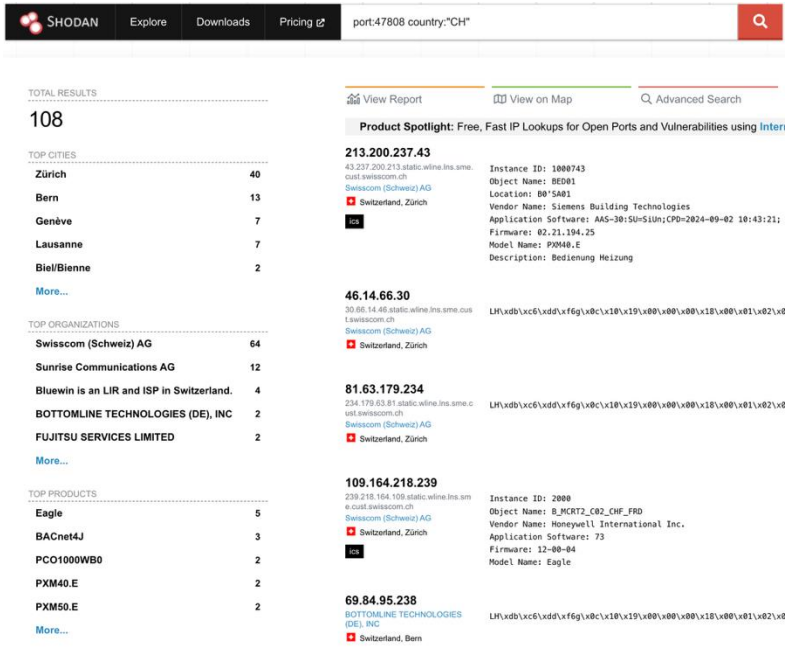
MASTER OF SCIENCE
IN ENGINEERING

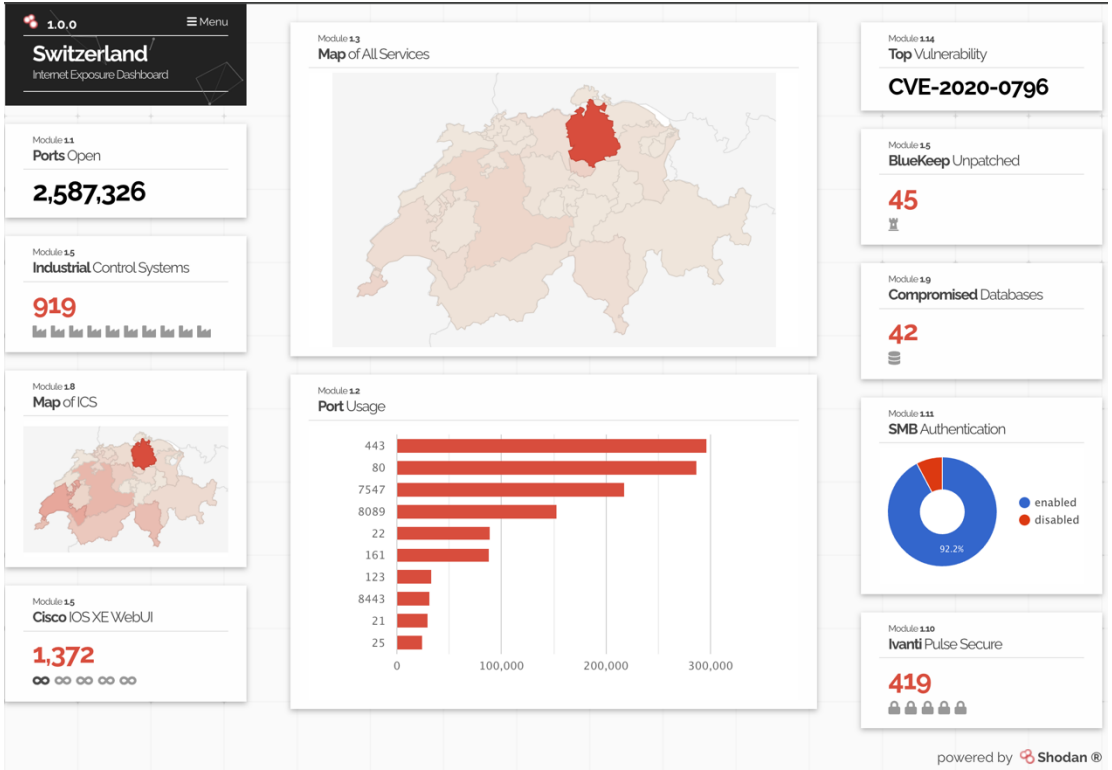
TSM_SecIndOpT

IEC 62443 (II)

Version: 1.0

Luca Haab | 26.05.2025 | Cours MSE





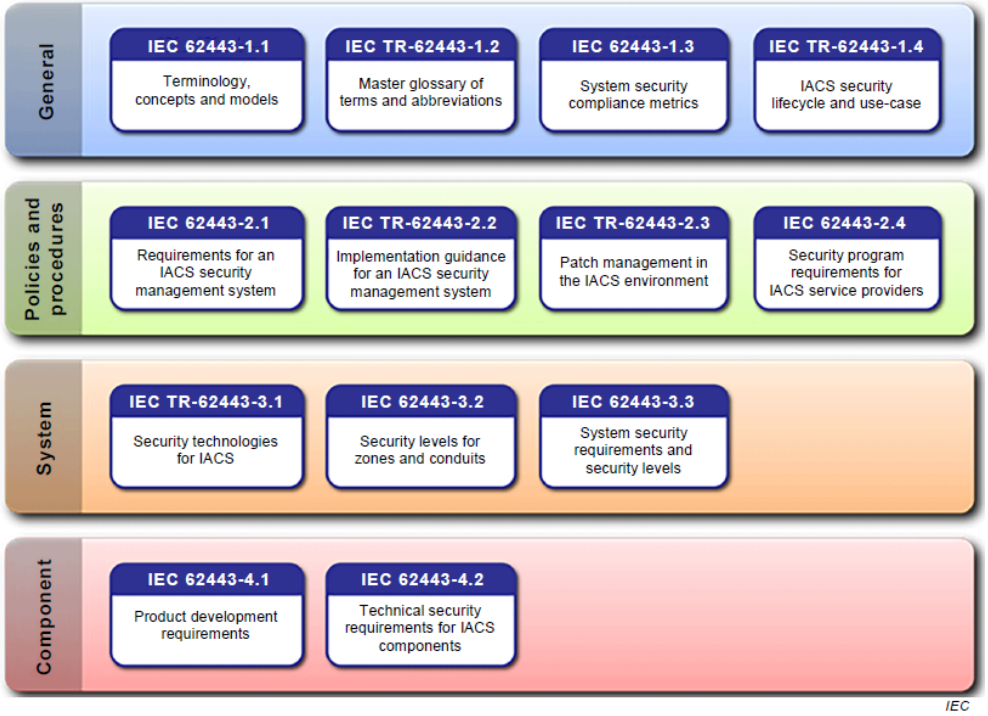
Source: own searches shodan.io, port 47808 relates to BACNet

IEC 62443

Recap

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."



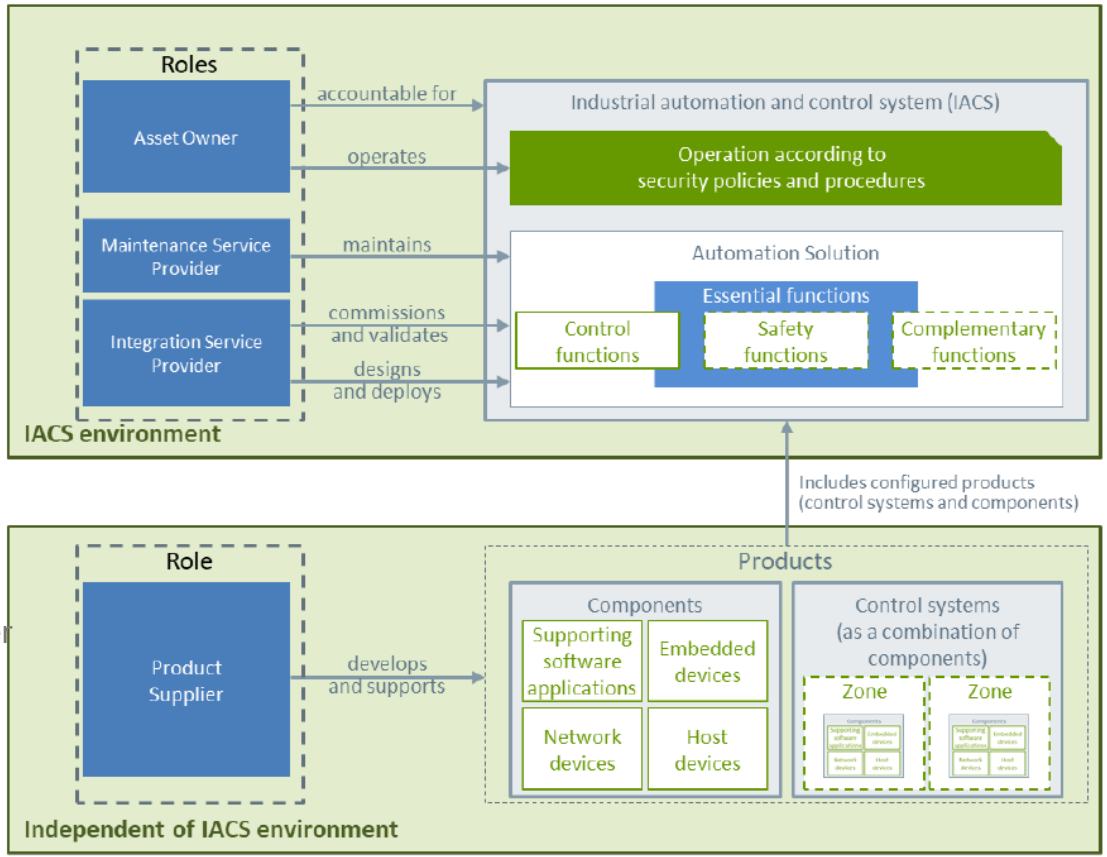
IACS: industrial automation and control systems

ISA/IEC 62443 – Scope & purpose

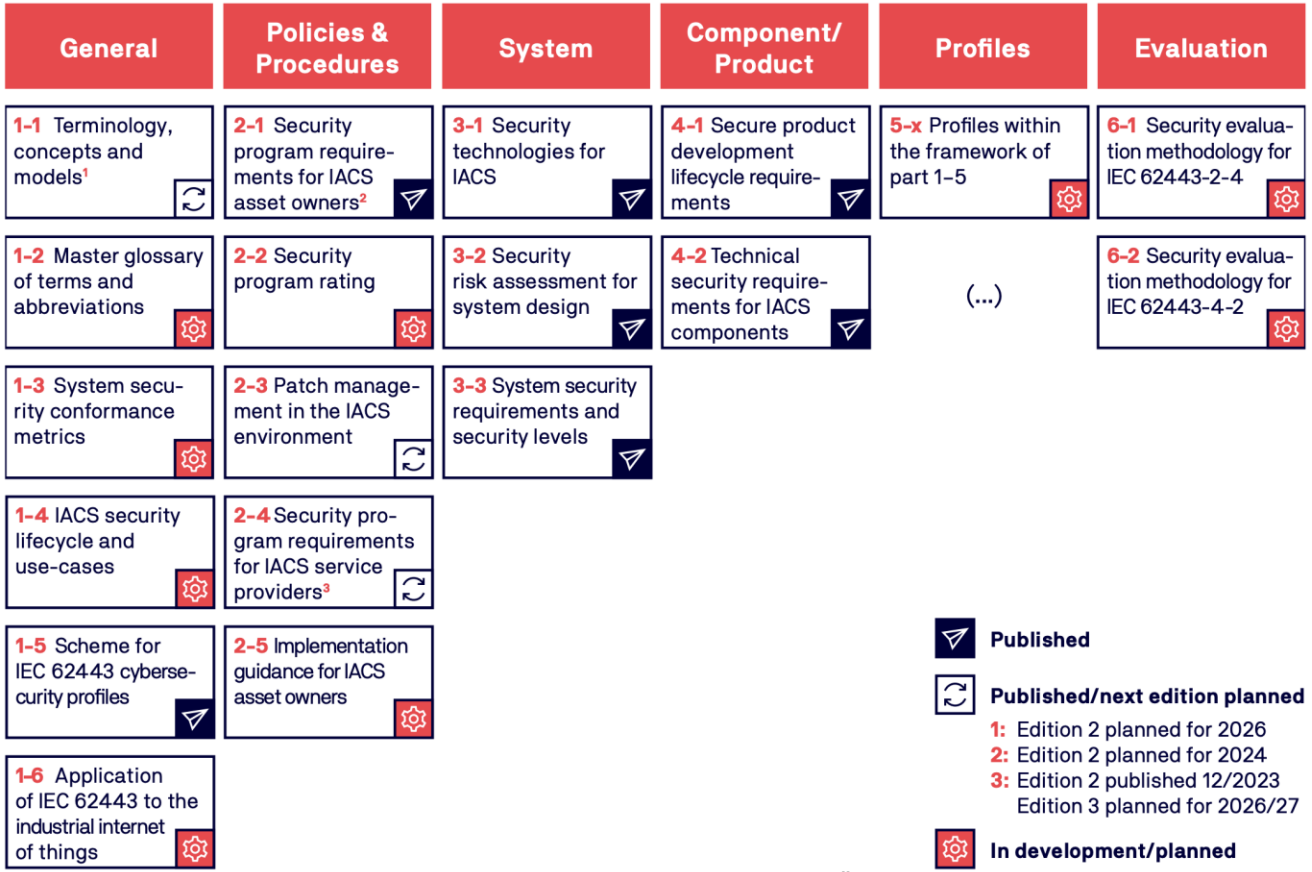
Holistic approach requires the considerations of 3 dimensions:

- Technologies
- Processes
- Human factors

… to be considered from any stakeholder perspective



ISA/IEC 62443 – Standard ext. families

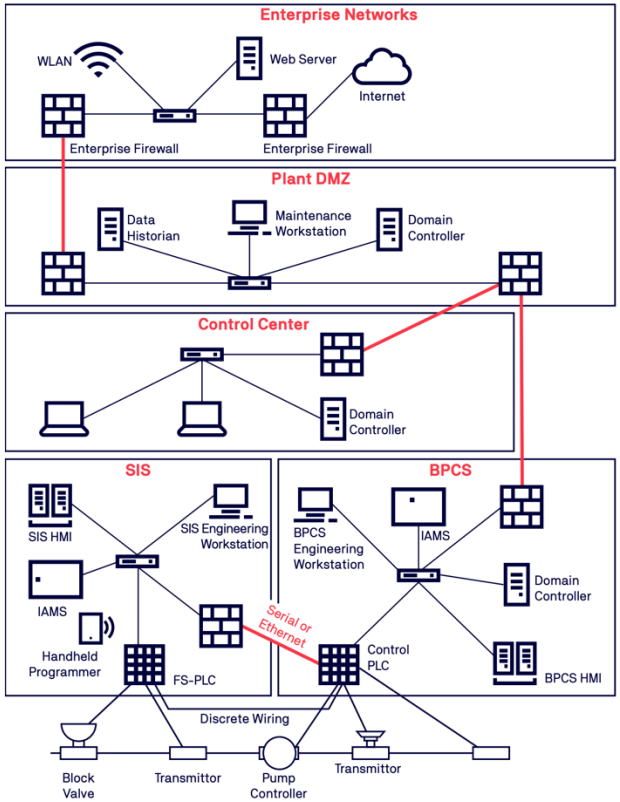


Source: Industrial Security Based on IEC 62443, TÜVIT (09/2024)

ISA/IEC 62443 – Key principles

Zones & Conduits

- **Security zones** are physical or logical grouping of assets that share common security requirements and isolating the critical control systems components.
- **Conduits** are the special type of security zone that groups communications that can be logically organized into a grouping of information flows within and also external to a zone. It can be a single service (i.e. Ethernet network) or be a multiple data carrier.



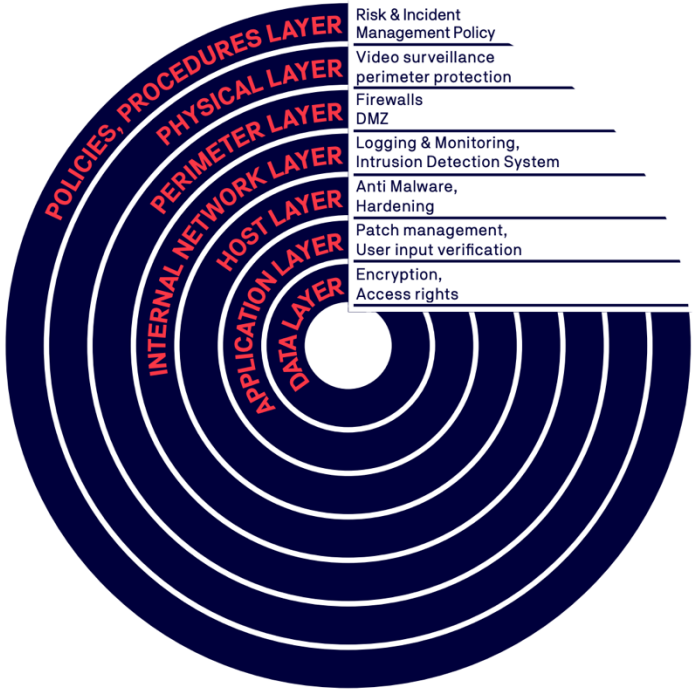
Source: IEC 62443-1-1: Industrial communication networks- Network and system security-Part 1-1: Terminology, concepts and models

swissuniversities

ISA/IEC 62443 – Key principles

Defense in depth

- **Data Layer** is the inner most layer and can be used for encryption of data, access rights etc.
- **Application Layer** is the next layer to data layer where SecDesign/Security review/patch management/… can be implemented.
- **Host Layer** is the layer after application layer and can be used for implementing OS hardening/anti-malware solutions etc.
- **Internal Network Layer** is the next layer after Host layer and can be used for implementation for Intrusion Detection System, logging and monitoring functionalities etc.
- **Perimeter Layer** is the next layer after internal network layer where firewalls or DMZ can be implemented.
- **Physical Layer** is the layer after perimeter layer, where for example video surveillance or perimeter protection can be used.
- **Policies, Procedures Layer** is the outermost and the last layer where the security policies procedures, guidelines, etc. for the IACS networks are defined



Source: Industrial Security Based on IEC 62443, TÜVIT (09/2024)

ISA/IEC 62443 – Key principles

Security Level	Description	Target	Skills	Motivation	Means
SL1	Capability to protect against casual or coincidental violation	Misconfiguration	No awareness	Confusion	No objective
SL2	Capability to protect against intentional violation using simple means with low resources, generic skills and low motivation	No security measures implemented, hacker	Basic	Low	Straight forward
SL3	Capability to protect against intentional violations using sophisticated means with moderate resources, IACS specific skills and moderate motivation	Only moderate security measures implemented, high level hacker	Industrial specific	Average	Intentional
SL4	Capability to protect against intentional violations using sophisticated means with extended resources, IACS specific skills and high motivation	Economical Damage	Highly sophisticated	High	Agressive

ISA/IEC 62443 – Key principles

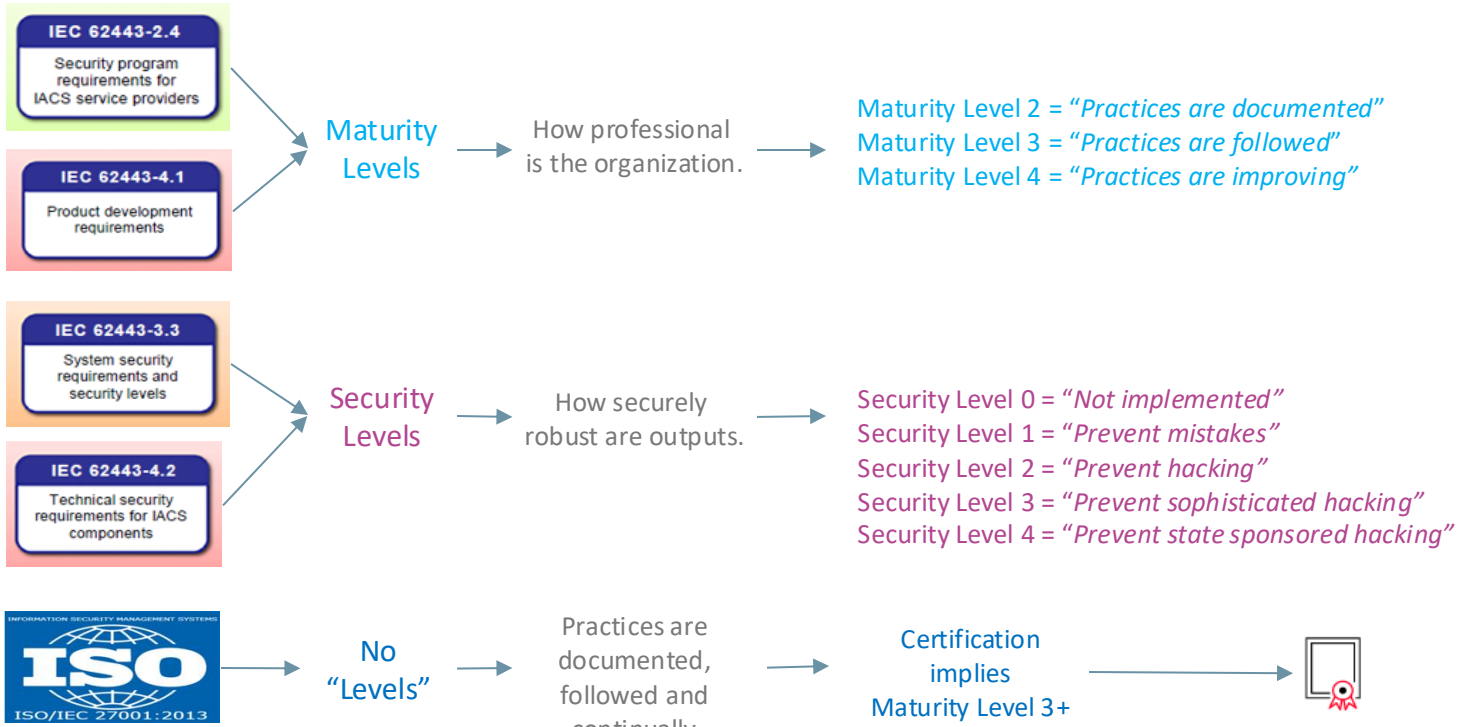
Security levels

- 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

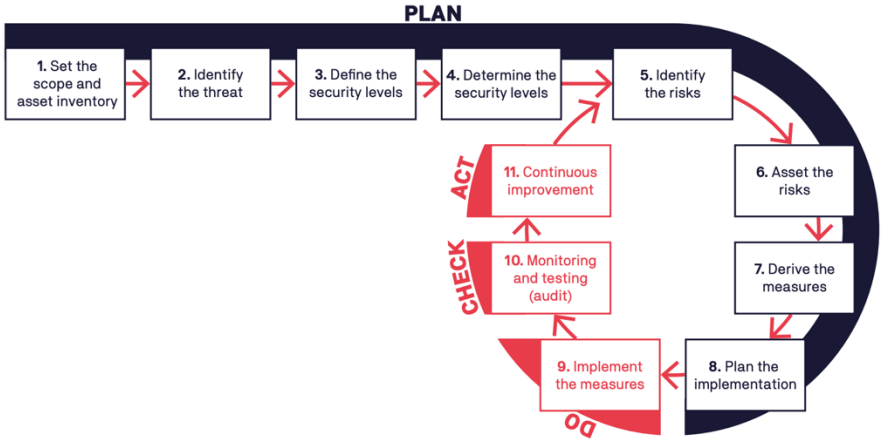
ISA/IEC 62443 – Key principles

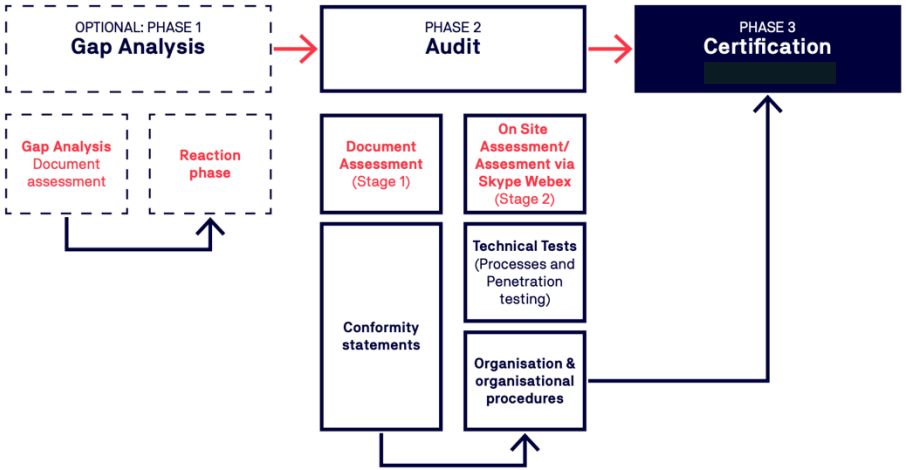
Maturity Level	IEC 62443-4-1	Description
1	Initial	Capability of performing a service without a documented process that is poorly controlled **(Process)**
2	Managed	Capability of performing a service in a formal documented characterized process with evidence of expertise and trained personnel **(Process + Documentation)**
3	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 **(Process + Documentation + Evidence)**
4	Improved	Capability of performing ML3 level including demonstration of continuous improvement, e.g. internal audit report **(Process + Documentation + Evidence + Continuous Improvement of Process)**

ISA/IEC 62443 – Levels In a Picture



ISA/IEC 62443 – Obtaining a certification





Source: Industrial Security Based on IEC 62443, TÜVIT (09/2024)

IEC 62443 - Parts

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

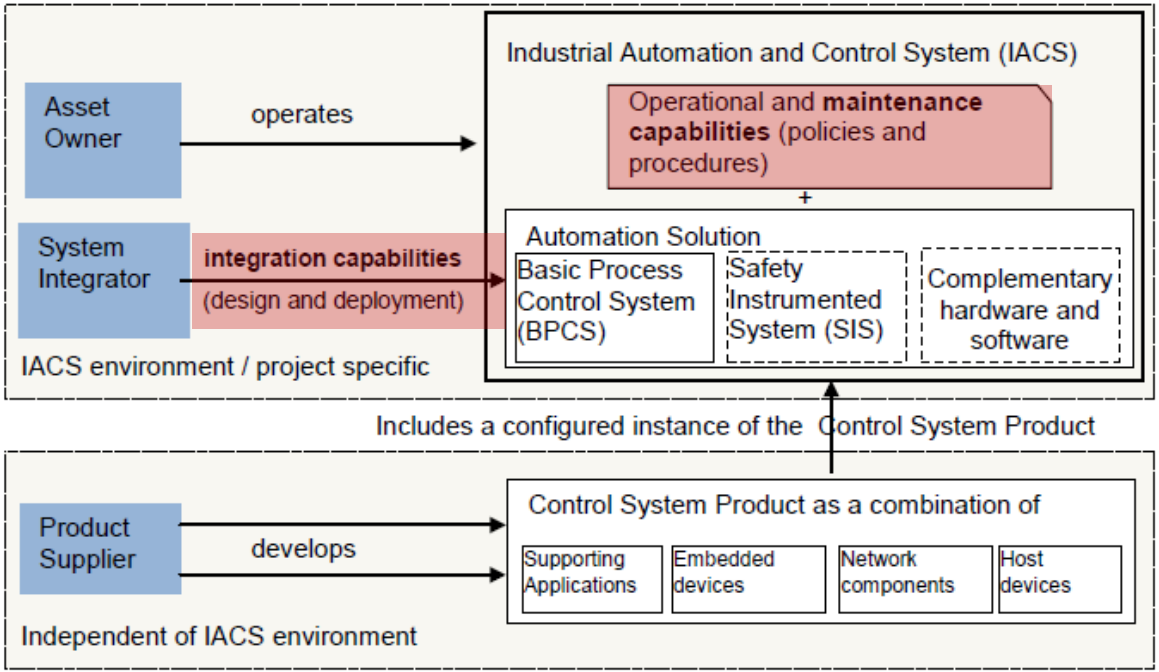
- defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements

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



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

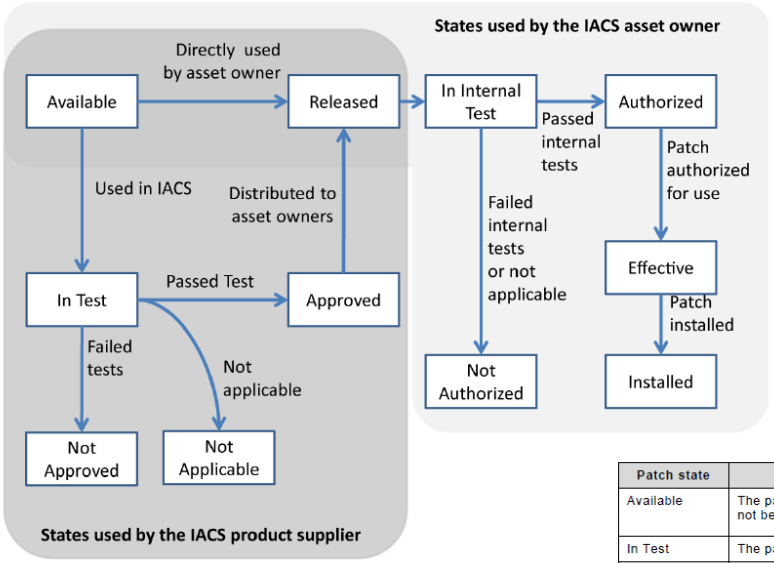
Value	SP Req ID	Description
Solution staffing	SP.01.XX	Requirements related to the assignment of personnel by the service provider to Automation Solution related activities.
Assurance	SP.02.XX	Requirements related to providing confidence that the Automation Solution security policy is enforced
Architecture	SP.03.XX	Requirements related to the design of the Automation Solution
Wireless	SP.04.XX	Requirements related to the use of wireless in the Automation Solution
SIS	SP.05.XX	Requirements related to the integration of SIS into the Automation Solution
Configuration management	SP.06.XX	Requirements related to the configuration control of the Automation Solution
Remote access	SP.07.XX	Requirements related to the remote access to the Automation Solution
Event management	SP.08.XX	Requirements related to the event handling in the Automation Solution
Account management	SP.09.XX	Requirements related to the administration of user accounts in the Automation Solution
Malware protection	SP.10.XX	Requirements related to the use of anti-malware software in the Automation Solution
Patch Management	SP.11.XX	Requirements related to the security aspects of approving and installing software patches
Backup/Restore	SP.12.XX	Requirements related to the security aspects of backup and restore

Column	Column description
Req ID	Requirement ID
BR/RE	Base Requirement/Requirement Enhancement indicator
Functional area	Keyword representing the main functional area of a requirement
Topic	Keyword representing the main topic associated with a requirement. The same topic may apply to more than one functional area.
Subtopic	Keyword representing the subtopic addressed by the requirement. The same technical topic may apply to more than one functional area and/or activity
Doc?	Deliverable documentation is required to be provided to the asset owner (yes/no). NOTE Some requirements may require the service provider to maintain documentation that is not considered a deliverable. However, the asset owner may have agreements with the service provider to see or have this documentation delivered to it.
Requirement description	The text of the requirement.
Rationale	Text that describes the background, justification, and other aspects of the requirement to assist the reader in its understanding

ISA/IEC 62443-2-4 – Examples

- Exercice 5

ISA/IEC 62443-2-3 – Patch management



Patch management state model

Patch state	Patch state definition	Managed by
Available	The patch has been provided by a third party or an IACS supplier but has not been tested.	Asset owner Product supplier
In Test	The patch is being tested by an IACS supplier.	Product supplier
Not Approved	The patch has failed the testing of the IACS supplier and should not be used, unless and until the IACS supplier confirms that the patch has been Approved.	Product supplier
Not Applicable	The patch has been tested and is not considered relevant to IACS use.	Product supplier
Approved	The patch has passed testing by the IACS supplier.	Product supplier
Released	The patch is released for use by the IACS supplier or third party, or the patch may be directly applicable by the asset owner for their internally developed systems.	Asset owner Product supplier
In Internal Test	The patch is being tested by the asset owner testing team.	Asset owner
Not Authorized	The patch has failed internal testing, or may not be applicable.	Asset owner
Authorized	The patch is released by the asset owner and meets company standards for updatable devices, or by inspection did not need testing.	Asset owner
Effective	The patch is posted by the asset owner for use.	Asset owner
Installed	The patch is installed on the system.	Asset owner

ISA/IEC 62443-2-3 – Patch management

Operating an IACS patch management

Establishing a patching program is difficult enough, but if patching efforts are not sustained or optimized over time they will not fulfil the objective of reducing security vulnerabilities

- Change management
  - Activity of patch management is subject to change controls and should adhere to the change management process
- Vulnerability awareness
  - It is very important that asset owners recognize this and maintain a constant vigilance of the vulnerabilities that exist. These must include an awareness of discovered zero-day threats and vulnerabilities that affect their critical systems.
  - Consider interfaces with CERT's
- Outage scheduling
  - Asset owners should assess the applicability of the vulnerability to their systems as alert notifications are released announcing the new vulnerabilities.
- Security hardening
  - Security hardening does not replace patch management, it reduces the applicable patches by removing unnecessary software, which then does not need to be patched and possibly limits the effects of certain exploits.
- Inventory and data maintenance
  - Tracking vulnerabilities and patches status is key for maintaining a sufficient supervision of operating products and residual risks
  - Automated tools are recommended
- Procuring or adding new devices
  - Placing these vulnerable systems in the IACS environment not only puts those systems at risk, but they then become the weakest link on that network and can potentially allow the other systems to become compromised. It is important to ensure new systems are fully patched prior to connecting them to the IACS network
- Patch management reporting and KPIs
  - The impacts of poor patch management should be measured using KPIs that facilitate a continuous improvement process. The following are examples of KPIs: Nbr of assets compromised due to missing patches, Nbr of patches available, Nbr of patches applied…

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

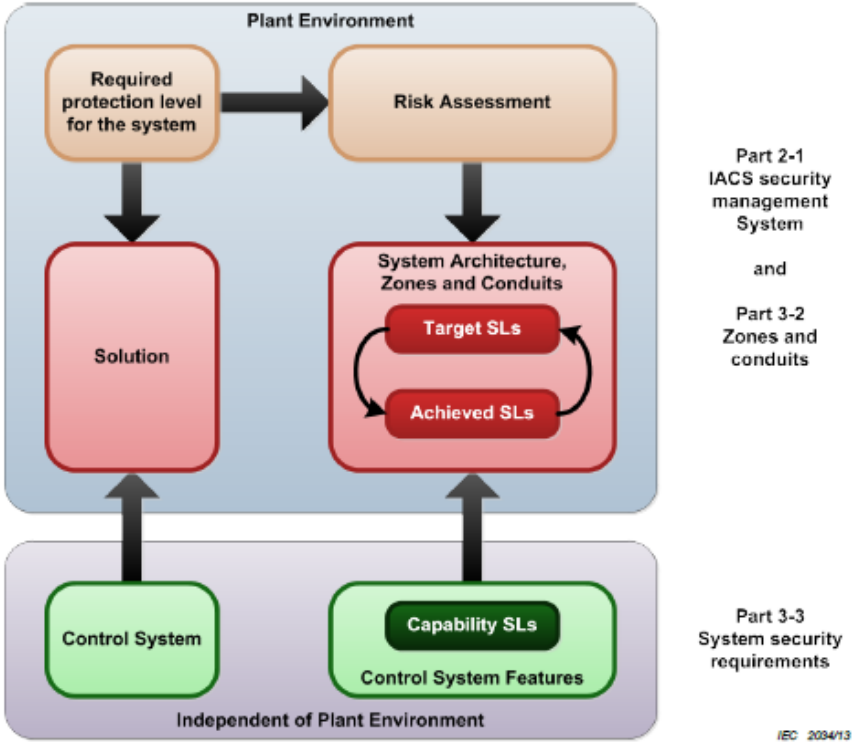
ISA/IEC 62443-3-3

- 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 62443-3-3 – 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 62443-3-3 – System requirements

Requirements are derived and allocated per Security levels as illustrated here

- SR: System requirements
- RE: Requirements enhancement

Those requirements are not component specific, they are describing capabilities to be ensured on System level and should therefore be distributed to relevant component later one, based on SL per zone / conduit.

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓
SR 1.2 – Software process and device identification and authentication	5.4		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1			✓	✓
SR 1.3 – Account management	5.5	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management	5.5.3.1			✓	✓
SR 1.4 – Identifier management	5.6	✓	✓	✓	✓
SR 1.5 – Authenticator management	5.7	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1			✓	✓
SR 1.6 – Wireless access management	5.8	✓	✓	✓	✓
SR 1.6 RE 1 – Unique identification and authentication	5.8.3.1		✓	✓	✓
SR 1.7 – Strength of password-based authentication	5.9	✓	✓	✓	✓
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	5.9.3.1			✓	✓

ISA/IEC 62443-3-3 – Examples

- Exercice 6

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

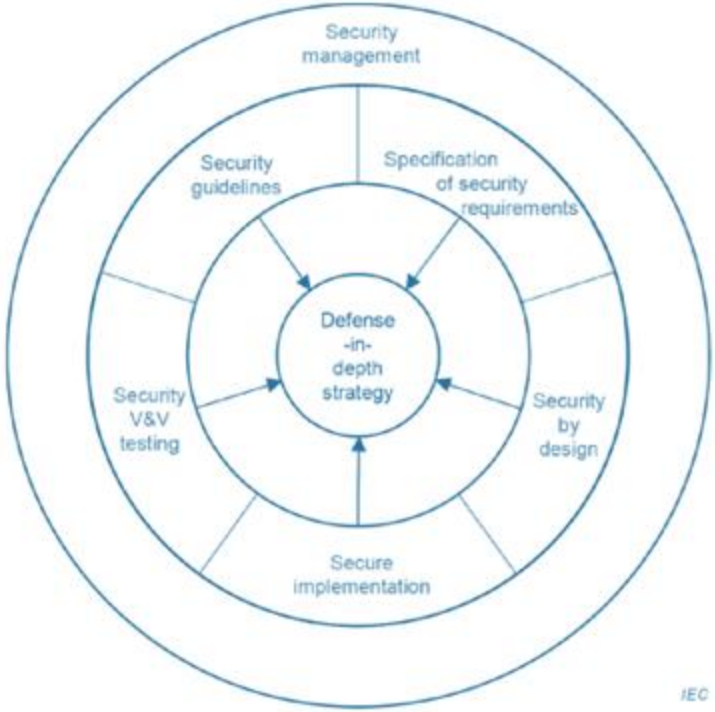
ISA/IEC 62443-4-2

- 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 62443-4-1 – SDLC

Security management	SM-1 Development process
	SM-10 Custom developed components from third-party suppliers
	SM-11 Assessing and addressing security-related issues
	SM-12 Process verification
	SM-13 Continuous improvement
	SM-2 Identification of responsibilities
	SM-3 Identification of applicability
	SM-4 Security expertise
	SM-5 Process scoping
	SM-6 File integrity
	SM-7 Development environment security
	SM-8 Controls for private keys
	SM-9 Security requirements for externally provided components
Security requirements	SR-1 Product security context
	SR-2 Threat model
	SR-3 Product security requirements
	SR-4 Product security requirements content
	SR-5 Security requirements review
Secure by design	SD-1 Secure design principles
	SD-2 Defense in depth design
	SD-3 Security design review
	SD-4 Secure design best practices
Secure implementation	SI-1 Security implementation review
	SI-2 Secure coding standards
Security verification and validation testing	SVV-1 Security requirements testing
	SVV-2 Threat mitigation testing
	SVV-3 Vulnerability testing
	SVV-4 Penetration testing
	SVV-5 Independence of testers
Management of security-related issues	DM-1 Receiving notifications of security-related issues
	DM-2 Reviewing security-related issues
	DM-3 Assessing security-related issues
	DM-4 Addressing security-related issues
	DM-5 Disclosing security-related issues
	DM-6 Periodic review of security defect management practice
Security update qualification	SUM-1 Security update qualification
	SUM-2 Security update documentation
	SUM-3 Dependent component or operating system security update documentation
	SUM-4 Security update delivery
	SUM-5 Timely delivery of security patches
Security guidelines	SG-1 Product defense in depth
	SG-2 Defense in depth measures expected in the environment
	SG-3 Security hardening guidelines
	SG-4 Secure disposal guidelines
	SG-5 Secure operation guidelines
	SG-6 Account management guidelines
	SG-7 Documentation review

ISA/IEC 62443-4-1 – Threat Model Hints

Product suppliers need to perform a risk assessment on a product abstraction level, by creating a threat model which should include following characteristics:

- correct flow of categorized information throughout the system;
- trust boundaries;
- processes;
- data stores;
- internal and external communication protocols implemented in the product;
- externally accessible physical ports including debug ports;
- circuit board connections such as Joint Test Action Group (JTAG) connections or debug headers which might be used to attack the hardware;
- potential attack vectors including attacks on the hardware, if applicable;
- potential threats and their severity as defined by a vulnerability scoring system (for example, CVSS);
- mitigations and/or dispositions for each threat;
- security-related issues identified;
- external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application.

Those elements would represent key information for maintaining smart asset inventory on system level, as well as consistency between risk assessment levels

ISA/IEC 62443-4-1 – Secure Update

- [62443-4-1/11.2.1] – Security Update Qualification

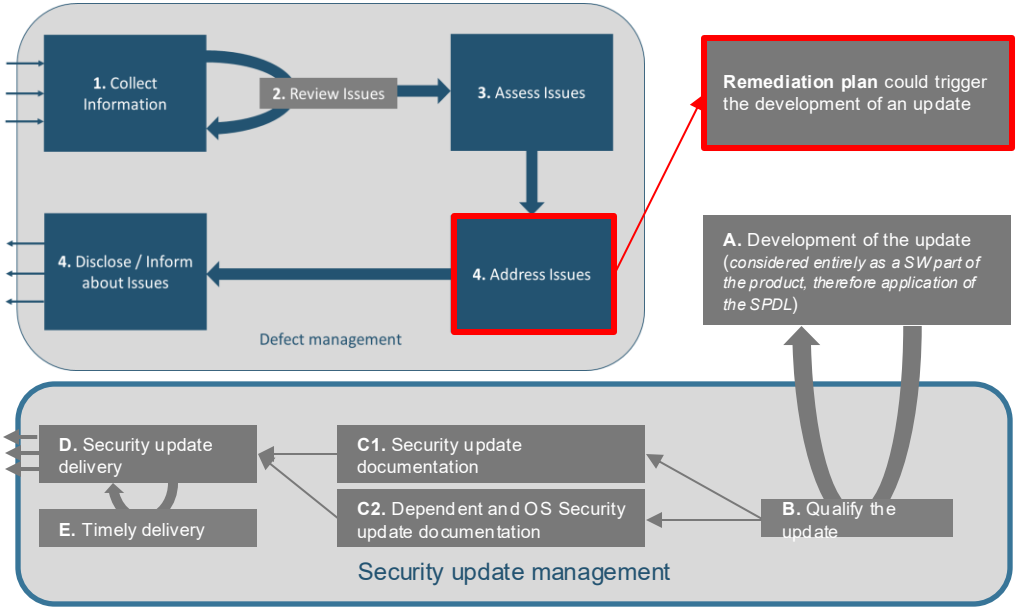
  A process shall be employed for verifying that
  - security updates created by the product developer address the intended security vulnerabilities;
  - security updates do not introduce regressions, including but not limited to patches created by: a) the product developer; b) suppliers of components used in the product; and c) suppliers of components or platforms on which the product depends.

- [62443-4-1/11.3.1] – Security update documentation

  A process shall be employed to ensure that documentation about product security updates is made available to product users that includes but is not limited to:
  - the product version number(s) to which the security patch applies;
  - instructions on how to apply approved patches manually and via an automated process;
  - description of any impacts that applying the patch to the product can have, including reboot;
  - instructions on how to verify that an approved patch has been applied;
  - risks of not applying the patch and mediations that can be used for patches that are not approved or deployed by the asset owner.

- [62443-4-1/11.4.1] – Dependent component or operating system security update documentation

  A process shall be employed to ensure that documentation about dependent component or operating system security updates is made available to product users that includes but is not limited to:
  - stating whether the product is compatible with the dependent component or operating system security update;
  - [illegible] updates that are unapproved by the product vendor, the mitigations that can be used in lieu of not applying the update.



ISA/IEC 62443-4-2 – Requirements

Component Requirements (of any type) are segmented in 2 main categories:

- Common Component Security Constraints (CCSC)
  - Constraints which are required to be applied during implementation of any relevant requirements from IEC 62443-4-2

- Foundational requirements (FR)
  - 7 categories that are addressing requirements based on security primitives criteria (see later)
  - SL-A achieved can be seen as a vector of this 7 FR ([X;X;X;X;X;X;X]) but a certification can be claimed only on the lowest SL achieved through applicable FR
    - e.g. a component where the entire set of requirements has been identified as applicable and has been assessed as [4;**1**;3;2;4;3;2], then a certification for SL1 is the only achievable level at this stage

    Depending on the targeted Security Level, one or multiple Requirement Enhancements (RE) need to be considered as well

ISA/IEC 62443-4-2 – CCSC

Common Component Security Constraints (CCSC)

1. CCSC 1: Support of essential functions (IEC 62443-4-2/4.2)
   - The components of the system shall adhere to specific constraints as described in IEC 62443-3-3:2013, Clause 4.
   - To determine the required ESSENTIAL FUNCTION, a benefit-risk analysis (between safety and security) should be conducted to determine which functionality can be sacrificed (“degraded mode”), and which cannot.
2. CCSC 2: Compensating countermeasures (IEC62443-4-2/4.3)
   - When one or more requirements specified in 62443-4-2 cannot be met without the assistance of a compensating countermeasure that is external to the targeted component, the documentation for that component shall describe the appropriate countermeasures applied by the system to allow the requirement to be met when the component is integrated into a system.
   - e.g. If logging features are not implementable for a good reason, documentation related to the needs of IDS/IPS (Intrusion Detection/Prevention System) could be derived for reaching a certain SL “under specific condition”
3. CCSC 3: Least privilege (IEC62443-4-2/4.4 and IEC TR 60601-4-5/4.4)
   - Individual system components shall provide the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability shall be available when required. Granularity of permissions and assignment is dependent on the type of device and the product documentation for the device should define this in the product documentation.
   - e.g. “DENY ALL” and create roles with adequate rights
4. CCSC 4: Secure development process (IEC62443-4-2/4.5)
   - All of the components defined in this document shall be developed and supported following the secure product development processes described in IEC 62443-4-1 or equivalent.
   - «You cannot provide security capabilities of a product without ensuring its secure development»

ISA/IEC 62443-4-2 – Foundations

1) Identification and authentication control (IAC),
   - Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets.
2) Use control (UC),
   - Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.
3) System integrity (SI),
   - Ensure the integrity of the component to protect against unauthorized manipulation or modification.
4) Data confidentiality (DC),
   - Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure.
5) Restricted data flow (RDF),
   - Segment the control system via zones and conduits to limit the unnecessary flow of data.
6) Timely response to events (TRE), and
   - Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.
7) Resource availability (RA).
   - Ensure the availability of components against the degradation or denial of essential services.

ISA/IEC 62443-4-2 – Req' s

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

Most of the requirements on component level are considered as generic though some specificities and tailoring can be 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)
  Ex. PLC, IED, ECU…
- Host Device Requirements (HDR)
  Ex. Operator workstation, Data historian…
- Network Device Requirements (NDR)
  Ex. 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	✓	✓	✓	✓

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
CR 5.1 – Network segmentation	✓	✓	✓	✓
NDR 5.2 – Zone boundary protection	✓	✓	✓	✓
RE (1) Deny all, permit by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
NDR 5.3 – General purpose, person-to-person communication restrictions	✓	✓	✓	✓
FR 6 – Timely response to events (TRE)				
CR 6.1 – Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
CR 6.2 – Continuous monitoring		✓	✓	✓

ISA/IEC 62443-4-1/2 – Examples

- Exercice 7

References

- IEC 62443 Wikipedia
- IEC 62443 Publications (entire 62443 suite)
- CH NCSC Recommendations ICT minimum standard
- CH NCSC Measures to protect industrial control systems