STANDARDISATION : PART 2

LICORICE

reLIable and sCalable tOols foR self-sovereIgn identity and data protection framEwork

THE EVOLUTION OF STANDARDIZATION IN CYBERSECURITY

Led by Antonio Kung (Trialog), François Zamora (Orange), and Jean Caire (RATP)

www.licorice-horizon.eu
@LICORICE Project
@Li_corice_
@LICORICE_project

Evolution of Standardization in Cybersecurity: Part 2

This document is the continuation of the work initiated by Antonio Kung (FR – Trialog), François Zamora (FR – Orange), and Jean Caire (FR – RATP), following the publication of a French paper by SEE[1] in October 2024. Building on discussions with Norbert Bensalem (FR, JTC 1 SIF facilitator), the French national body has graciously made it available to ISO/IEC JTC 1/SC 27.

Through LICORICE, the second part of this document is now accessible to a broader international audience, showcasing the bridge that LICORICE has built as one of the project's key achievements.

This blog offers a comprehensive overview of the changing context in standardization and the evolution of standardization practices.

The Changing Context

Cybersecurity Frameworks

Moves towards the creation of a cybersecurity community can be traced back to the 2000s with a focus on prevention:

- The NIST (National Institute of Standards and Technology) in the United States published the report NIST SP 800-53 in 2005.[2] which can be considered as the **security controls reference catalog**. From 2010, NIST added controls on privacy. The latest version is revision 5 published in 2020. It contains no less than 450 pages and will continue to evolve in the future.
- The cybersecurity community published the Common Vulnerability Scoring System (CVSS) in 2003.[3], a system for evaluating the criticality of vulnerabilities according to a score between zero and ten. Version 4 of this system was published in 2023.

In 2014, NIST published its **cybersecurity framework (CSF)**[4]. This framework changed the landscape by integrating the management of cybersecurity incidents, thus completing a vision of risk management based on the two phases (risk assessment and risk treatment) with five functions: *Identify* (corresponding to risk assessment), *Protect, Detect, Respond, Recover* (corresponding to treatment of risk). A list of activities is associated with each function, and the concept of organizational profile is defined, allowing organizations to select relevant activities. NIST released version CSF 2.0 in 2024. It adds an additional function (*Govern*), and explains the correspondence between activities in version 2.0 and controls in the NIST SP 800-53 controls catalog. Since 2018, NIST has also been leading an equivalent initiative on a **privacy framework**[5].

[1] https://see.asso.fr/produit/ree-2024-3/

[2] https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

[3] https://www.first.org/cvss/

[4] https://www.nist.gov/cyberframework

[5] https://www.nist.gov/privacy-framework

NIST further published SP 800-160 vol.2 in 2019 and 2021[6] on the **engineering of resilient cyber systems**, and SP 800-160 vol.1[7] in 2022, on the **engineering of trusted secure systems**.

Note also contributions of MITRE[8] to the work of NIST, with the provision of two online sites. The first, published in 2013, is a knowledge base that categorizes and describes cyber attacks[9]. The second is the "cyber resilience engineering framework".[10], which accompanies SP 800-160 vol.2 by visualizing the correspondences between the controls of the NIST SP 800-53 catalog and the activities of CSF 2.0.

Standardization follows this evolution, with ISO/IEC 27100 (concepts and overview of cybersecurity), with ISO/IEC 27110 (guidelines for the development of a cybersecurity framework) which is directly influenced by the cybersecurity framework of the NIST. We will also note the ISO/IEC 27035 series on incident management, as well as the start of the ISO/IEC 9138 series on systems resilience, the first part of which on concepts and vocabularies will be published shortly.

Ecosystems

We use the term ecosystem to characterize an infrastructure and associated services based on a community of organizations and stakeholders. We use this term for example for smart cities, but we can also use it in application domains (e.g. transport, energy, health).

Ecosystems are becoming increasingly complex due to the number of organizations and stakeholders involved, the diversity of their roles, and the diversity of technologies (artificial intelligence, digital twins or virtual worlds). Standardization accompanies this development in the following way:

- standards on **systems of systems engineering**, with ISO/IEC/IEEE 21841 (taxonomy of systems of systems), ISO/IEC/IEEE 21839 (impact of systems of systems on the life cycle), or ISO/IEC/IEEE 21840 (use of ISO/IEC/IEEE 15288, reference standard on the life cycle, for system of systems).
- standards on **smart cities**, with the ISO/IEC 30145 series on a reference framework in smart cities, or the ISO/IEC 27570 on privacy guidelines for smart cities.
- standards on **trustworthiness**, with ISO/IEC 5723 on vocabulary, ISO/IEC 31303 on an overview and concepts, ISO/IEC 30149 on the principles of trust for the Internet of Things, or ISO/IEC 30147 on the integration of trustworthiness activities in the lifecycle of an IoT system, based on the ISO/IEC/IEEE 15288 standard.
- standards on **governance**, with ISO/IEC 38500 on information technology governance, ISO/IEC 38501-1 on data governance, ISO/IEC 38507 on the impact of artificial intelligence, and ISO/IEC 38509 on responsible governance for social inclusion.

[6] https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

[7] https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

[8] https://www.mitre.org/

[9] https://attack.mitre.org/

[10] https://crefnavigator.mitre.org/

Regulations

The European Union can adopt two types of legislation, directives which require transposition at national level and regulations which are binding legislative acts.

Regulation influences standardization, particularly in Europe with the concept of *harmonized standards*. These are standards developed by a European standardization body (CEN[11], CENELEC[12] or ETSI[13]), following a request from the European Commission concerning union legislation. Manufacturers, other economic operators or conformity assessment bodies use these harmonized standards to demonstrate that products, services or processes comply with this legislation. The table below lists the regulations that impact cybersecurity.

The following draft harmonized standards are under development or discussion:

- Concerning the RED directive on the cybersecurity of radio equipment, the standards EN 18031-1, EN 18031-2, EN 18031-3 are under development.
- Concerning the AI act, several standards are being developed by CEN-CENELEC JTC21, including one on risk management and one on trustworthiness.
- Concerning the Cyber Resilience act, a standardization request is being finalized, and CEN-CENELEC has set up a working group (JTC 13/WG 9).
- Concerning the data act, a standardization request is being prepared.

Recent relevant regulations impacting Cybersecurity

Regulations	Description	Application
General Data Protection Regulation (GDPR)	The GDPR applies to any organization that operates in the union or processes the data of a citizen of the union. The EDPB (EU Data Protection Board) ensures the consistency of the application of the GDPR. The notion of consent plays a major role in the GDPR, particularly on data transfers to an external party or outside the union.	Applied since May 2018
Cybersecurity Act	The Cybersecurity Act strengthens the role of the EU Cybersecurity Agency (ENISA) and establishes a cybersecurity certification framework for products and services.	Applied since June 2019
Legislation on Artificial Intelligence (AI Act)	This regulation concerns artificial intelligence systems. Five risk categories are identified: unacceptable (e.g. social rating), high (e.g. AI system in healthcare), general purpose generative AI, limited (e.g. image generation and manipulation), minimal. Particular attention is paid by the regulation to cyber security, which must be ensured at a sufficient level for high-risk AI systems.	Applied since August 2024
NIS2 (Network and Information System Security) Directive on network and information security	Replaces the NIS directive of July 2016. It aims to ensure a high and common level of security. It specifies the terms of cooperation between national IT security incident response centers (CSIRTs), and adds a framework for the preparation and management of cyber crises (EU-CyCLONe)	Currently being transposed for application no later than October 2024
Directive on the resilience of critical entities	Critical entities provide essential services to maintain key societal functions, supporting the economy, protecting public health and safety, and preserving the environment. Sectors concerned are energy, transport, banking, financial markets, health, drinking water, waste water, digital infrastructure, public administration, space, food production. Member States need to have identified critical entities for the sectors listed in the CER Directive by July 17, 2026.	Currently being transposed for application no later than October 2024

[11] https://www.cencenelec.eu/about-cen/

[12] https://www.cencenelec.eu/about-cenelec/

[13] https://www.etsi.org/

	They will use this list of essential services to carry out risk assessments and then to identify critical entities. Once identified, these critical entities will have to adopt measures to strengthen their resilience	
Digital Operational Resilience Act (DORA)	DORA aims to strengthen the IT security of financial entities (banks, insurance companies, investment firms) so that the financial sector in Europe can remain resilient in the event of serious operational disruptions. It applies to 20 different types of financial entities and third-party IT service providers.	Application planned for January 2025.
EUCC Implementing Regulation	This regulation complements that of the European Union's cybersecurity. It involves the adoption of a cybersecurity certification scheme based on common criteria (EUCC). The scheme is based on the ISO/IEC 15408 standard	Application planned for February 2025
Modification of the RED directive on radio equipment	The amendment to the RED directive adds cybersecurity requirements to (1) radio equipment connected to the Internet, (2) radio equipment processing personal data, including that designed for childcare, or those that are designed to be worn on the body or on clothing, and (3) equipment allowing the transfer of money or virtual currency.	Application planned for August 2025
Data Act	The Data Regulation aims to create a framework for the secure sharing of digital data, particularly for data from Internet of Things devices.	Publication on December 2023 and application planned for September 2025
Cyber Resilience Act (CRA)	This regulation creates a European framework for the cyber security of products containing digital elements The obligations relate to security-by-design (taking into account the security of devices from the design stage) and the ongoing management of known security vulnerabilities.	Publication planned for 2024 for application in 2027.

Evolution of standardization Practices

Flexible Use of Standards

International standardization must work on two challenges.

The first challenge is the establishment of a practice of standard construction that enables the use of cross-cutting standards in vertical domains through **standard profiles**. Cross-cutting aspects include regulations (see previous table), characteristics (e.g., trust, ethics, resilience, respect for privacy), processes (e.g., lifecycle, architecture, evaluation), and technologies (e.g., artificial intelligence, digital twins, virtual worlds). To make it happen, this practice will require significant work in the coordination process between standardization committees.

The second challenge is the transition to a SMART standard format[14] (applicable machine standard, readable and transferable). This format will allow for the move from a paper format to a format customized by a context represented by standard profiles. This format is generated online, and is constantly up to date. Ultimately, a SMART standard could integrate parts from different committees, or even different organizations (e.g. a harmonized European standard could integrate parts of an international standard).

Flexible Use of Architecture Standards

In order to support a system and architecture vision of complex systems, standardization must also align with a practice of architectural standards making it possible to combine architectural standards according the context of use, through **architecture profiles**. ISO/IEC started working on the issue in 2018, in particular on the topic of reference architectures and architecture patterns. ISO/IEC JTC 1/SC 41 (Internet of things and digital twins) plans to work on the creation of a architecture pattern repository.

The following standards should be mentioned: ISO/IEC/IEE 42024 (architecture fundamentals), ISO/IEC/IEE 42042 (reference architecture), ISO/IEC 30141 (reference architecture for the Internet of Things), ISO/IEC 40141 (guidelines on reference architectures).

Flexible Use of Cybersecurity Architecture Standards

Taking cybersecurity into account in complex systems requires supplementing architecture profiles with **cybersecurity architecture profiles**. Initially, we can consider these profiles as a documentation practice that can be used in security protection profiles (e.g. used in the EUCC implementing regulation). Ultimately, these profiles may themselves be subject to evaluation. The ISO/IEC JTC 1/SC 27 (cybersecurity) committee is working on ISO/IEC 27115 which specifies a framework for the description of cybersecurity architectures and their evaluation based on ISO/IEC/IEEE 42030 (architecture evaluation). ISO/IEC 27115 further specifies a cybersecurity architecture pattern that can be used as the starting point to develop architecture profiles.

[14] https://www.iso.org/fr/smart

Integration of Human and Artificial Cognitive Factors

The integration of human and artificial cognitive factors in complex systems will require new standardisation practices, as exemplified by the work associated with the implementation of the AI Act in Europe. The major challenge of the integration of AI is to provide an architecture of standards that enable the advent of trustworthy complex systems. Cybersecurity standards will play a pivotal role: enabling the definition of cybersecurity profiles standards protecting deployed AI mechanisms. These issues are the subject of exploratory and normative work in certain member states of the union, but also at the level of European standardization (CEN CENELEC ETSI) and at the international level in ISO/IEC JTC 1/SC 27 or ISO/IEC JTC 1/SC 40.

Standardisation Series Blog Conclusions

This blog series have provided a comprehensive analysis of standardization and showed the profound influence on cybersecurity standardization. By describing challenges on flexible reuse of standards, of architecture standards and of cybersecurity architectures in standards, it has pointed out the need for a common practice of architecture.

Jean Caire and Sylvain Conchon have proposed a global vision on this subject[15]. They have modelled the cyber space model into three strata, the **anthropogenic stratum** which represents human beings organized in social networks, the **cybernetic stratum** which represents all the information and their distribution vectors, and the **physical stratum** which represents the resulting behaviours and actions. This model is presented in ISO/IEC 27100 (Cybersecurity Concepts and Overview), and can serve as a starting point. Taking such an architectural perspective will enable a clear view on governance needs, and pave the way to priorities such as digital sovereignty.

[15] https://hal.science/hal-02071177v1/file/lm21_com_4D_4_172_Caire.pdf

Annex List of standards mentioned in the standardization series blogs

Reference	Title in English	Status	URL
ISO PAS 5112	Road vehicles — Guidelines for auditing cybersecurity engineering	Edition 1 published in 2022	https://www.iso.org/standard/80840.html
ISO/IEC TS 5723	Trustworthiness — Vocabulary	Edition 1 published in 2022	https://www.iso.org/standard/81608.html
ISO/IEC TR 6114	Cybersecurity — Security considerations throughout the product life cycle	Edition 1 published in 2023	https://www.iso.org/standard/82056.html
ISO/SAE PAS 8475	Road vehicles — Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF)	Under development	https://www.iso.org/standard/83187.html
ISO/SAE TR 8477	Road vehicles — Cybersecurity verification and validation	Under development	https://www.iso.org/standard/83188.html
ISO/IEC 9837-1	Software and systems engineering — Systems resilience - Part 1: Concepts and vocabulary	Under development	https://www.iso.org/standard/83604.html
ISO/IEC/IEEE 15288	Systems and software engineering — System life cycle processes	Edition 2 published in 2023.	https://www.iso.org/standard/81702.html
ISO/IEC 15408-1	Evaluation criteria for IT security Part 1: Introduction and general model	Edition 4 published in 2022.	https://www.iso.org/standard/72891.html
ISO/IEC 15408-2	Evaluation criteria for IT security Part 2: Security functional components	Edition 4 published in 2022	https://www.iso.org/standard/72892.html
ISO/IEC 15408-3	Evaluation criteria for IT security Part 3: Security assurance components	Edition 4 published in 2022	https://www.iso.org/standard/72906.html
ISO/IEC 15408-4	Evaluation criteria for IT security Part 4: Framework for the specification of evaluation methods and activities	Edition 4 published in 2022	https://www.iso.org/standard/72913.html
ISO/IEC 15408-5	Evaluation criteria for IT security Part 5: Pre-defined packages of security requirements	Edition 4 published in 2022	https://www.iso.org/standard/72917.html
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques	Edition 1 published in 2018	https://www.iso.org/standard/69373.html
ISO/SAE 21434	Road vehicles — Cybersecurity engineering	Edition 1 published in 2021	https://www.iso.org/standard/70918.html
ISO/IEC/IEEE 21839	Systems and software engineering — System of systems (SoS) considerations in life cycle stages of a system	Edition 1 published in 2019	https://www.iso.org/standard/71955.html
ISO/IEC/IEEE 21840	Systems and software engineering — Guidelines for the utilization of ISO/IEC/IEEE 15288 in the context of system of systems (SoS)	Edition 1 published in 2019	https://www.iso.org/standard/71956.html
ISO/IEC/IEEE 21841	Systems and software engineering — Taxonomy of systems of systems	Edition 1 published in 2019	https://www.iso.org/standard/71957.html
ISO TR 23244	Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations	Edition 1 published in 2020	https://www.iso.org/standard/75061.html
ISO TR 23249	Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management	Edition 1 published in 2022	https://www.iso.org/standard/80805.html
ISO TR 23644	Blockchain and distributed ledger technologies (DLTs) — Overview of trust anchors for DLT-based identity management	Edition 1 published in 2023	https://www.iso.org/standard/81773.html
ISO 24946	Requirements and guidance for improving, preserving, and assessing the privacy capability of DLT systems.	Under development	https://www.iso.org/standard/88614.html
ISO 25126	Information security controls based on ISO/IEC 27002 for distributed ledger services	Under development	https://www.iso.org/standard/89024.html
ISO/IEC 27001	Information security management systems — Requirements	Edition 3 published in 2022	https://www.iso.org/standard/27001
ISO/IEC 27002	Information security management systems — Information security controls	Edition 3 published in 2022	https://www.iso.org/standard/75652.html
ISO/IEC 27006-1	Requirements for bodies providing audit and certification of information security management systems Part 1: General	Edition 1 published in 2024	https://www.iso.org/standard/82908.html

ISO/IEC 27005	Guidance on managing information security risks	Edition 4 published in 2022	https://www.iso.org/standard/80585.html
ISO/IEC 27019	Information security controls for the energy utility industry	Edition 2 published in 2024	https://www.iso.org/standard/85056.html
ISO/IEC 27035-1	Information security incident management Part 1: Principles and process	Edition 2 published in 2023	https://www.iso.org/standard/78973.html
ISO/IEC 27035-2	Information security incident management Part 2: Guidelines to plan and prepare for incident response	Edition 2 published in 2023	https://www.iso.org/standard/78974.html
ISO/IEC 27035-3	Information security incident management Part 3: Guidelines for ICT incident response operations	Edition 1 published in 2020	https://www.iso.org/standard/74033.html
ISO/IEC 27035-4	Information security incident management Part 4: Coordination	Currently being published	https://www.iso.org/standard/80973.html
ISO/IEC 27090	Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and failures in artificial intelligence systems	Under development	https://www.iso.org/standard/56581.html
ISO/IEC 27091	Artificial Intelligence — Privacy protection	Under development	https://www.iso.org/standard/56582.html
ISO/IEC TS 27110	Cybersecurity framework development guidelines	Edition 1 published in 2021	https://www.iso.org/standard/72435.html
ISOIEC TS 27115	Cybersecurity evaluation of complex systems — Introduction and framework overview	Under development	https://www.iso.org/standard/81627.html
ISO/IEC 27400	Cybersecurity — IoT security and privacy — Guidelines	Edition 1 published in 2022	https://www.iso.org/standard/44373.html
ISO/IEC 27402	Cybersecurity — IoT security and privacy — Device baseline requirements	Edition 1 published in 2023	https://www.iso.org/standard/80136.html
ISO/IEC 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics	Edition 1 published in 2024	https://www.iso.org/standard/78702.html
ISO/IEC 27404	Cybersecurity — IoT security and privacy — Cybersecurity labelling framework for consumer IoT	Under development	https://www.iso.org/standard/80138.html
ISO/IEC TR 27550	Security techniques — Privacy engineering for system life cycle processes	Edition 1 published in 2019	https://www.iso.org/standard/72024.html
ISO/IEC 27556	User-centric privacy preferences management framework	Edition 1 published in 2022	https://www.iso.org/standard/71674.html
ISO/IEC 27559	User-centric privacy preferences management framework	Edition 1 published in 2022	https://www.iso.org/standard/71677.html
ISO/IEC 27561	Privacy operationalisation model and method for engineering (POMME)	Edition 1 published in 2024	https://www.iso.org/standard/80394.html
ISO/IEC TR 27563	Security and privacy in artificial intelligence use cases — Best practices	Edition 1 published in 2023	https://www.iso.org/standard/80396.html
ISO/IEC TS 27564	Privacy protection - Guidance on the use of models for privacy engineering	Under development	https://www.iso.org/standard/89319.html
ISO/IEC 27566-1	Age assurance systems — Part 1: Framework	Under development	https://www.iso.org/standard/88143.html
ISO/IEC 27566-3	Age assurance systems Part 3: Benchmarks for benchmarking analysis	Under development	https://www.iso.org/standard/88147.html
ISO/IEC TS 27570	Privacy protection — Privacy guidelines for smart cities	Edition 1 published in 2021	https://www.iso.org/standard/71678.html
ISO/IEC 27701	Age assurance systems Part 3: Benchmarks for benchmarking analysis	Under development	https://www.iso.org/standard/85819.html
ISO/IEC 27706	Requirements for bodies providing audit and certification of privacy information management systems	Edition 2 under development	https://www.iso.org/standard/82894.html
ISO/IEC 29100	Security techniques — Privacy framework	Edition 2 published in 2024	https://www.iso.org/standard/85938.html
ISO/IEC 29134	Security techniques — Guidelines for privacy impact assessment	Edition 2 published in 2023	https://www.iso.org/standard/86012.html
ISO/IEC 29184	Online privacy notices and consent	Edition 1 published in 2020	https://www.iso.org/standard/70331.html
ISO/IEC 30141	Internet of Things (IoT) — Reference architecture	Edition 2 currently being published	https://www.iso.org/standard/88800.html

ISO/IEC 30145-1	Smart City ICT reference framework Part 1: Smart city business process framework	Edition 1 published in 2021	https://www.iso.org/standard/76371.html
ISO/IEC 30145-2	Smart City ICT reference framework Part 2: Smart city knowledge management framework	Edition 1 published in 2020	https://www.iso.org/standard/76372.html
ISO/IEC 30145-3	Smart City ICT reference framework Part 3: Smart city engineering framework	Edition 1 published in 2020	https://www.iso.org/standard/76373.html
ISO/IEC 30147	Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processe	Edition 1 published in 2021	https://webstore.iec.ch/en/publication/62644
ISO/IEC TS 30149	Internet of Things (IoT) - Trustworthiness principles	Edition 1 published in 2024	https://webstore.iec.ch/en/publication/67281
ISO/IEC 31303	Trustworthiness — Overview and concepts	Under development	https://www.iso.org/standard/84977.html
ISO 31700-1	Privacy by design for consumer goods and services - Part 1: High-level requirements	Edition 1 published in 2023	https://www.iso.org/standard/84977.html
ISO TR 31700-2	Privacy by design for consumer goods and services - Part 2: Use cases	Edition 1 published in 2023	https://www.iso.org/standard/84978.html
ISO/IEC 38500	Information technology — Governance of IT for the organization	Edition 3 published in 2024	https://www.iso.org/standard/81684.html
ISO/IEC 38505-1	Governance of IT — Governance of data	Edition 2 under development	https://www.iso.org/standard/87195.html
ISO/IEC 38507	Governance of IT — Governance implications of the use of artificial intelligence by organizations	Edition 1 published in 2022	https://www.iso.org/standard/56641.html
ISO/IEC TR 38509	Governance of IT – Responsible governance for social inclusion	Under development	https://www.iso.org/standard/89911.html
ISO/IEC TR 40141	Internet of Things (IoT) – Reference architecture guidance	Under development	URL not yet available[16]
ISO/IEC/IEEE 42024	Enterprise, systems and software — Architecture fundamentals	Under development	https://www.iso.org/standard/87510.html
ISO/IEC/IEEE 42030	Software, systems and enterprise — Architecture evaluation framework	Edition 1 published in 2019	https://www.iso.org/standard/73436.html
ISO/IEC/IEEE 42042	Enterprise, systems and software — Reference architectures	Under development	https://www.iso.org/standard/87310.html
IEC TS 62443-1-1	Network and system security - Part 1-1: Terminology, concepts and models	Edition 1 published in 2009	https://webstore.iec.ch/en/publication/7029
IEC TS 62443-1-5	Security for industrial automation and control systems - Part 1-5: Scheme for IEC 62443 security profiles	Edition 1 published in 2023	https://webstore.iec.ch/en/publication/67461
IEC 62443-2-1	Network and system security - Part 2-1: Establishing an industrial automation and control system security program	Edition 1 published in 2010	https://webstore.iec.ch/en/publication/7030
IEC TR 62443-2-3	Security for industrial automation and control systems - Part 2-3: Patch management in the IACS environment	Edition 1 published in 2015	https://webstore.iec.ch/en/publication/22811
IEC 62443-2-4	Security for industrial automation and control systems - Part 2-4: Security program requirements for IACS service providers	Edition 2 published in 2023	https://webstore.iec.ch/en/publication/67631
IEC TR 62443-3-1	Network and system security - Part 3-1: Security technologies for industrial automation and control systems	Edition 1 published in 2009	https://webstore.iec.ch/en/publication/7031
IEC 62443-3-2	Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	Edition 1 published in 2020	https://webstore.iec.ch/en/publication/30727
IEC 62443-3-3	Network and system security - Part 3-3: System security requirements and security levels	Edition 1 published in 2013	https://webstore.iec.ch/en/publication/7033
IEC 62443-4-1	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	Edition 1 published in 2018	https://webstore.iec.ch/en/publication/33615

[16] https://www.iec.ch/dyn/www/f?p=103:38:514154074248996::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:20486,23,126453

IEC 62443-4-2	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	Edition 1 published in 2019	https://webstore.iec.ch/en/publication/34421
IEC TS 62443-6-1	Security for industrial automation and control systems - Part 6-1: Security evaluation methodology for IEC 62443-2-4	Edition 1 published in 2024	https://webstore.iec.ch/en/publication/67462
IEC TS 62443-6-2	Security evaluation methodology for IEC 62443 - Part 4-2: Technical security requirements for IACS components	Under development	https://webstore.iec.ch/en/publication/67462
IEC 62278	Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)	Edition 1 published in 2002	https://webstore.iec.ch/en/publication/6747
IEC 63452	https://www.iec.ch/dyn/www/f?p=103:14:405172316768605::::FSP_ORG_ID:28802	Under development	https://www.iec.ch/ords/f?p=103:38:510103743024977::::FSP_ORG_ID,FSP_APEX_PAGE,FSP_PROJECT_ID:1248,23,109433