CERTX

IEC62443 in a nutshell

BY CERTX, SPIN OFF OF HEIA-FR

Content

- CertX – Who we are
- Definitions, exemples and trends
- What about Cybersecurity reference documents ?
- IEC 62443 principles
- Perspectives of a larger landscape
- Q & A

Certx / ROSAS / HEIA-FR

Who we are

CertX – Cybersecurity Certification Body

www.certx.com

- **Accreditation Forum** : **IAF (Certification) and ILAC** (**Inspection**) are the world organisations of Conformity Assessment Accreditation Bodies and other bodies interested in conformity assessment in the fields of management systems, products, services, personnel and other similar programs of conformity assessment.
- **In Switzerland:** the **Swiss Accreditation Service (SAS),** as part of the Swiss State Secretariat for Economic Affairs (SECO), is responsible for accreditation of conformity assessment bodies by the recognition of the IAF.
- **From Support to Certification:** ROSAS creates CertX as the first Swiss Certification Body for Cybersecurity and Functional Safety

ROSAS
Center Fribourg

Creation of a spin-off

CertX – Certification Services

www.certx.com

CertX offers certification services in the following areas:

- **CERTIFICATION of PRODUCTS** in compliance of Functional Safety and Cyber Security Standards and Regulations
- **CERTIFICATION of ENGINEERS and MANAGERS** to ensure that relevant Standards, Processes and Regulations are being applied in their daily work.
- **CERTIFY CORPORATE PROCESSES and ORGANIZATIONS** to ensure that applicable Safety and Cyber Security Standards and Regulations are being incorporated into the Quality Management systems of the company and applied corporate wide.

Increasing degree of organisational focus

IEC 61508: Key Functional Safety Standard	EN 5012X: Railways
ISO 26262: Automotive	IEC 60601: Medical Devices
ISO 13849: Industrial machinery and Robotics	IEC 61511: Process industry
IEC 62061: Industrial machinery and Robotics	IEC 62443: Industrial Cyber Security

CertX – Assessment & Training Services

www.certx.com

Preliminary Assessment Services

- Technology Benchmarking
- Threat Identification / Modelling
- Gap Analysis

Certification Services

- Secure Process for Development *(ISA/IEC62443-4-1)*
- Secure Process for Integration Service *(ISA/IEC62443-2-4)*
- Certification for System *(ISA/IEC62443-3-3/4-1)*
- Certification for Component *(ISA/IEC62443-4-2/4-1)*

Training Services

- ISA/IEC62443 Cybersecurity Red/Black/Master Belt Certification (4-days courses + 1/2-day exam)
- Cybersecurity Principle (1/2-day course)
- IT Security Awareness (1/2-day course)
- OT Security Awareness (1/2-day course)
- Introduction to GDPR for SME (1/2-day course)

CertX Cybersecurity team will be happy to get an informal discussion with you to develop courses tailored to your current needs

Definitions, exemples and trends

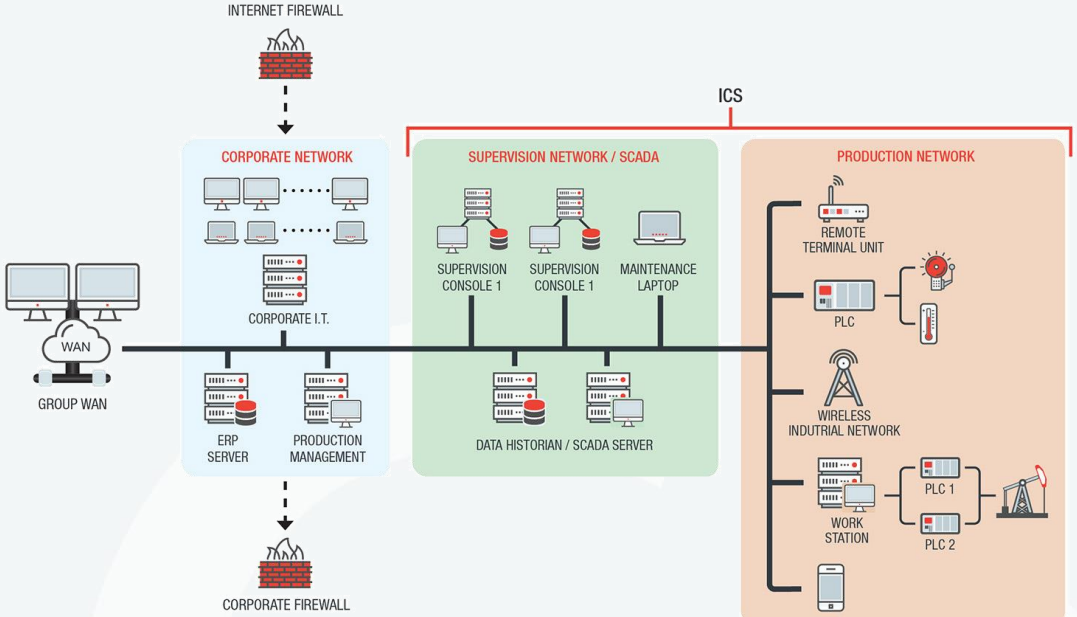
What is ICS / IACS?

An **Industrial Control System (ICS)** comprises …

«*systems that are used to monitor and control industrial processes.*» [def. Wikipédia]

An **Industrial Automation and Control System (IACS)** is a …

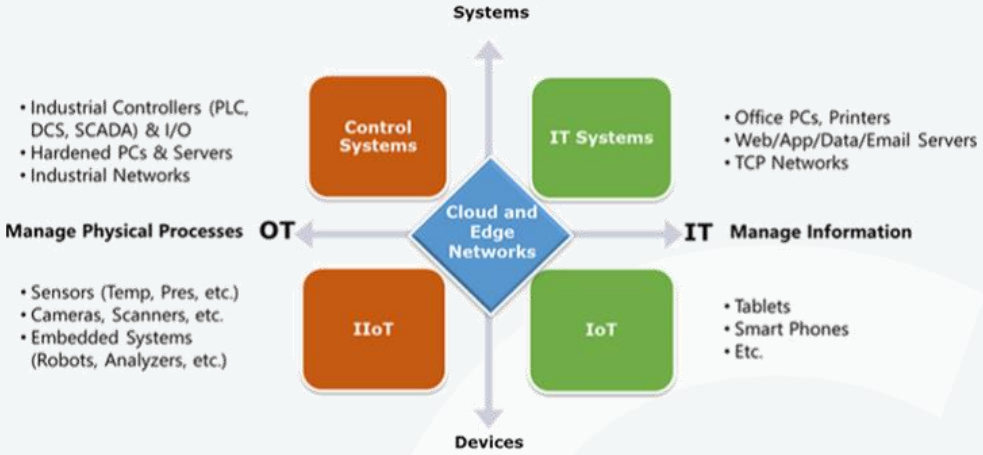
«*collection of processes, personnel, hardware, and software that can affect or influence the safe, secure and reliable operation of an industrial process*» [def. IEC62443-1-1]



OT/IT – Different paths for same goals

OT properties:

- Deterministic
- Processes are the assets
- Patch… decade ?



IT properties:

- Dynamic
- Data are the assets
- Patch Tuesday

Src: https://www.arcweb.com/blog/it-ot-cybersecurity-convergence

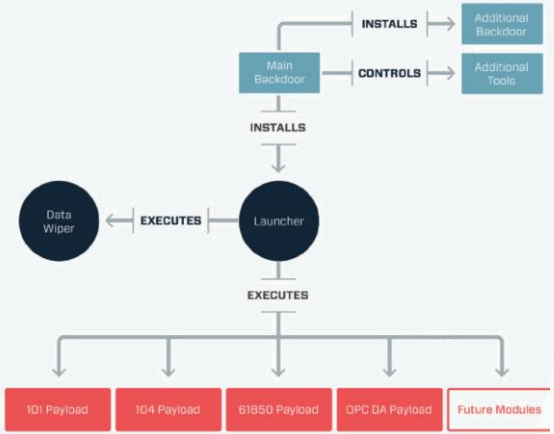
OT/IT – Different paths with similar traps

The human error as a major common source of failure

Example of cyber incident: CrashOverride

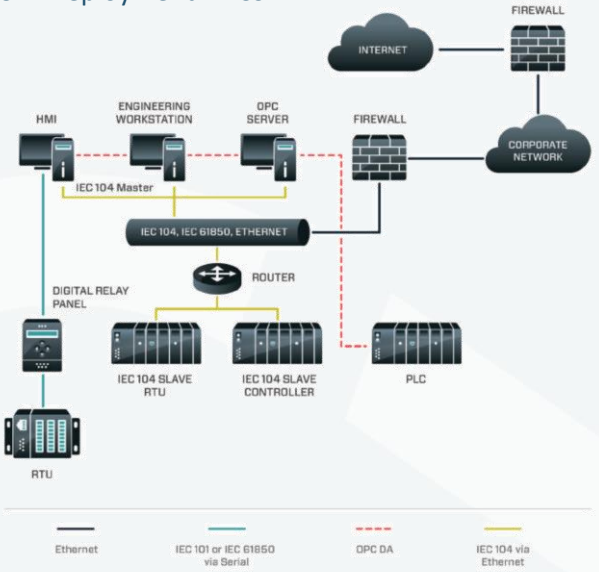
CrashOverride History

- Linked to SANDWORM APT and BlackEnergy
- Responsible of multiple Blackout in/near Kiev (Ukraine) in 2015, 2016 and 2017
- Target: Electric Grid Operations



Pragmatic approach

1. Initiated by phishing campaign
2. Pivoting from corporate network to ICS
3. Deployment in ICS



What are the critical trends ?

- Controls systems use more commercial off the shelf (COTS) software and hardware
- Implementing Internet Protocols (IP) exposes control systems to same vulnerabilities as business systems
- Increased use of remote monitoring and access
- Tools & Services to automate attacks are commonly available (Shodan, Autosploit, Tritton framework…)

A standardized approach seems therefore to be essential in the context of setting up secure systems.

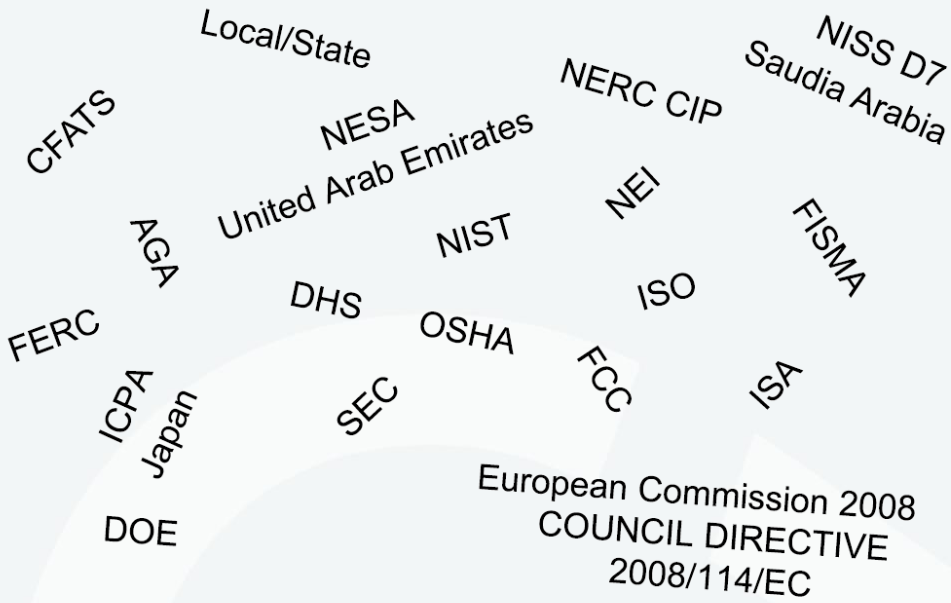
What about Cybersecurity Reference documents ?

A huge world of reference documents…

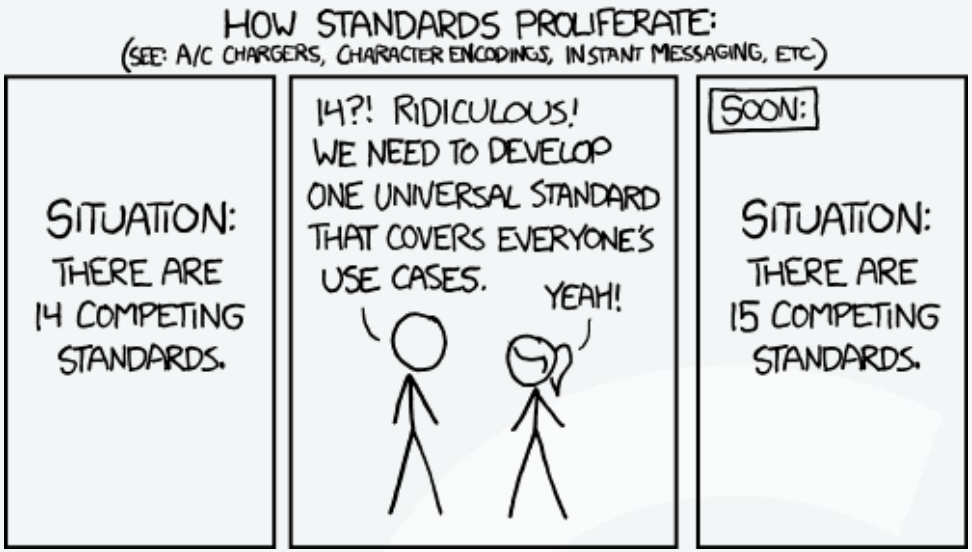
Multiple document types: Regulations, norms, **standards**, best practices…

What is a standard:

- Voluntary documents
- Collaborative approach
- Contains both normative and informative elements
- There is no requirement on anyone to use them unless a regulation mention it or absence of regulation



… with a same single goal



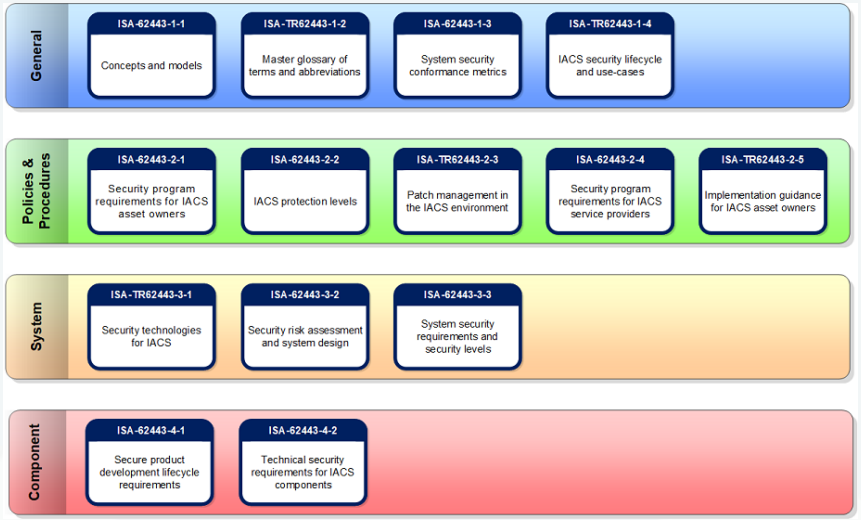
… but few of these cover both **human**, **technological** and **organizational** aspects of the development, the integration and the operation of **Industrial and Automation Control System (IACS)**

Standardized Approach – IEC62443

Designed to cover **Control System Cybersecurity** which is defined as hardware and software components of an **Industrial Automation and Control System (IACS)**

Manufacturing and control systems include, but are not limited to:

- hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

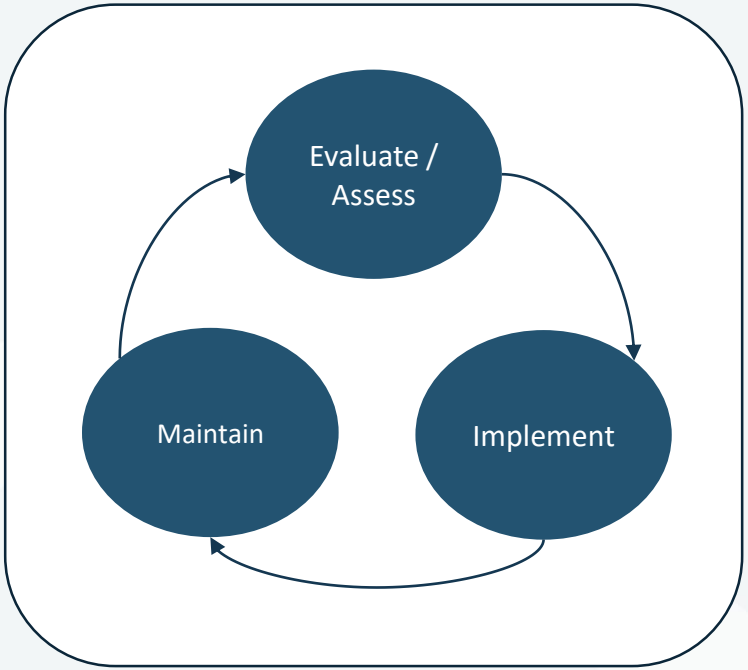


Source: isa,org/isa99

IEC 62443 principles

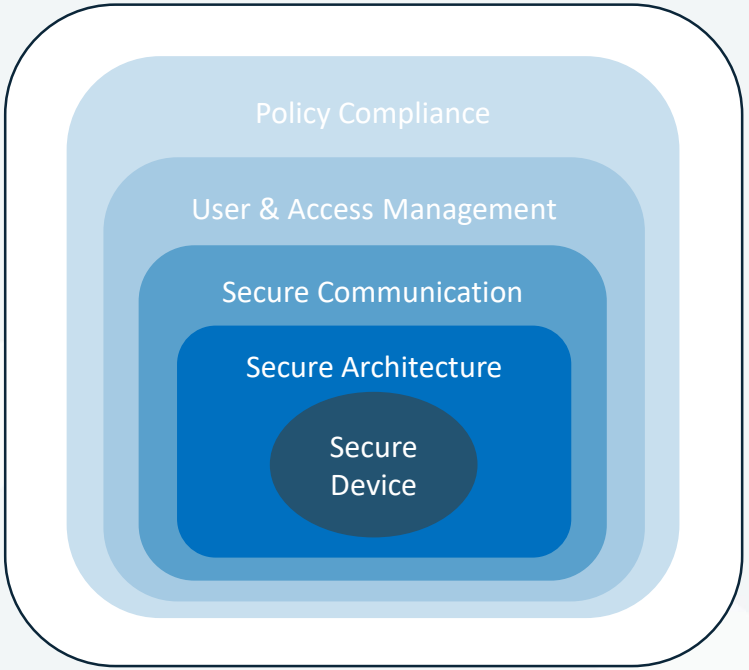
IEC62443 – Security mindsets

- **See Cybersecurity as an ongoing process and not a goal that can be reached**
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- Security Levels
- Requirements
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



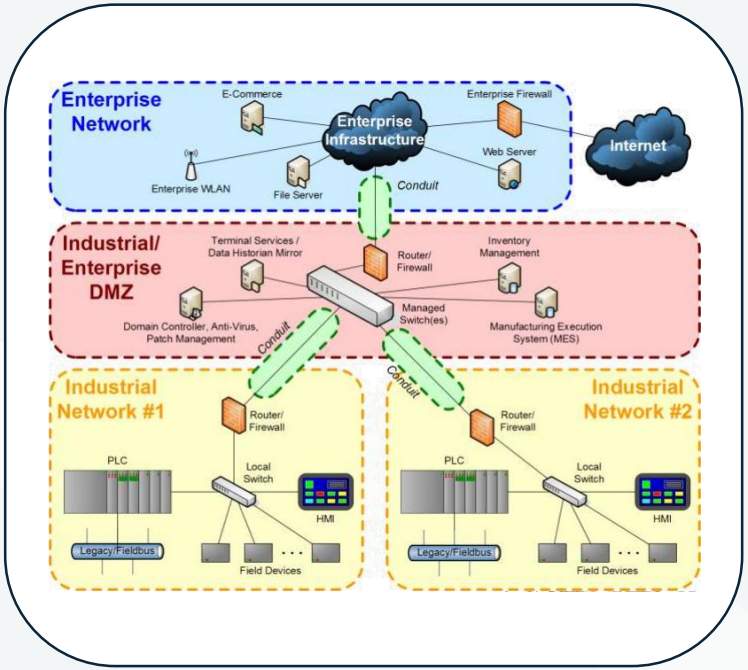
IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- **Security by Design <-> Defense-in-depth**
- Zones & Conduits Diagram
- Security Levels
- Requirements
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



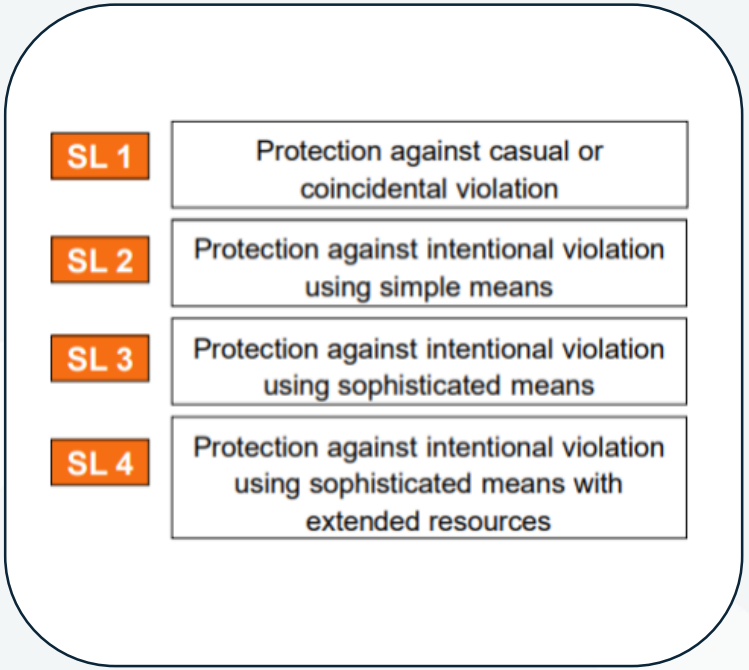
IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- **Zones & Conduits Diagram**
- Security Levels
- Requirements
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



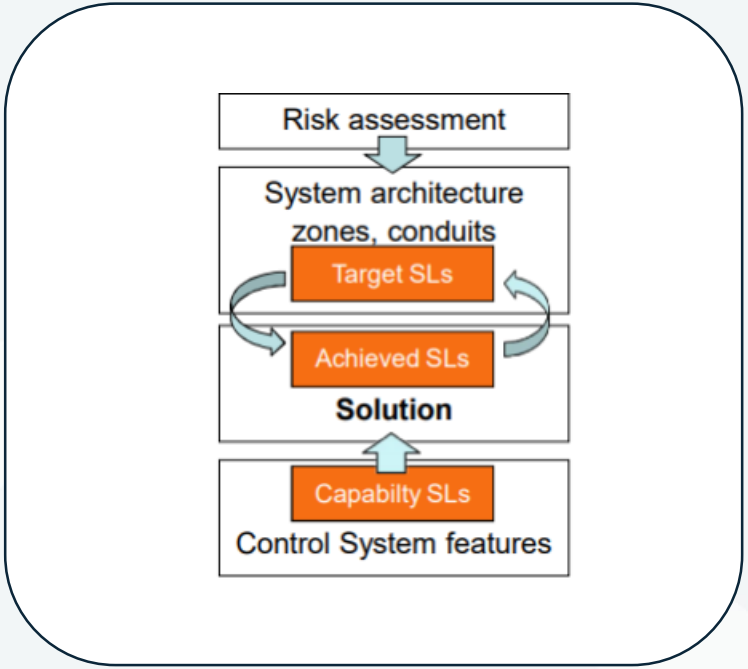
IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- **Security Levels**
- Requirements
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



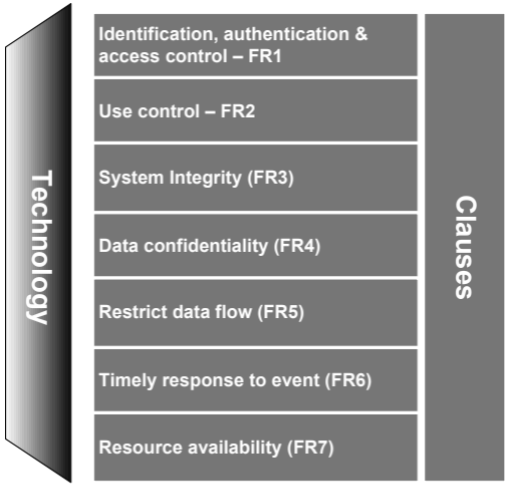
IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- **Security Levels**
- Requirements
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- Security Levels
- **Requirements**
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



IEC 62443-3-3 et IEC 62443-4-2: technology

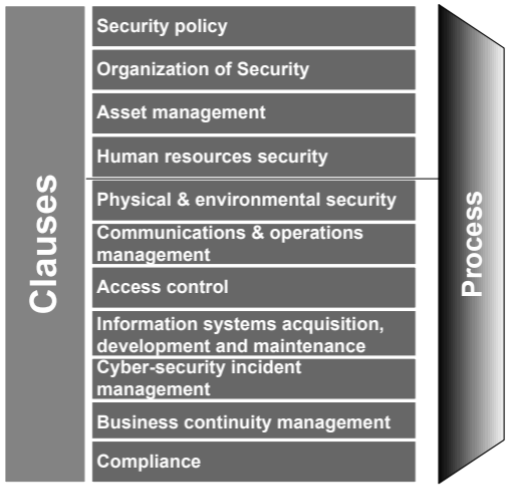
IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- Security Levels
- **Requirements**
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 3 – System integrity (SI)					
SR 3.1 – Communication integrity	7.3	✓	✓	✓	✓
SR 3.1 RE 1 – Cryptographic integrity protection	7.3.3.1			✓	✓
SR 3.2 – Malicious code protection	7.4	✓	✓	✓	✓
SR 3.2 RE 1 – Malicious code protection on entry and exit points	7.4.3.1		✓	✓	✓
SR 3.2 RE 2 – Central management and reporting for malicious code protection	7.4.3.2			✓	✓
SR 3.3 – Security functionality verification	7.5	✓	✓	✓	✓
SR 3.3 RE 1 – Automated mechanisms for security functionality verification	7.5.3.1			✓	✓
SR 3.3 RE 2 – Security functionality verification during normal operation	7.5.3.2				✓
SR 3.4 – Software and information integrity	7.6	✓	✓	✓	✓
SR 3.4 RE 1 – Automated notification about integrity violations	7.6.3.1			✓	✓
SR 3.5 – Input validation	7.7	✓	✓	✓	✓
SR 3.6 – Deterministic output	7.8	✓	✓	✓	✓
SR 3.7 – Error handling	7.9		✓	✓	✓
SR 3.8 – Session integrity	7.10		✓	✓	✓
SR 3.8 RE 1 – Invalidation of session IDs after session termination	7.10.3.1			✓	✓
SR 3.8 RE 2 – Unique session ID generation	7.10.3.2			✓	✓
SR 3.8 RE 3 – Randomness of session IDs	7.10.3.3				✓
SR 3.9 – Protection of audit information	7.11		✓	✓	✓
SR 3.9 RE 1 – Audit records on write-once media	7.11.3.1				✓

IEC62443 – Security mindsets

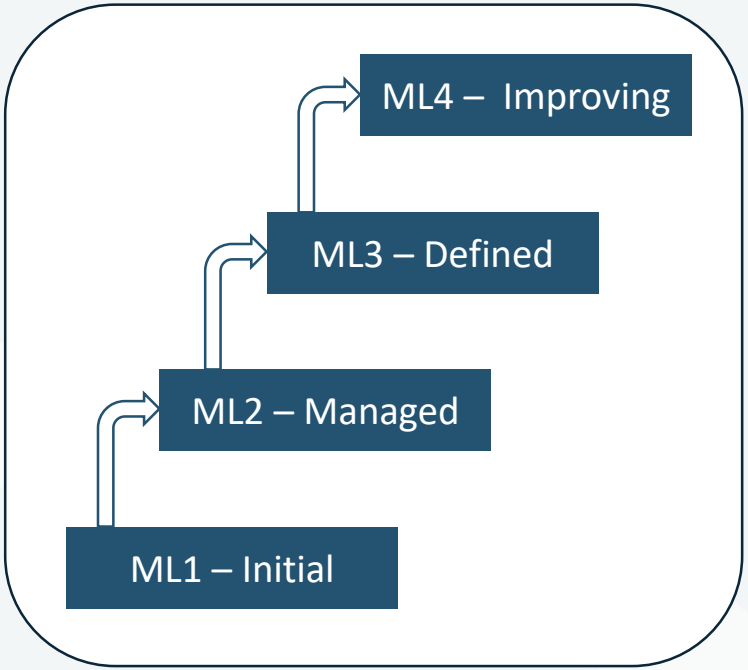
- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- Security Levels
- **Requirements**
- Maturity Level
- Roadmap for both Asset owner, service provider and product manufacturer



IEC 62443-2-1 (dérivée de ISO 27002) : process

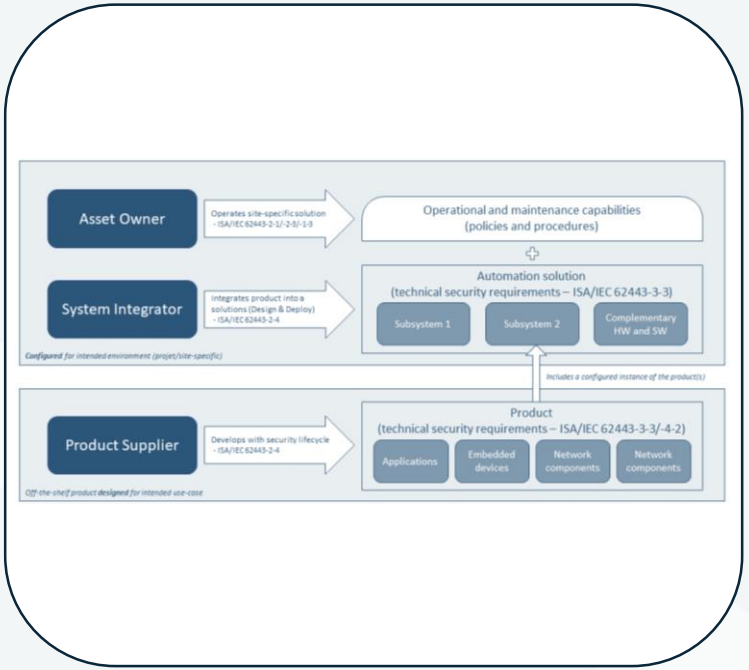
IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- Security Levels
- Requirements
- **Maturity Level**
- Roadmap for both Asset owner, service provider and product manufacturer



IEC62443 – Security mindsets

- See Cybersecurity as an ongoing process and not a goal that can be reached
- Security by Design <-> Defense-in-depth
- Zones & Conduits Diagram
- Security Levels
- Requirements
- Maturity Level
- **Roadmap for both Asset owner, service provider and product manufacturer**



Perspectives of a larger landscape

IEC62443 as cybersecurity framework

Currently, IEC62443 covers aspects related to IACS for domain such as the following:

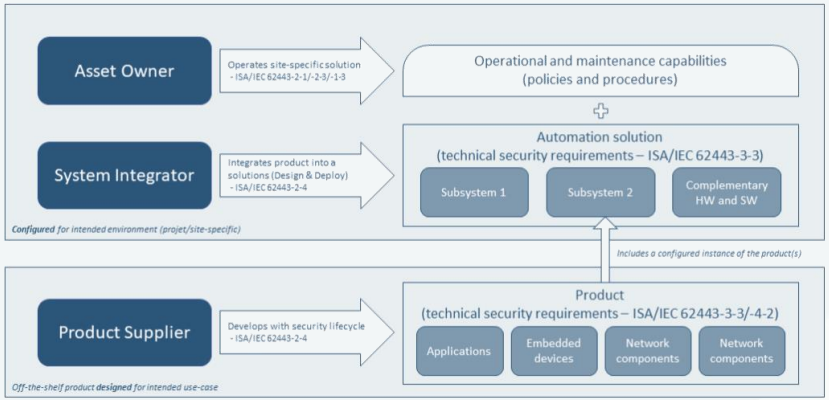
- Chemicals Processing
- Petroleum Refining
- Food and Beverage
- Energy
- Pharmaceuticals
- Water
- Manufacturing

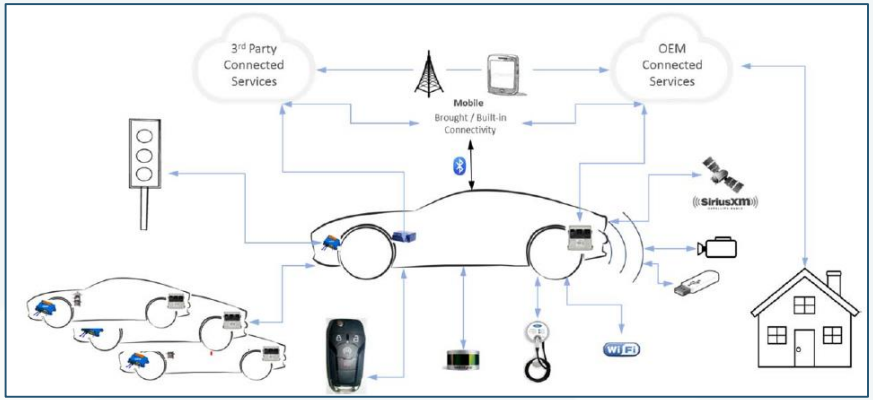
… but some other domain see IEC62443 as a potential alternative to follow:

- Automotive / Smartmobility
- Medical devices

Cybersecurity in Automotive world

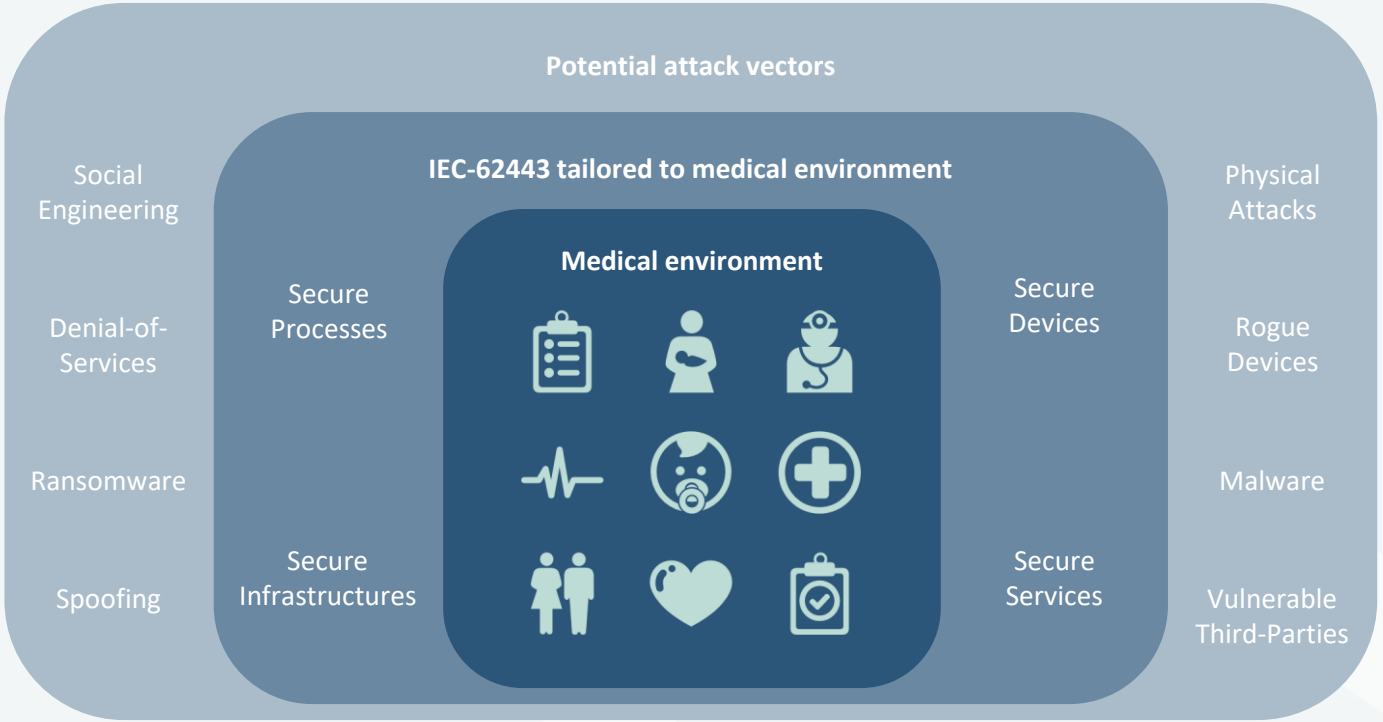
Includes vehicles, other traffic participants, infrastructures, customers and authorities





→ **ISO-21434 (partly based on IEC62443) under development and followed/supported by CertX**

Cybersecurity in Medical world



Questions

Thank you for your attention

You can contact me at **kilian.marty@certx.com**

Your Contact for Cybersecurity at CertX

www.certx.com

- M.sc. in Telecommunication networks and IT Security
- ISA/IEC 62443 Certified
- IEC 61508 Certified
- Member of IEC technical committee TC65 covering IEC-62443 standards

Kilian Marty
Head of Cybersecurity Department
T +41 26 309 29 94
kilian.marty@certx.com

CertX AG
Route de l'Ancienne Papeterie 106
1723 Marly, Switzerland

www.certx.com

CertX support customers with qualified assessors