Laborelec
RESEARCH & INNOVATION

OT Cybersecurity Workshop
ETN - Bergen (N)

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

Agenda

Jos Menting

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

Agenda

- Introduction
- OT Cybersecurity
- The threat landscape
- Best practices
  - Organizational aspects
  - Standards, guidelines
  - Best Practice example
  - Projects
- Lessons learned (anonymized examples of real incidents)
- Conclusions and Q&A

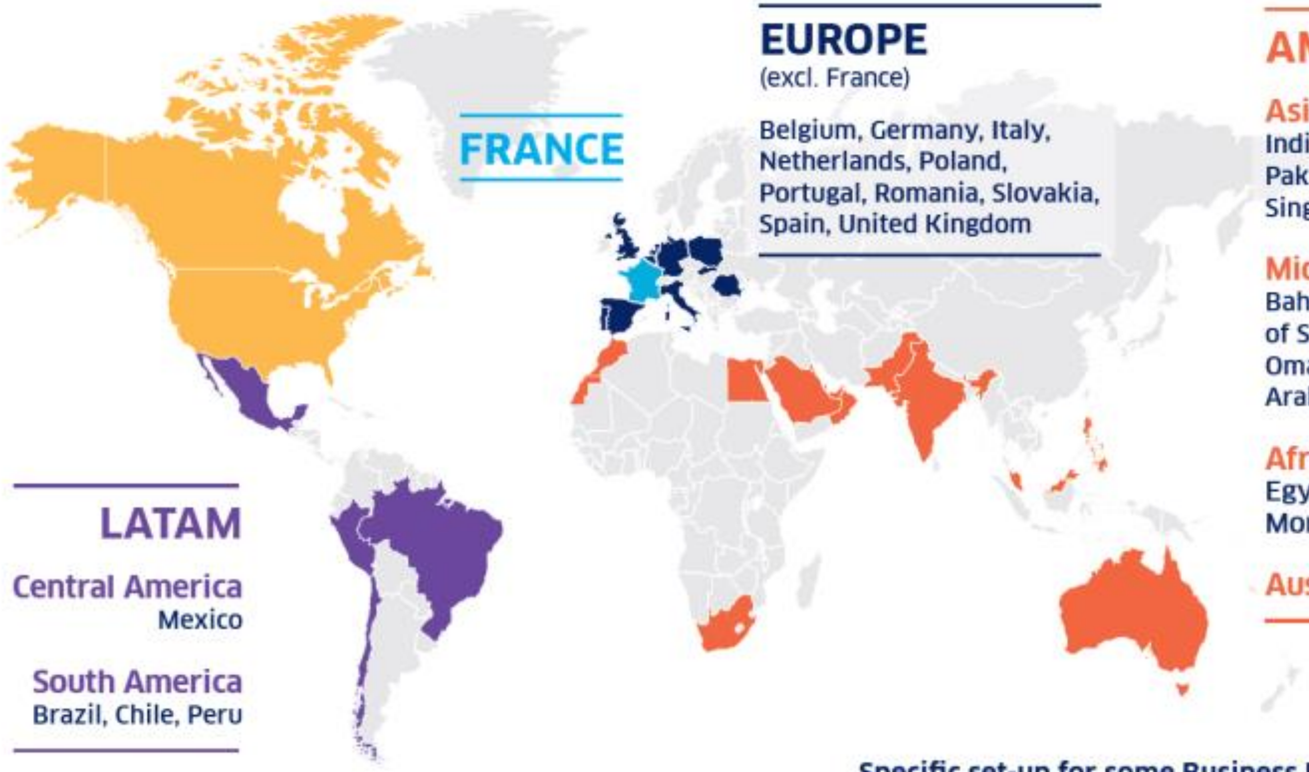
Introduction

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

ENGIE, operating around the world

A STRONG FOOTPRINT IN FRANCE AND IN 4 REGIONS

France, Europe (excl. France), LATAM, NORTHAM, AMEA



NORTHAM

North America
Canada,
United States

FRANCE

EUROPE

(excl. France)

Belgium, Germany, Italy, Netherlands, Poland, Portugal, Romania, Slovakia, Spain, United Kingdom

LATAM

Central America
Mexico

South America
Brazil, Chile, Peru

AMEA

Asia
India, Malaysia, Pakistan, Philippines, Singapore

Middle-East
Bahrain, Kingdom of Saudi Arabia, Kuwait, Oman, Qatar, United Arab Emirates

Africa
Egypt, South Africa, Morocco

Australia

Specific set-up for some Business Entities

In France

- 🟦 ENGIE Solutions France
- 🟦 Storengy, Elengy, NaTran, GRDF

In Belgium

- □ Nuclear

Worldwide

- ■ GBU Supply & Energy Management
- ■ TRACTEBEL

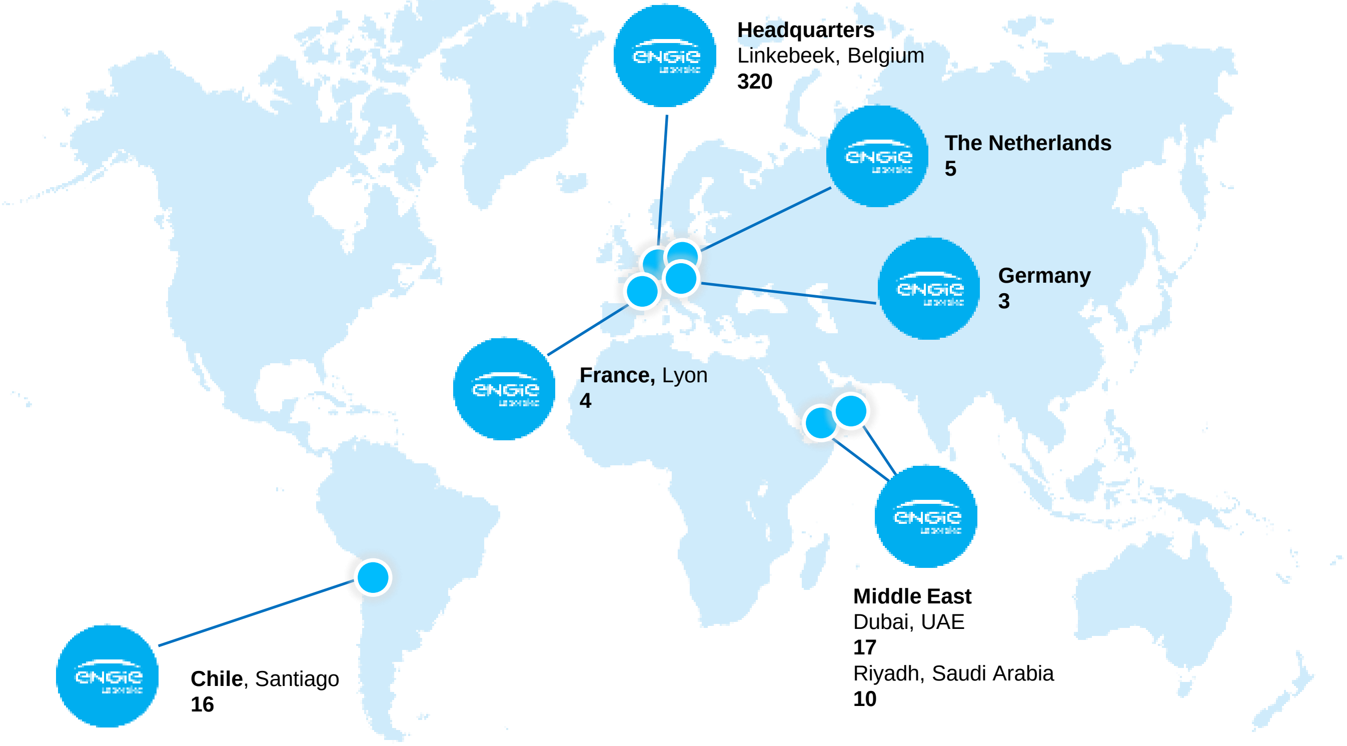
LABORELEC - a research and innovation center, supported by a unique and multi-located group of experts

- Laborelec is a **leading center of expertise and research** in electrical energy technologies with headquarters in Belgium and 6 subsidiaries on 3 continents
- Supporting the **energy transition** and accelerating the **net zero carbon journey**
- With a **highly qualified workforce** of over 379 colleagues (PhDs, engineers, specialist technicians) from 23 different nationalities

379

COLLEAGUES

23% 77%



Headquarters
Linkebeek, Belgium
320

The Netherlands
5

Germany
3

France, Lyon
4

Middle East
Dubai, UAE
17
Riyadh, Saudi Arabia
10

Chile, Santiago
16

OT Cybersecurity

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

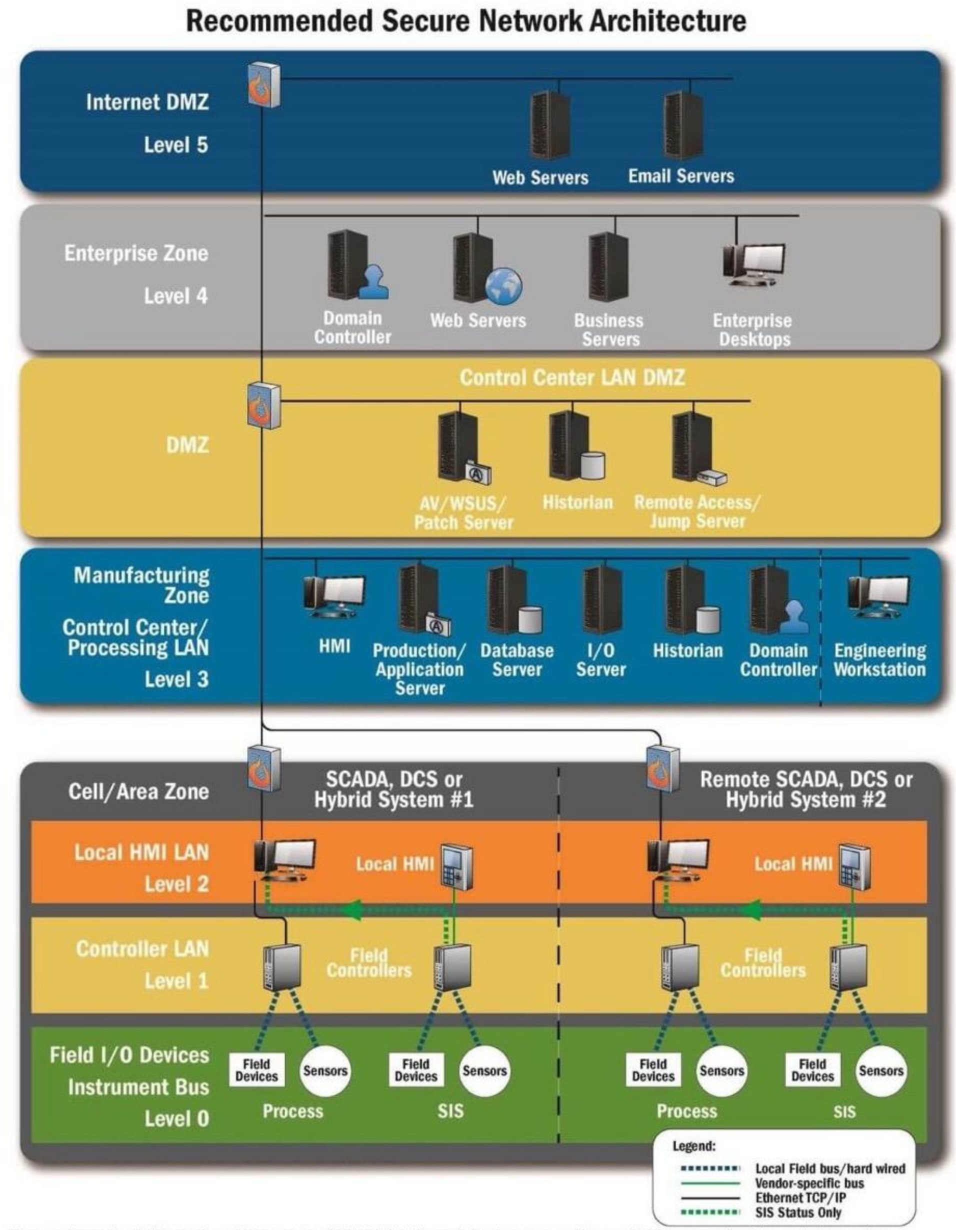
Basic model for OT Cybersecurity

- Purdue model for ICS Cybersecurity
  - Level 0 = field
  - Level 1 = Controllers
  - Level 2 = Local HMI
  - Level 3 = Control Center, historian, engineering station

DMZ

  - Level 4 = Enterprise network
  - Level 5 = External connection(s) / Internet

DMZ



Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies

Cyber resilience = 3 pillars

Technical solutions

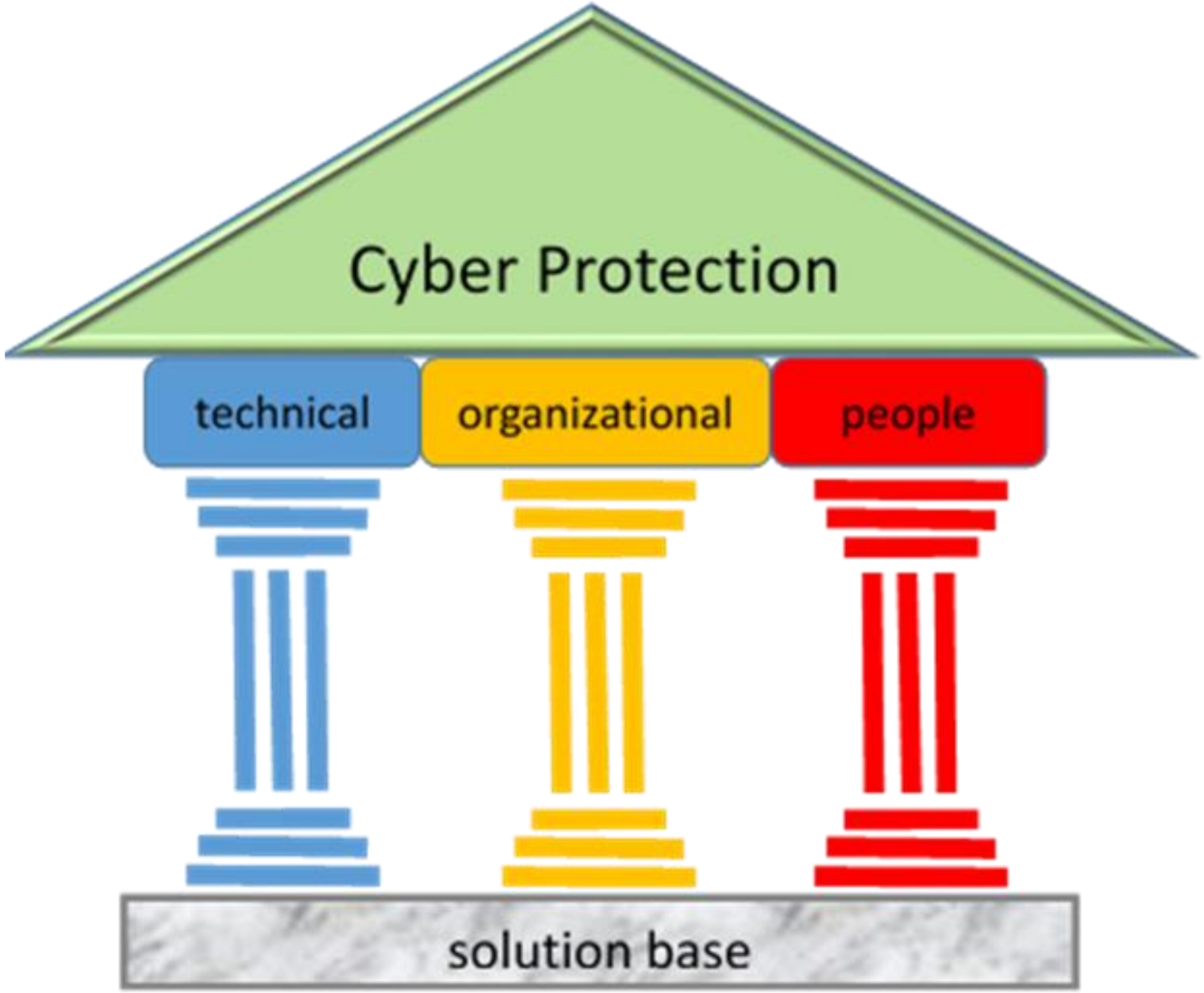
- ○ Secure architecture
- ○ Hardening
- ○ Monitoring

Organizational measures

- ○ Policies and procedures
- ○ Roles and responsibilities

People

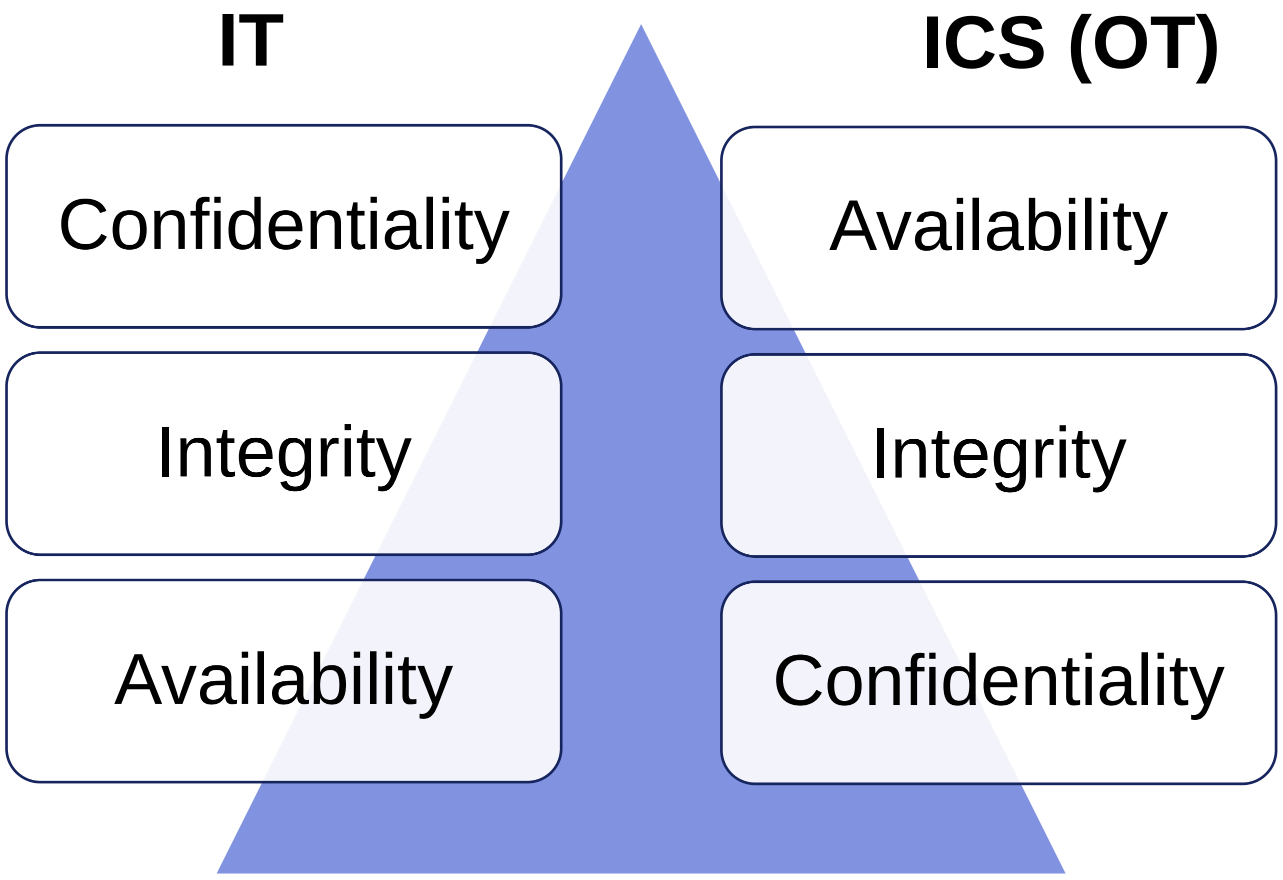
- ○ Training
- ○ Knowledge management



the cybersecurity building blocks

Source: MIT CAMS

CIA versus AIC → IT versus OT



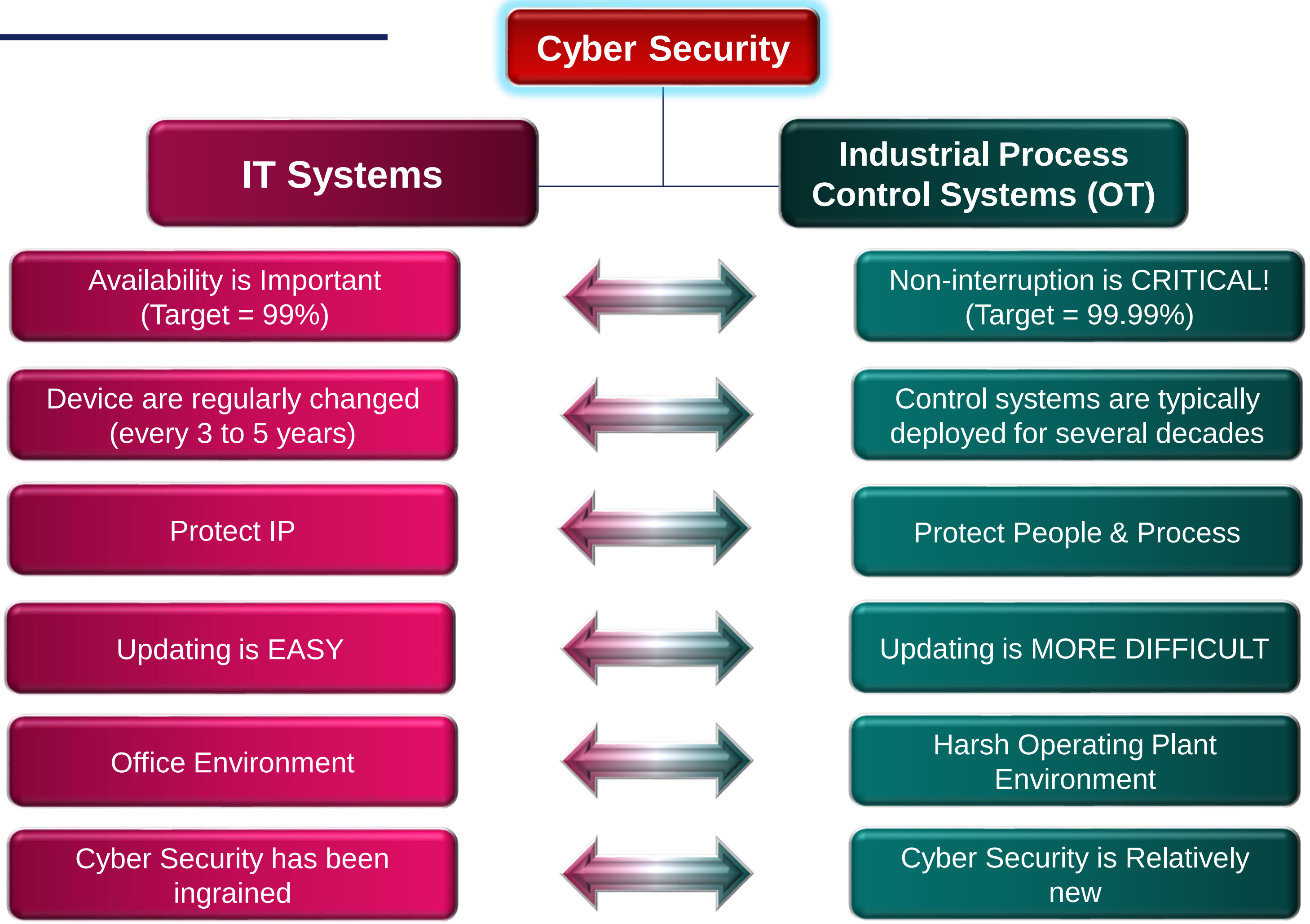
IT	ICS (OT)
Confidentiality	Availability
Integrity	Integrity
Availability	Confidentiality

C = authorized access only

I = accuracy and completeness of information

A = reliable and timely access

IT-OT differences



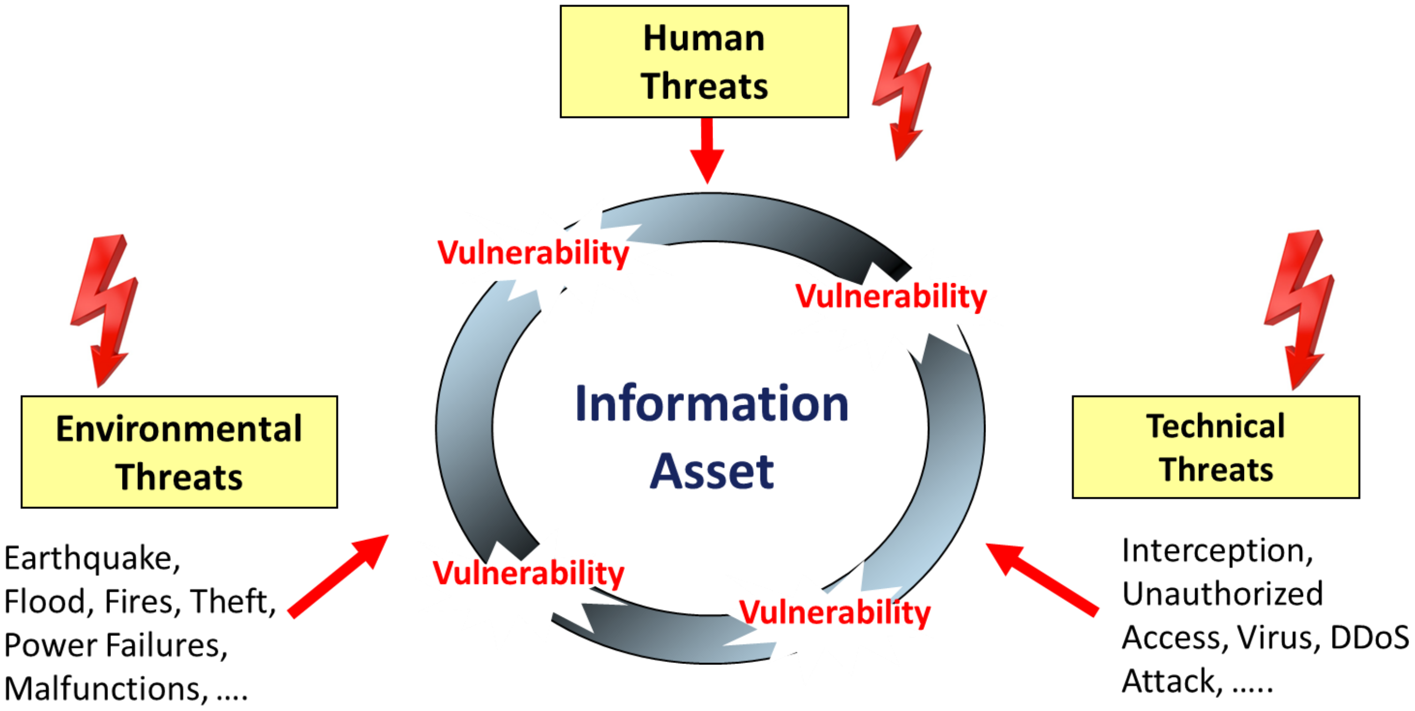
Cyber Security

IT Systems	Industrial Process Control Systems (OT)
Availability is Important (Target = 99%)	Non-interruption is CRITICAL! (Target = 99.99%)
Device are regularly changed (every 3 to 5 years)	Control systems are typically deployed for several decades
Protect IP	Protect People & Process
Updating is EASY	Updating is MORE DIFFICULT
Office Environment	Harsh Operating Plant Environment
Cyber Security has been ingrained	Cyber Security is Relatively new

The Threat Landscape

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

Threat Landscape



Human Threats

Environmental Threats

Earthquake, Flood, Fires, Theft, Power Failures, Malfunctions, ….

Information Asset

Vulnerability

Vulnerability

Vulnerability

Vulnerability

Technical Threats

Interception, Unauthorized Access, Virus, DDoS Attack, …..

- **External threats**
  - Random attacks (virus, DDOS, ..)
  - Remote access
  - Supply chain
  - Targeted !
  - …
- **Internal threats**
  - Maintenance
  - Insider !
  - ...

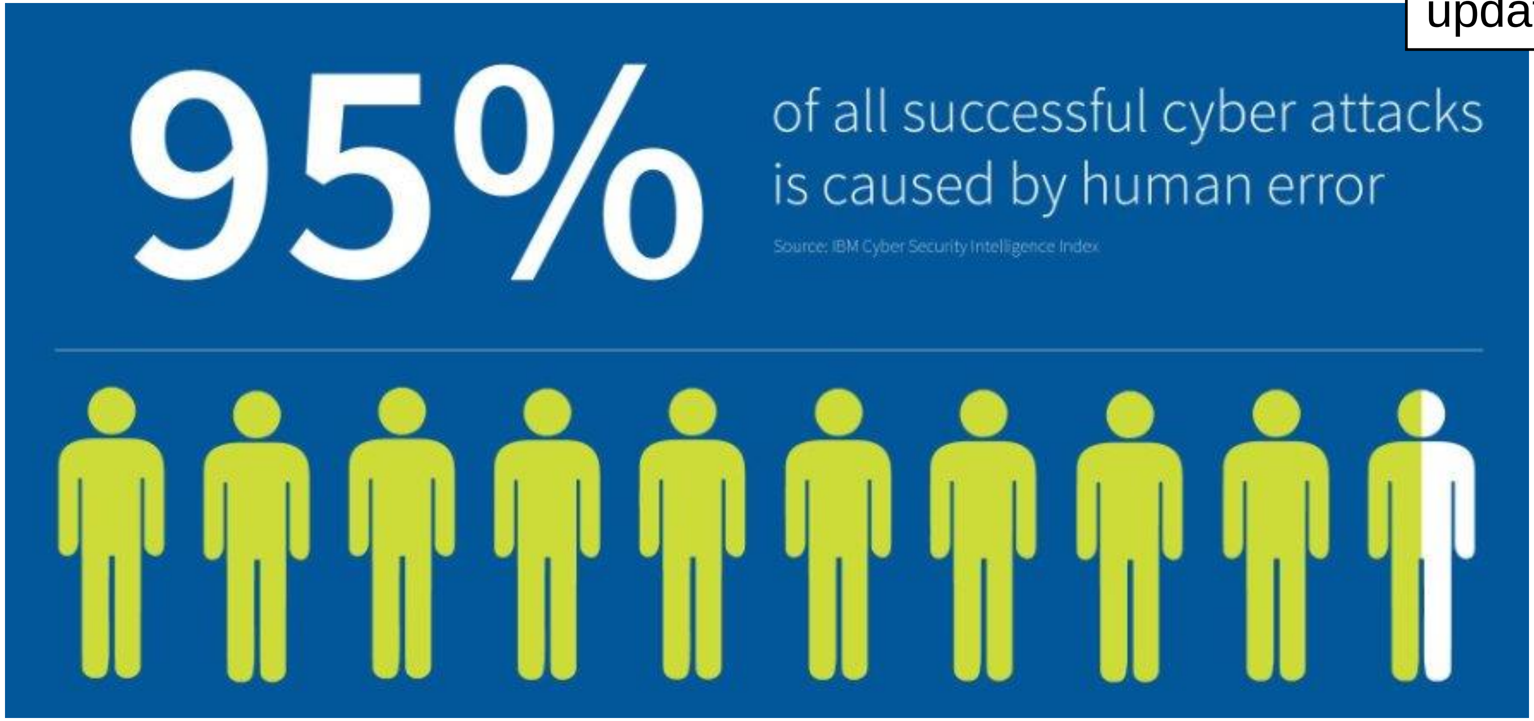
! = low frequency, high impact

The answer to this is a Risk Assessment

Biggest threat

- **Humans are the #1 propagation vector for cyber-attacks**
  - — Intentional: Disgruntled employees, hackers
  - — Unintentional: Maintenance staff, suppliers, DCS data users, etc

Examples:
▪ Use of infected USB keys
▪ injection of virus while updating the software

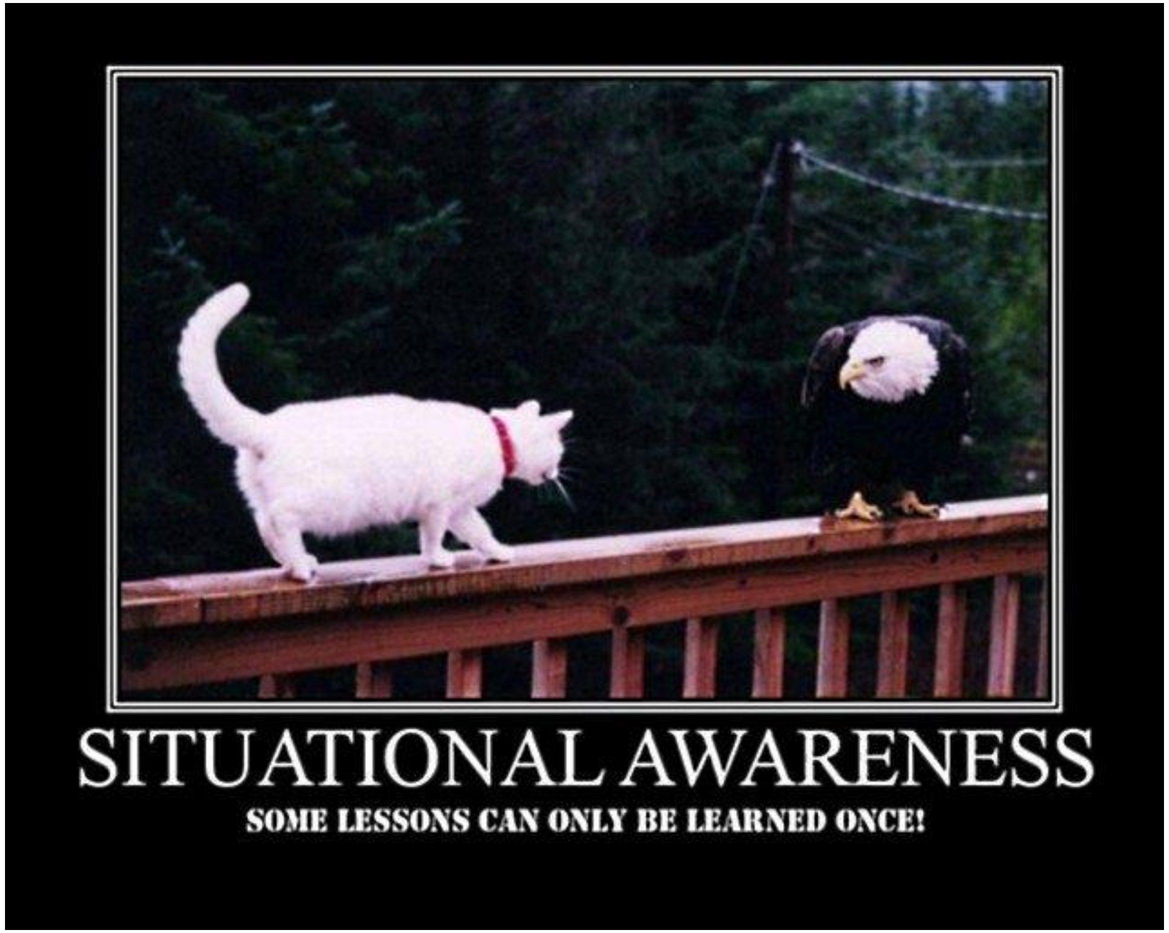


95% of all successful cyber attacks is caused by human error

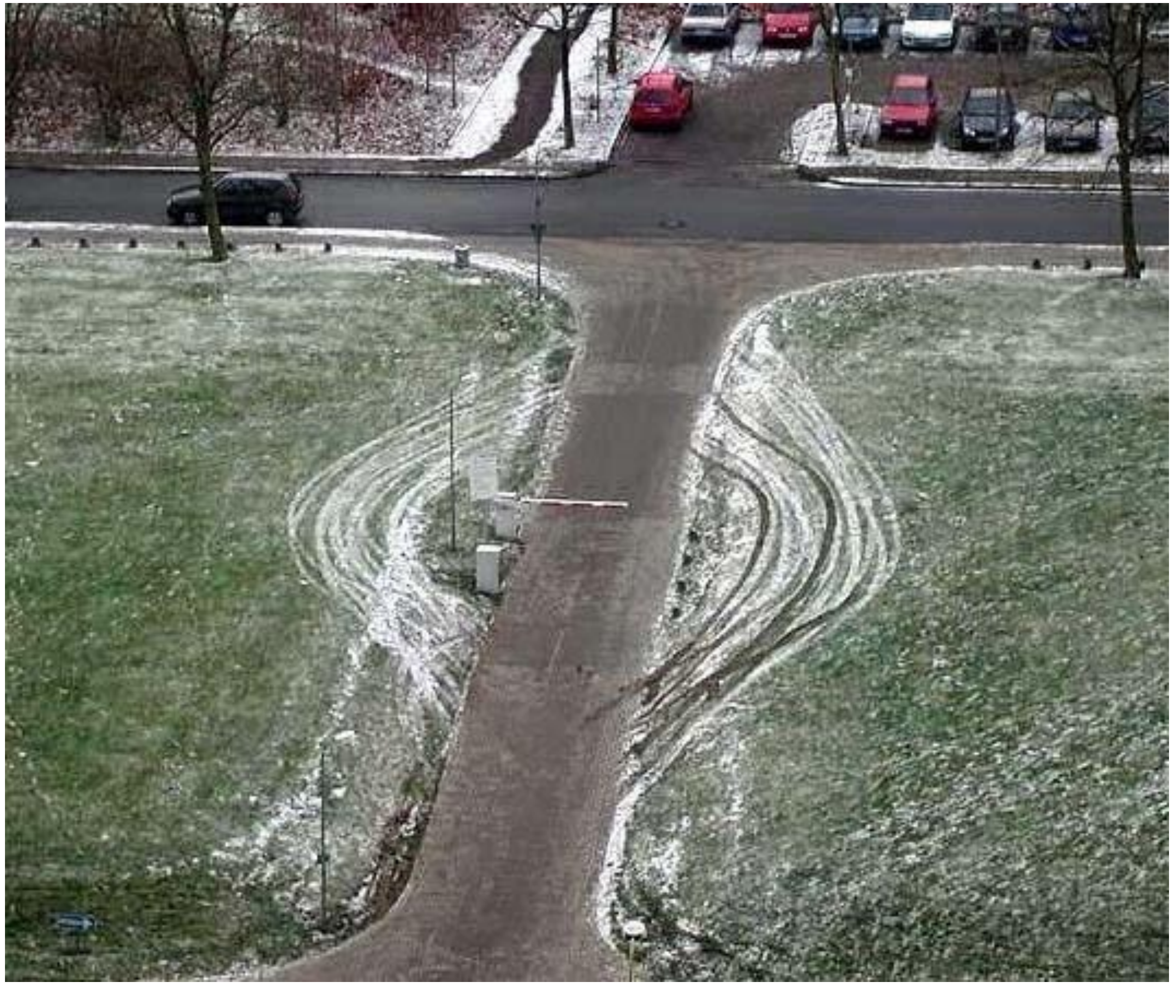
Source: IBM Cyber Security Intelligence Index

Situational Awareness

- **Awareness** is fundamental to understand, to prevent and to protect the assets from cybersecurity risks
- Being aware of cyber threats requires **continuous** attention, monitoring and re-evaluation of the situation
- It is essential to **react timely** to assess the actual situation in a relevant and accurate way (resilience)
- People must be **trained** to do so → create a cybersecurity culture
- It is a recurrent process



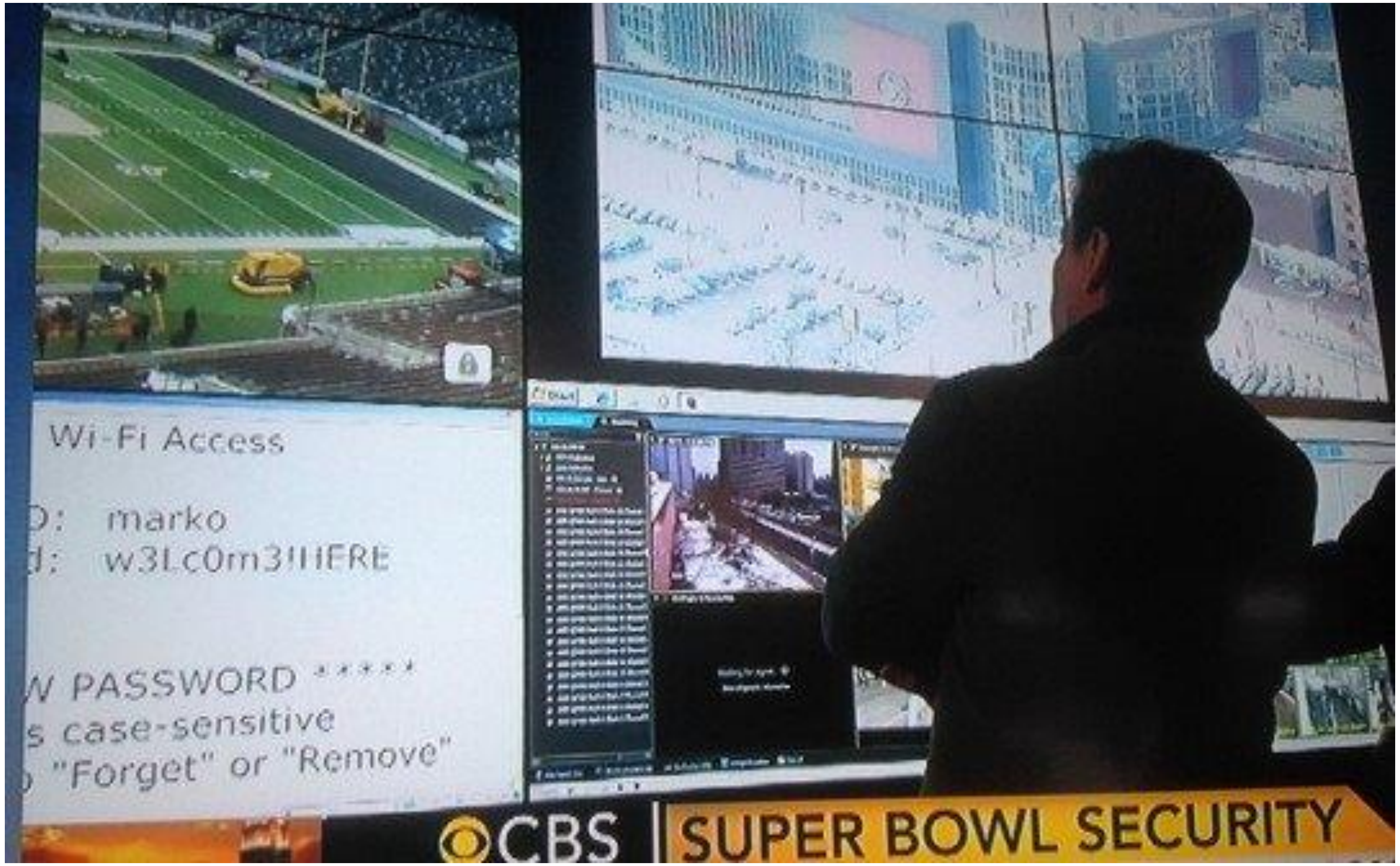
We bought a new Firewall … !



- Putting just physical security measures in place is not sufficient
- Define the rules you want and put them in place
- Educate the people
- Monitor
- Take corrective action if needed

Proof of human error

Superbowl security command centre accidently broadcasted the pass code life on TV !



Wi-Fi Access

D: marko
d: w3Lc0m3!HERE

W PASSWORD *****
s case-sensitive
"Forget" or "Remove"

Impact and Resilience

- **Impact** can be direct or indirect and vary in time
  - Loss of production
  - System damage
  - Financial (penalties)
  - Reputational
  - Human (physical, injuries)
  - Environmental

- **Resilience** limits impact and allows recovery
  - Containment of the attack (segregated networks)
  - Procedures in place
  - Back-up and restore
  - Spare parts
  - Trained staff

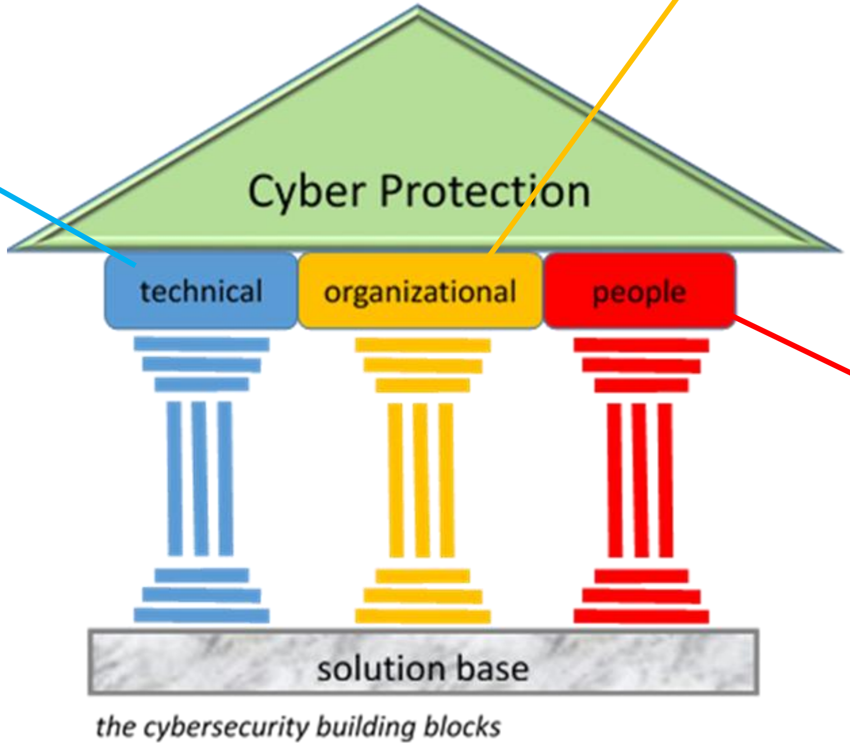
Best Practices

ENGIE

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

How to organize

- Identity Management
- Authentication
- Access control
- Secure design
- Data security
- System Configuration
- Third party access



the cybersecurity building blocks

- Cyber Strategy
- Policies and Procedures
- Risk Management
- Supply Chain Management
- Asset Management
- Incident response
- Incident reporting

- Awareness
- Training
- Resources
- Oversight
- Roles and responsibilities

Documentation

- **Legislative documents**
  - Describe the actions you are obliged to address, no matter what
    - Local law
    - EU (e.g. NIS2)
    - ENTSO-E

- **Company guidelines**
  - Internal documents of the company that must be followed
    - Fit to the internal company policies regarding security aspects

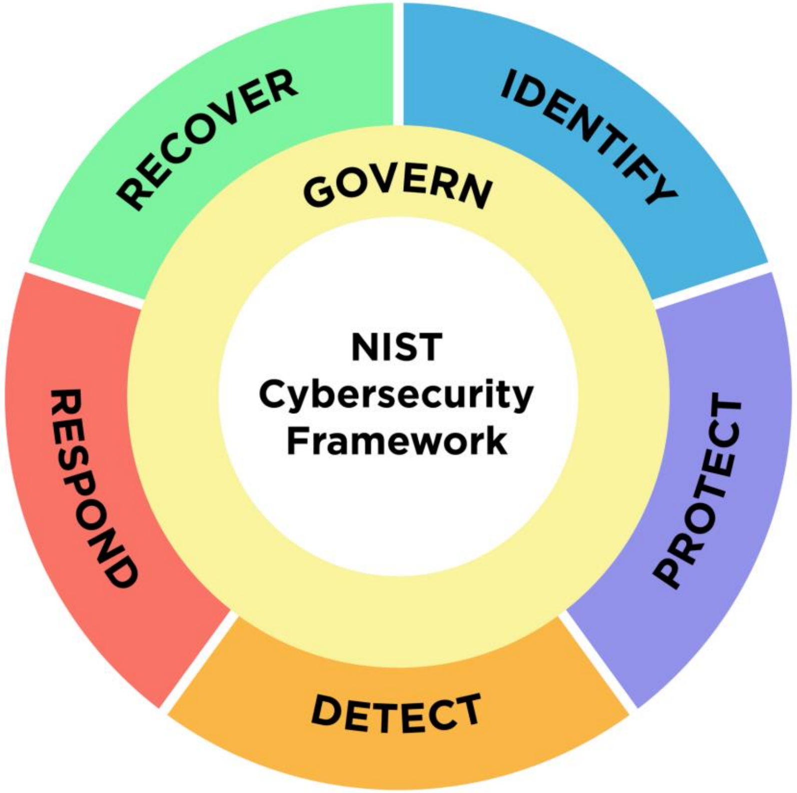
- **Standards**
  - Documents that are useful in providing comprehensive solutions on handling the individual cybersecurity aspects, like
    - NIST CSF
    - IEC62443
    - ISO27k
    - …

NIST CSF

- The NIST Cybersecurity Framework (NIST CSF) provides comprehensive guidance and best practices that private sector organizations can follow to improve information security and cybersecurity risk management

- Aims helping organizations to better understand and improve their management of cybersecurity risk

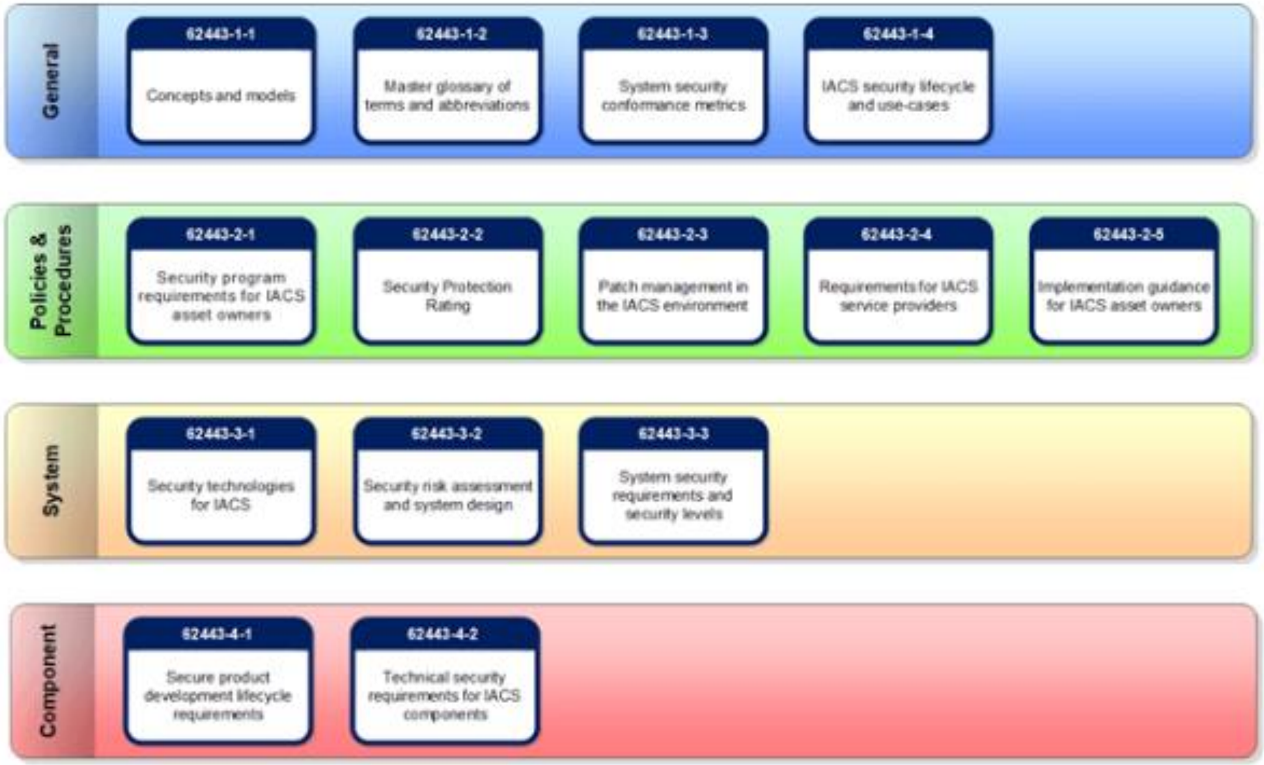
- Recurring 5-step program



Source: National Institute of Standards and Technology

ISA/IEC62443

- Setting cybersecurity benchmarks in all industry sectors that use IACS
- IEC62443 is more of a way to ensure the continuity of your business operations in industrial environments
- Evaluate cybersecurity capabilities in and identifies areas for improvement
- Addresses many fields and subjects, such as:
  - System design and criteria
  - Maturity levels
  - Risk Assessments
  - Vendor Requirements
  - … and much more …. like: terminology, security program, secure development and life cycle, ….
- It is a shared responsibility

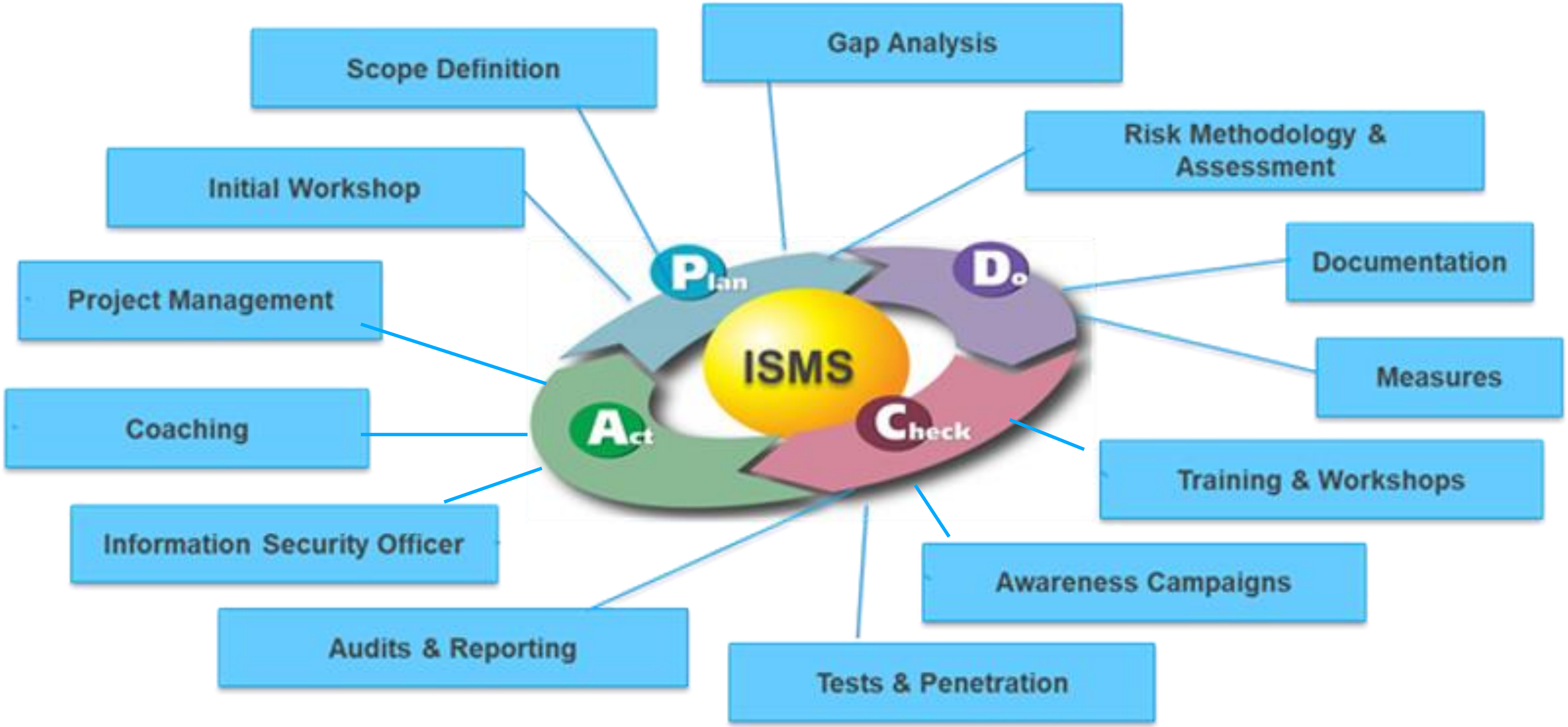


General	62443-1-1 Concepts and models	62443-1-2 Master glossary of terms and abbreviations	62443-1-3 System security conformance metrics	62443-1-4 IACS security lifecycle and use-cases	
Policies & Procedures	62443-2-1 Security program requirements for IACS asset owners	62443-2-2 Security Protection Rating	62443-2-3 Patch management in the IACS environment	62443-2-4 Requirements for IACS service providers	62443-2-5 Implementation guidance for IACS asset owners
System	62443-3-1 Security technologies for IACS	62443-3-2 Security risk assessment and system design	62443-3-3 System security requirements and security levels		
Component	62443-4-1 Secure product development lifecycle requirements	62443-4-2 Technical security requirements for IACS components			

Source: ISA

ISMS (Information Security Management System - ISO 27001

A standard framework for managing information security



Internal guideline

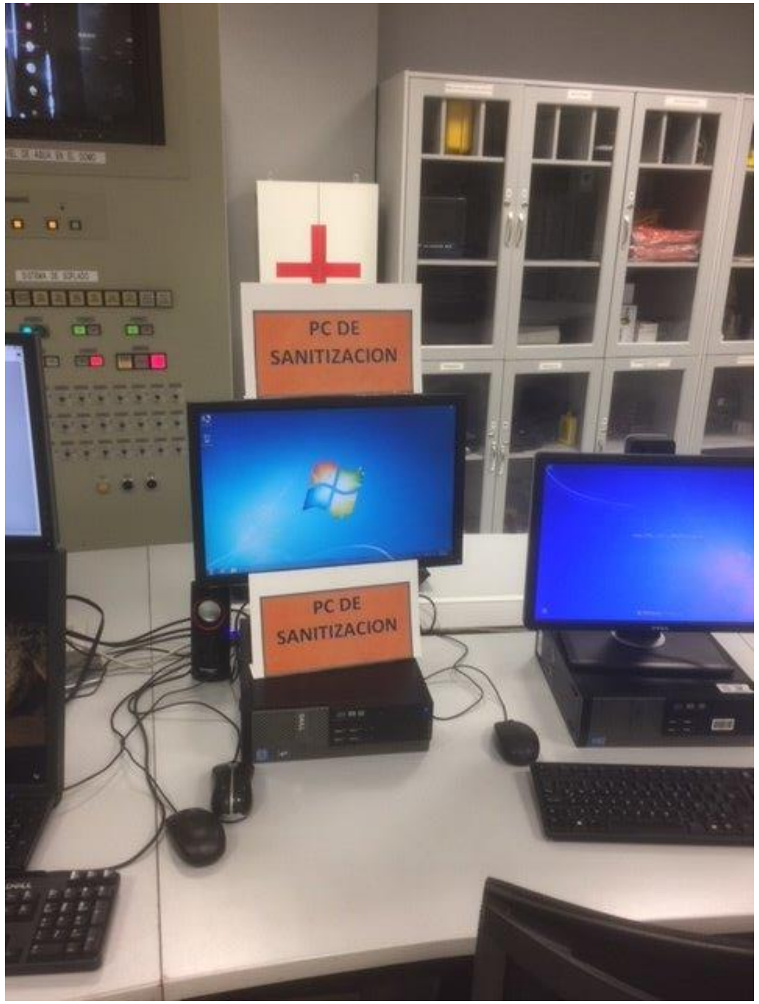
- Guide to follow for addressing the company's cybersecurity strategy

- Needs to address (in function of need)
  - Security governance
  - Awareness and training
  - Risk Management
  - Asset Management
  - Vulnerabilities
  - Changes and projects
  - Secure design
  - Access control (physical included)
  - Monitoring
  - Incident response and resilience

- For bringing good value the guide needs to be implemented on sites and subsequently controlled (assessments)

Best practice, example for portable media

- Always check external media (USB, external hard drive, CD-rom, etc) before connecting to the ICS
- External service providers may have procedures in place for their portable media; those need to be checked before connecting
- If available, use a dedicated Media Sanitization Station to check the USB key for viruses. Always follow the appropriate site procedure!
- If any virus is found report this using the adequate site procedure
- Regularly check the station and keep it up to date
- Do not forget to train the people



Portable media breache ‘air-gapped’ systems !

Projects

- Is ICS Cybersecurity an option?
- When to consider?
- Build-in versus bolt-on
- Supplier and end user/operator perspective
  - Supplier maturity level
  - Operator maturity level

Lessons learned

Real, firsthand, OT cyber incidents

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	●	●	●

Real incidents

Case 1: **Remote take over**

- What: Remote takeover by misuse of telephone service connection in a district heating and power production facility
- Impact: plant upsets cause water temperature facing unacceptable variations and power fluctuations
- How: The supplier intentionally reconnected secretly the physically separated modem so that he could remotely access the automation system without being noticed by the plant operator
- Motive: plant used as live demo capability for other customers
- Mitigating action: second line breaker installed with strict procedure

Case 2: **Unintentional changes in the DCS Software in a 350MW power plant**

- What: unintentional changes in the DCS software during an outage modified the start-up software of the boiler
- Impact: After the overhaul, the plant tripped multiple times at 10% load, thus missing the scheduled target by 3 days
- How: the I&C engineer let another, not authorized external technician, doing testing works on Motor Operated Valves on the DCS engineering station. After closing the engineering station in the wrong way, part of the software program for starting-up the boiler was damaged
- Motive: human behavior, not following the guidelines, unauthorized access
- Mitigating action: training, awareness

Real incidents

Case 3: **Infected PI database**

- What: a power plant long term data storage system got infected by a virus
- Impact: loss of valuable data from the production environment
- How: The antivirus scanner on IT level did not catch the day-zero virus. The virus entered the Corporate network and propagated to the PI server
- Motive: a non-targeted attack
- Mitigating action: up-to-date antivirus system, firewall, DMZ

Case 4: **Virus in power plant HMI and Trojan in shaft-line starting device**

- What: the operator interface (HMI) could no longer be used. The operator had to push the emergency shutdown button
- Impact: full load plant shut down with important loss of revenues, however serious damage to the shaft-line was avoided
- How: the virus “Back.Door.14742” was injected **2 month** before during the installation of a new software release. After scanning other automation systems a dormant Trojan “sdbot.dr” was found in the shaft-line starting device
- Motive: a non-targeted attack?
- Mitigating action: additional antivirus measures, application of vendor requirements, procedures adapted

Real incidents

Case 5: **Disappeared dongle**

- What: The dongle, containing the software license key for the engineering station, disappeared and was not found back
- Impact: The engineering station of the DCS was no longer usable, hampering normal operations and maintenance work; cost for a new license (45k€)
- How: The dongle looked like a normal USB jump drive and was not physically attached to the engineering station
- Motive: .. most likely personal gain (theft)
- Mitigating action: physical lock and warning

Case 6: **DCS exposed to corporate network**

- What: A power plant DCS was found freely accessible from the corporate network
- Impact: none, situation was settled before
- How: due to lack of IT knowledge I&C requested IT to exchange a router in the automation environment. Neither of them reloaded the access list
- Motive: miscommunication, no clear working procedure available
- Mitigating action: procedure written and enforced

Real incidents

Case 7: **Spurious plant trips**

- What: A water and power plant suffered from spurious trips and unintended load changes
- Impact: huge financial losses, important contractual dispute
- How: a backdoor was found in a remote monitoring system, bypassing all security devices
  - it provided external access directly to the automation highway of the gas turbine
  - the plant had no up-to-date view of the network architecture received from the OEM
  - the local supplier’s maintenance manager had unauthorized access to the automation system
- Motive: ignorance, lack of awareness
- Mitigating action: re-design of the remote connection, adding a lock-box with procedure, training

Conclusions

PUBLIC	RESTRICTED	INTERNAL	SECRET
○	◉	◉	◉

Conclusions

- OT Cybersecurity is no longer an option
- Things **do** happen
- It requires continuous attention and resources
- There are solutions
- SUGGESTION: Creation of an ETN - SIG (Special Interest Group) on OT Cybersecurity (.. for end users) ?

Q&A

Jos Menting

We provide solutions to help our customers around the world successfully come through the energy transition

ENGIE Laborelec
Rodestraat 125
1630 Linkebeek
Belgium

Contact
+32 (0)2 382 02 11
nathanaël.wybou@engie.com

Industrial Cybersecurity