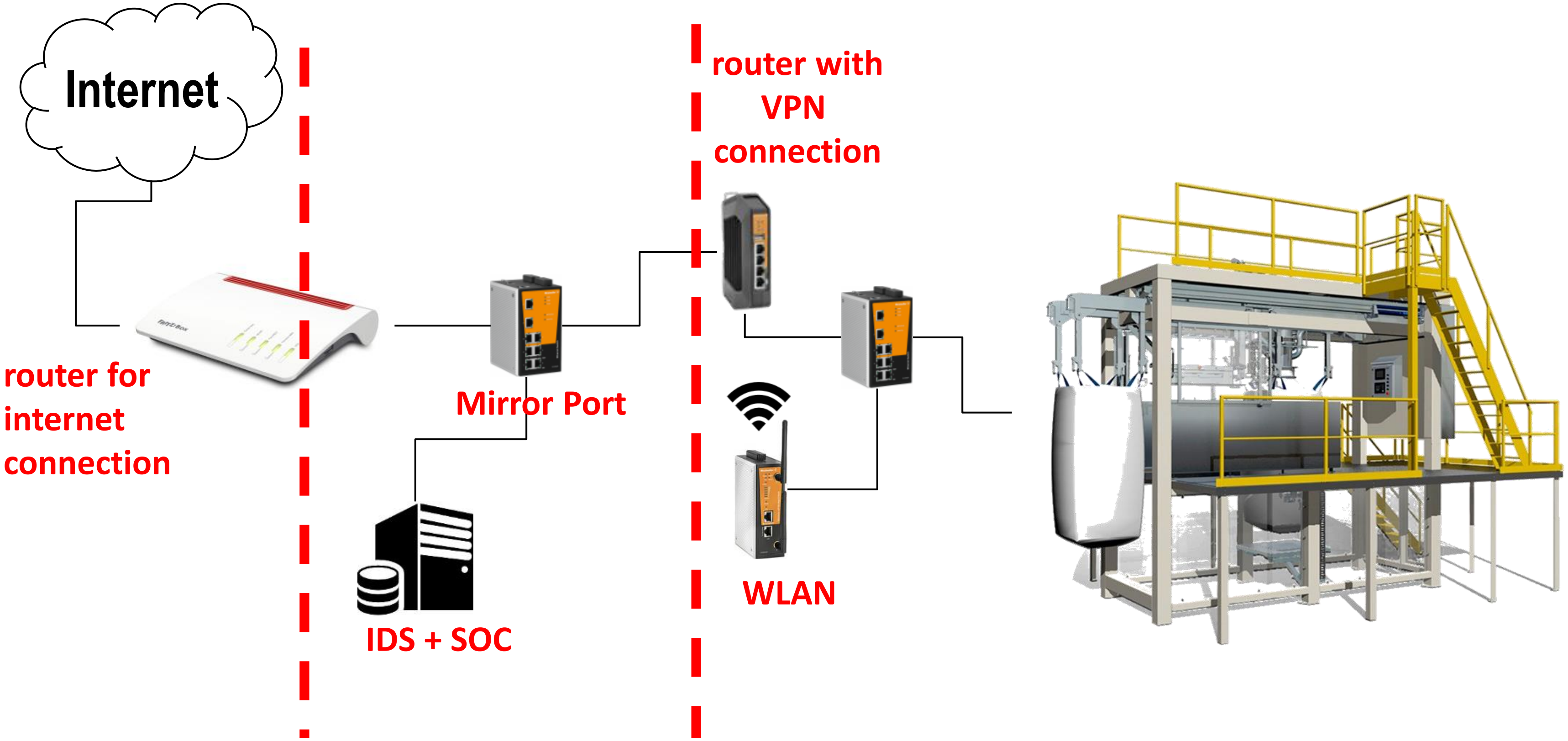
Physical protection

Network / Segmentation



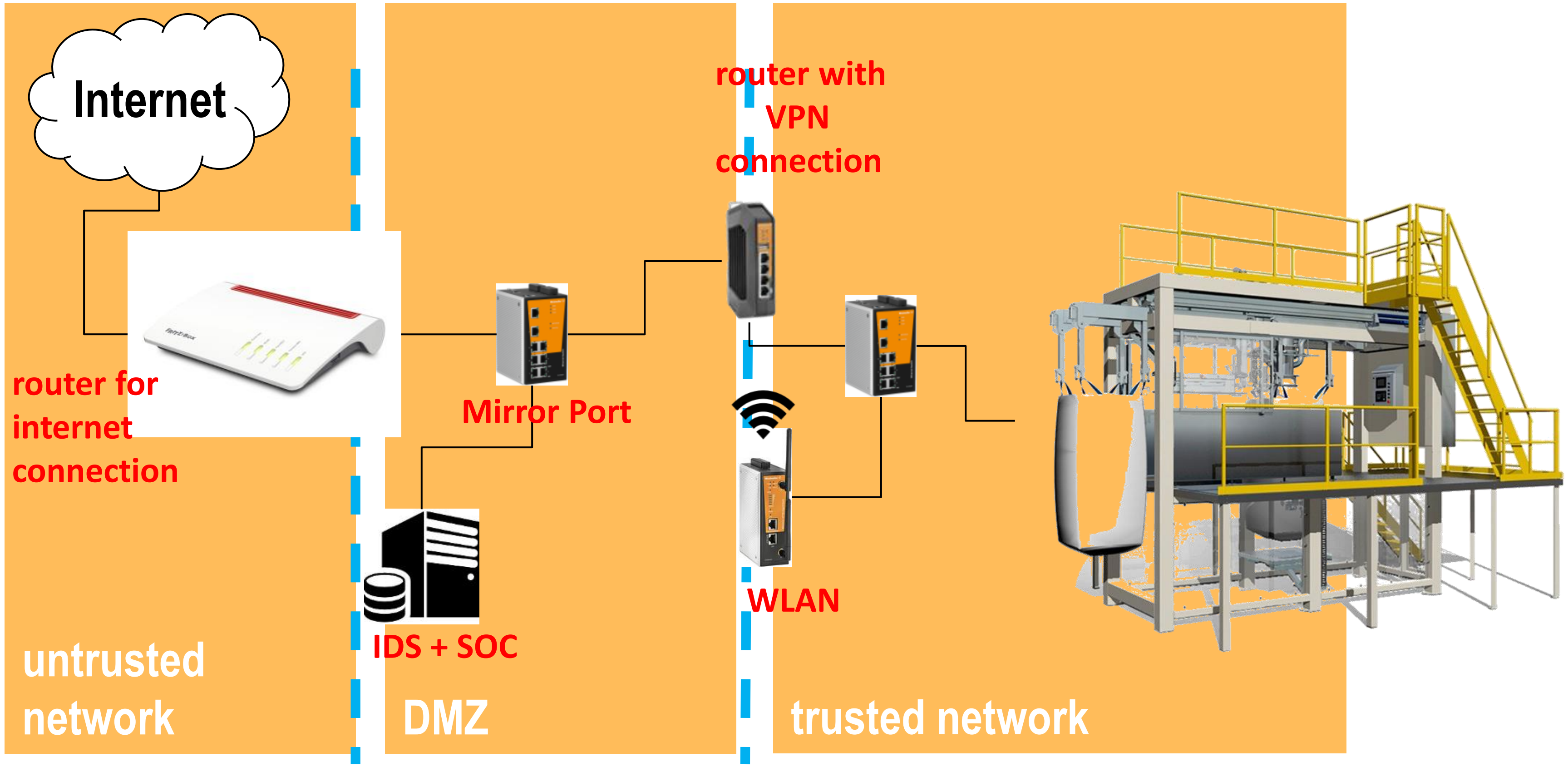
FHI INDUSTRIËLE AUTOMATISERING

Defense in Depth: Network Segmentation



IDS: Intrusion Detection System
SOC: Security Operation Center (SOC)

Defense in Depth: Network Segmentation



IDS: Intrusion Detection System
SOC: Security Operation Center (SOC)

Defense in Depth: Switch & Router functions

VLAN
Can segment the network into logical groups separating critical components from each other

ACL/ MAC/ IP-Filter
Filters packages on IP and port layer2
Reduces access. Only registrated devices can get access

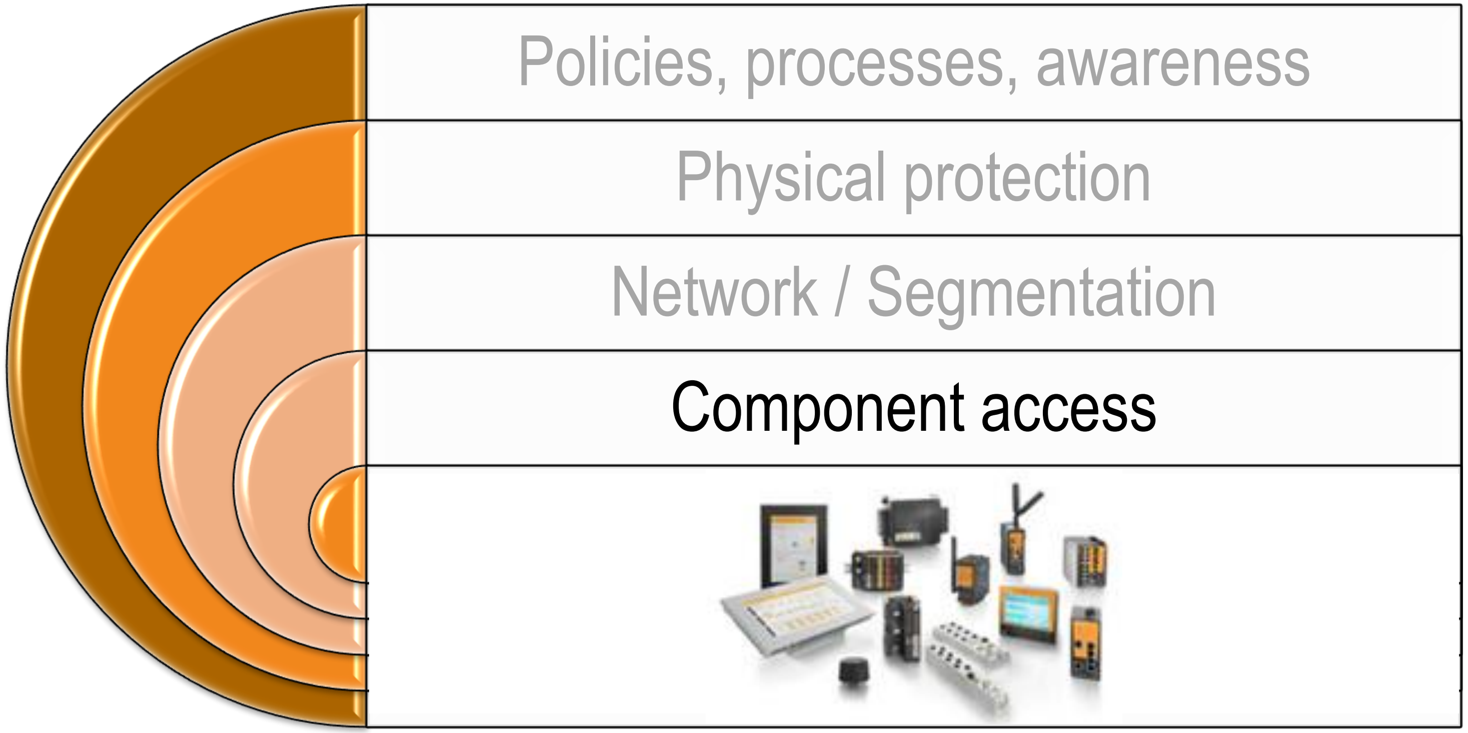
Mirrorport
Allows sniffing on communication with IDS-Systems to see unwanted traffic

SPI (statefull inspection firewall)
Blockes unwanted traffic

VPN (virtual private network)
Allows encrypted secure connection through untrusted networks *(IPsec, OpenVPN)*

Segmentation
Open Ports and services are reduced to a minimum

Defense in Depth



Policies, processes, awareness

Physical protection

Network / Segmentation

Component access

Best practice

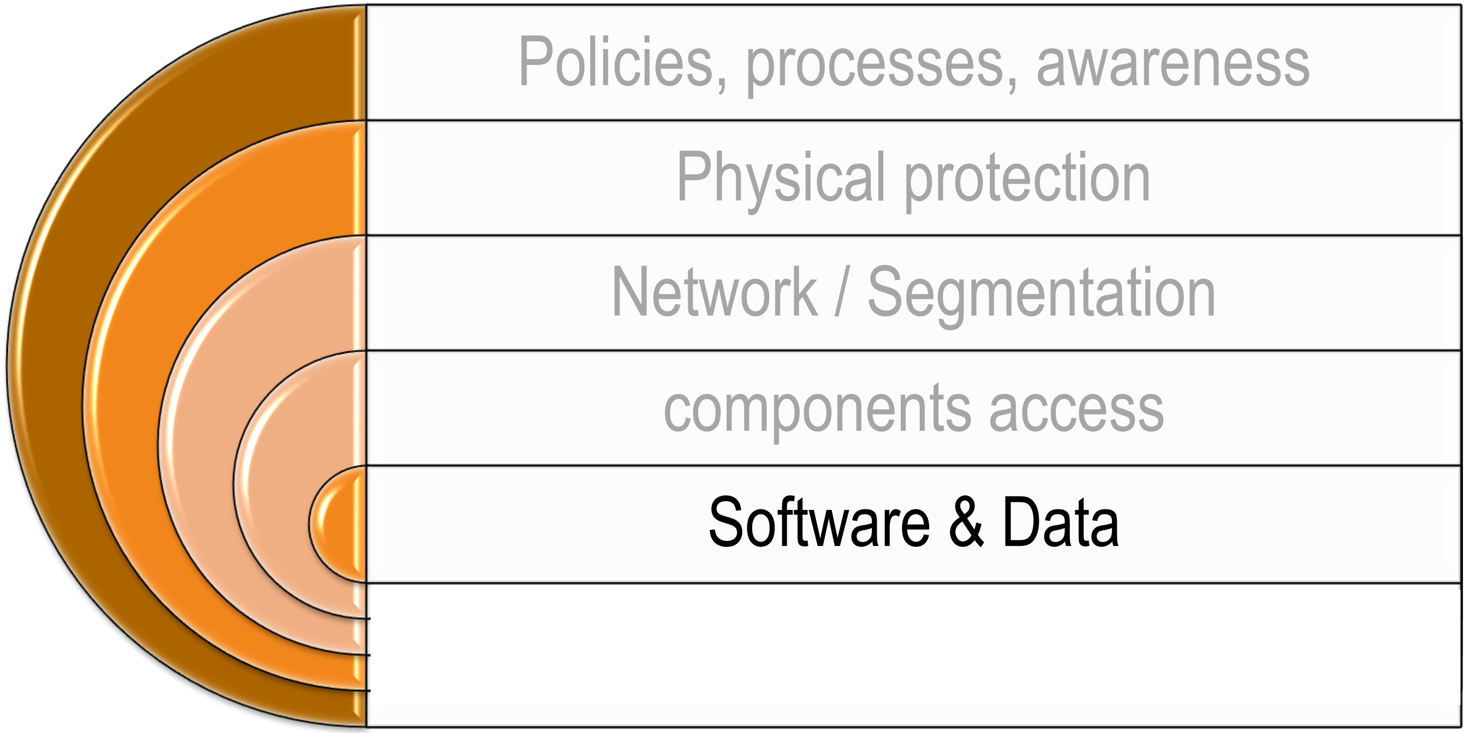
- Use lowest privileg for a user account as possible
- Use a strong password. Always change default passwords.
- Revoke rights when personnel change departments or leave the company (RADIUS / TACAS+)
  Integration into a higher-level Identification & Access Management system where possible (RADIUS / TACAS+)

Defense in Depth: Component access

Access rights, as much as necessary, as little as possible!

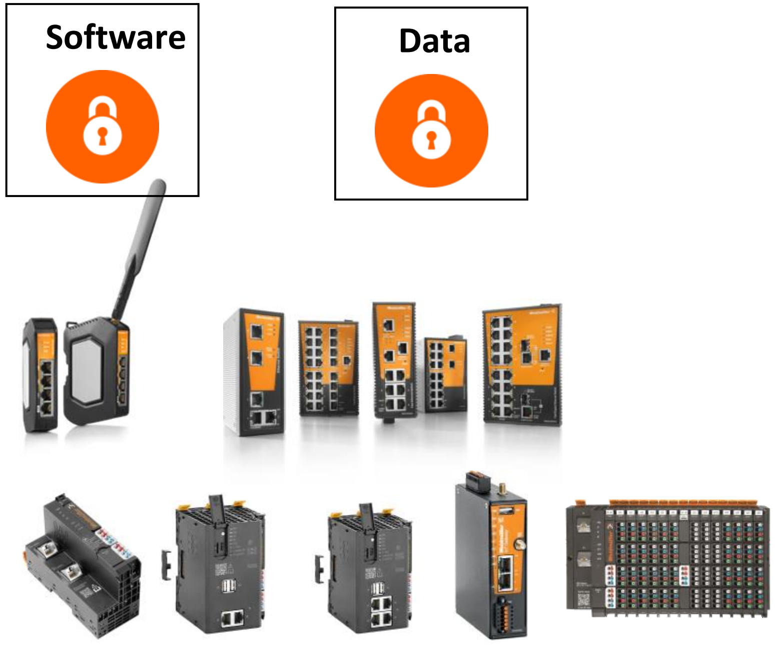
	Admin (OT)	Operator	Service	Machine Specialist	IT
IPC	setting up	Executing Programs	Customize Configurations	Programming	-
PLC		Executing Programs	Customize Configurations	Programming	-
HMI		Executing Programs		Programming	-
Router	setting up	-	-	setting up	Maintenance/ Integration
Switches	setting up	-	-	setting up	Maintenance/ Integration

Defense in Depth

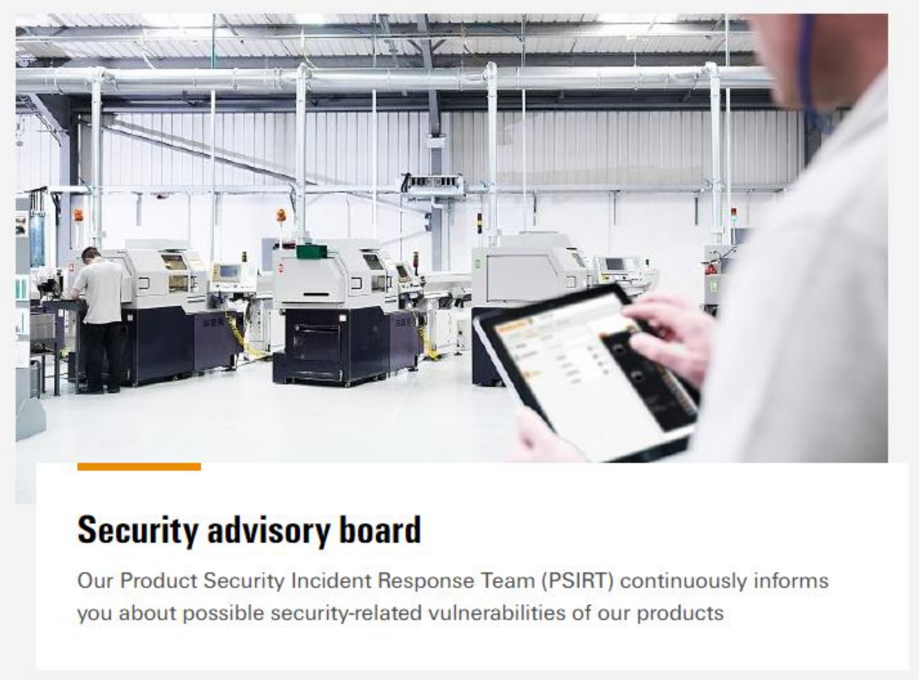


Defense in Depth: software & Data

- Secure hardened Linux systems
- Secure Firmware (f.e. TPM2 chip)
- Secure boot
- Updates & Backup/ Restore functionality
- Functional updates and security patches.



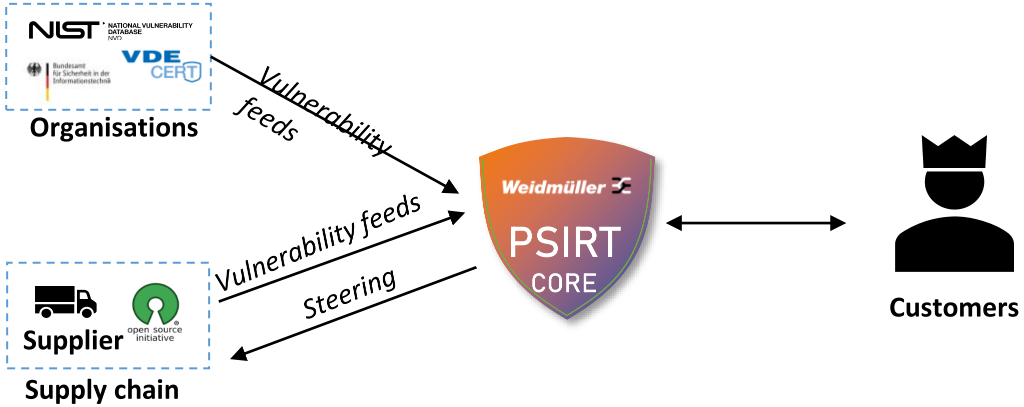
How Weidmüller manages vulnerabilities – PSIRT



Security advisory board

Our Product Security Incident Response Team (PSIRT) continuously informs you about possible security-related vulnerabilities of our products

VDE CERT



Weidmüller

Thank you for your attention and

Let’s connect!

Marcel Tuit
Business development manager machinery
at Weidmüller Benelux

Vocabulary

ENISA	De Europese Agentschap voor Cybersecurity
NIS2	Network and Information Security
SEC	Securities and Exchange Commission
RED DA	Radio Equipment Directive (RED) - European Commission
EU – Machinery Act	EU Machinery Regulation - New safety requirements on plant and machinery
EU - Cyber Resiliance Act	Legal framework that describes the cybersecurity requirements
CSMS	Cyber Security Management System
IDS	Intrusion Detection System
SOC	Security Operation Center
PSIRT	Product Security Incident Response Team
NIST	National Institute of Standards and Technology
VDE	Verein Deutsche Elektriker: Association for Electrical, Electronic & Information Technologies
CERT@VDE	CERT@VDE is part of the non-profit VDE
TPM2	Trusted Platform Module -is an international standard for a secure cryptoprocessor