MSE | MASTER OF SCIENCE IN ENGINEERING

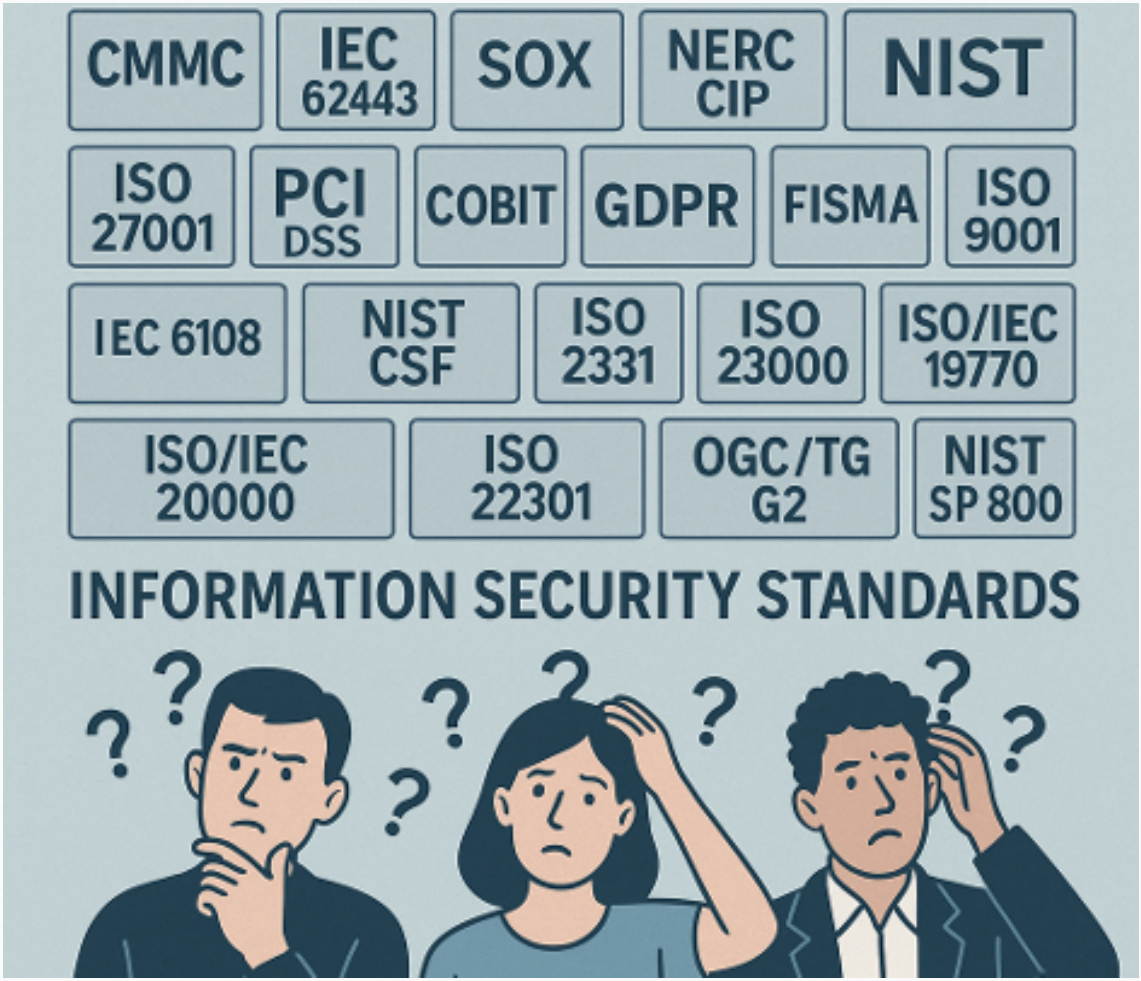
IEC 62443(-4-1/2)

Luca Haab

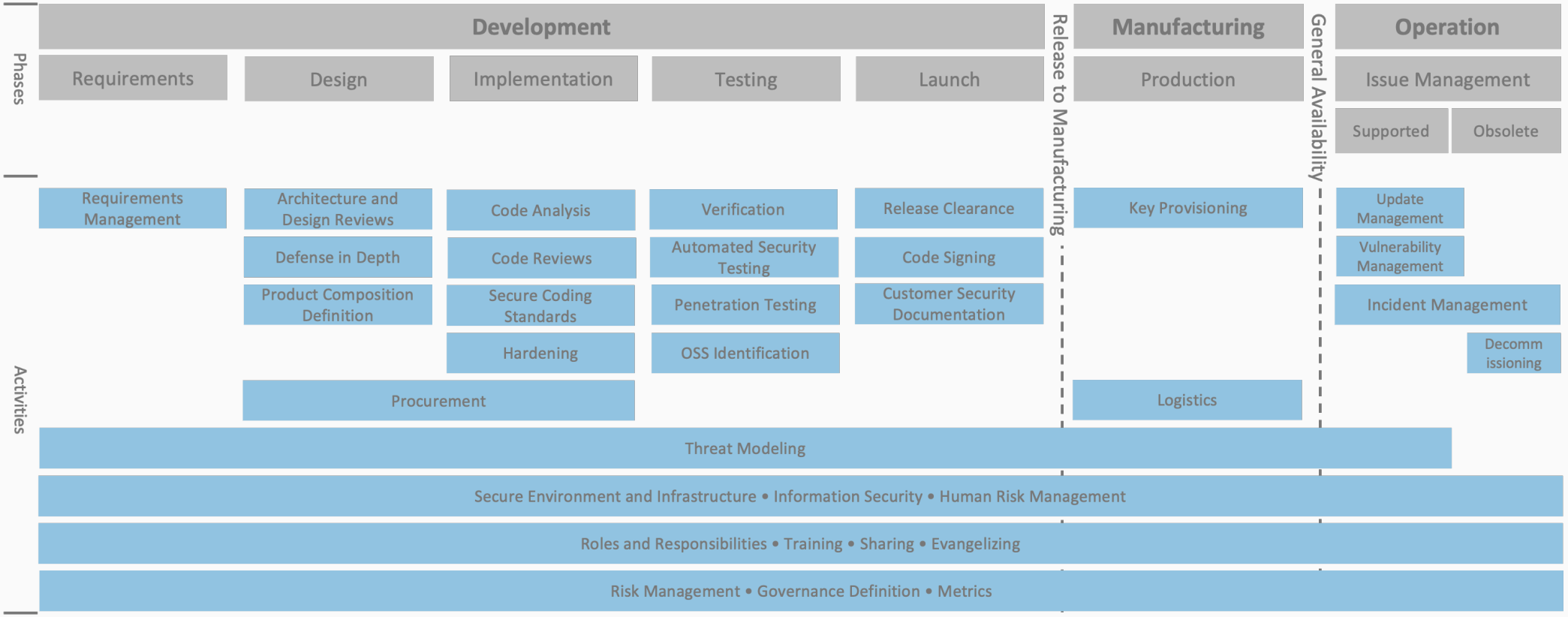
December 14, 2025

Imagine a situation

Every Company Has to Go Through the Same...



(Technical) Activities within a Company



Standardization: a way to structure this

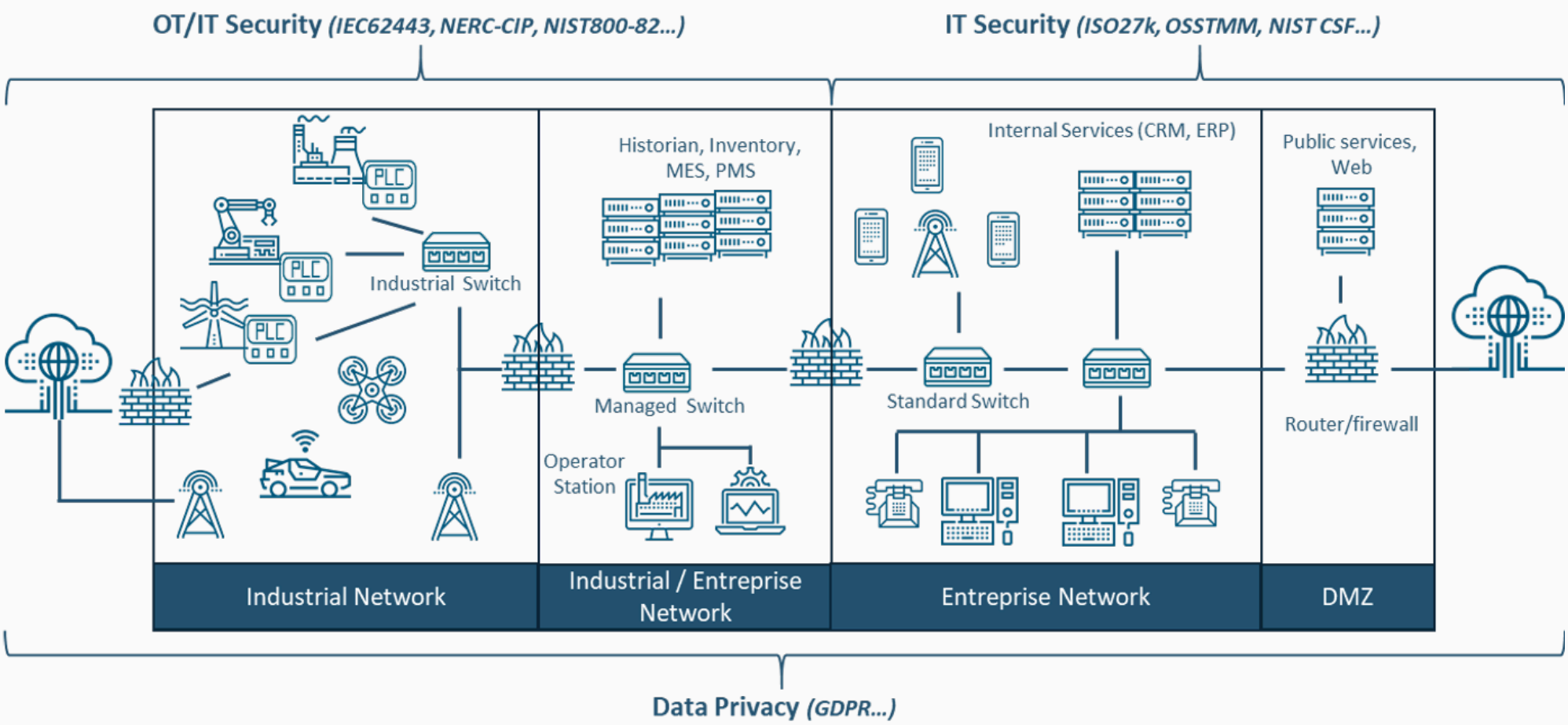
Standardization: an opportunity

Companies want standardization as it allows them to:

- maximize the business benefits (by being a leader in cybersecurity);
- institutionalize the best practices in the standards;
- be compliant with contract obligations, national laws regulations & directives.
- (*minimize business risks*)

Source: https://x.com/Raedalis/status/1370252431024660482

IT & OT - Threat combined



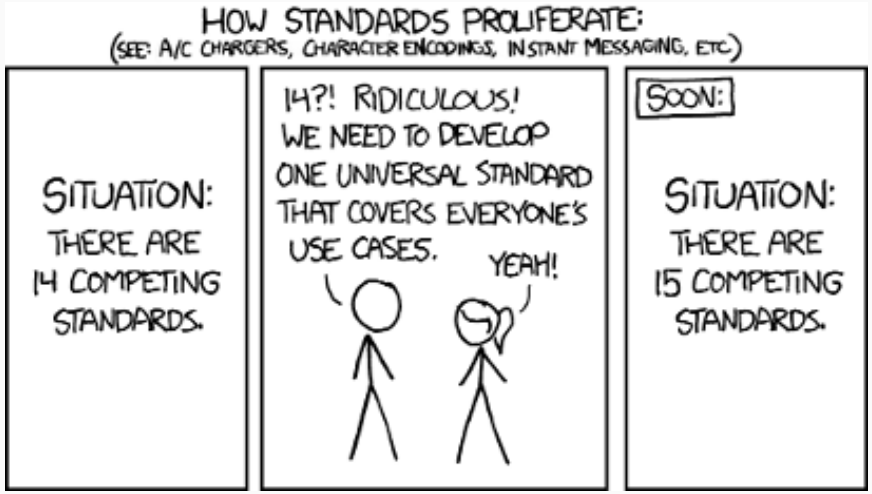
IT & OT - Constraints and conditions

Cyber security topic	**IT / «office» environment**	**OT / Industrial environment**
Technology support lifecycle	Typical lifetime of 2-3 years High number of suppliers	Typical lifetime of 10-20 years, low number of suppliers ⇒ Legacy systems are strong issues
Patching strategy	Usually remotely managed, Automated & regular (patch Tuesday principle)	Long delay with strong planification, responsbility usually on supplier side, might strongly impact business continuity
Test & audit	Usually automated, sufficiently resilient for supporting on-line testing & evaluation	Usually customized solutions reducing possibility for automation, too critical nature requiring offline testing
Asset classification	Common activity performed on a yearly basis	Usually performed on-demand / on-request only (lack of asset supervision...)
Incident-response & forensics	Common activity legally required (e.g. GDPR)	Usually based on system reboot, forensics not really addressed
Physical security	Strong differences from office environment (low protection) to data centers (high protection)	Usually high protection, dedicated building / rooms etc
Secure SW development	Security usually integrated as a fundamental dimension of development lifecycle	Historically not connected to outside networks and physically isolated, therefore security has not been considered «by-design». Add-on Security layers are complex to be integrated into ICS architecture later on

IT & OT - Constraints and conditions

Cyber security topic	**IT / «office» environment**	**OT / Industrial environment**
Endpoint security	«Easy» to be deployed and managed remotely	Performance (e.g. realtime, memory) are usually limited therefore the footprint of such items might be critical for ensuring intended functions & safety. Custom solutions are existing but complex to manage

Regulations, Standards & Guidance

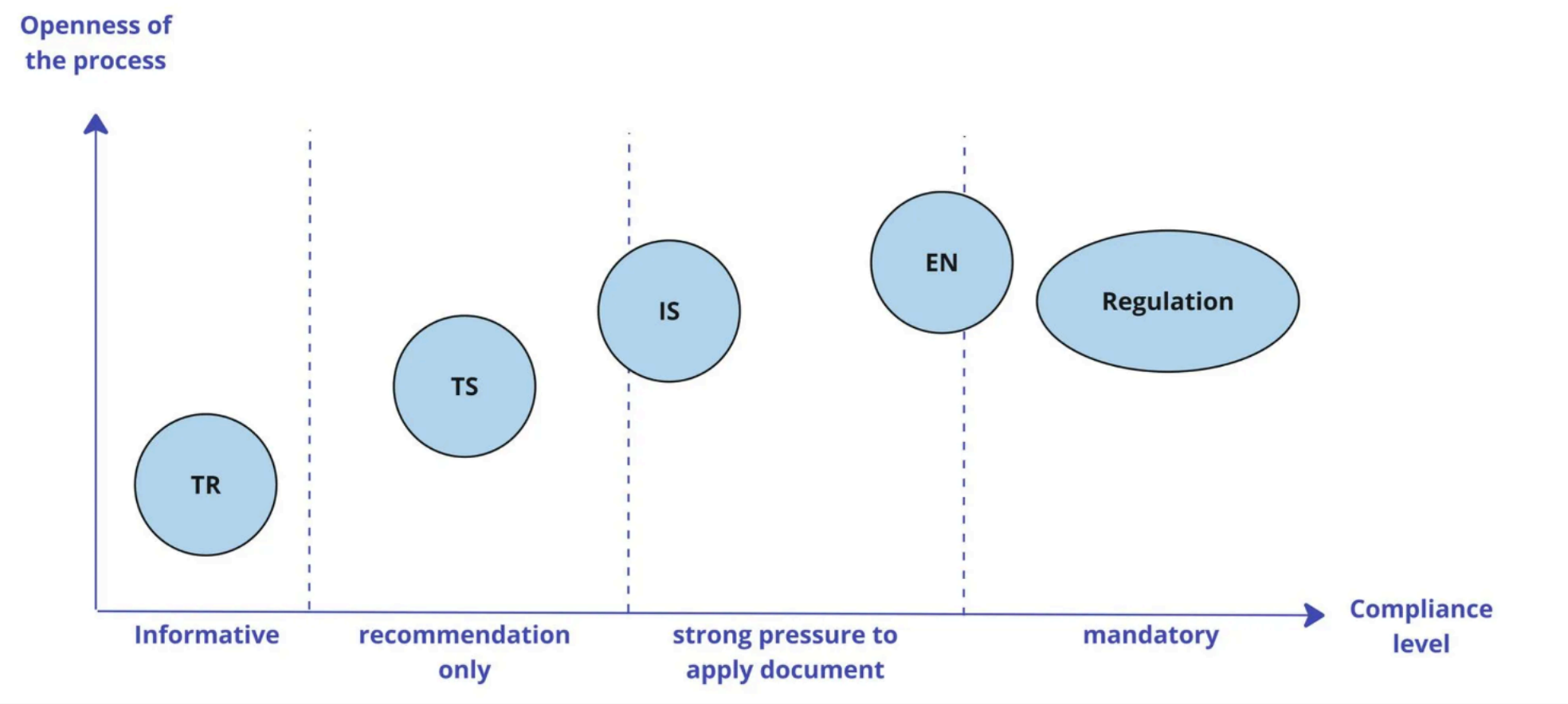


Sometimes it might be complicated to spot the right references for a *given organization role*, *environment* or *product development*... and standards in industrial cyber security fields are even trickier due to a **certain lack of maturity & stability in State-of-the-Art definition**.

Regulations, Standards & Guidance

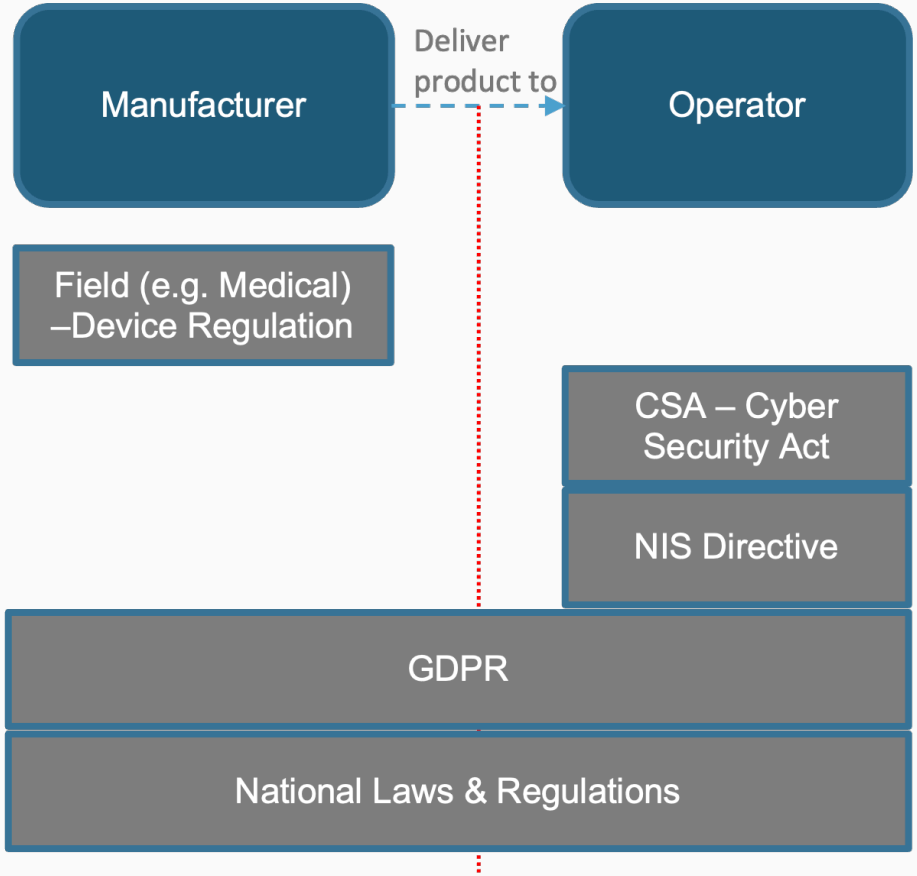
- **Regulations** - legally bindings, usually bound to a specific industry or geographic area (national or international) e.g. *NIS Directive*, *GDPR* etc
- **Standards & norms** - Usually considered as State-of-the-Art definition, consensus-based document, not mandatory (excepting if contractual) e.g. *ISA/IEC 62443* standard series, *ISO/IEC 27000* series, *ISO 9001*... Typical product, process and management system certification are based on them
- **Guidance & best practices manual** - More "dynamic" because out of standardization scheme, supportive document with tangible inputs e.g. *NIST* documents, *ENISA* reports etc

Regulations, Standards & Guidance

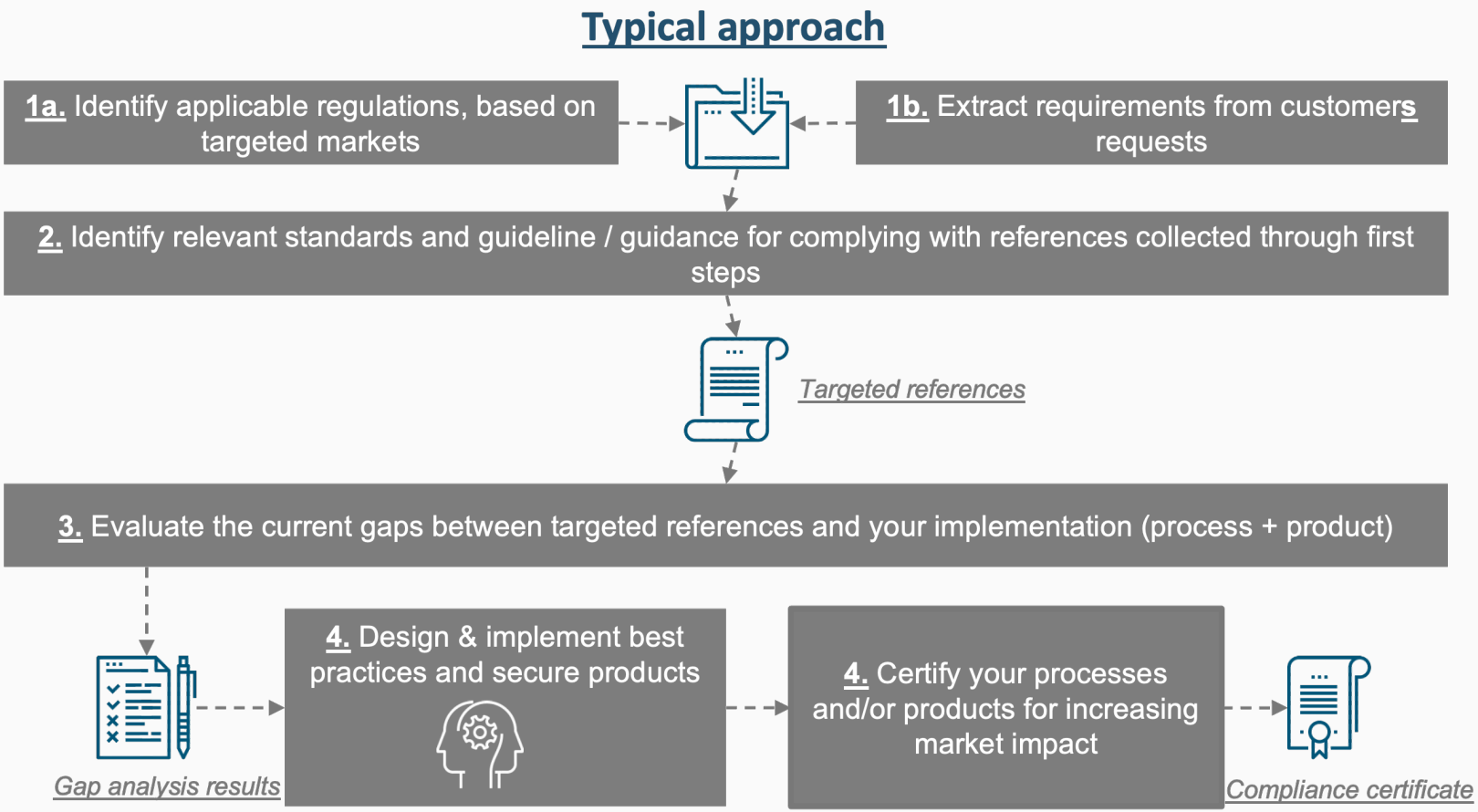


From Regulation to Standards

- Field Regulation (e.g MDR - Medical Device Regulation)
  - IEC62304, IEC62443 series, IEC80001-2-8...
- CSA Cyber Security Act
  - ISO27000 series, IEC15408...
- NIS Directive
  - ISO27000 series, IEC62443 series...
- GDPR -ISO27000 series, ISO27701...
- National Laws & Regulations
  - Strongly related with national authorities



Regulations, Standards & Guidance



ISA/IEC 62443 - History

Initially developed by the *International Society of Automation* (*ISA*) *Committee* on *Security for Industrial Automation & Control Systems* (ISA99)

- 700+ members, representing companies across many sectors including chemicals, food & beverage, pharmaceuticals, health, manufacturing, petroleum refining, energy, water, mobility...

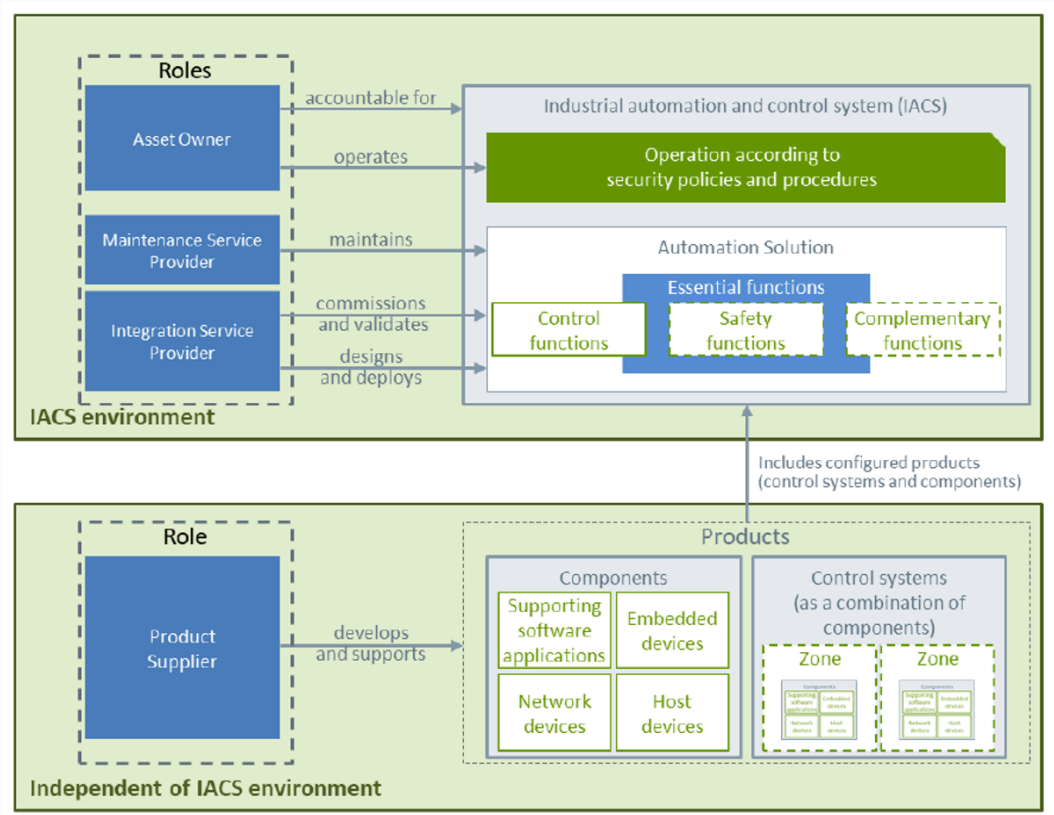
Note: *IEC technical committee 65*, *working group 10* collaborates with the *ISA* to build the *IEC* version, which is the reason why the standard is commonly called *ISA/IEC 62443*.

ISA/IEC 62443 - Scope & purpose

The scope of ISA/IEC 62443 is defined as any **software**, **hardware**, **personnel**, and **policies** that are involved in or have influence over the safety, security, and reliability of the ***IACS operations***. Since IACS components can be physical systems, ISA/IEC 62443 stresses the importance of safety. Specifically, a compromise of these physical systems can lead to risk of human life or safety, damage to machinery, financial impact, and harm caused to the environment.

Holistic approach requires the considerations of 3 dimensions:

- Technologies
- Processes
- Human factors

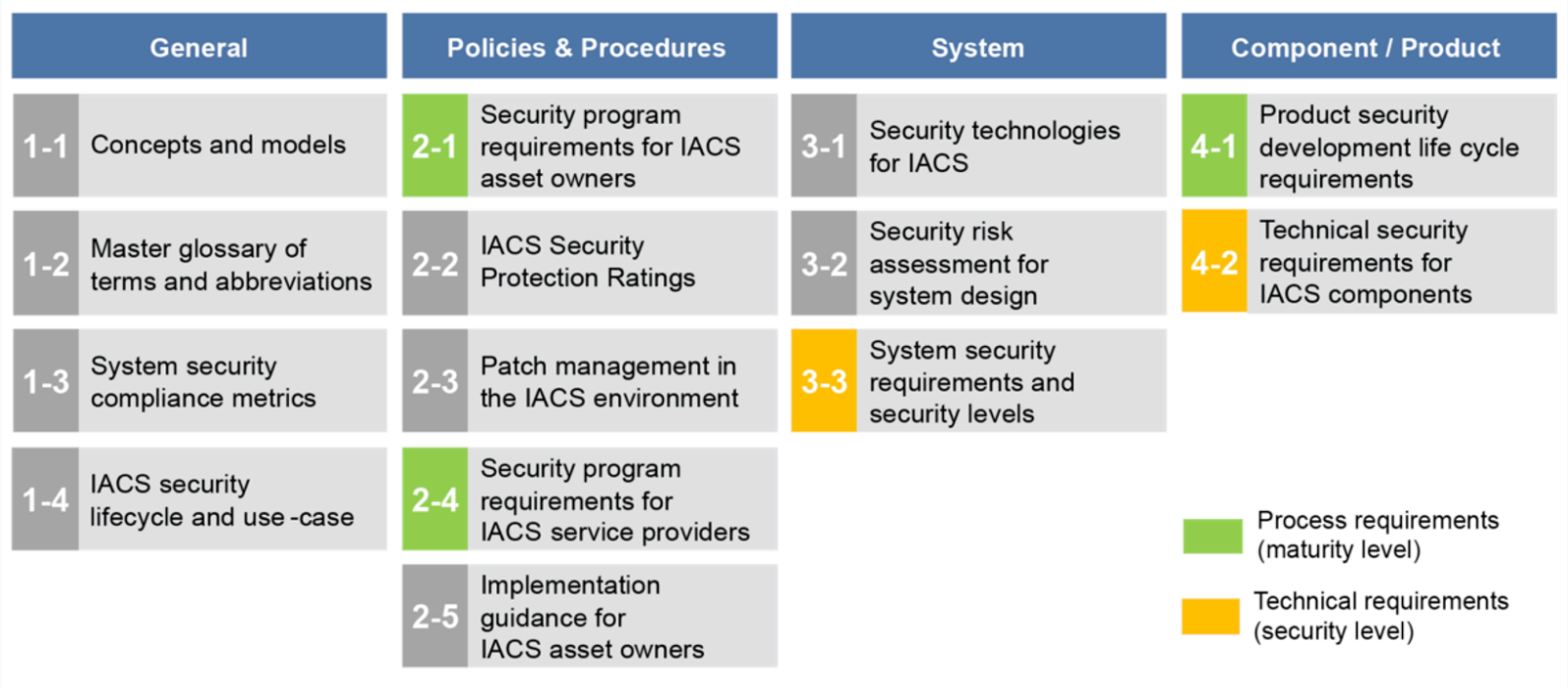


ISA/IEC 62443 - Scope & purpose

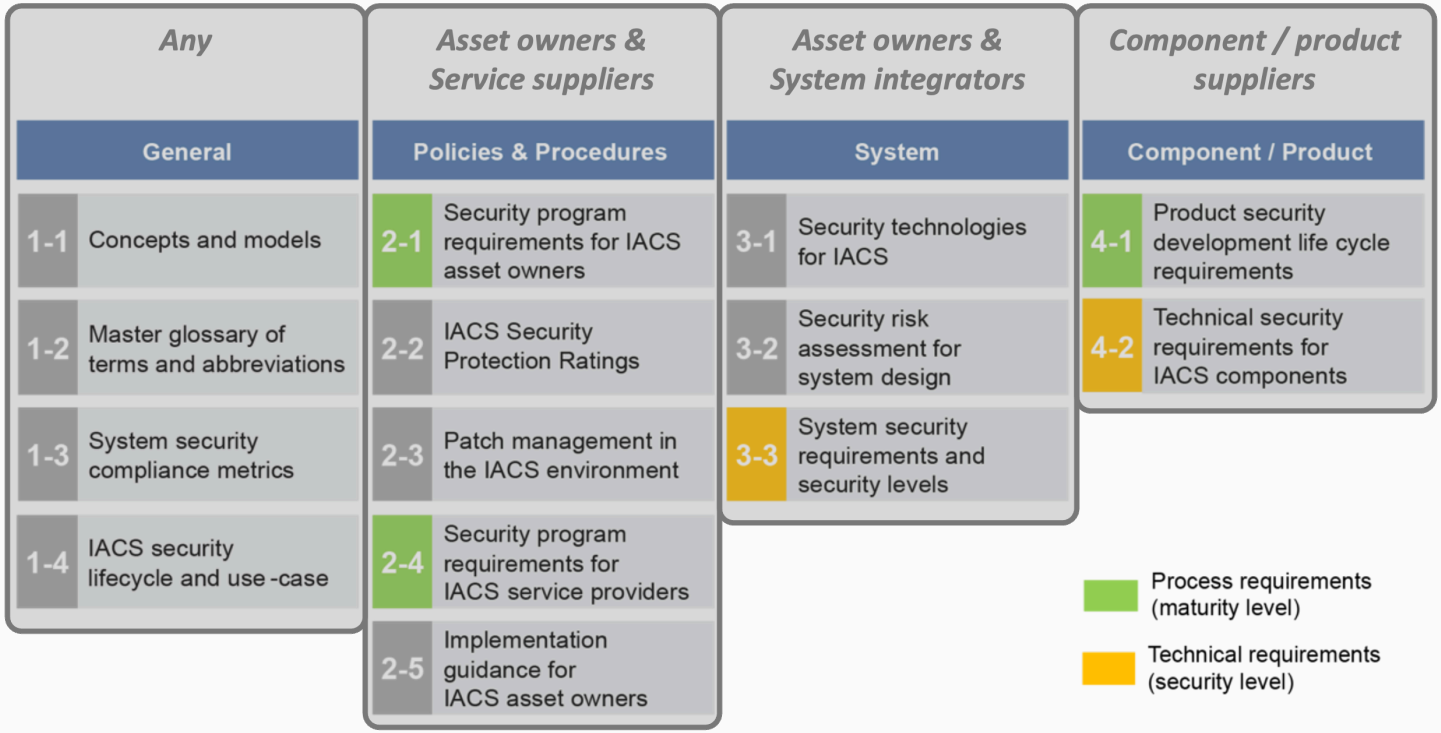
... to be considered from any stakeholder perspective

ISA/IEC 62443 - Standard families

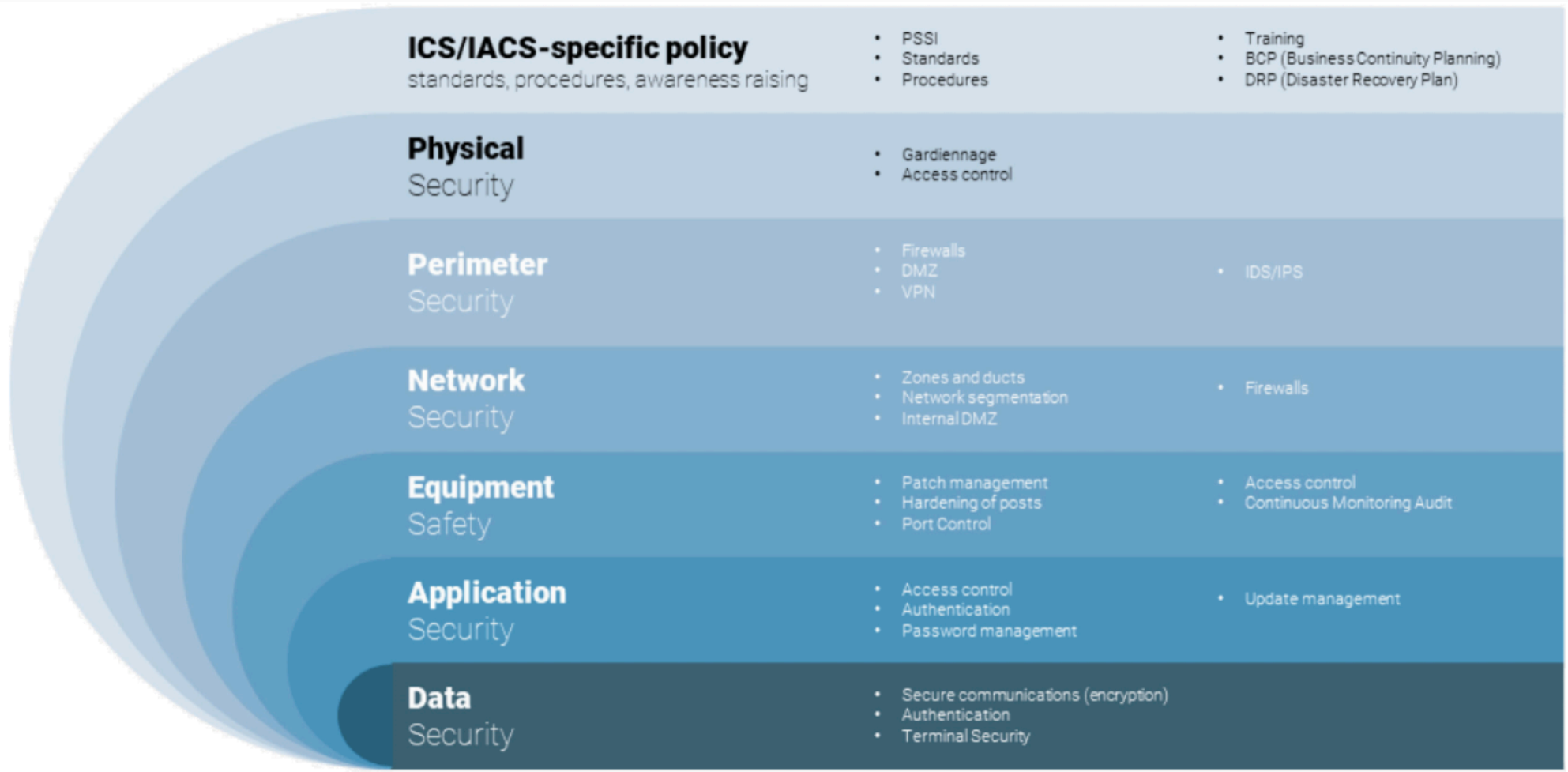
ISA/IEC 62443 is a complete standard family specifying requirements and practices to be implemented into/by organizations for using, developing, operating and/or maintaining IACS (Industrial and Automation Control Systems) infrastructure.



ISA/IEC 62443 - Stakeholders



ISA/IEC 62443 - Key Principles

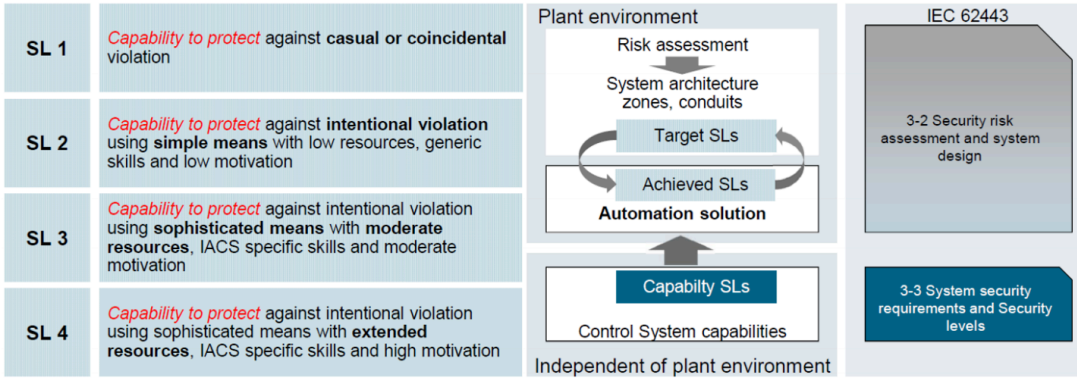


ISA/IEC 62443 - Key Principles: Security Levels

Security levels

A specific security metric has been defined in the scope of the IEC 62443 (Note: *Security Levels* are also called *SL*):

- Categorized on 5 levels (including 0)
- Allow operators to compare cyber security «maturity» of components and systems
- 3 sub-levels: SL-Capability, SL-Target, SL-Achieved
- Same scale on both system and component levels



Warning

SL 0: No special requirement or protection required.

ISA/IEC 62443 - Key Principles: Maturity Levels

Maturity Levels are based on the *CMMI-DEV model*. These levels define the benchmark which are required to be met by the requirements defined the standards IEC 62443 2-4 and IEC 62443 4-1. Each level is progressively advanced than the previous level. The service providers and the asset owners are required to identify the maturity level associated with the implementation of each requirement.

Level	**CMMI-DEV**	**IEC 62443-4-1**	**Description**
1	Initial	Initial	Capability of performing a service without a documented process that is poorly controlled
2	Managed	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel
3	Defined	Defined (Practiced)	Capability of performing ML2 level including evidence of practicing the process e.g. Documented process plus list of participants in the training of personnel
4	Quantitatively managed	"Improved"	"Capability of performing ML3 level including demonstration of continuous improvement e.g. internal audit report"
5	Optimized		

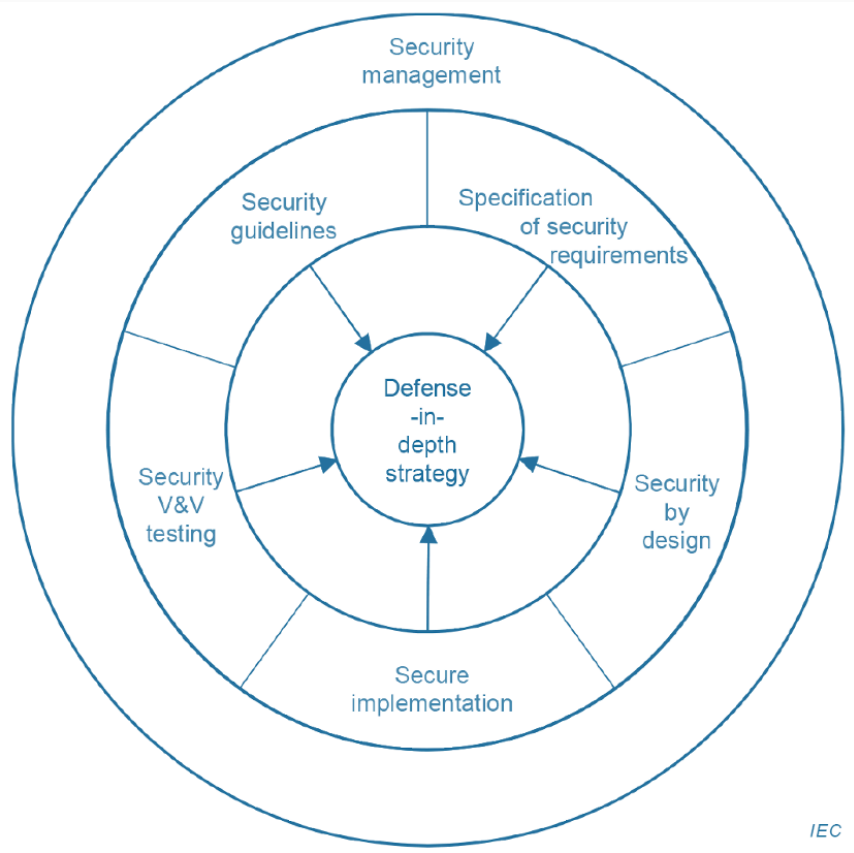
ISA/IEC 62443-4-X - Key parts

- ISA/IEC 62443-4-1
  - describes product development life-cycle requirements related to cyber security for products intended for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.
  - implementation of such SDLC (Secure Development Life Cycle) practices is considered as a prerequisite (called common cyber security constraints) for certifying a technical capabilities of a product acc. To ISA/IEC 62443
- ISA/IEC 62443-4-2
  - provides the cyber security technical requirements for the components that make up an IACS, specifically the embedded devices, network components, host components and software applications.
  - defines technical requirements, in alignment with capability from ISA/IEC 62443-3-3, but focused on capabilities on component level, and depending on component type

ISA/IEC 62443-4-1 - SDLC

Processes, practices and requirements related to them are described by the IEC62443-4-1 and categorized as follow:

1. General security management (SM)
2. Specification of security requirements (SR)
3. Security by design (SD)
4. Secure implementation (SI)
5. Security verification and validation testing (SVV)
6. Management of security-related issues (DM)
7. Security update management (SUM)
8. Security guideline (SG)



ISA/IEC 62443-4-2

- CR: (generic) Component Requirements
- RE: Requirements Enhancement

As introduced earlier, most of the requirements on component level are considered as generic, but some specificities and tailoring are made for some of those, depending on the type of component, as follow:

- *Software Application Requirements* (*SAR*) Ex. Software module/layer/application...
- *Embedded Device Requirements* (*EDR*) E.g. PLC, IED, ECU...
- *Host Device Requirements* (*HDR*) E.g. Operator workstation, Data historian...
- *Network Device Requirements* (*NDR*) E.g. Switch, VPN terminator, Gateways...

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
RE (2) Multifactor authentication for all interfaces			✓	✓
CR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for authenticators			✓	✓
NDR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
CR 1.7 – Strength of password-based authentication	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users			✓	✓
RE (2) Password lifetime restrictions for all users (human, software process, or device)				✓
CR 1.8 – Public key infrastructure certificates		✓	✓	✓
CR 1.9 – Strength of public key-based authentication		✓	✓	✓
RE (1) Hardware security for public key-based authentication			✓	✓

Resources

- IEC 62443 Wikipedia
- IEC 62443 Standards - a cornerstone of industrial cyber security (Author: *IEC*)
- IEC 62443 Publications
- (Swiss) National Cyber Security Centre (*NCSC*): Measures to protect industrial control systems