MASTER OF SCIENCE
IN ENGINEERING

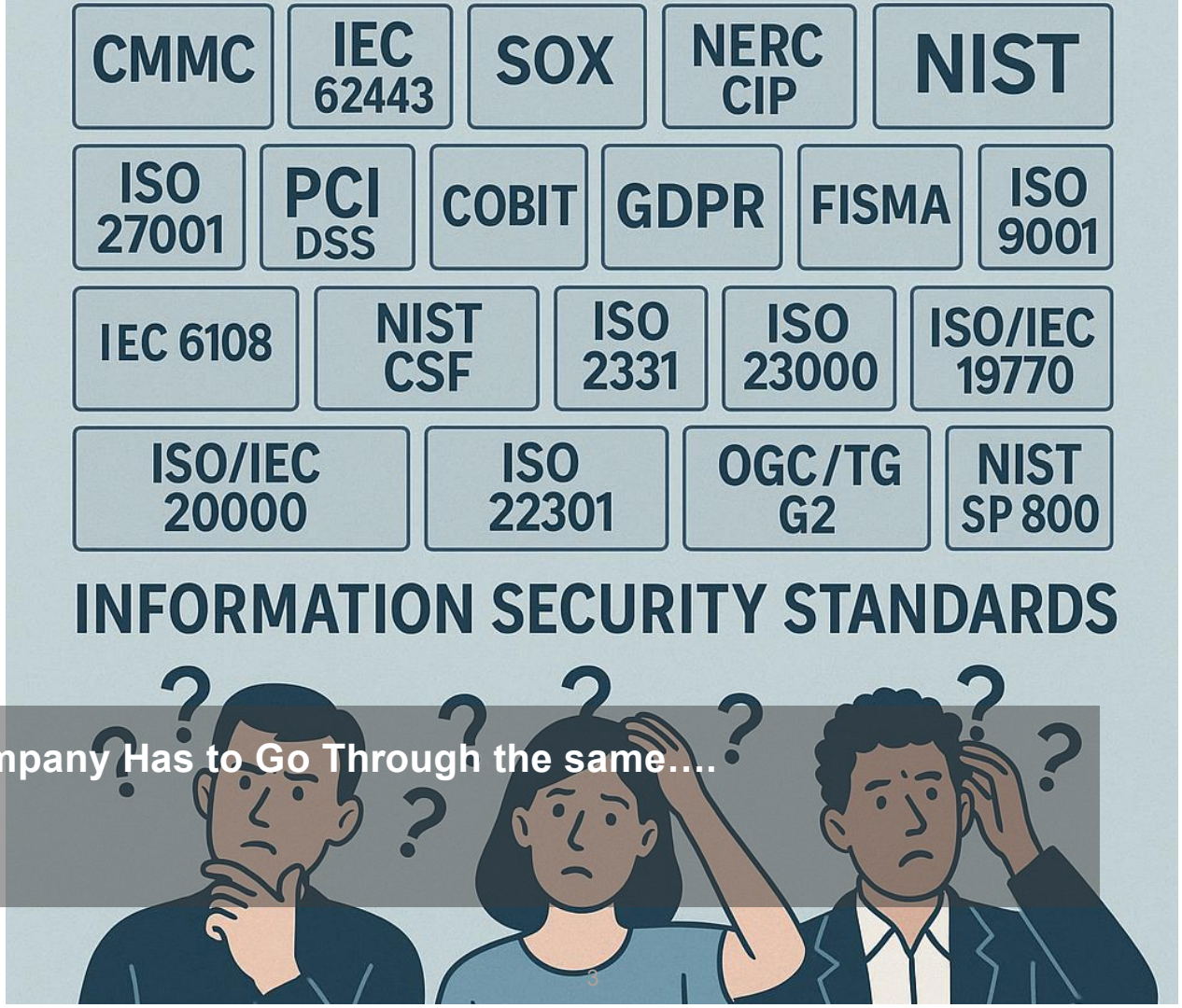
TSM_SecIndOpT

IEC 62443 (I)

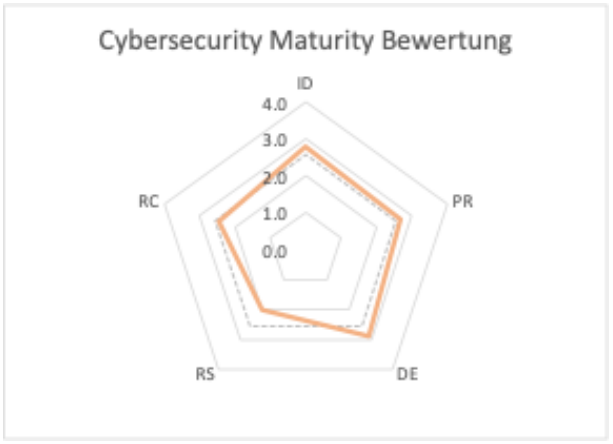
Version: 1.0

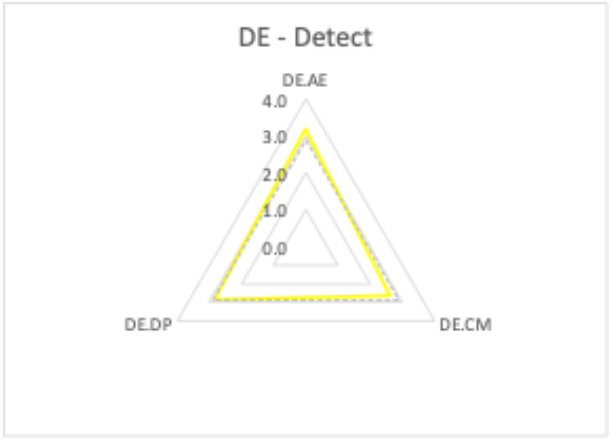
Luca Haab | 19.05.2025 | Cours MSE

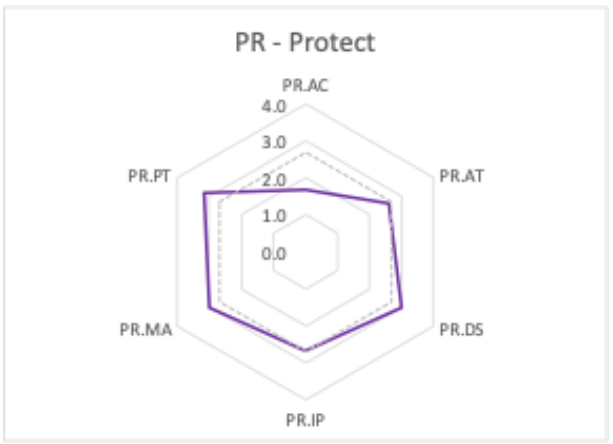

Imagine a situation

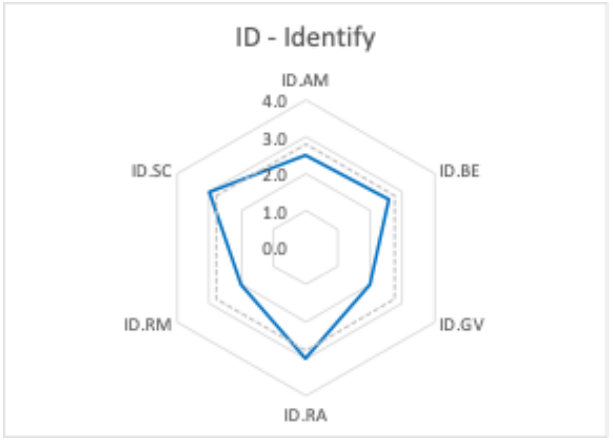


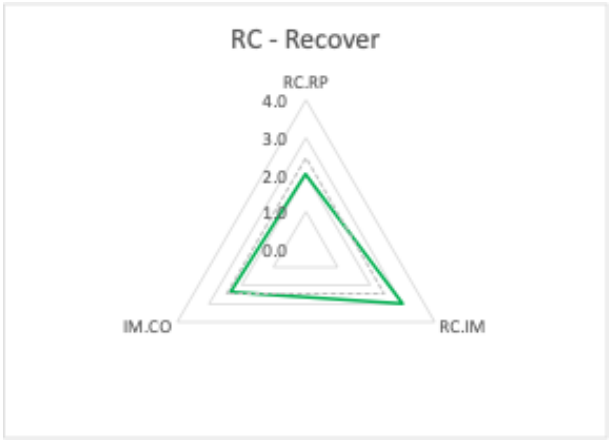
Every Company Has to Go Through the same….

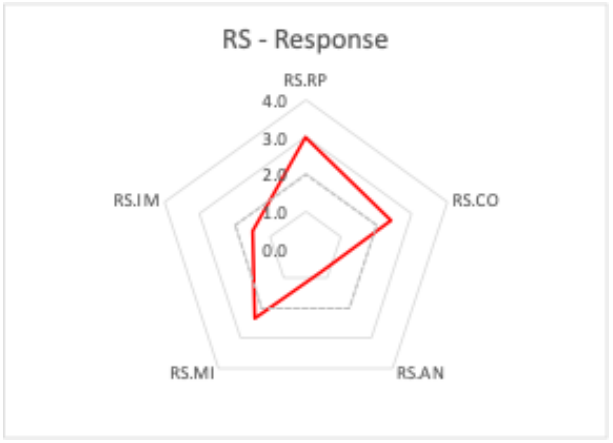








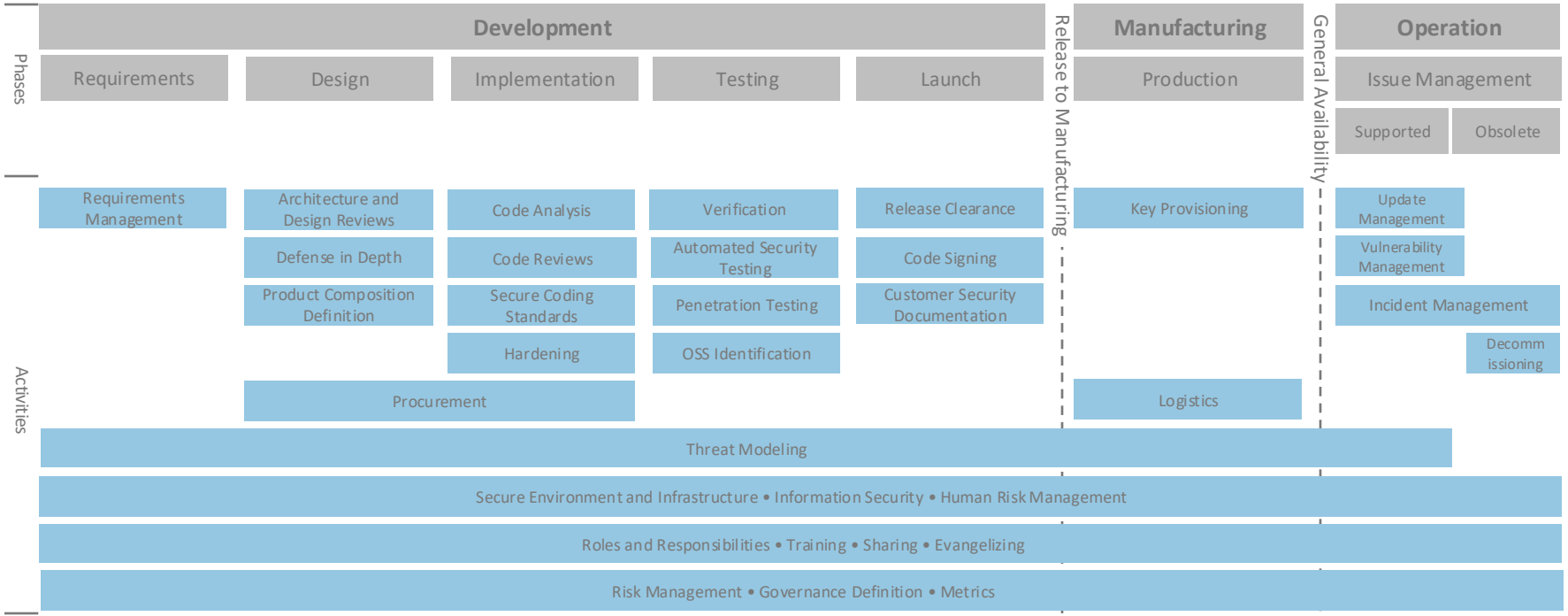


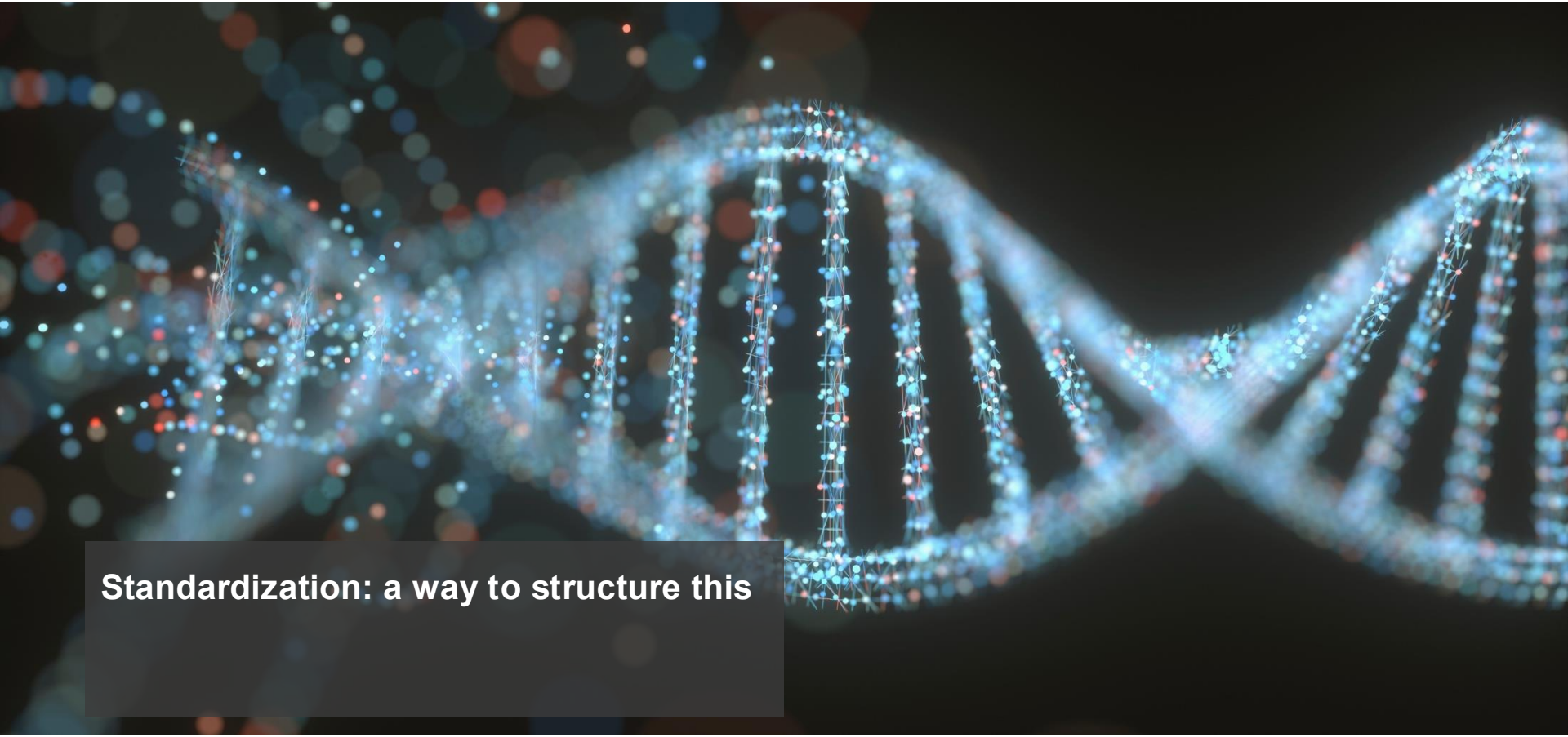


swissuniversities

Source: own, using Cybersecurity Minimalstandard – Assessment, Version 1.0, 1st January 2018

(Technical) Activities within a company





Standardization: a way to structure this

Standardization: an opportunity

- Companies want standardization as it allows them to:

I. **maximize** the business benefits (by being a leader in cybersecurity);

II. **institutionalize** the best practices in the standards;

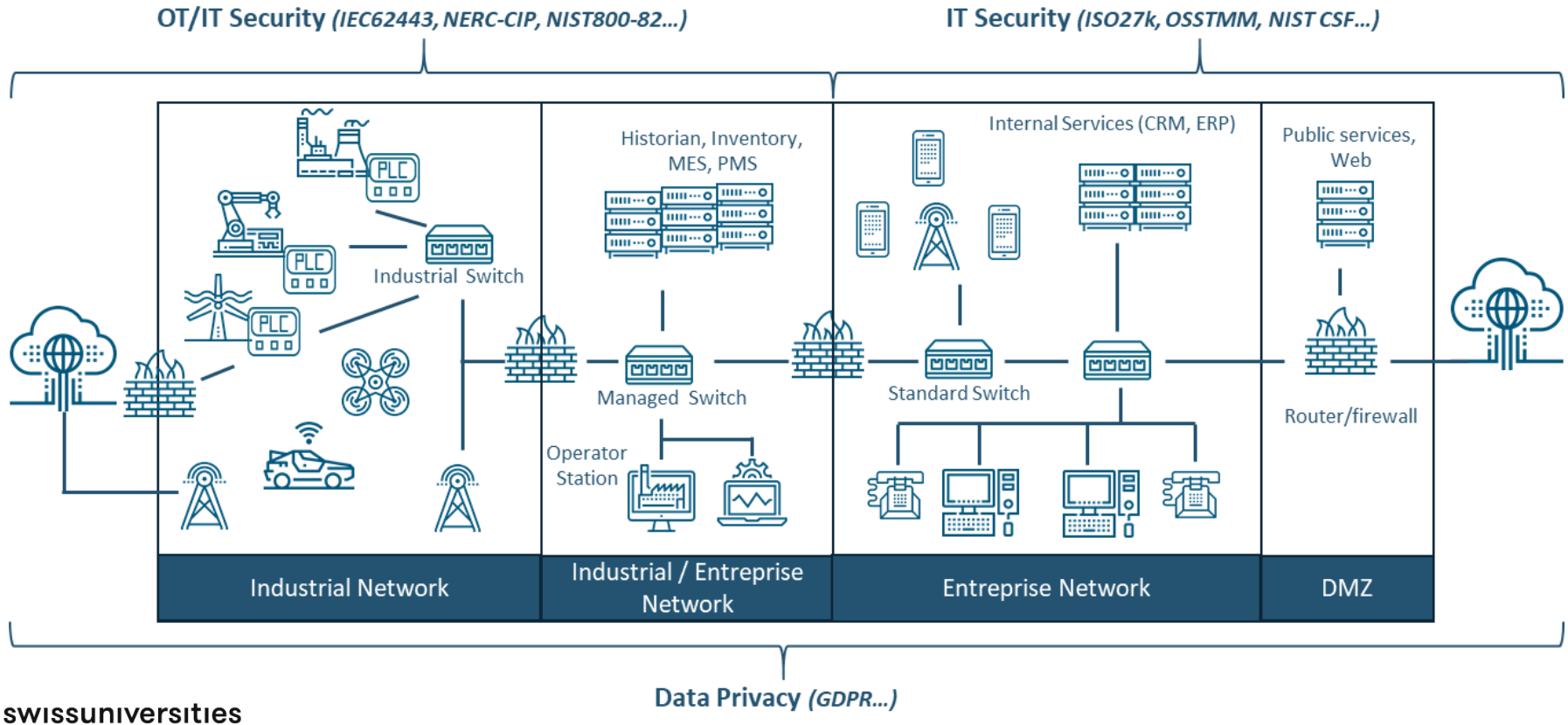
III. **be compliant** with contract obligations, national laws regulations & directives.

IV. (minimize business risks)

Be Aware

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

IT & OT – Threat combined

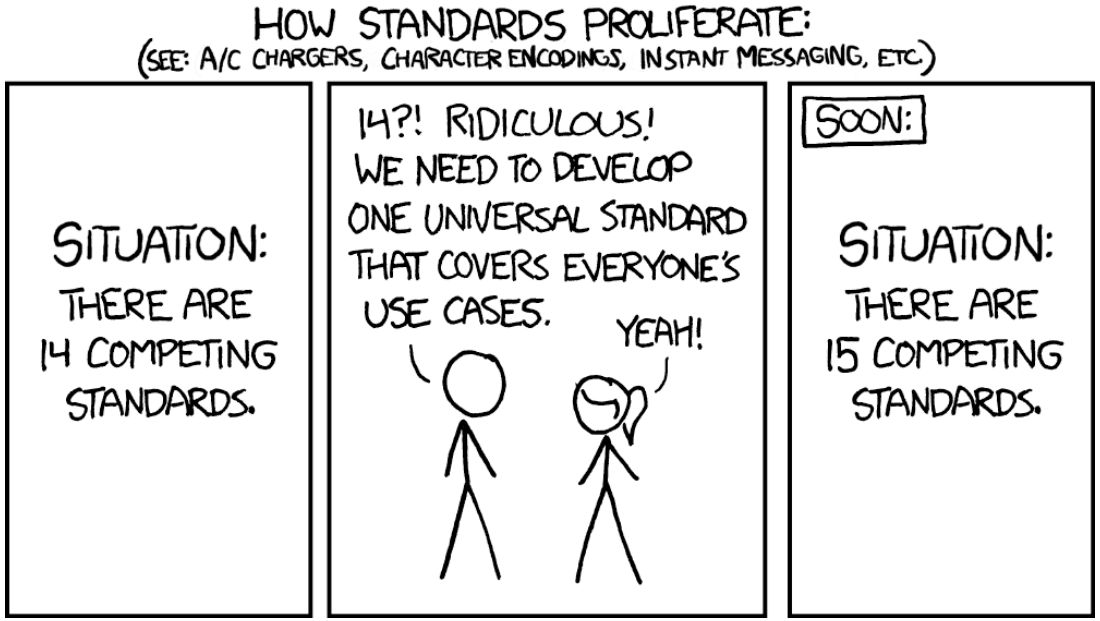


IT & OT – Constraints and conditions

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
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 (I)

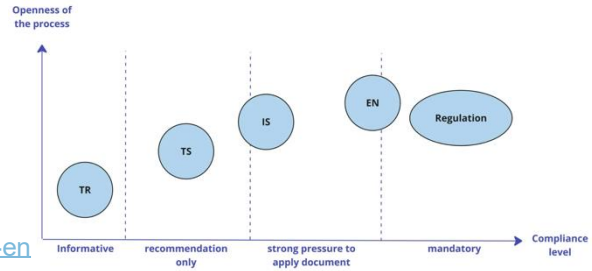
Sometimes it might be complicated to spot the right references for a *given organization role*, *environment* or *product development*… and standards in industrial cyber security fields are even more tricky due to a ***certain lack of maturity & stability in State-of-the-Art definition***



Regulations, Standards & Guidance (II)

Types

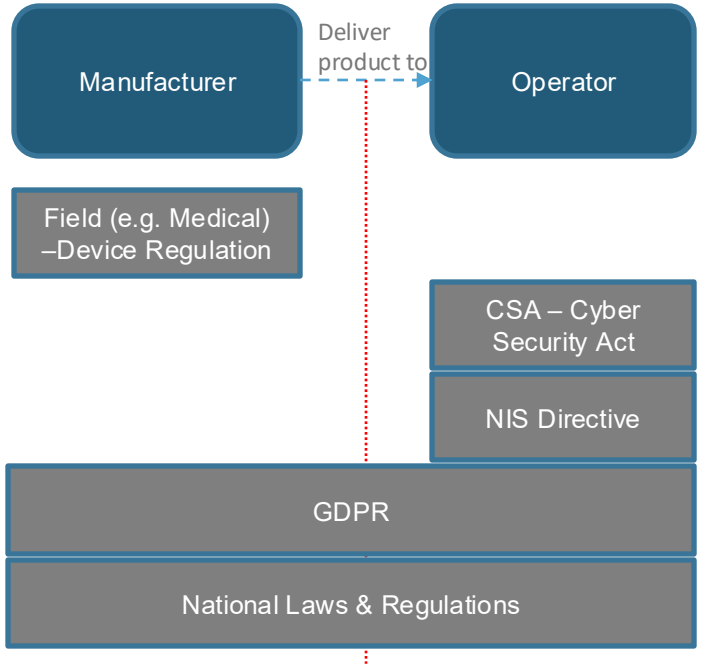
- **Regulations** – legally bindings, usually bound to a specific industry or geographic area (national or international)
  - e.g. NIS Directive, GDPR etc
- **Standards & norms** – Usually considered as State-of-the-Art definition, consensus-based document, not mandatory (excepting if contractual)
  - 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



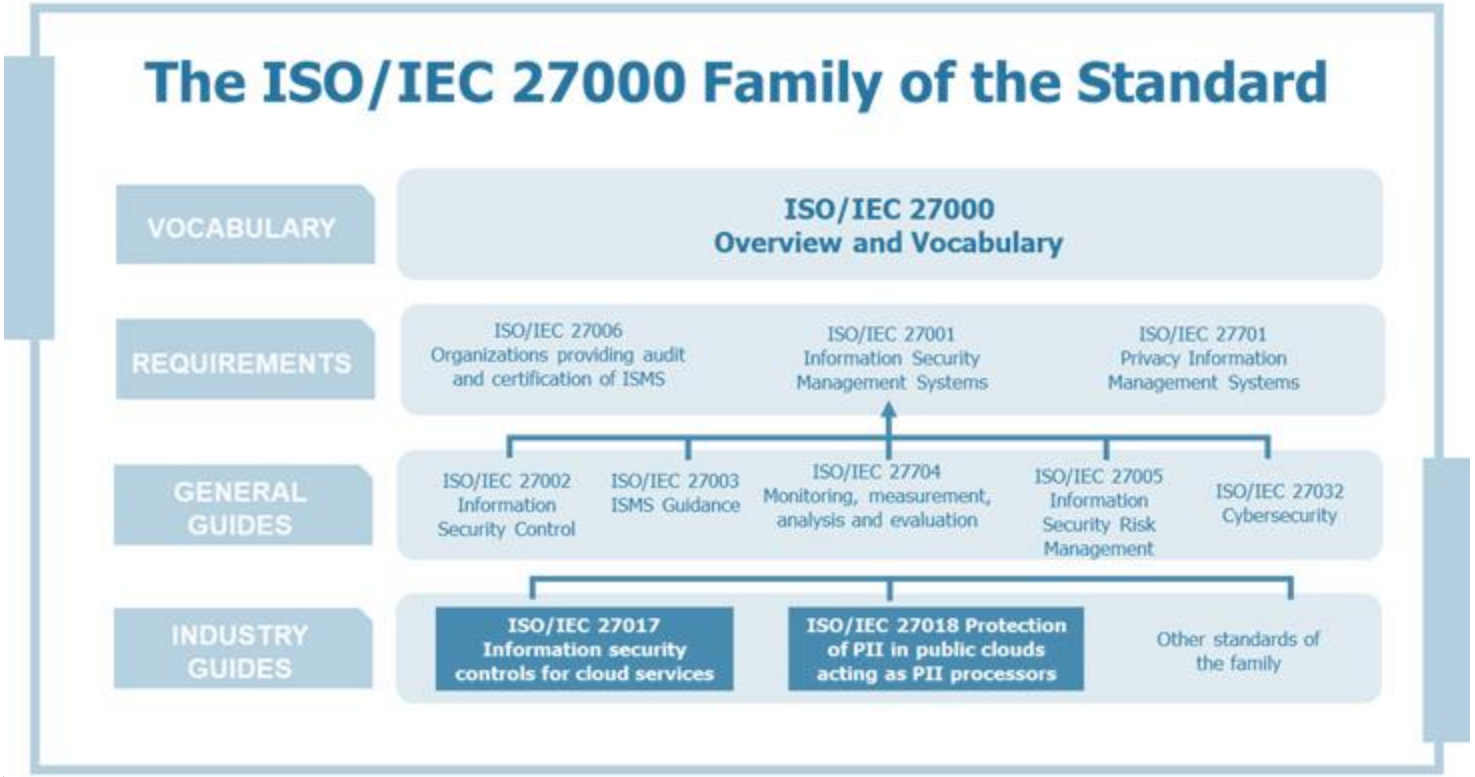
Source: https://www.normedconsulting.com/understanding-standards-tr-ts-is-and-en

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 (I)



Source: https://cfecertification.medium.com/the-iso-iec-27000-family-of-standards-2f04697f2e82

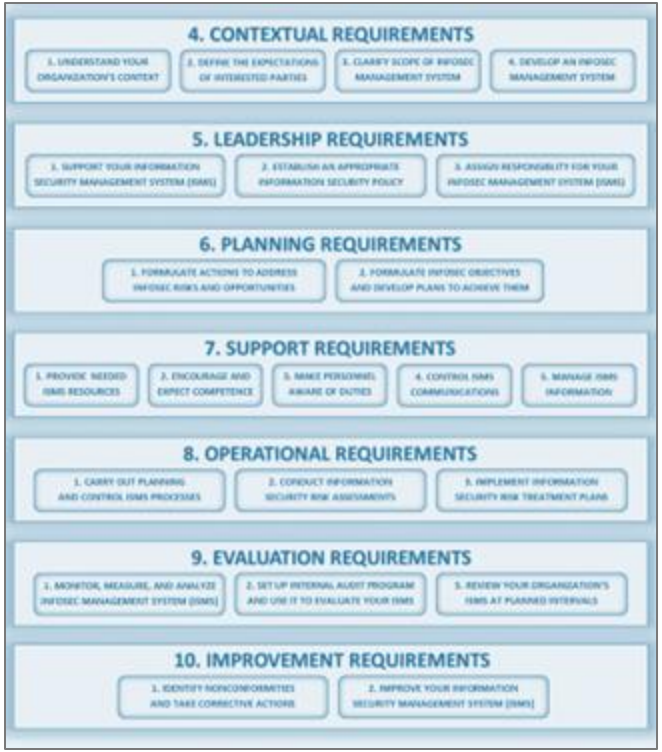
Regulations, Standards & Guidance (II)

ISO 27001 Information Security Management Systems (ISMS) is strongly focused on data as assets, that is why other frameworks has been developed, based on the same structure, but with other focuses – for instance

- IEC 62443-2-1 Cyber Security management System (CSMS), also called security program for asset owners
- ISO 27701 Privacy Information Management System (PIMS)

ISO 27001 structure:

- 2 sub-scopes: ISMS and Security Controls (A.1)
- Security Controls: 14 sections, 35 Objectives, 114 best practices
- Plan – Do – Check – Act on organization level



Regulations, Standards & Guidance (III)

Objectives overview:

Regulations, Standards & Guidance (IV)

Example 1: ISO 27001 – A.x – Area 10 – Cryptography

Objective A.10.1: Cryptographic controls :

- To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

  Topic A.10.1.1: Policy on the use of cryptographic controls

  - Security Control: A policy on the use of cryptographic controls for protection of information shall be developed and implemented.
  - *Implementation guidance from ISO 27002: When developing a cryptographic policy the following should be considered: a) […]*

  Topic A.10.1.2: Key management

  - Security Control: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.
  - *Implementation guidance from ISO 27002*: The policy should include requirements for managing cryptographic keys though their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys. It includes […]

Regulations, Standards & Guidance (VI)

Teaser: formal mapping is provided by ISA/IEC 62443-2-1 for illustrating interfaces and common approaches with ISO/IEC 27001

ISO/IEC 27001 requirement	Related IEC 62443 2 1 references
4.2.1a) Scope and boundaries of ISMS	4.3.2.2 CSMS Scope
4.2.1b) ISMS policy	4.3.2.3 Organizing for security 4.3.2.6 Security policies and procedures
4.2.1c) Risk assessment approach	4.2.3 Risk identification, classification and assessment
4.2.1d) Identify the risks	4.2.3 Risk identification, classification and assessment 4.3.4.2 Risk management and implementation
4.2.1e) Analyse and evaluate the risks	4.2.2 Business rationale 4.2.3 Risk identification, classification and assessment 4.3.4.2 Risk management and implementation
4.2.1f) Identify and evaluate options for the treatment of risks	4.3.4.2 Risk management and implementation
4.2.1g) Select control objectives and controls for the treatment of risks	4.3.4.2 Risk management and implementation
4.2.1h) Obtain management approval of the proposed residual risks	4.3.2.6 Security policies and procedures 4.3.4.2 Risk management and implementation

IEC 62443-2-1 requirement	Related ISO/IEC 27001 references
4.2.2 Business rationale	4.2.1e) Analyze and evaluate the risks 5.2.1 Provision of resources
4.2.3 Risk identification, classification and assessment	4.2.1c) Risk assessment approach 4.2.1d) Identify the risks 4.2.1e) Analyse and evaluate the risks 4.3.1 General document requirements A.6.2 External parties A.7.1 Responsibility for assets
4.3.2.2 CSMS Scope	4.2.1a) Scope and boundaries of ISMS 4.3.1 General document requirements

- ISO/IEC 27001 & 27002 have been updated in 2022, major differences are:
  - Less measures (114 → 93) but categorized on 4 dimensions (organization, human factors, technologies and physical); requirements related to Cloud services etc

Regulations, Standards & Guidance (VII)

- Recommendations and Guide “Minimum standard for improving ICT resilience”, released in December 2024
  - Issued by Swiss Confederation, Federal Office of National Economic Supply FONES, CH
    - https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/ikt-minimalstandards.html

- “Measures to protect industrial control systems (ICSs)”, released in January 2022
  - Issued by Swiss Confederation, National Cyber Security Center, Federal Department of Finance FDF, CH
    - https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ics.html

- Guide to Industrial Control Systems (ICS) Security, released in May 2015
  - Issued by NIST, National Institute of Standards and Technology, US
    - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-82r2.pdf

Other standards and guidance (CIS Critical Security Controls, COBIT, BSI 100-2) exist but decision has been taken to focus on ISA/IEC62443 and references related to it

Regulations, Standards & Guidance (VIII)

Document purpose

- Guidance for identifying key cyber security activities to done by ICS stakeholders, details about subtasks and references to technical standards to be used as guide
- This Minimum Standard explicitly does not seek to compete with the existing international standards. Rather, it is compatible with them while being more reduced in scope. It is intended to provide a more entry-level introduction to the issues, and yet ensure a high degree of protection
- Same approach for document dedicated to other actors

Document structure

- Based on NIST nomenclature [Identify; Protect; Detect; Respond; Recover]

Example for first activity from IDENTIFY domain (right)

2.2.1 Asset management

The data, individuals, devices, systems and facilities of an organisation are identified, catalogued and rated. Their rating should correspond to their criticality in the business processes that must be completed, and the organisation's risk strategy.

Description	Task
ID.AM-1	Draw up an inventory-taking process which ensures that you have a complete inventory of all your ICT assets at all times.
ID.AM-2	Produce an inventory of all of the software platforms/licences and applications within your organisation.
ID.AM-3	Catalogue all of your internal communication and data flows.
ID.AM-4	Catalogue all external ICT systems that are relevant to your organisation.
ID.AM-5	Prioritise the resources that you have inventoried (devices, applications, data, etc.) based on their criticality
ID.AM-6	Define clear cybersecurity roles and responsibilities.

Table 3: ID.AM tasks

Standard	Reference
CCS CSC 1	1, 2
COBIT 5	BAI09.01, BAI09.02, BAI09.05, DSS05.02, APO02.02, APO03.03, APO03.04, PO01.02, DSS06.03
ISA 62443-3:2013	SR 7.8
ISO 27001:2013	A.6.1.1, A.8.1.1, A.8.1.2, A.8.2.1, A.11.2.6
NIST-SP-800-53 Rev. 4	AC-4, CA-3, CA-9, PL-8, CM-8, AC-20, SA-9, CP-2, RA-2, SA-14, CP-2, PS-7, PM-11
BSI 100-2	M 2.225, M 2.393, B 2.10, M 2.193

Table 4: ID.AM references

"Minimum standard for improving ICT resilience"

Issued by Swiss confederation, Federal Office of National Economic Supply FONES

Regulations, Standards & Guidance (IX)

“Measures to protect industrial control systems (ICSs)“

Issued by Swiss Confederation, National Cyber Security Center, Federal Department of Finance FDF

Document purpose

- List of high-level security measures, which should be embedded in an overarching security process which ensures that the measures are applied, regularly verified and continuously improved

11 Measures to protect industrial control systems (ICSs)

1. Create and maintain asset databases for all devices
2. Establish life cycle and patch management for software
3. Define and use secure configurations
4. Plan and build robust network architectures
5. Implement multi-stage malware protection
6. Authentication and authorisation
7. Set up central log analysis
8. Ensure physical protection
9. Carry out and regularly test backup and recovery
10. Establish and practice security identity management processes
11. Establish a security culture

Contents

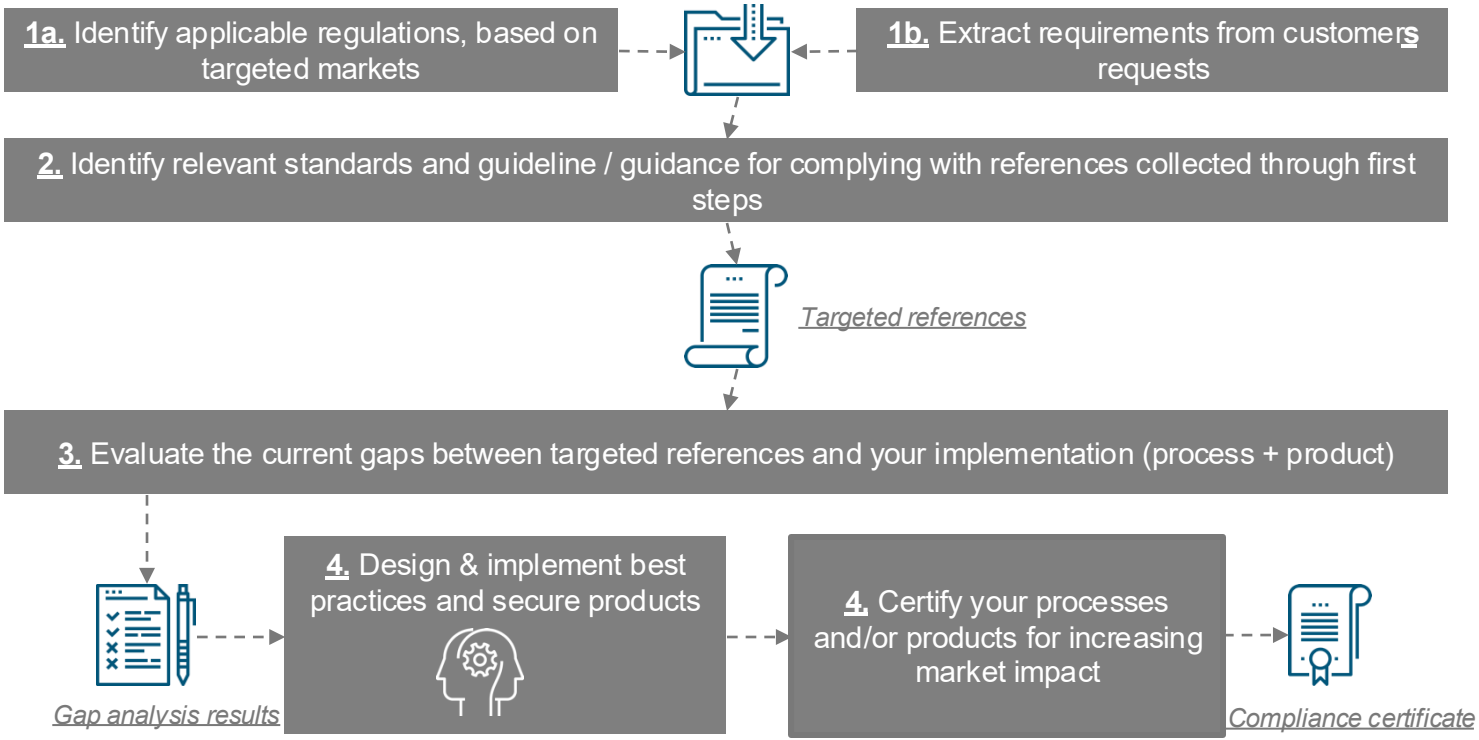
3.1 Asset database for devices

Measure	Keep a database in which all the elements of the control system, of peripheral systems and also of normal end devices are listed.
Reason	Effective and efficient protection is impossible without knowing which elements need to be protected and which elements are trustworthy.
Implementation notes	Various technical aids exist for achieving this goal. A network-based inventory tool can be used to gain an initial overview. However, great caution is advised with active scanners. Many ICSs are not prepared to receive unexpected network traffic, which can lead to a malfunction. Unknown devices that connect to the network for the first time should trigger an alarm. This can be based on the MAC addresses of the devices. Although a MAC address can easily be falsified, this measure already has a considerable detection effect.

Source: https://www.ncsc.admin.ch/ncsc/en/home/infos-fuer/infos-it-spezialisten/themen/massnahmen-schutz-ics.html

Regulations, Standards & Guidance (X)

Typical approach



Enter IEC 62443

ISA/IEC 62443 – History

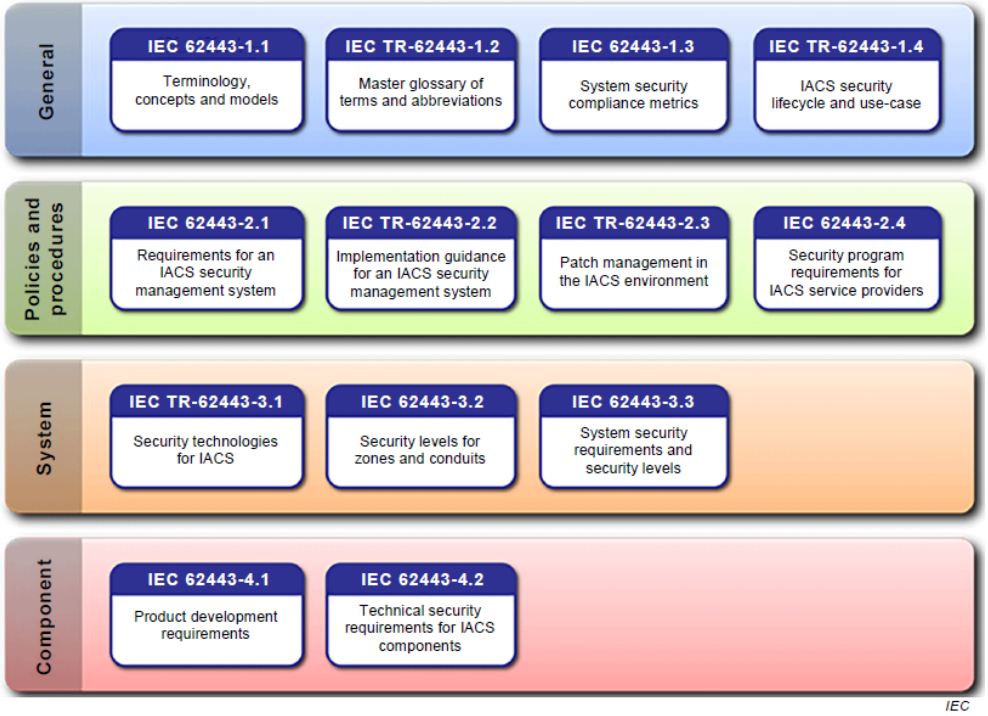
Initially developed by the *International Society of Automation* (ISA) Committee on Security for Industrial Automation & Control Systems (ISA99)

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

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 – High level view

"IEC 62443 is an international series of standards that address cybersecurity for operational technology in automation and control systems."



IACS: industrial automation and control systems

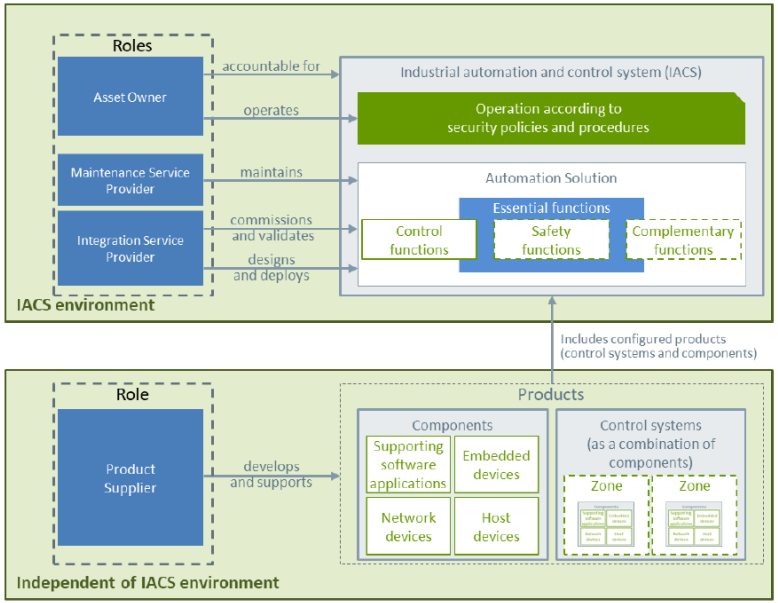
ISA/IEC 62443 – Scope & purpose

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:

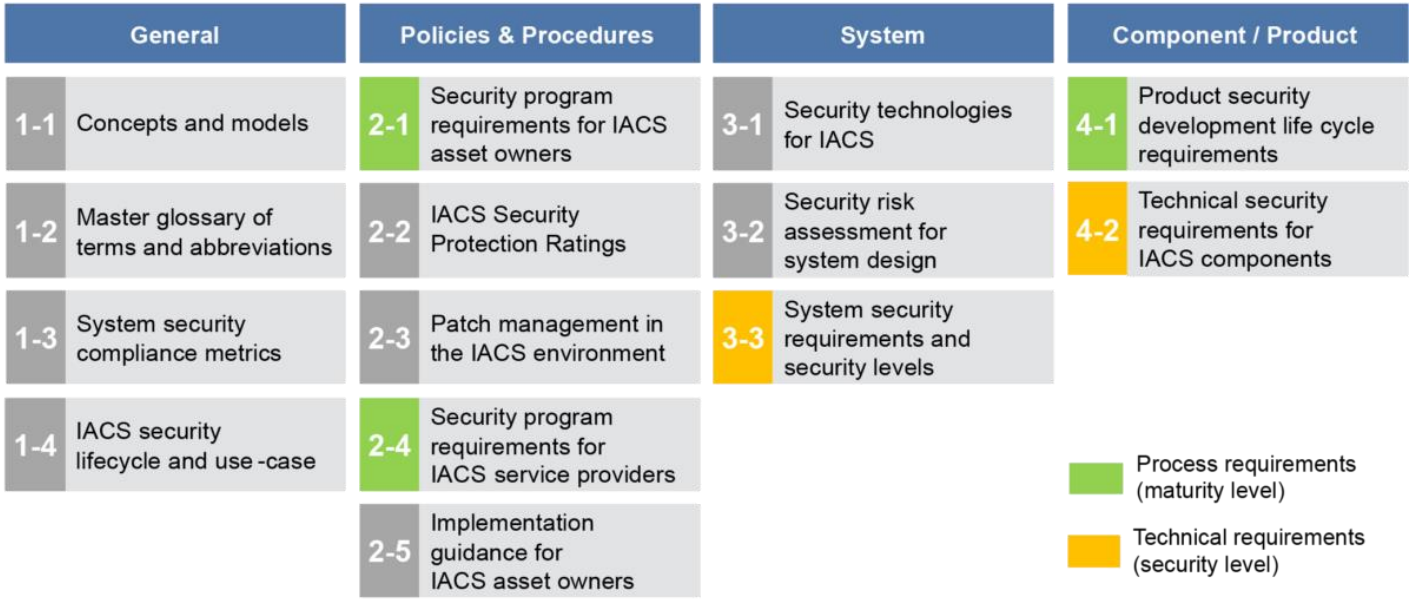
- Technologies
- Processes
- Human factors

… to be considered from any stakeholder perspective



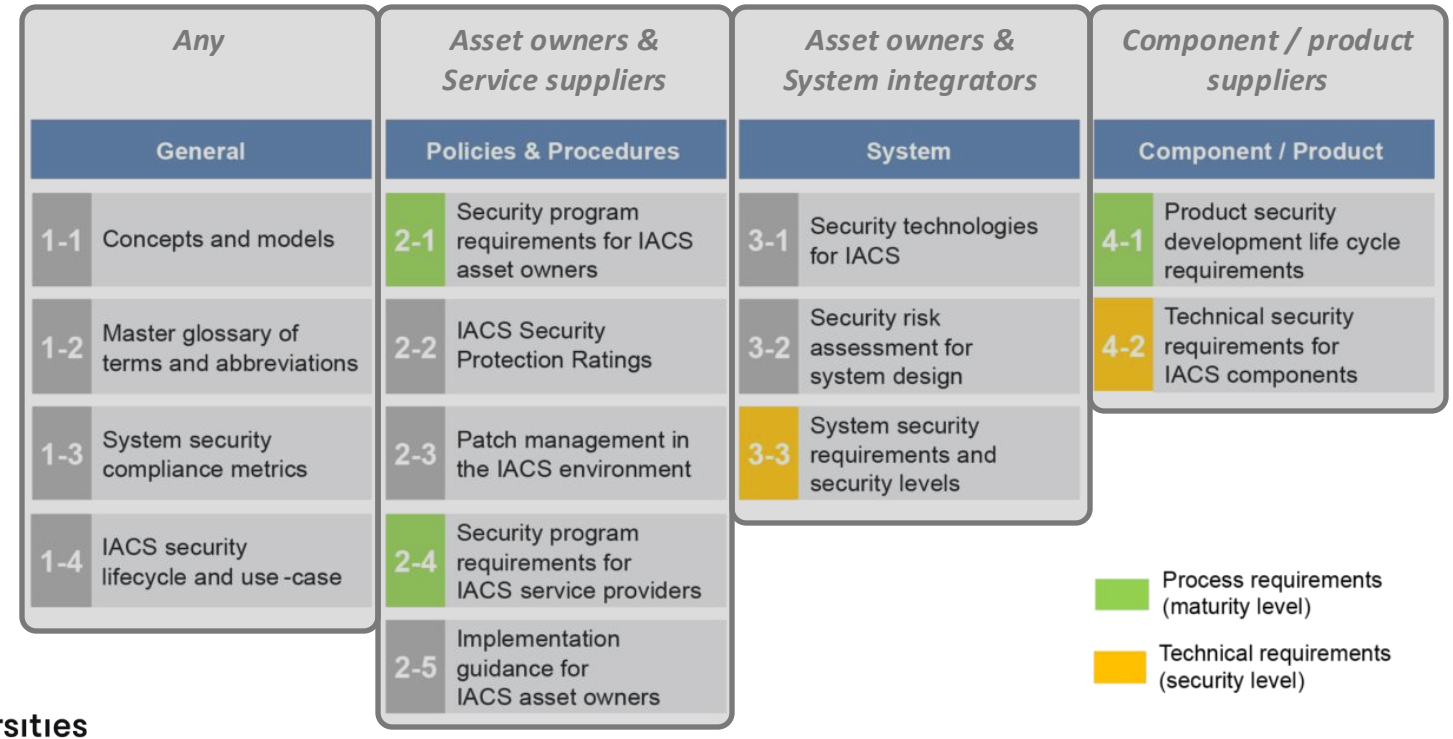
ISA/IEC 62443 – Standard families

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



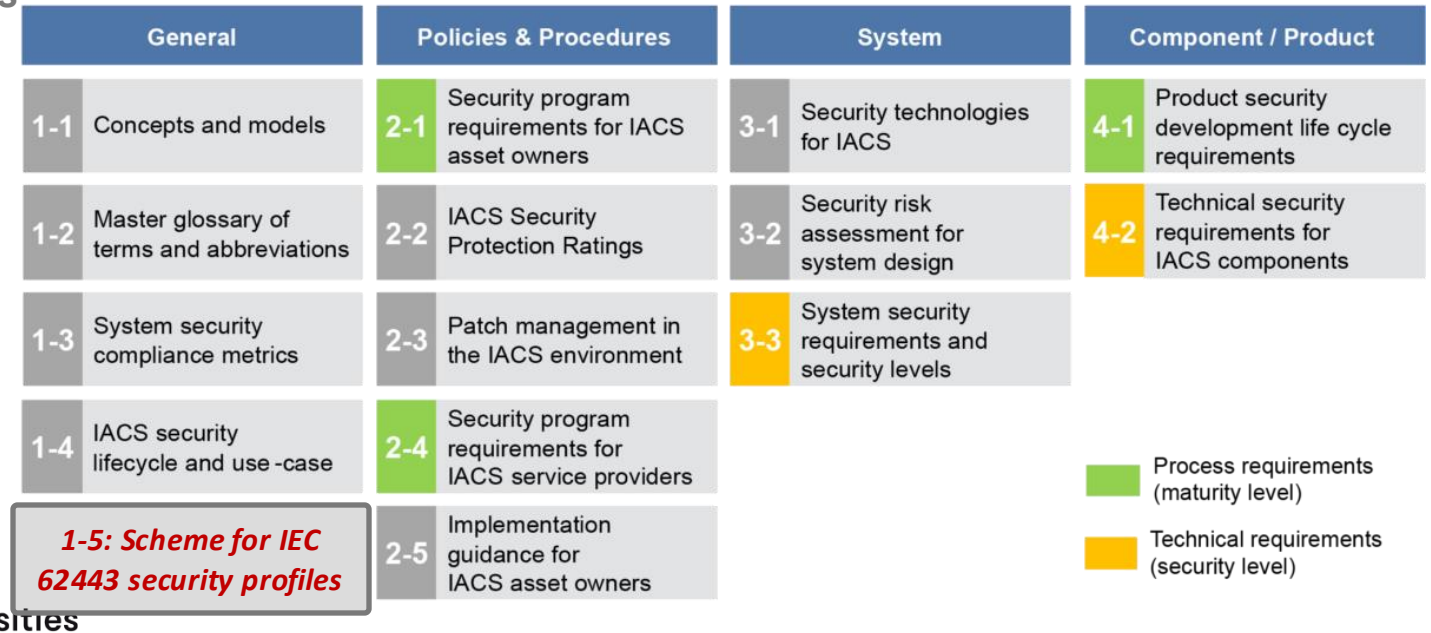
ISA/IEC 62443 – Stakeholders

This standard family has been structured based on abstraction levels and related stakeholders



ISA/IEC 62443 – Standard families

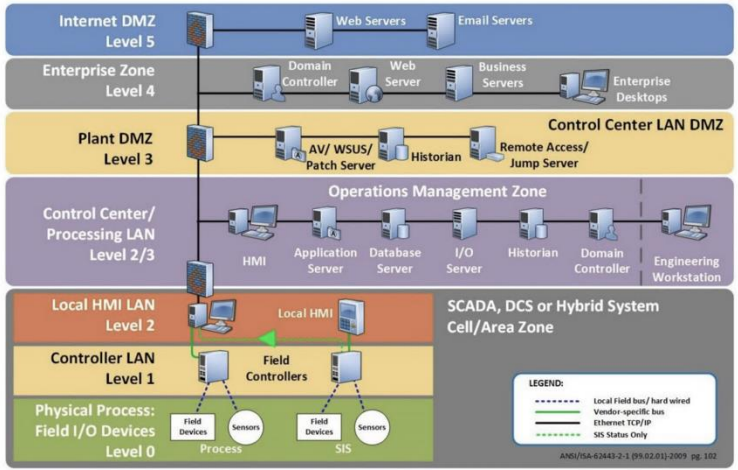
This standard family aims to be as generic as possible for cross-sector implementation, however several technical report [ISA/IEC 62443-1-X TR] is currently under development for providing tailored interpretation of this standard framework per industry / product type → **Available and called security profiles**

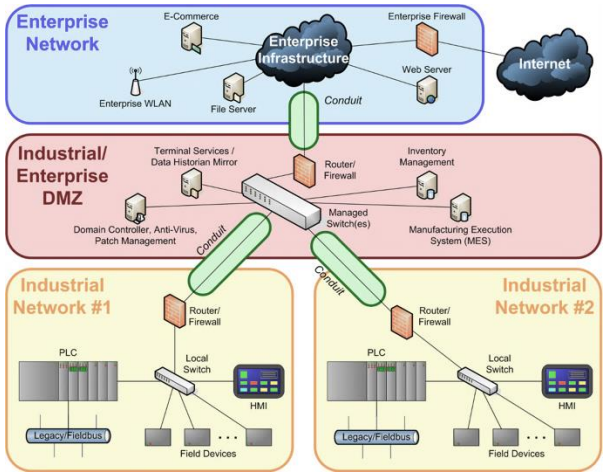


ISA/IEC 62443 – Key principles

Network segmentation into Zones & Conduits

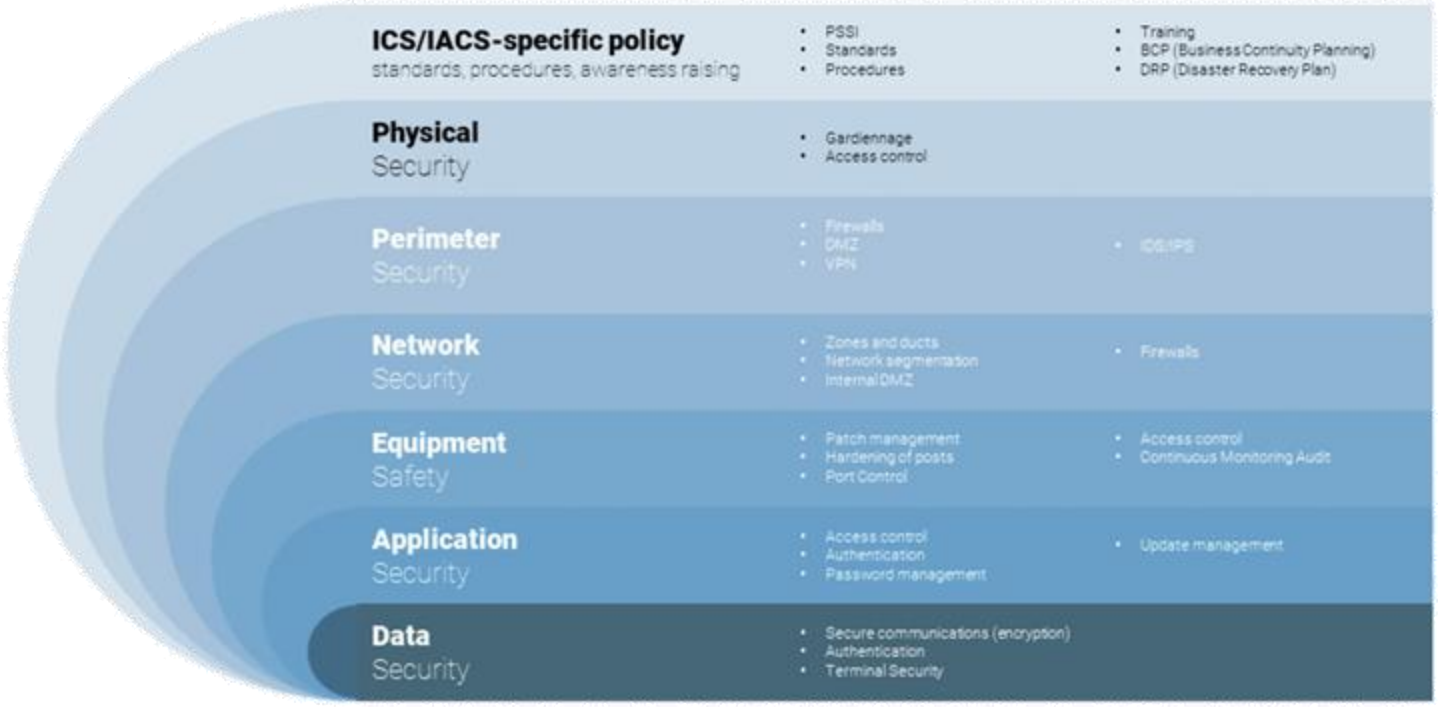
- Purdue model applied historically within automation sector is not that realistic nor strictly applicable anymore…
- Growing use of IP-based technologies, IIoT (Industrial IoT) devices and interest for remote management are illustrating it





ISA/IEC 62443 – Key principles

Defense in depth



ISA/IEC 62443 – Key principles

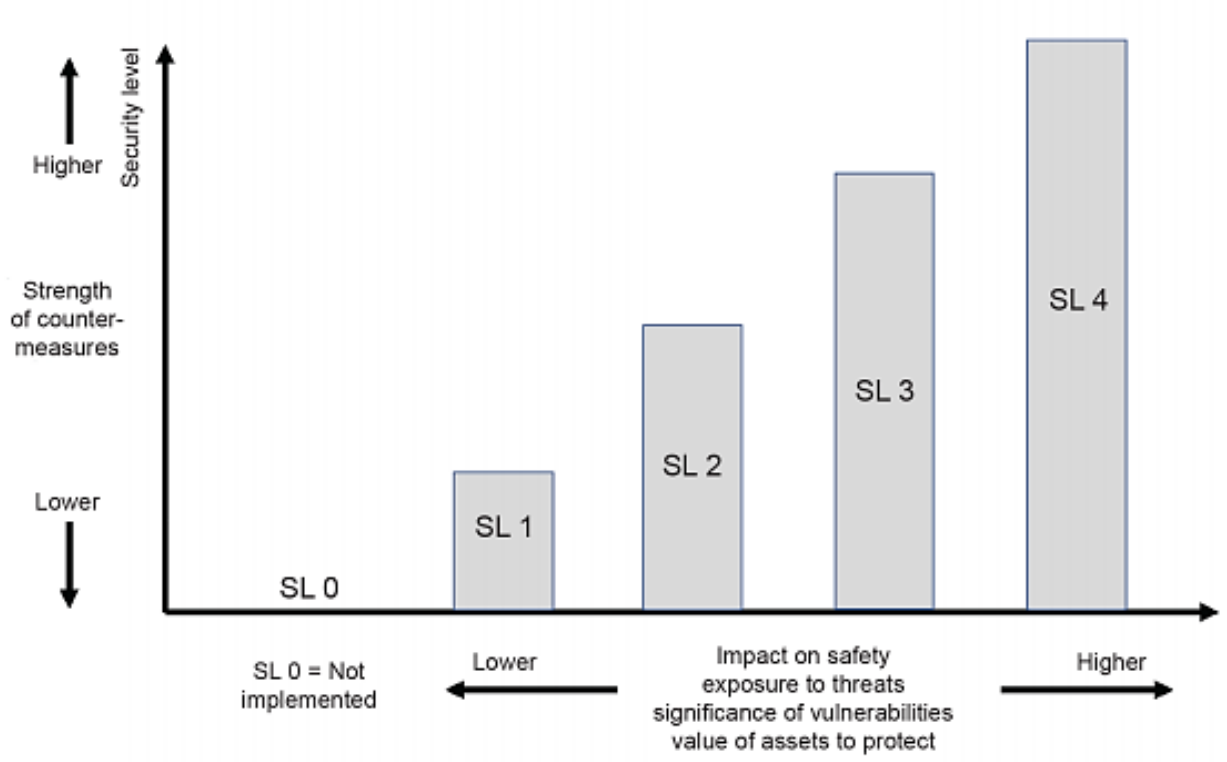
Security levels

- A specific security metric has been defined in the scope of the IEC 62443; the Security Level 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

4 Security Level (SL)	
SL 1	Protection against **casual or coincidental** violation
SL 2	Protection against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation

ISA/IEC 62443 – Key principles

Security levels

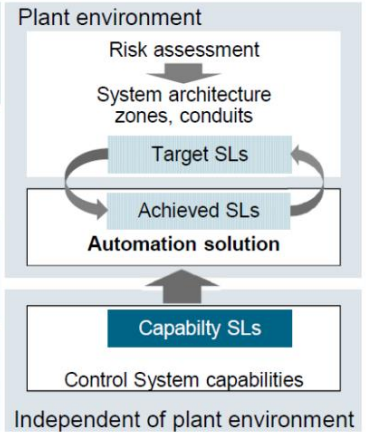


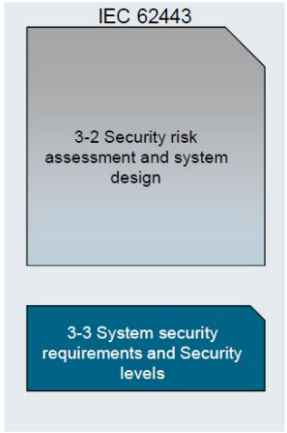
ISA/IEC 62443 – Key principles

Security levels

- SL-T: is the desired level of security for a particular zone and/or conduit. It is usually determined by performing a cyber security risk assessment on an environment.
- SL-C: is the security level that a component or system of an environment can provide when properly configured. This level states that a component is capable of meeting the required target security level SL-T natively without additional compensating measures
- SL-A: is the actual level of security for a particular environment or a specified zone and/or conduit of it. It is measured after an environmental design is available or when in place

SL 1	*Capability to protect* against **casual or coincidental** violation
SL 2	*Capability to protect* against **intentional violation** using **simple means** with low resources, generic skills and low motivation
SL 3	*Capability to protect* against intentional violation using **sophisticated means** with **moderate resources**, IACS specific skills and moderate motivation
SL 4	*Capability to protect* against intentional violation using sophisticated means with **extended resources**, IACS specific skills and high motivation





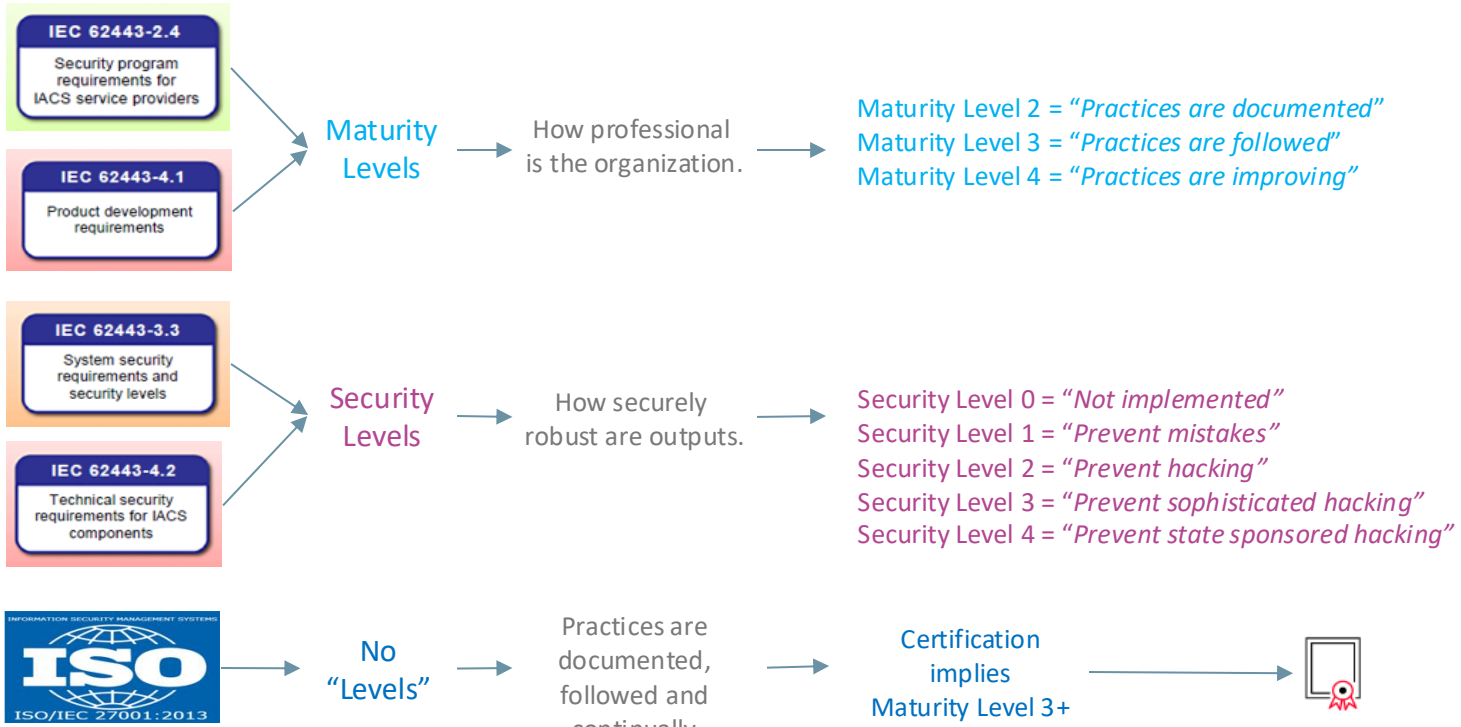
ISA/IEC 62443 – Key principles

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 – Levels In a Picture



ISO 27001

- “ISO/IEC 27001 is an international standard on how to manage information security.”
- “ISO/IEC 27001 requires that management:
  - Systematically examine the organization's information security risks, taking account of the threats, vulnerabilities, and impacts;
  - Design and implement a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable; and
  - Adopt an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

”

Source: https://en.wikipedia.org/wiki/ISO/IEC_27001

ISO 27001 & IEC 62443 – Comparable?

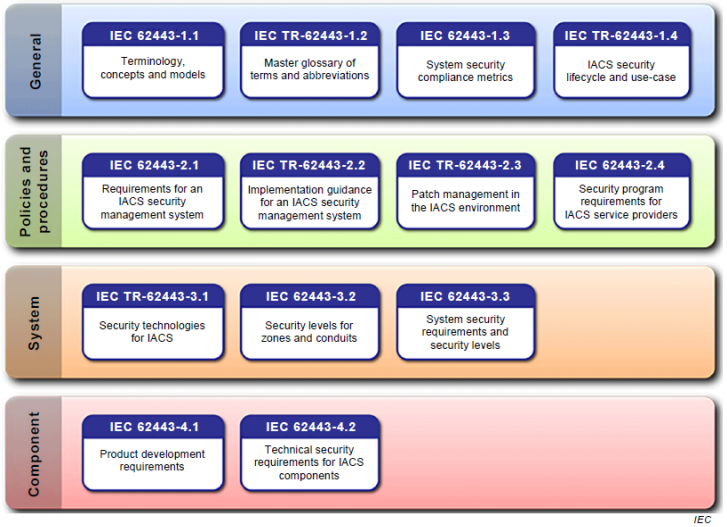
IEC 62443-2-4, IEC 62443-3-3, IEC 62443-4-1, IEC 62443-4-2	ISO/IEC 27001
"CyberSecurity certification for products and offerings in the IACS business environment."	"CyberSecurity certification to secure own cybersecurity operations and compliance to business expectations."
Mainly designed for industrial automation.	Mainly designed for business office environment & operations.
OT (Operations Technology).	IT (Information Technology).
More applicable to products.	More applicable to organizations.

Quotes from business owners

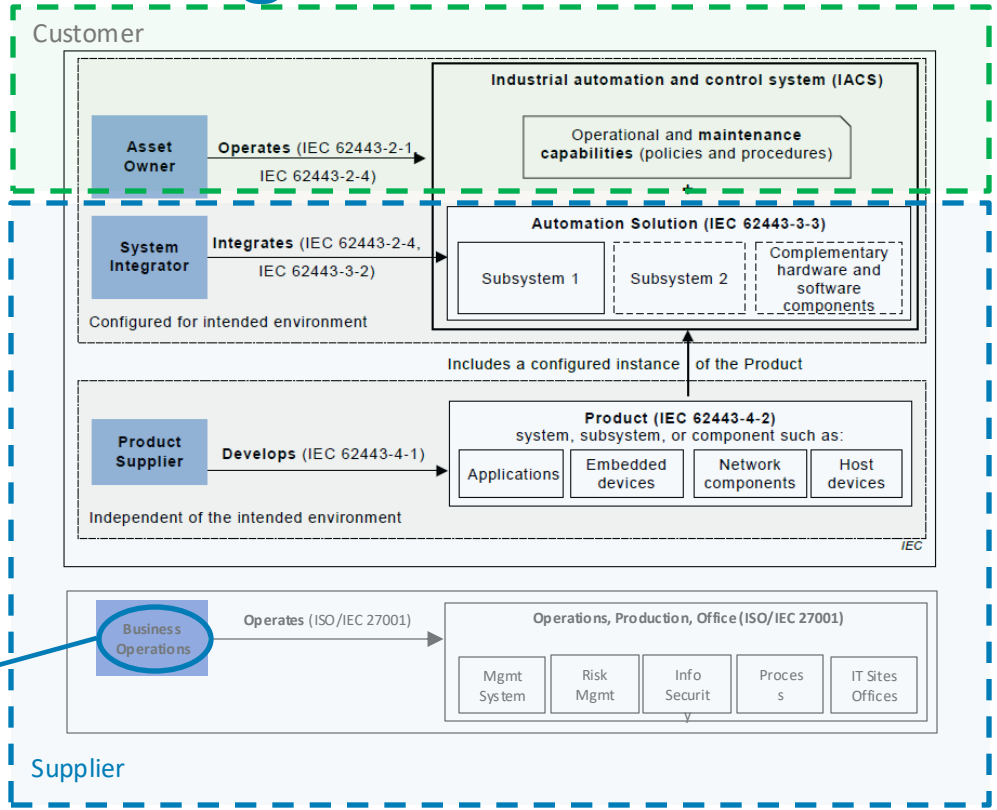
- "From the many existing Cybersecurity standards, these are the most common, successfully accepted, internationally recognized, globally applicable and suitable to our business"
- "Certification to both standards is desirable since ISO/IEC 27001 requirements can help protect the information used to implement IACS and ensure the development process is effective in implementing the security practices defined by IEC 62443."

Two Standards For Strong Value

From the IEC 62443 Family:



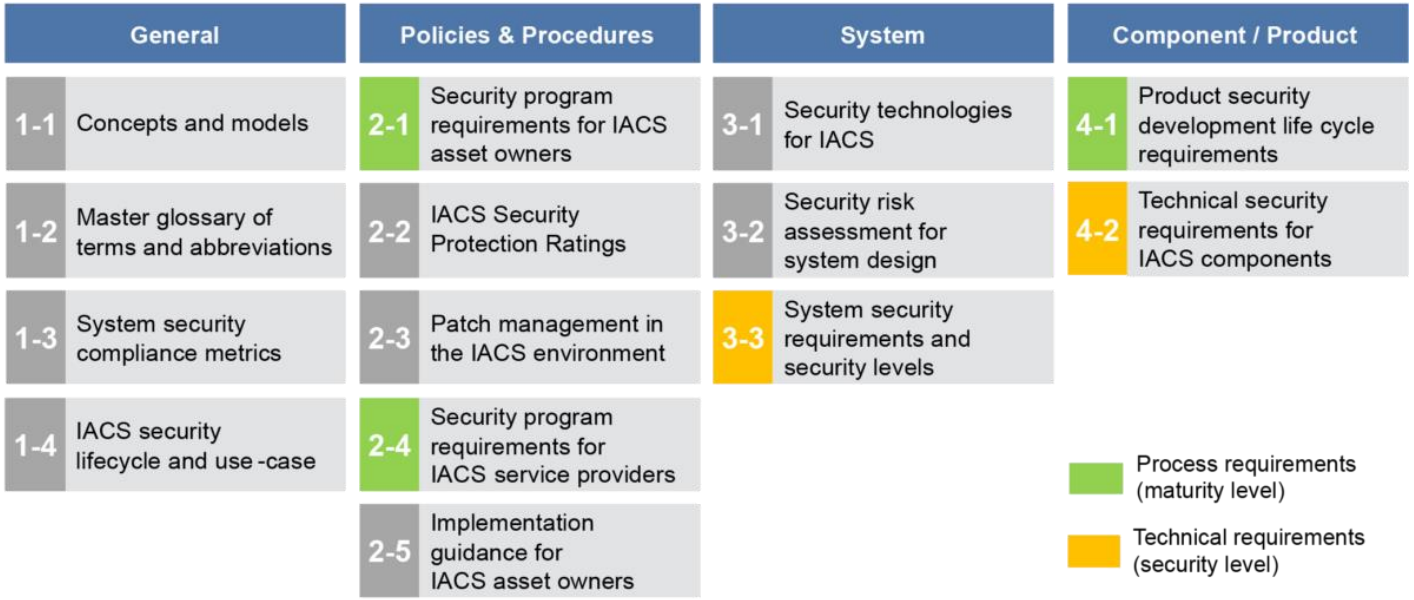
From the ISO/IEC 27000 Family:



IEC 62443 - Parts

ISA/IEC 62443 – Focus on some 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 infrastructure



ISA/IEC 62443-2-X – Key parts

ISA/IEC 62443-2-1 & ISA/IEC 62443-2-4 as normative parts

ISA/IEC 62443-2-1

- defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements

ISA/IEC 62443-2-4

- defines requirements for security capabilities to be supported by security programs of integration and maintenance service providers. Support for these capabilities means that the service provider can provide them to the asset owner upon request.

Note: ISA/IEC 62443-2-3 might also be considered as a good reference for patch management process implementation.

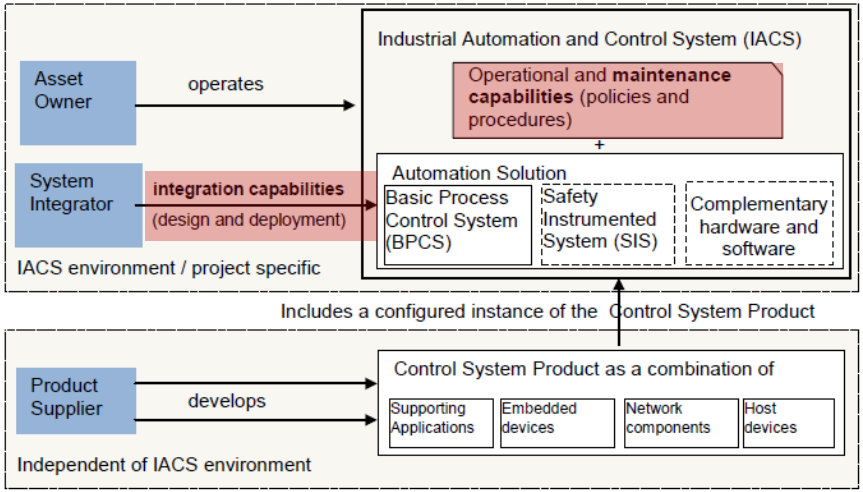
ISA/IEC 62443-2-4 – For Service suppliers

Use of this part by Asset Owners

- to request specific security capabilities from the service provider. More specifically, prior to such a request, IEC 62443-2-4 can be used by asset owners to determine whether or not a specific service provider's security program includes the capabilities that the asset owner needs

During negotiation between Asset Owners & Service Suppliers

- prior to the IACS service provider starting work on the Automation Solution, the asset owner will normally issue a Request for Quote (RFQ) that includes a document (e.g. a Statement of Work (SOW)) that defines its security policies and requirements, including which of the requirements specified in Annex A of that part apply



ISA/IEC 62443-2-4 – For Service suppliers

- Additionally, the asset owner does not normally specify how its security requirements will be implemented (e.g. backup and restore) – that is what the service provider has already specified in its policies and procedures. However, the asset owner may define constraints and parameters (e.g. password timeout values) for how the service provider's policies and procedures will be applied in its specific project.

- Maturity levels, based on well-known CMMI scale, are used to evaluate capability from suppliers

Level	CMMI-SVC	IEC 62443-2-4	IEC 62443-2-4 Description/Comparison to CMMI-SVC
1	Initial	Initial	At this level, the models are the fundamentally the same. Service providers typically perform the service in an ad-hoc and often undocumented (or not fully documented) manner. Requirements for the service are typically specified in a statement of work under contract with the asset owner. As a result, consistency across projects may not be able to be shown. NOTE "Documented" in this context refers to the procedure followed in performing this service (e.g. detailed instructions to service provider personnel), not to the results of performing the service. In most asset owner settings, all changes resulting from the performance of a services task are documented.
2	Managed	Managed	At this level, the models are the fundamentally the same, with the exception that IEC 62443-2-4 recognizes that there may be a significant delay between defining a service and executing (practicing) it. Therefore, the execution related aspects of the CMMI-SVC Level 2 are deferred to Level 3. At this level, the service provider has the capability to manage the delivery and performance of the service according to written policies (including objectives). The service provider also has evidence to show that personnel who will perform the service have the expertise, are trained, and/or are capable of following written procedures to perform the service. The service discipline reflected by Maturity Level 2 helps to ensure that service practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3	Defined	Defined (Practiced)	At this level, the models are the fundamentally the same, with the exception that the execution related aspects of the CMMI-SVC Level 2 are included here. Therefore, a service at Level 3 is a Level 2 service that the service provider has practiced for an asset owner at least once. The performance of a Level 3 service can be shown to be repeatable across the service provider's organization. Level 3 services may be tailored for individual projects based upon the contract and statement of work from the asset owner.
4	Quantitatively Managed	Improving	At this level, Part 2-4 combines CMMI-SVC levels 4 and 5. Using suitable process metrics, service providers control the effectiveness and performance of the service and demonstrate continuous improvement in these areas, such as more effective procedures or the installation of system capabilities with higher security levels (see IEC 62443-3-3). This results in a security program that improves the service through technological/procedural/management changes. See IEC 62443-1-3 for a discussion of metrics.
5	Optimizing		

ISA/IEC 62443-2-4 – For Service suppliers

IACS integration service provider activities typically include:

- analyzing the physical, electrical, or mechanical environment the Automation Solution is to control (e.g. the physical process to be controlled, such as those used in manufacturing, refining and pharmaceutical processes),
- developing an Automation Solution architecture in terms of devices and control loops and their interconnectivity with engineering and operator workstations, and possibly the inclusion of a Safety Instrumented System (SIS),
- defining how the Automation Solution will connect to external (e.g. plant) networks,
- installing, configuring, patching, backing up, and testing that lead to the handover of the Automation Solution to the asset owner for operation.
- gaining approval of the asset owner for many of the decisions made and outputs generated during the execution of these activities.
- Maintenance activities generally start after handover of the Automation Solution to the asset owner has occurred and may continue until the asset owner no longer requires them.
- They are typically short and frequently recurring, and typically include one of more of the following:
  - patching and anti-virus updates,
  - equipment upgrades and maintenance, including small engineering adjustments not directly related to control algorithms,
  - component and system migration,
  - change management,
  - contingency plan management.

ISA/IEC 62443-2-4 – Example of capability

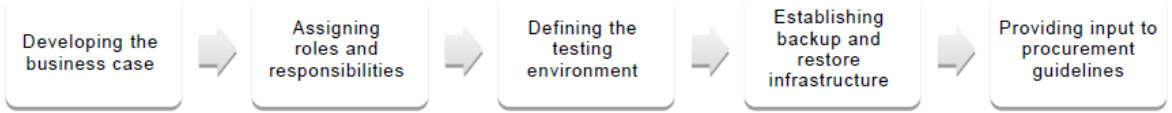
Table A.1 *(continued)*

Req ID	BR/RE	Functional area	Topic	Subtopic	Doc?	Requirement description	Rationale
SP.09.05	BR	Account management	Passwords	Composition	No	The service provider shall have the capability to ensure that password policies can be set to achieve a minimum complexity commonly accepted by both the security and industrial automation communities. NOTE At the time of this writing, minimal password complexity is: 1) at least eight characters in length and 2) a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special characters (e.g.% and #).	The capability specified by this BR is used to ensure that the service provider can support a broad range of asset owner password complexity policies. Using complex passwords makes password discovery more difficult. Having this capability means that the service provider has an identifiable process for ensuring that the Automation Solution supports complex passwords. The password complexity used within a specific Automation Solution is beyond the scope of this requirement. See IEC 62443-3-3 for related security requirements for systems used in Automation Solutions, and IEC 62443-3-2 for the use of risk assessments to aid in the determination of the level of password complexity to be used for a specific Automation Solution. Also see IEC 62443-2-1 for password policy requirements for asset owners.
SP.09.06	BR	Account management	Passwords	Expiration	No	The service provider shall have the capability to ensure that passwords for local and system-wide (e.g. domain) user accounts are configured to automatically expire after they have been in use for a period of time specified by the asset owner.	The capabilities specified by this BR and its RE are used to ensure that passwords can be changed periodically. Passwords that remain unchanged increase the risk that they will be disclosed/discovered and used to gain unauthorized access to the system. In addition, changing passwords periodically limits the length of time an attacker has to discover a password. Having this capability means that the service provider has an identifiable process for ensuring that passwords can be configured to automatically expire after they have been in use for an asset owner specified number of days. When and how often the service provider verifies that the password expiration period is Automation Solution specific, but verification is typically done as part of the handover process and at after or during each maintenance cycle. The asset owner's security policy should set the expiration period based on a risk assessment and this value should be periodically be reviewed. See IEC 62443-3-2 for more information on risk assessment, IEC 62443-3-3 for related requirements for control systems product capabilities, and IEC 62443-2-1 for related requirements for asset owners. NOTE IEC 62443-2-1 does not explicitly mention lifetime requirements for passwords, but does address more general password policies.

ISA/IEC 62443-2-3 – Patch management

Planning an IACS patch management process

- Developing the business case
  - The first step in establishing an IACS patch management program is developing the business case that can be presented to senior management in order to secure the necessary funding, resources and support
- Establishing and assigning roles and responsibilities
  - It is critical to the success of the program to have clearly defined and communicated ownership, accountability, roles and responsibilities throughout the asset owner organization to perform IACS patch management.
- Testing environment and infrastructure & establishing backup and restoration infrastructure
  - Additional steps may include guidelines on the implementation of a testing environment, automated patch deployment and installation infrastructure and backup/restoration infrastructure.
- Providing input to procurement guidelines
  - The last step is to provide input to the procurement requirements and legal terms and conditions to ensure that product suppliers are supporting the asset owner's IACS security objectives.



ISA/IEC 62443-3-X – Key parts

ISA/IEC 62443-3-2 & ISA/IEC 62443-3-3 as normative parts

ISA/IEC 62443-3-2

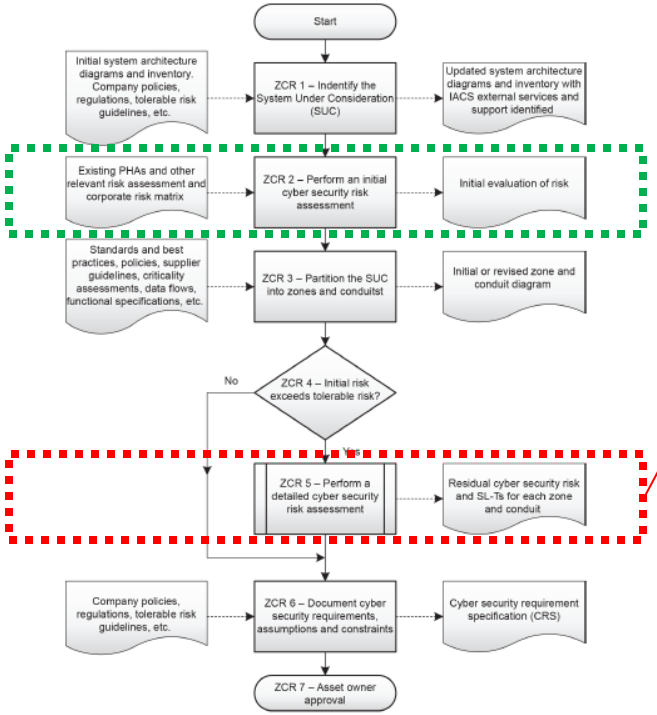
- defines a set of engineering measures that will guide an organization through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels

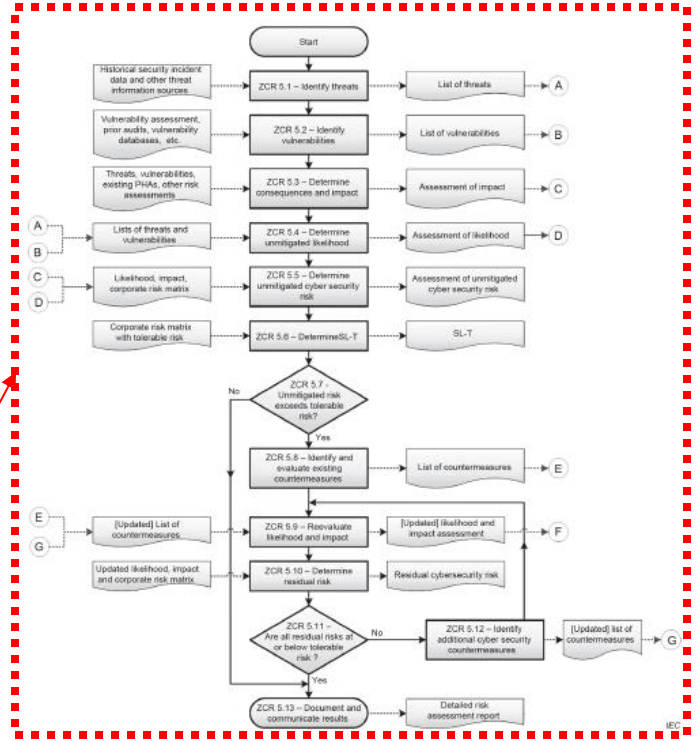
ISA/IEC 62443-3-3

- defines technical requirements to be respected on IACS / System level, based on several assumptions as follow
  - a security program has been established and is being operated in accordance with IEC 62443-2-1.
  - a patch management program is implemented consistently with the recommendations detailed in IEC/TR 62443-2-3

ISA/IEC 62443-3-2 – Risk assessment

2-step approach: Initial risk assessment / Detailed risk assessment

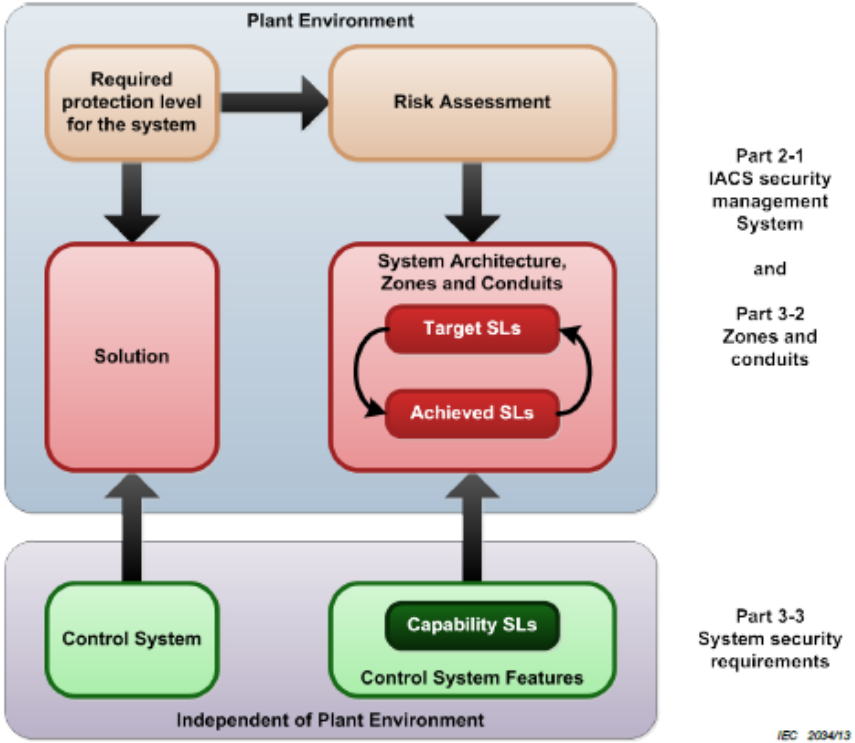




ISA/IEC 62443-3-3 – System requirements

- Technical system requirements are derived from risk assessment (62443-3-2).
- The requirements are “catalogued” within this ISA/IEC 62443-3-3 part, based on 7 dimension (called FR - Foundational Requirements) as follow

1. Identification and authentication control (IAC),
2. Use control (UC),
3. System integrity (SI),
4. Data confidentiality (DC),
5. Restricted data flow (RDF),
6. Timely response to events (TRE)
7. Resource availability (RA).



ISA/IEC 62443-4-X – Key parts

ISA/IEC 62443-4-1 & ISA/IEC 62443-4-2 as normative 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

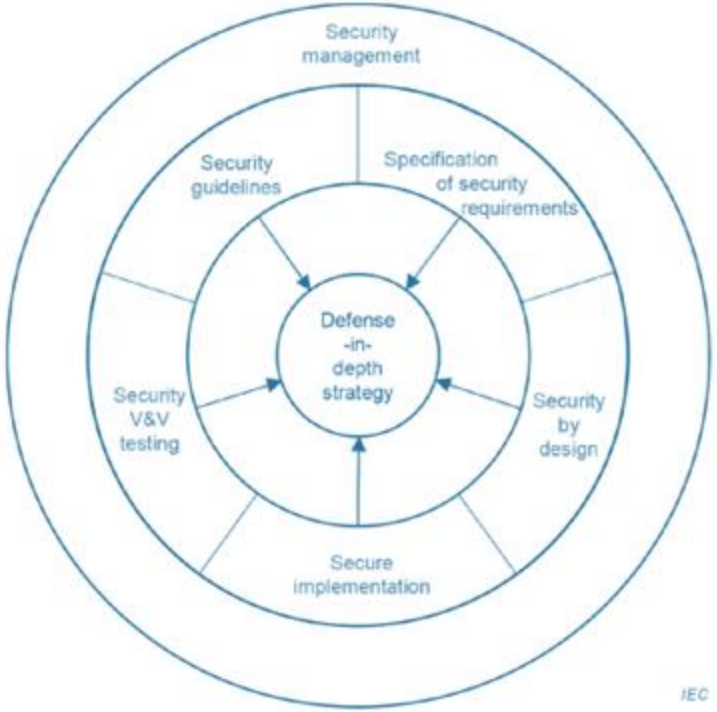
ISA/IEC 62443-4-2

- 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 Certifications

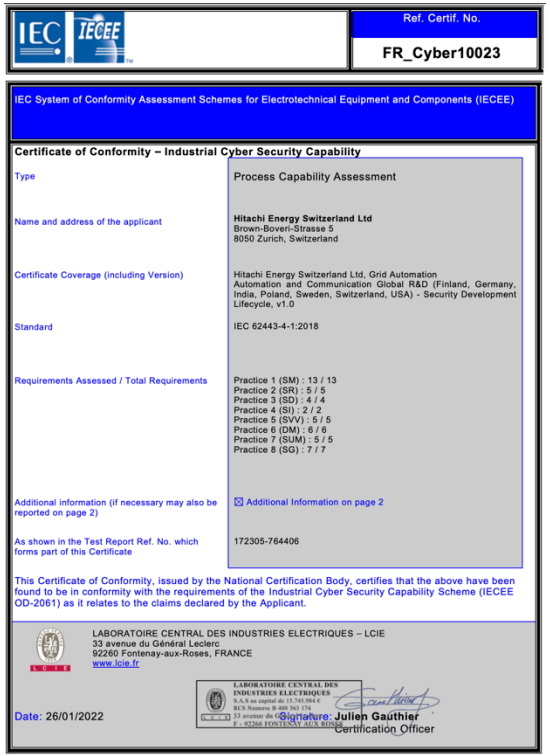
ISA/IEC 62443-4-2 Product certifications

- Based on the Security Scale defined by standard parts (SL)
  - SL-1 / SL-2 / SL-3 / SL-4
  - Considered as an SL-C on component-level
  - SL is defined during application phase for defining compliance targets and applicable requirements

ISA/IEC 62443-4-1 SDLC certifications

- Based on the Security Scale defined by standard parts (ML)
  - (ML-1) / ML-2 / ML-3 / ML-4
  - Considered as a maturity level
  - ML is an output from the certification phase

Certifications for Product suppliers



IEC IECEE

Ref. Certif. No.
FR_Cyber10023

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Process Capability Assessment
Name and address of the applicant	**Hitachi Energy Switzerland Ltd** Brown-Boveri-Strasse 5 8050 Zurich, Switzerland
Certificate Coverage (including Version)	Hitachi Energy Switzerland Ltd, Grid Automation Automation and Communication Global R&D (Finland, Germany, India, Poland, Sweden, Switzerland, USA) - Security Development Lifecycle, v1.0
Standard	IEC 62443-4-1:2018
Requirements Assessed / Total Requirements	Practice 1 (SM) : 13 / 13 Practice 2 (SR) : 5 / 5 Practice 3 (SD) : 4 / 4 Practice 4 (SI) : 2 / 2 Practice 5 (SVV) : 5 / 5 Practice 6 (DM) : 6 / 6 Practice 7 (SUM) : 5 / 5 Practice 8 (SG) : 7 / 7
Additional information (if necessary may also be reported on page 2)	☒ Additional Information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	172305-764406

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant.

LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES – LCIE
33 avenue du Général Leclerc
92260 Fontenay-aux-Roses, FRANCE
www.lcie.fr

Date: 26/01/2022

LABORATOIRE CENTRAL DES INDUSTRIES ELECTRIQUES
S.A.S au capital de 15.745.984 €
RCS Nanterre B 409 363 174
33 avenue du Général Leclerc
F - 92260 FONTENAY AUX ROSES

Signature: Julien Gauthier
Certification Officer

Source :
https://publisher.hitachienergy.com/preview?DocumentID=9AKK108466A4759&LanguageCode=en&DocumentPartId=&Action=Launch

ISA/IEC 62443 Certifications

ISA/IEC 62443-2-1 Security Program (=CSMS) & ISA/IEC 62443-2-4 IACS Services

- Based on the Security Scale defined by standard parts (ML)
  - (ML-1) / ML-2 / ML-3 / ML-4
  - Considered as a maturity level
  - ML is an output from the certification phase

ISA/IEC 62443-3-3 System certifications

- Based on the Security Scale defined by standard parts (SL)
  - SL-1 / SL-2 / SL-3 / SL-4
  - Considered as an SL-C on component-level
  - SL is defined during application phase for defining compliance targets and applicable requirements

Certifications for other stakeholders

IEC IECEE CB SCHEME

Ref. Certif. No.
DK-125644 -UL

IEC System of Conformity Assessment Schemes for Electrotechnical Equipment and Components (IECEE)

Certificate of Conformity – Industrial Cyber Security Capability

Type	Product Capability Assessment
Name and address of the applicant	Hitachi Energy Switzerland Ltd Global Technology Management Bruggerstrasse 72, 5400 Baden, Switzerland
Certificate Coverage (including Version)	Hitachi Energy Switzerland Ltd Global Technology Management, Grid Automation, Automation & Communication Substation Automation and Service Reference Architecture (v1.0) Date: 2021-11-24 Grid Automation Controller – MicroSCADA X Gateway & HMI – MicroSCADA X Protection Devices – RELION Remote Terminal Unit/Gateway – RTU500 System Data Manager – SDM600 Multi-Service Platform – FOX615 Communication NMS – FOXMAN-UN Wireless Mesh Routers – TROO600 Wireless NMS – SuprOS Remote Access Platform – Genubox
Standard	IEC 62443-3-3:2013
Requirements Assessed / Total Requirements	Identification and Authentication Control – (13/13) Use Control – (12/12) System Integrity – (9/9) Data Confidentiality – (3/3) Restricted Data and Flow – (4/4) Timely Response to Events – (2/2) Resource Availability – (8/8)
Additional information (if necessary may also be reported on page 2)	☐ Additional Information on page 2
As shown in the Test Report Ref. No. which forms part of this Certificate	4789697688 issued on 2022-03-08

This Certificate of Conformity, issued by the National Certification Body, certifies that the above have been found to be in conformity with the requirements of the Industrial Cyber Security Capability Scheme (IECEE OD-2061) as it relates to the claims declared by the Applicant

UL

☐ UL (US), 333 Pfingsten Rd IL 60062, Northbrook, USA
☒ UL (Demko), Borupvang 5A DK-2750 Ballerup, DENMARK
☐ UL (JP), Marunouchi Trust Tower Main Building 6F, 1-8-3 Marunouchi, Chiyoda-ku, Tokyo 100-0005, JAPAN
☐ UL (CA), 7 Underwriters Road, Toronto, M1R 3B4 Ontario, CANADA

For full legal entity names see www.ul.com/ncbnames

Date: 2022-03-25.

Signature:

Jan-Erik Storgaard

Source: https://publisher.hitachienergy.com/preview?DocumentID=9AKK108466A7250&LanguageCode=en&DocumentPartId=&Action=Launch

References

- IEC 62443 Wikipedia
- IEC 62443 Publications
- Recommendations ICT minimum standard
- Measures to protect industrial control systems