STANDARDISATION : PART 1

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 1

This document was 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 the ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection) committee[2]

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

The blog offers a comprehensive overview of existing standards, both at the domain and conformance assessment levels.

Background

The recent Crowdstrike outage[3] reminded us to what extent we can lack control over the complexity of computer systems.

What about our cybersecurity practice? This paper provides an overview of current standards, including at the domain level, as well as at the conformance assessment level. It then describes the new situation, in terms of cybersecurity frameworks, ecosystems and regulations, and ends with future projects concerning the variation of standards, architectures, and cybersecurity architectures.

Abbreviations

- ISO: International Organization for Standardization
- IEC: International Electrotechnical Commission
- JTC: Joint Technical Committee
- SC: Sub Committee

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

[2] https://www.iso.org/committee/45306.html

[3] The computer outage of July 19, 2024 was caused by a faulty update of Falcon Sensor, software from the cybersecurity company CrowdStrike. This defective update caused the blocking of 8.5 million computers and servers worldwide. It was estimated in August 2024 that the outage will cost $5.4 billion in damages to the 500 largest US companies (https://fortune.com/2024/08/03/crowdstrike-outage-fortune-500-companies-5-4-billion-damages-uninsured-losses/).

Overview of Current Standards

Cybersecurity for Information and Communication Technologies (ICT)

Standardization of cybersecurity for ICT mainly managed by the ISO/IEC JTC 1/SC 27 (Information security, cybersecurity and privacy protection) committee. The committee includes five main working groups:

- WG1: Information security management systems
- WG2: Cryptography and security mechanisms
- WG3: Security evaluation, testing and specifications
- WG4: Security Controls and Services
- WG5: Identity management and privacy technologies

SC 27 has published 245 standards, and is currently developing 70 standards. While it is not possible to describe all of them, we can cluster them according to the following topics:

- Standards on **organizational aspects** of information security management systems, with ISO/IEC 27001 on requirements, ISO/IEC 27002 on information security measures, or ISO/IEC 27005 on recommendations for risk management linked to information security information.
- Standards on **organizational aspects** of related to life cycles, with ISO/IEC 27110 on the development of cybersecurity frameworks, the ISO/IEC 27035 series on incident management, or ISO/IEC 6114 on security considerations throughout the product life cycle.
- Standards on **technology** such as
    - Blockchains and distributed ledger technologies (DLT), with ISO/IEC 23249 on identity management mechanisms using DLTs, ISO/IEC 23649 on trust anchors in DLT-based identity management systems, ISO/IEC 23244 and ISO/IEC 24946 on privacy, and ISO/IEC 25126 on security controls for DLTs.
    - Internet of Things, with ISO/IEC 27400 on security and privacy guidelines, ISO/IEC 27402 on baseline device requirements, ISO/IEC 27403 on IoT domotics, or ISO/IEC 27404 on a framework for cybersecurity labels of consumer products.
    - Artificial intelligence with ISO/IEC 27563 on use cases, ISO/IEC 27090 on security ISO/IEC 27091 on privacy.

The SC27 is also responsible for standards on privacy. We can also present them according to similar topics:

- Standards on **essential aspects** with ISO/IEC 29100 which describes the principles, and ISO/IEC 29134 which provides the guidelines for the privacy impact study.
- Standards on **organizational aspects** of privacy management systems, with ISO/IEC 27701 on requirements and guidelines.
- Standards on **operational aspects** relating to privacy engineering, often called "privacy-by-design", with the ISO 31700 series on requirements for consumer products, the ISO/IEC 27550 on the life cycle, the ISO/IEC 27561 on the operationalization of the principles, or ISO/IEC 27564 on recommendations on the use of models.
- Standards on **data de-identification** such as ISO/IEC 20889 (terminology and classification of data de-identification techniques for the protection of privacy) or ISO/IEC 27559 (Framework for data de-identification for the protection of privacy).

- Standards on **consent and preference management** with ISO/IEC 29184 (notices on privacy protection and online consent) or ISO/IEC 27556 (user-centered framework for managing privacy preferences).
- Finally, we will cite the standards relating to **age assurance** like ISO/IEC 27566 which can be used for instance to help protect minors from adult sites.

Cybersecurity in Vertical Domains

While ICT cybersecurity standards can be considered as common to all vertical domain, they are not sufficient. This is why specific standards have been developed at the vertical level:

- In the industrial field, standards of the IEC 62443 series[4], developed with the help of association such as ISA (International society of automation)[5] or WIB (user's association of instrumentation and process control)[6] cover the cybersecurity of industrial automation and control systems or IACS. This series is guided by functional safety concerns, takes into account the diversity of systems and associated consequences in the event of incident, organizational (maturity levels) and technical (security levels) aspects. It includes:
    - general standards with parts 1-1, 1-5,
    - methods and procedures standards parts 2-1, 2-2, 2-3, 2-4,
    - system standards with parts 3-1, 3-2, 3-3 and
    - component standards with parts 4-1, 4-2.

  IEC 62443 takes a system engineering vision with:

    - the concept of defense in depth which aims to distribute security measures according to security levels, and
    - a description of systems in zones and conduits: zones constitute domains with common security requirements, and conduits group interactions between two necessary zones and provide secure communication.

- Further to using the IEC 62443 series, the energy utility industry has also published ISO/IEC 27019 to provide guidance on the use of ISO/IEC 27002 applied to process control systems.
- In the automotive field, the United Nations UNECE R155 regulation published in 20217 calls for car manufacturers to certify their cybersecurity management systems. This certification is mandatory for vehicle approval. In order to support this certification, ISO and SAE worked on standards, initially starting from the context of functional safety standards[8], to develop ISO/SAE 21434 which focuses on cybersecurity engineering. Two other standards are under development, ISO/SAE 8475 which addresses cybersecurity assurance levels and target attack feasibility, and ISO/SAE 8477 on verification and validation of cybersecurity.
- the railway sector is currently developing IEC 63452 (Railway applications - cybersecurity) which aims to apply the principles of IEC 62443 to railway applications, by relying on a high-level life cycle of operational safety or railways applications as defined in EC 62278 (Railway applications - Specification and demonstration of reliability, availability, maintainability and safety), and by identifying the interplay and necessary exchanges of information between the cybersecurity process and the railway safety process.

[4] https://www.iec.ch/blog/understanding-iec-62443

[5] https://www.isa.org/

[6] https://www.wib.nl/

[7] https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[8] Supported by the ISO 26262 standard (Road vehicles – Functional safety) published in 2011.

- Other domains also have their own standards (railway, aeronautics, medical devices). They all show the need for a system, lifecycle and architecture perspective, which we will cover in the coming blog about standardisation.

Conformity Assessment

Conformity assessment is carried out by CASCO[9], the ISO committee that develops policy guidance and publishes standards on conformity assessment. Many of the published document are common to ISO and IEC. In short, *conformity assessment* focuses on verifying that requirements specified in a standard are met. It starts with an *object of conformity assessment*, which is the entity to which the specified requirements apply. Conformity assessment activities aim to provide confidence in the object of conformity.

CASCO provides strict rules on the principle of separation between requirements to be evaluated, and requirements of the evaluation process itself[10].

In terms of ICT cybersecurity, we can cite the following standards:

- For compliance with ISO/IEC 27001 on information security management systems, ISO/IEC 27006 on the requirements for bodies providing audit and certification of information security management systems.
- For compliance with ISO/IEC 27701 on privacy management systems, ISO/IEC 27706 on the requirements for bodies providing audit and certification of privacy information management systems.
- For information technology security compliance, ISO/IEC 15408 series on evaluation criteria for IT security, and ISO/IEC TS 27115 on cybersecurity assessment of complex systems.

At the level of business areas

- For compliance with IEC 62443 in the industrial field, evaluation standards have been added with part 6-1 on the evaluation of requirements of part 2-4 concerning IACS service providers and part 6-2 on the evaluation of requirements of Part 4-2 relating to IACS components.
- For compliance with ISO/SAE 21434 in the automotive field, ISO 5112 which provides guidelines for auditing cybersecurity engineering

These standards are used as references for the implementation of certification programs such as those of AFNOR for ISO/IEC 27001 certifications.[11] or ISO/IEC 27701[12], that of ANSSI for common criteria (ISO/IEC 15408)[13], that of the IECEE[14] for IEC 62443, or that of TÜV NORD[15] for ISO/SAE 21434.

[9] https://www.iso.org/fr/casco.html

[10] clause 33 of part 2 of the ISO directives: https://www.iso.org/sites/directives/current/part2/

[11] https://certification.afnor.org/numerique/certification-iso-27001

[12] https://certification.afnor.org/numerique/iso-27701-protection-vie-privee

[13] https://cyber.gouv.fr/comprendre-la-certification

[14] IEC System for Conformity Assessment Schemes for Electrotechnical Equipment and Components: https://www.iecee.org/certification

[15] https://www.tuev-nord.de/en/company/certification/services/isosae-21434/

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