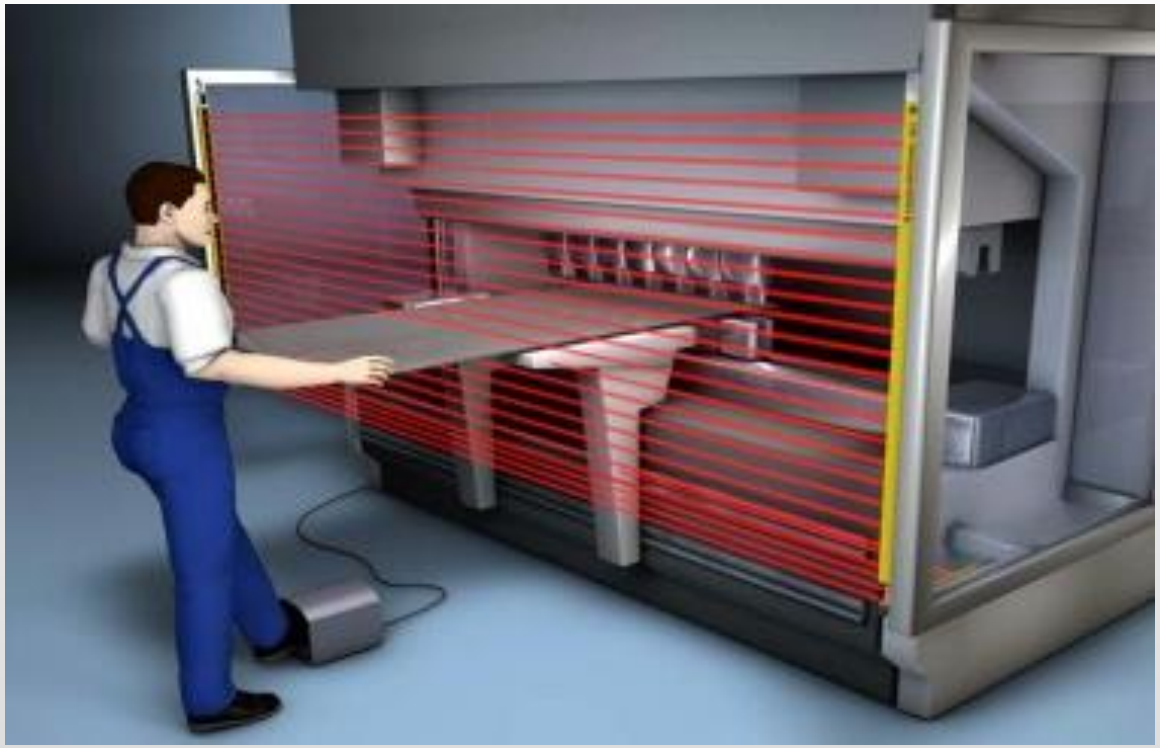
Wat is het doel van Cybersecurity? Welke methodes en technologieën zijn er om dit te bereiken.

Compliance vanuit product perspectief

Cybersecurity vs Safety

The Goals are different!



Functional Safety:
Protection of the Human from the Machine

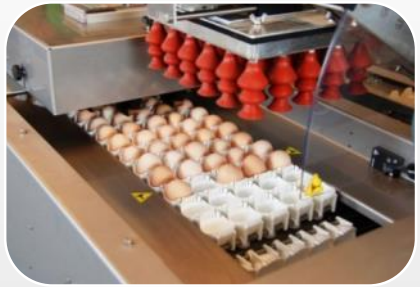
Cybersecurity:
Protection of Data and the Machine from the unauthorized Human

Cybersecurity: Goals

What goals does Cybersecurity have?

Confidentiality

Availability



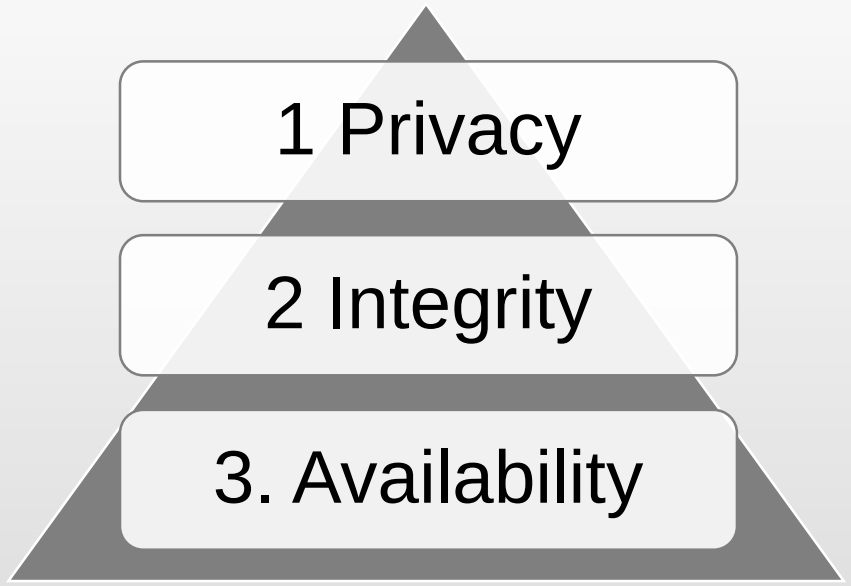
Integrity

Non-Repudiation

Information is transmitted over channels. Therefore, measures are taken to protect these channels.
Other sensible assets are the automation system and the operator stations. They have to be protected likewise against misuse.
Depending on the industrial branch the exposure to security threats is different.
Anyhow, a framework for IT security is currently being laid out (IEC 27000ff)

Cybersecurity: Goals

What goals does Cybersecurity have?



Office

Automation

Cybersecurity: Goals

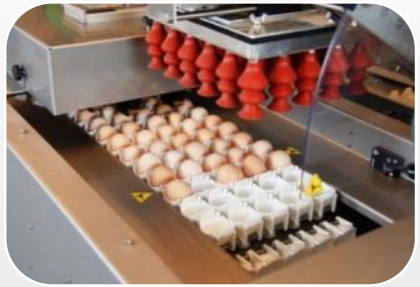
To which threats the goals are exposed?

Confidentiality

Unauthorized Access to Information

Availability

Denial of Service (DoS) or Prevention of Authorized Access



Integrity

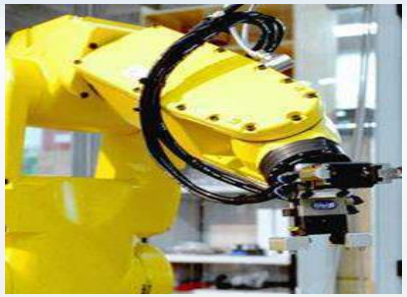
Unauthorized Modification or Theft of Information

Non-Repudiation

Denial of Action that took place or Claim of Action that did not take place, Accountability

Cybersecurity: Legislation

What does KRITIS mean for the target industries?



Process and organizational design according to "best practice", recommendations

Process and organizational design according to laws and regulations

CRITICAL infrastructure: special importance for the

- **the continued existence of the State, or**
- **Protection of the population (security of supply, public order)**

Energy: "BDEW White Paper"

Obligation to report cyber attacks to BSI

Cybersecurity: Legislation

What does KRITIS mean for the target industries?

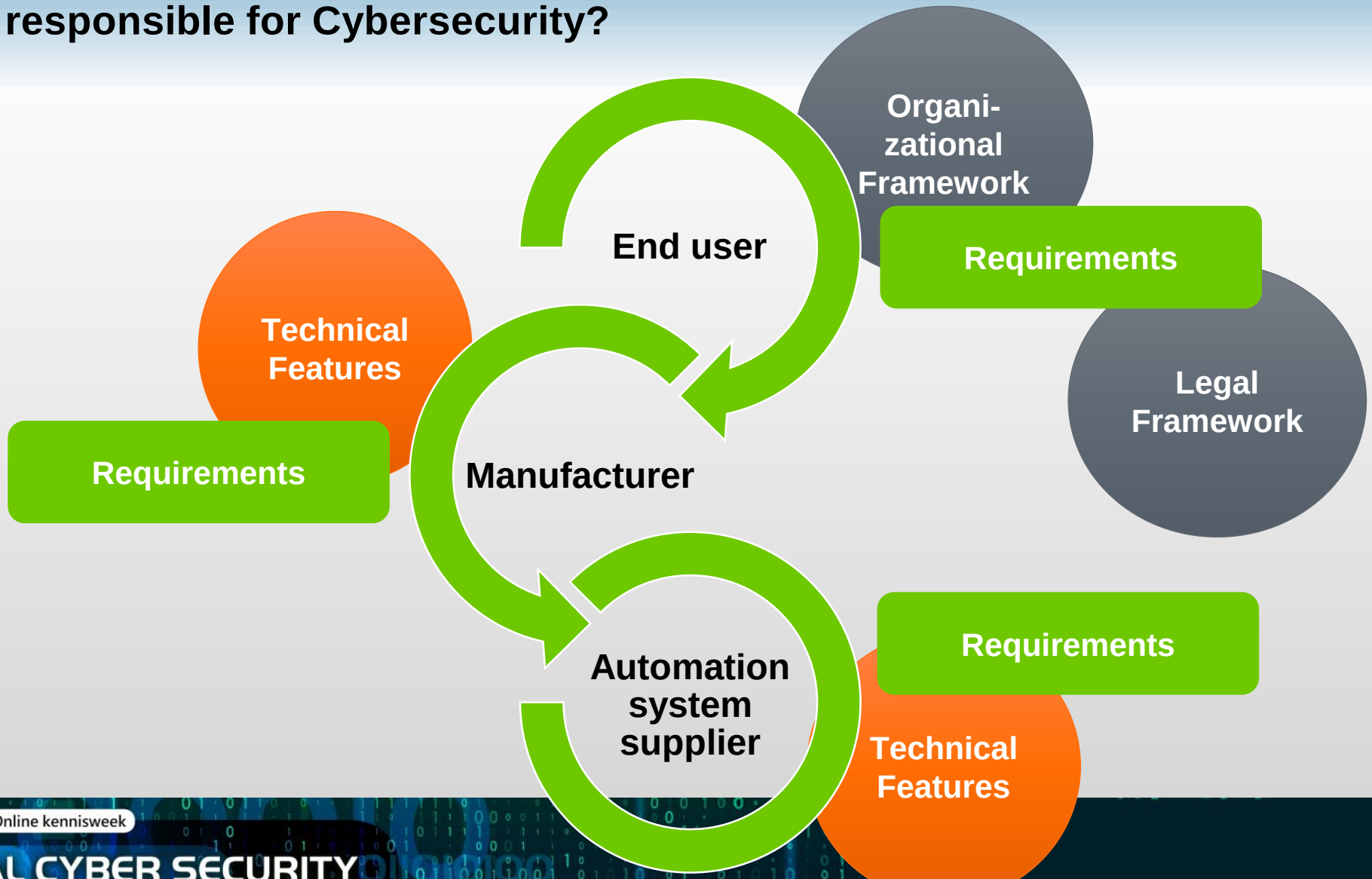
- Access to automation network from the office network for analysis and logistic control
- lower availability leads to profit losses

- Maintenance and service complicated for on board staff → remote support
- Implementation of preventive maintenance schemes

- Remote service and diagnosis of wide-spread installations → reduce personnel cost
- Legal requirements for documentation of emissions, consumptions

Cybersecurity: General concept

Who is responsible for Cybersecurity?



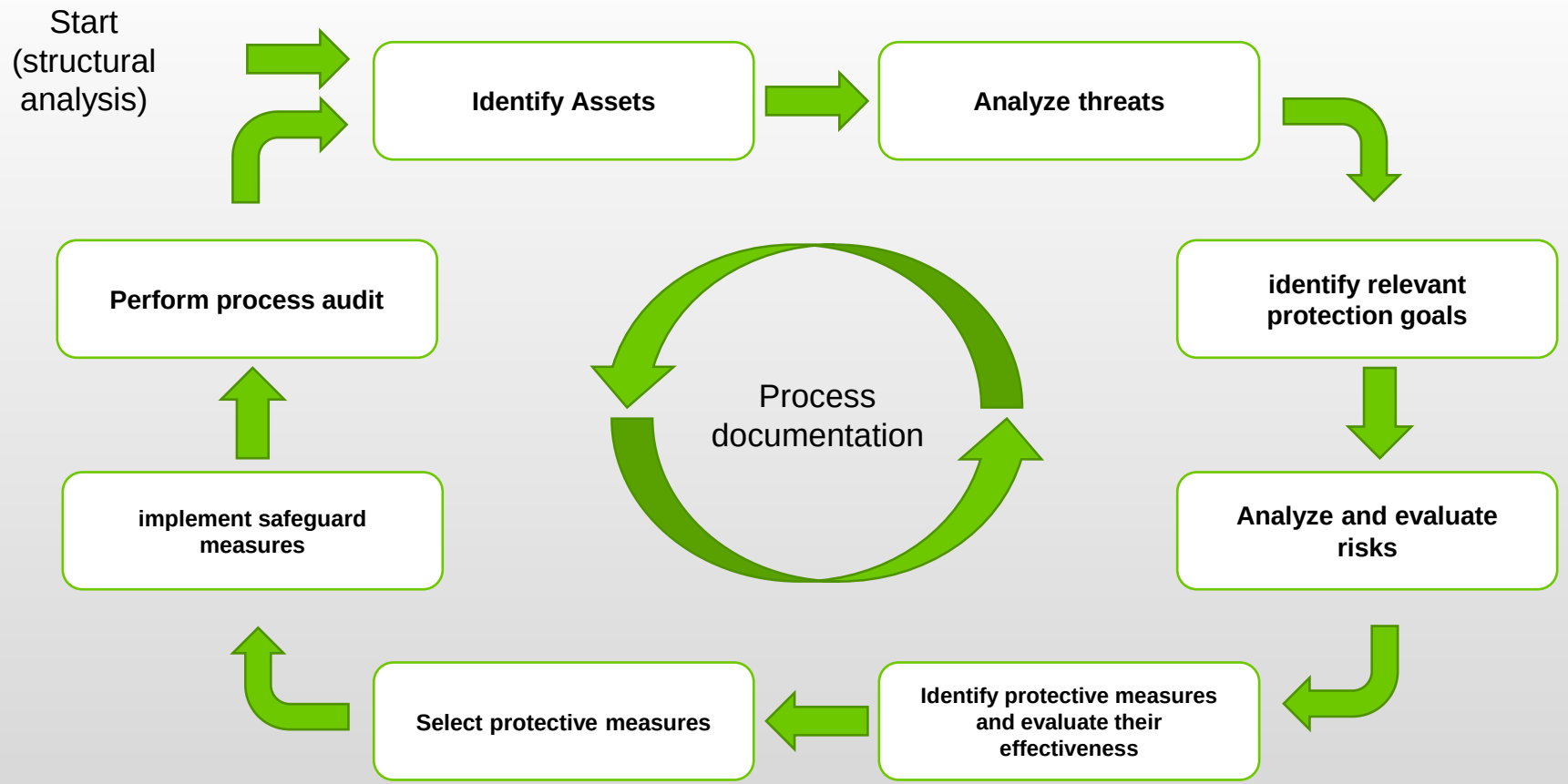
Cybersecurity: Responsibilities

How do the different parties act together?

Example: User Access Rights	Organizational Measure	Technical Measure
End user	• Definition of responsibilities (Line operator, service, commissioning service) • Access to Documentation • Periodic Check of role based access rights	• Restrict Access to the Assets
Equipment Manufacturer	• Definition of Access to Programming tools and Asset SW	• Implementing role based access model in the SW • Assign Functions/Permissions to users • Delete/De-Activate Admins / Programming users after commissioning • Access protection to cabinets
Automation System Manufacturer	• Periodic Check of Vulnerability of SW and HW	• Provide role and user management in the automation SW

Cybersecurity: Concept development and implementation

How do I implement Cybersecurity? What do the regulations all have in common?



source: VDI2182

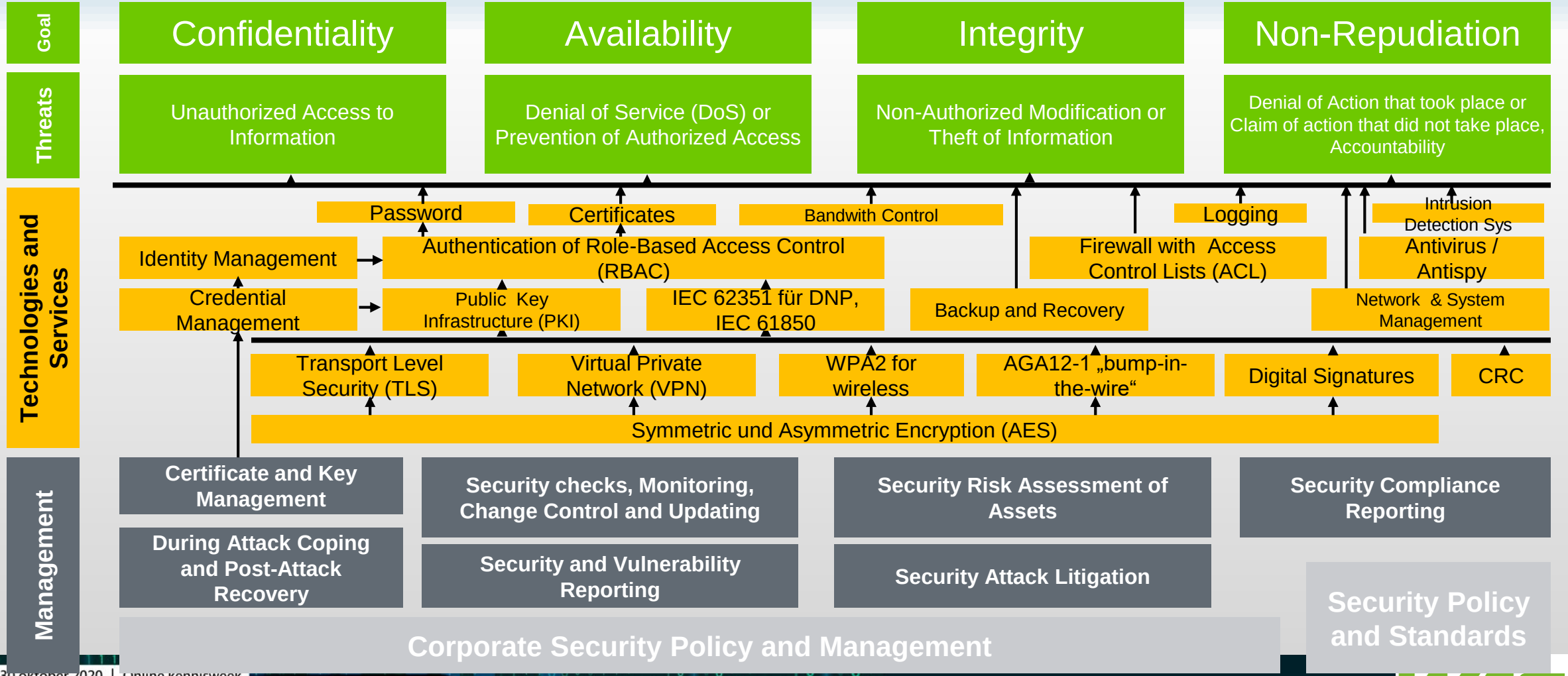
Cybersecurity: Solution Concepts

Defense-in-Depth: What is the meaning of this concept?

Level	Description
Permissions	Implement the „need-to-know“-principle in the company
Network	Implement a Segmented Network with Access Control and Logs
Employee	Raising awareness and defining rules of conduct
Limit / Borderline of the Enterprise Network	Implement restrictive Firewalls and rule-based Defense Systems

Cybersecurity: Technologies and Methods

Threats, Goals, Concepts known: What methods and technologies are existing?



Technische oplossingen

Vanuit product perspectief

Cybersecurity: Technologies and Services

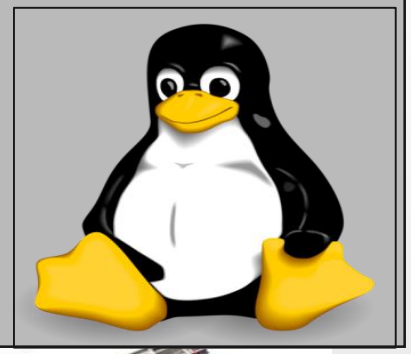
Which tools does a LINUX device provide?

Security Services

- Password protection, user management
- SSL/TLS 1.2 Encryption
- SSH – secure shell
- VPN (OpenVPN, IPSec)
- Firewall
- MAC-White list

Integrated in Linux

- Syslog
- SD-Card reader
- FTPs, SFTP, SCP
- optional: Rsync, Backup
- optional: Virus scanner
- optional: Fail2Ban



possible

not possible

Technologies and Services

Password | Certificates | Bandwith Control | Logging | Intrusion Detection Sys

Identity Management → Authentication of Role-Based Access Control (RBAC) | Firewall with Access Control Lists (ACL) | Antivirus / Antispy

Credential Management → Public Key Infrastructure (PKI) | IEC 62351 für DNP, IEC 61850 | Backup and Recovery | Network & System Management

Transport Level Security (TLS) | Virtual Private Network (VPN) | WPA2 for wireless | AGA12-1 „bump-in-the-wire“ | Digital Signatures | CRC

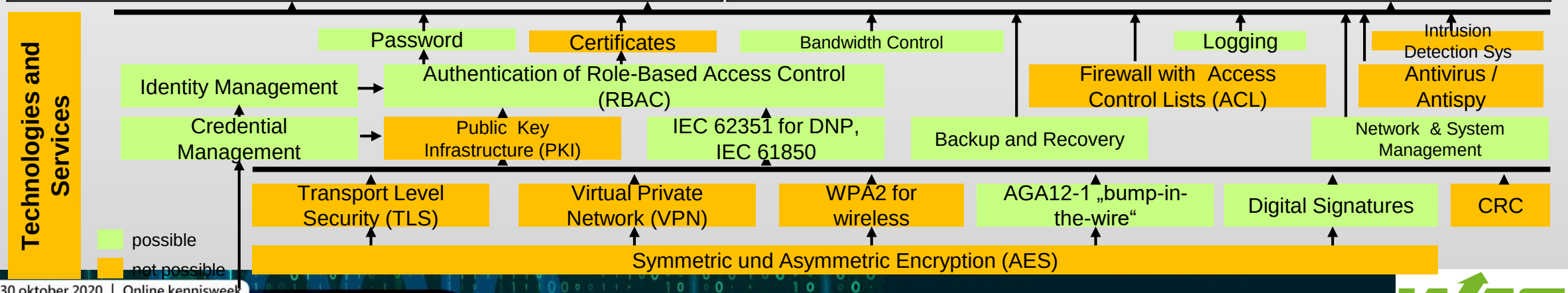
Symmetric und Asymmetric Encryption (AES)

Cybersecurity: Technologies and Services

Which tools do the Switches provide?

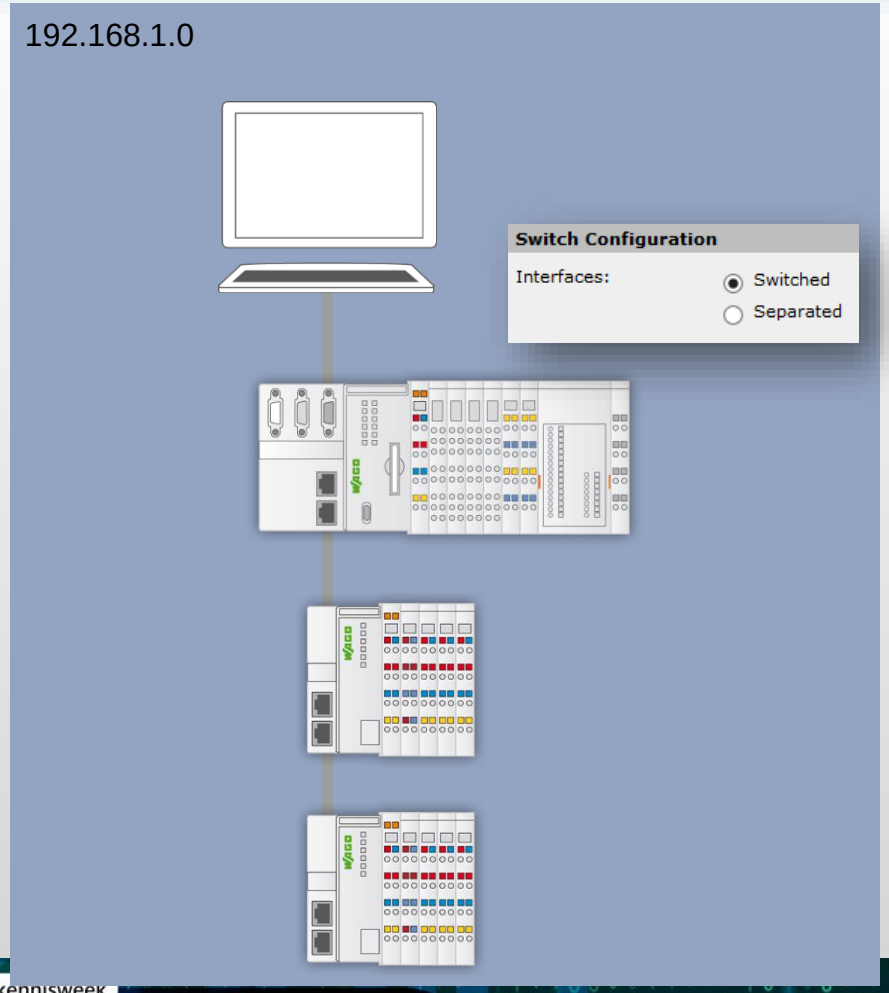
Integrated Services
- Logs, Alarms (by email)
- SNMP v2, v3
- Parameter Backup/Restore

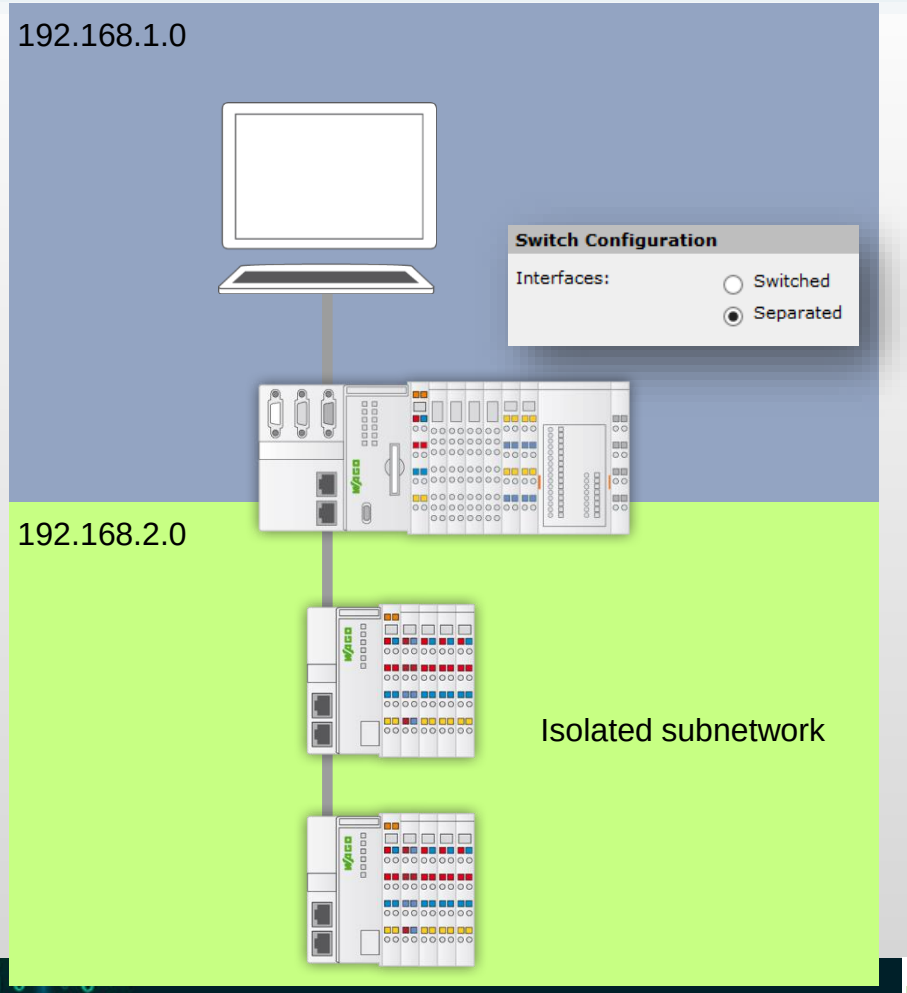
Security Services
- Password Protection, User Management
- SSL/TLS 1.2 Encryption
- Bandwidth Limitation
- Bandwidth Control
- MAC-White list
- ARP-Inspection
- DHCP-Snooping
- L2,L3-Access Control List
- 802.1x Port Access Control



Configurable Ethernet interfaces

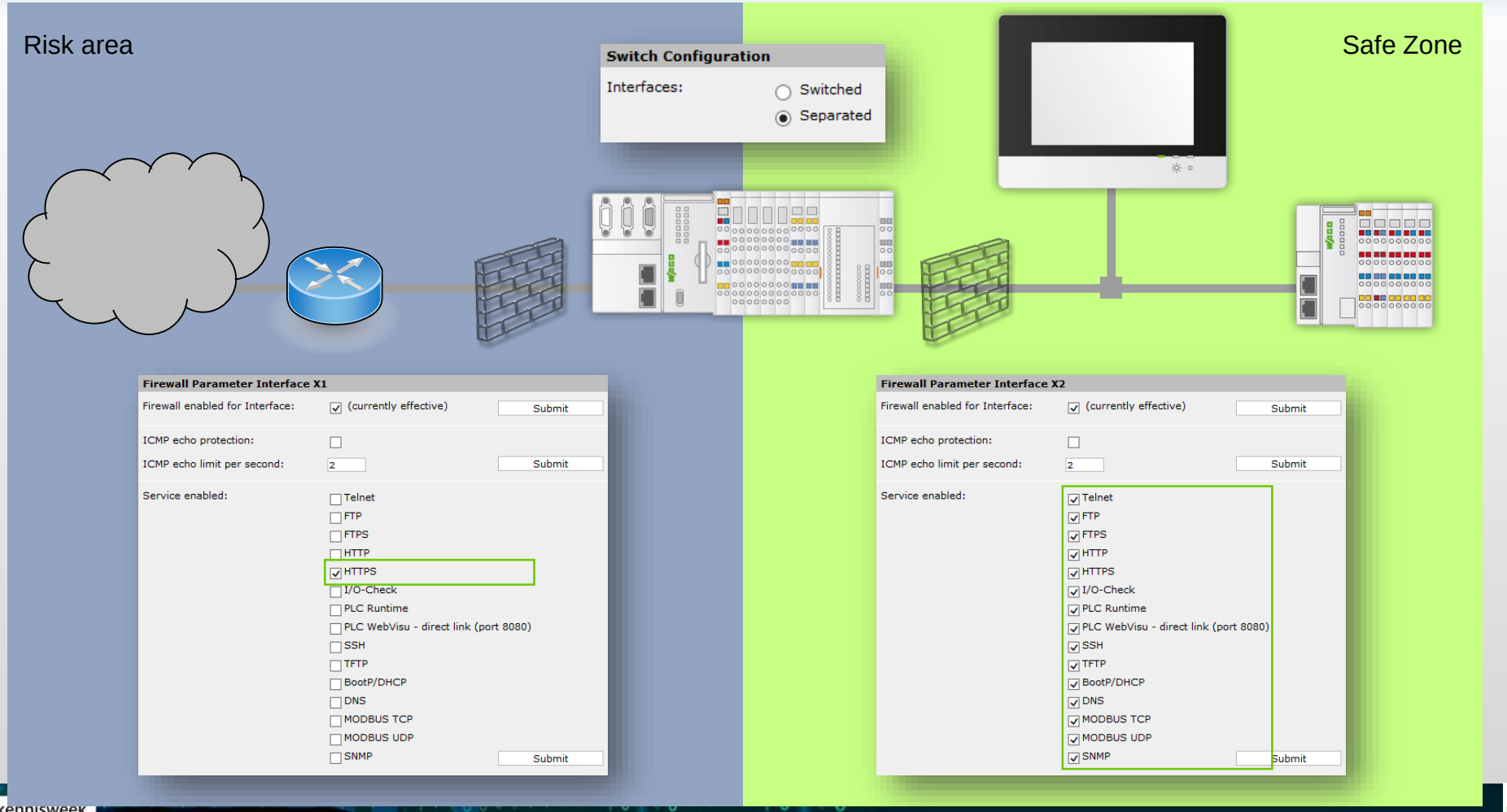
Integrated switch or 2 separate interfaces





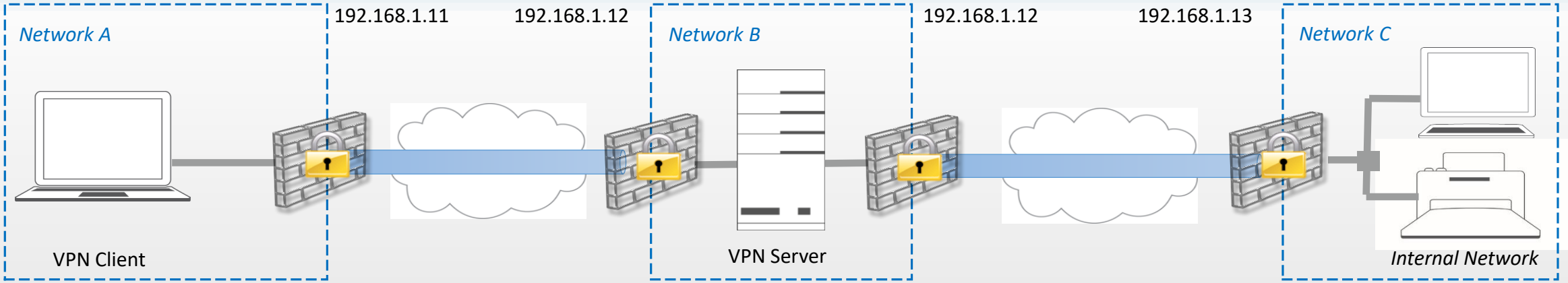
Interface configurable Firewall

Allow or block each service individually

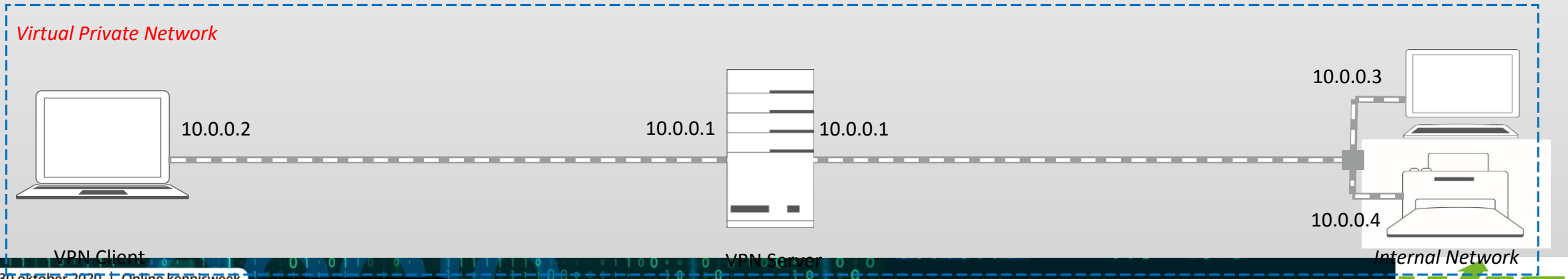


Virtual Private Network

Physical view

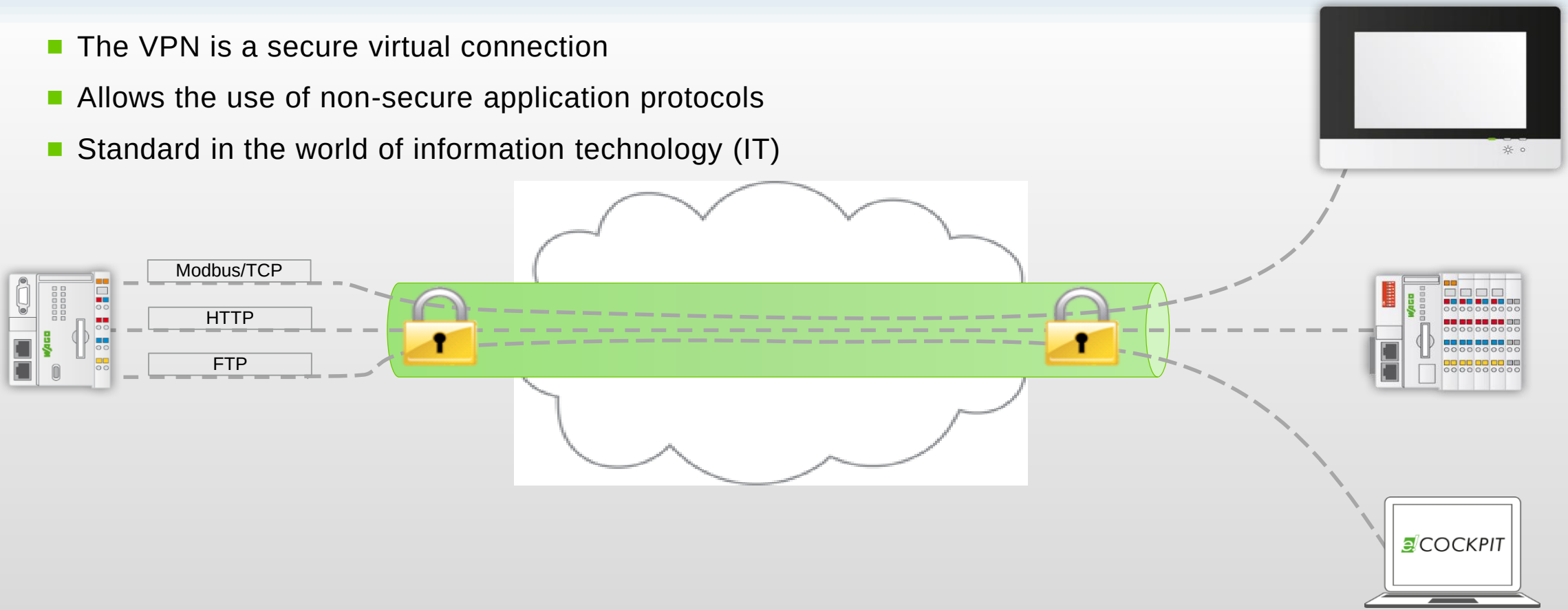


Logical view



Virtual Private Network

- The VPN is a secure virtual connection
- Allows the use of non-secure application protocols
- Standard in the world of information technology (IT)



Stapplannen voor implementatie cyber security maatregelen

Status en toelichting

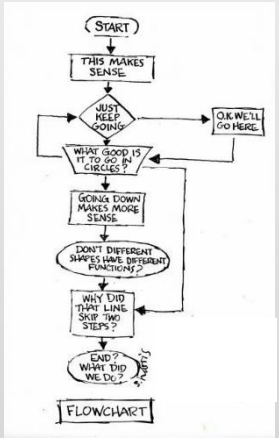
Cybersecurity in production plants step by step... Organization and processes

1. management commitment

- Top-Down Process
- similar to secrecy or commercial responsibility

2. Organization of responsibilities and processes

- management representative
- Knowledge about office and production area
- Integration of suppliers and system integrators



3. Preparation of a guideline

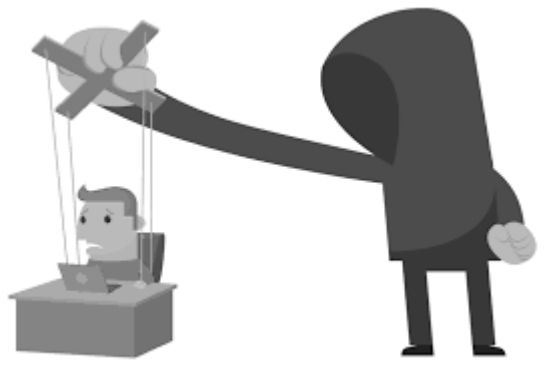
- Written record of expected behavior and how it is spread/practiced
- Sanctions for non-compliance
- Office: Installing programs, handling USB sticks, ...
- Production: Installing updates, handling protective devices
- Criteria for the selection of Ethernet-capable components for manufacturing

Cybersecurity in production plants step by step... Organization and processes

4. Training of staff

- The human being the softest factor in the production system
- Convenience and apparent "efficiency" conflict with effective protection against cyber attacks

→Awareness raising is necessary in regular intervals



5. Procurement and supply of knowledge

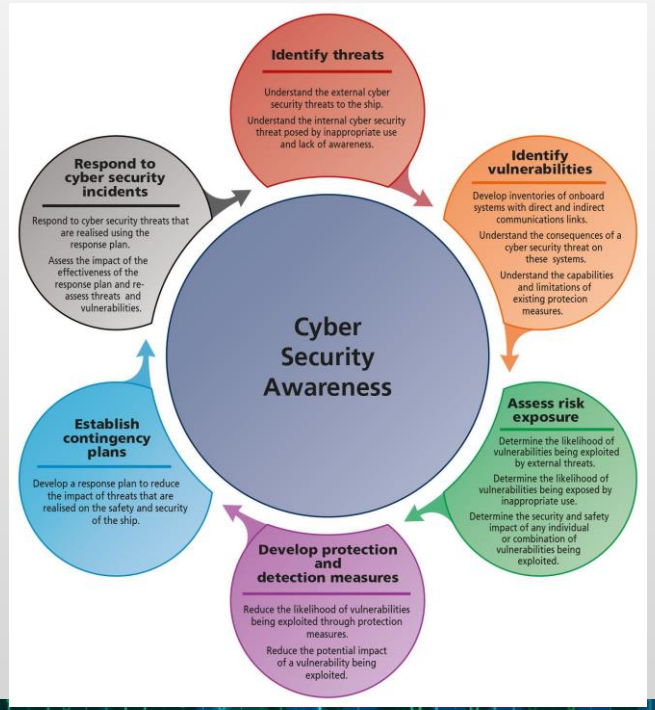
- Threats and methods of cyber attacks are constantly changing
- Sources for detected threats and their remediation:

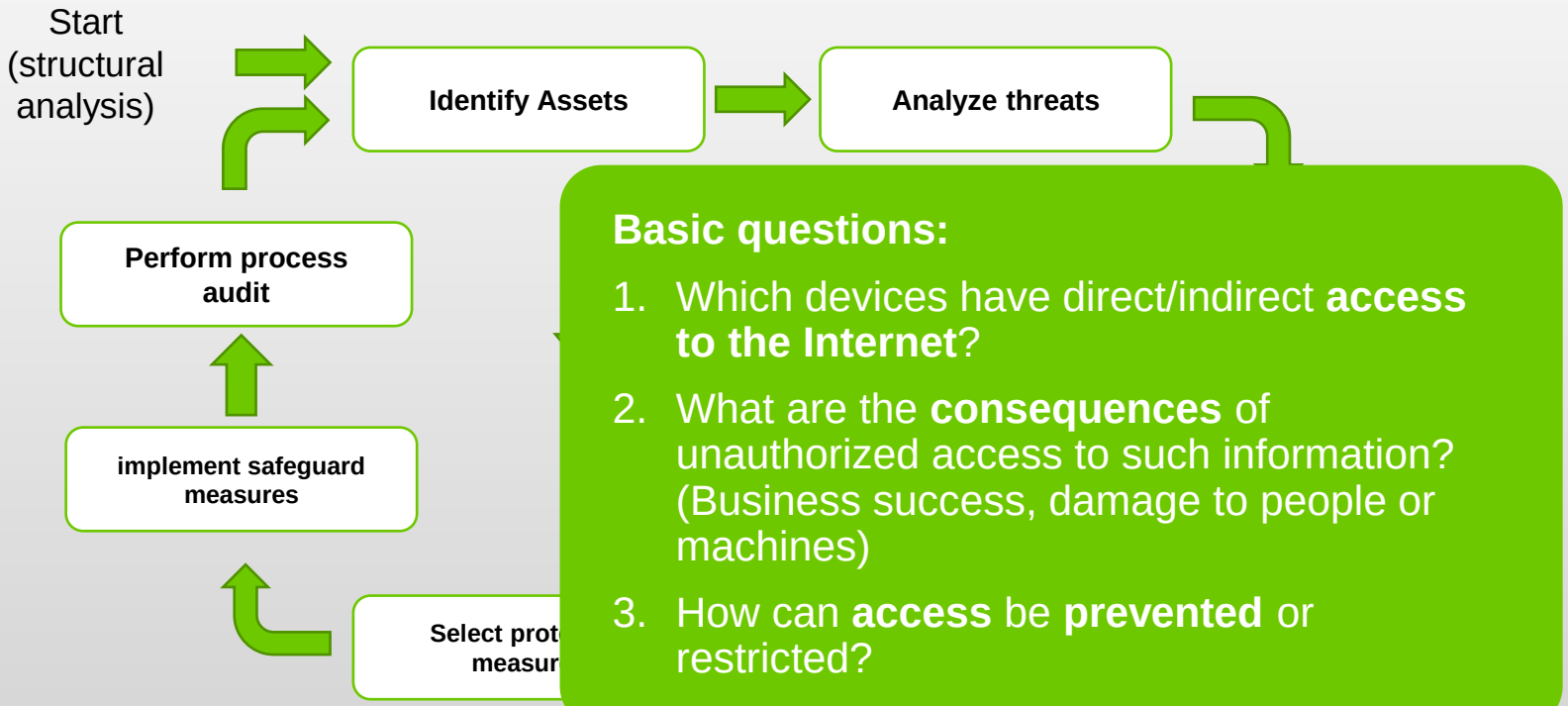
https://ics-cert.us-cert.gov/alerts

Cybersecurity in production plants step by step... Organization and processes

6. asset identification, valuation and protection

Recommendations for taking action suggest a structured procedure that is repeated periodically.
A plant and its additions are divided into different classes similar to an FMEA system.





Basic questions:

1. Which devices have direct/indirect **access to the Internet**?
2. What are the **consequences** of unauthorized access to such information? (Business success, damage to people or machines)
3. How can **access** be **prevented** or restricted?

source: VDI2182

Quelle: BIMCO, 01.2018, The Guidelines on Cyber Security onboard Ships

Cybersecurity in production plants Technical implementation - Open on all sides?

7. regulation of external access

man to machine:

- Electronic accesses:
  - Programming
- Physical access:
  - Switch cabinet
  - Sensors/actuators

!
- social engineering
- Insufficient gradation of authorizations

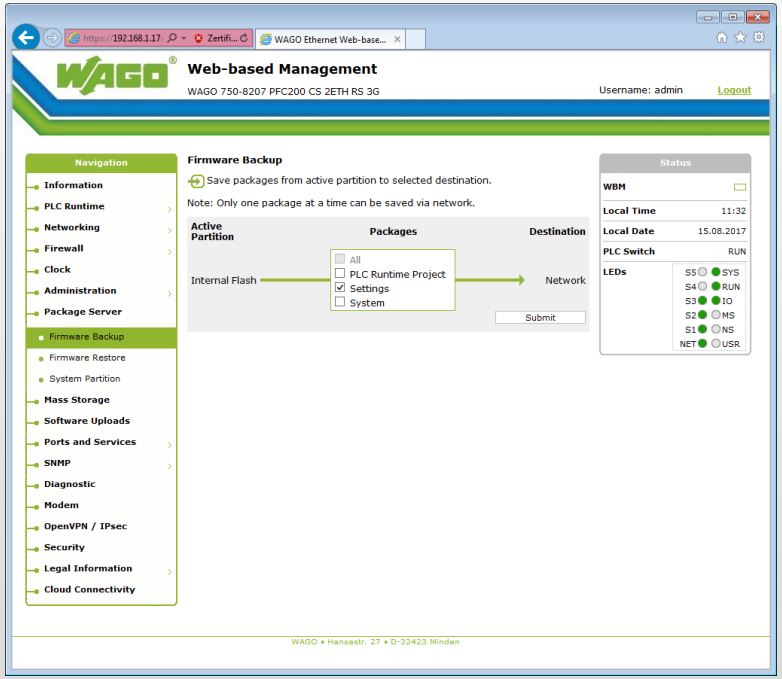
machine-to-machine:

- Electronic accesses:
  - Monitoring
  - Control system

!
- **Data loss, data modification**

Cybersecurity in production plants Technical implementation - safe is safe

8. data backup

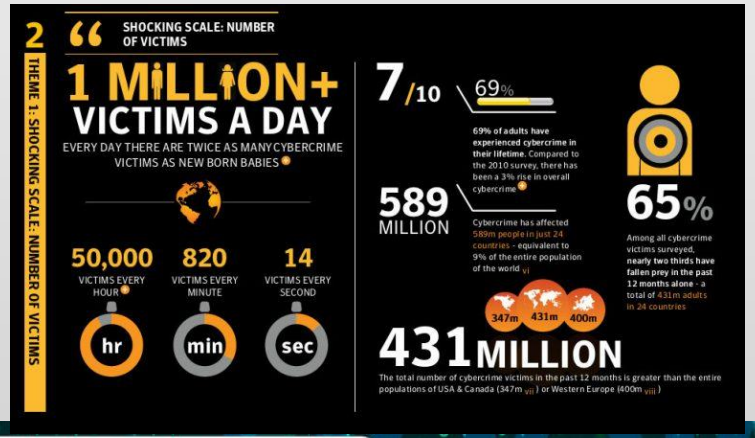


Create backups frequently, then disconnect from the backup media

Cybersecurity in production plants Prevention and emergency - Training and staying up to date

9. handling of malfunctions / failures

In the case of cyber attacks, there is often a long period of time between the emergence of the vulnerability and its abuse.



10. handling of IT security incidents

- Stop the data outflow
- production restart
- Communication plan for customers and suppliers, possible obligation to notify crisis companies
- Cause analysis
- Re-evaluation of the situation and threat

Cyber security Normen

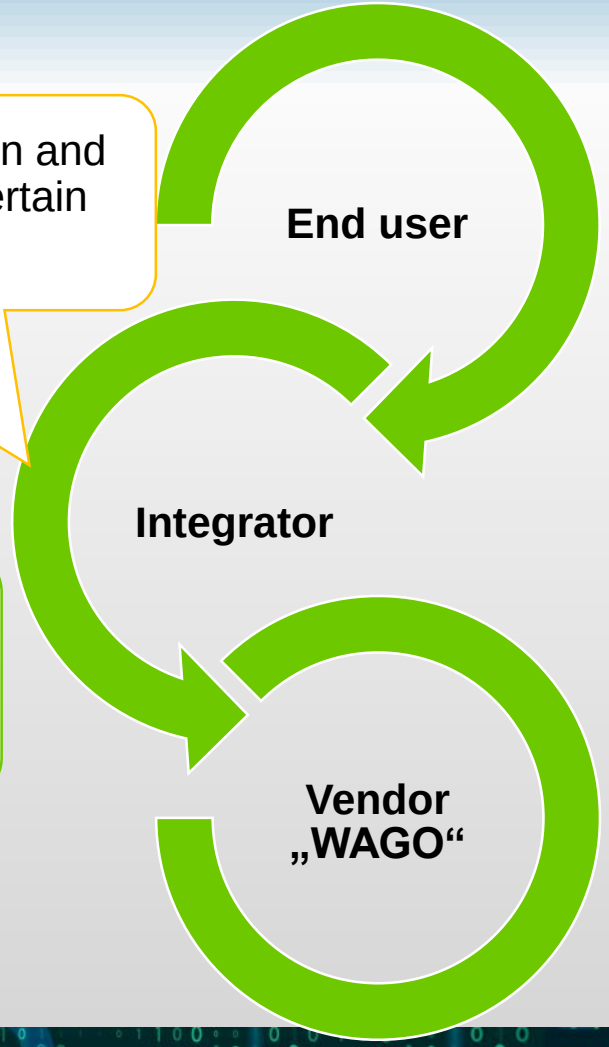
Status en toelichting

Applicability of Sub-Standards of IEC 62443

This is the benefit for the end user: He can refer to the certified product and the required security level (SL) in specification.

IEC 62443 looks along the value chain and has sub-standards which apply to certain steps in the chain of supply.

Independent certification for higher credibility



IEC 62443-2-4
Policies and Process

IEC 62443-3-3
System Specification

IEC 62443-4-1
Secure Development Lifecycle

IEC 62443-4-2
Component Specification

Additional security requirements

DNVGL-CP-0231
Cyber security capabilities of control system components

VDE V 0831-104:2015-10
Electric signaling systems for railways;

German version **EN 50159:2010**
Communication, signaling and processing systems

NA 163
"Security Risk Assessment of SIS (Safety Instrumented Systems)“

NA 169
'Automation Security Management in the Process Industry'

VDMA 24774:2016-06

BACnet Secure Connect

Energy:
IEC 62351
Standards for Securing Power System Communications

ISO 27019
Information security controls for the energy utility industry

IEEE 1686 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

IEC 62443

Overview of norms, standards and guidelines

IT security

Norms / Standards / Guidelines

- ISO/IEC 27001 and following
- NIST SP 800-53
- NIST SP 800-82
- ISO/IEC 15408: Common Criteria
- ISA SP99
- IEC 62443
- VDI/VDE 2182
- IEC 62351
- VdS 3473

Manufacturer associations / authorities

- PROFINET Security Guideline
- Securing EtherNet/IP Networks
- NAMUR NA 115, NE 153
- BSI: *Industrial Control System Security und andere*
- SANS - *Critical Controls for Effective Cyber Defense*
- Homeland Security / ICS-CERT

Laws / Regulations

- IT Security Act
- Ordinance on the determination of critical infrastructures according to the BSI Act (BSI-KritisV)
- Law on the supply of electricity and gas (Energy Industry Act - EnWG)
- Safety catalogue according to § 11 para. 1a EnWG

Details IEC 62443

IEC 62443 sub standards can be divided into different fields: It shall help to enable „secure-by-design“ products by looking at processes and products/systems.

Certification of Process / Organization

General		Policies & Procedures		System		Component / Product	
1-1	Terminology, Concepts and Models	**2-1**	Requirements for an IACS security management system	**3-1**	Security technologies for IACS	**4-1**	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	**2-2**	Implementation guidance for an IACS security management system	**3-2**	Security risk assessment and system design	**4-2**	Technical security requirements for IACS components
1-3	System security compliance metrics	**2-3**	Patch management in the IACS environment	**3-3**	System security requirements and security levels		
1-4	IACS security lifecycle and use-case	**2-4**	Security program requirements for IACS service providers				

Certification of Product / System

Technical Presentation March 2020

Target Security Level

Certfication acc. to IEC 62443-4-2

SL1

SL2

SL3

SL4

The security level only indicates what can be reached. The device must be configured properly to achieve this SL.

This Security Level means that the devices should be used in a layered environment (Defense-in-Depth) with at least one router/firewall in front to limit the exposure.

Protection against intentional violation using simple means with low resources, generic skills and low motivation

Insider (Disgruntled employees or contractors…)
or **Intruder** (Thrill-seeking, hobbyist, malicious organization…)

Higher levels resist to terrorist and cyber criminals (SL3) and government driven attacks (SL4)

Vragen?

Diederick Nab
Projectmanager
industrial automation

WAGO

WAGO Nederland B.V.
Postbus 2070
7301 DB Apeldoorn
Laan van de Ram 19
7324 BW Apeldoorn
www.wago.com

Tel. +31 (0)55 36 83 500
Mobiel +31 (0)6 54 30 86 21
diederick.nab@wago.com