CISSAN

Collective intelligence supported by security aware nodes

D7.1 CISSAN Standardization Action Plan

Editors: Ilgin Safak (contact: ilgin.i.safak@jyu.fi), JYU, and Kurt Tutschku (contact: kurt.tutschku@bth.se), BTH

Abstract

This report outlines CISSAN's Standardization Action Plan. The plan discusses strategies, priorities, and activities pertaining to project alignment with abiding standards and best practices, regulatory frameworks, and standards through the project's lifecycle. From CISSAN's technical scope, the action plan mentions relevant standards and standardization bodies pertaining to the areas of cybersecurity, threat intelligence sharing, and post-quantum cryptography. It illustrates the gaps and the ways standardization needs are fulfilled across work packages and use cases. It outlines the methods to analyse the progress of standardization, collaborate to edits, and certify that the outcomes of the project are compliant, ready for the industry, and interoperable. The plan prioritizes standardization activities to facilitate CISSAN results be deployed in real-world situations, and improves the enduring standardization of the project's solutions, along with their interoperable and competitive advantages.

Project CISSAN

Public Report

April 2025

Participants in project CISSAN are (in alphabetical order with project coordinator first):

- University of Jyväskylä (coordinator)
- Affärsverken Karlskrona AB
- Arctos Labs
- Bittium Biosignals Ltd
- Bittium Wireless Ltd
- Blekinge Tekniska Högskolan
- Blue Science Park
- Clavister AB
- Councilbox Ltd
- Geodata ZT GmbH
- Mattersoft
- Mint Security Ltd
- Netox Ltd
- Nodeon Ltd
- Savantic AB
- Scopesensor Ltd
- Techinova AB
- Wirepas Ltd

CISSAN-Collective intelligence supported by security aware nodes

D7.1 CISSAN Standardization Action Plan

Editors: Ilgin Safak, University of Jyväskylä and Kurt Tutschku, Blekinge Tekniska Högskola (BTH)

Project coordinator: Ilgin Safak, University of Jyväskylä

CELTIC published project result

Executive Summary

This document defines the CISSAN Standardization Action Plan, which is CISSAN's strategy for aligning the CISSAN platform with existing and emerging cybersecurity standards to ensure secure, interoperable, and industry-ready solutions. The objective of the standardization plan is to ensure that the platform complies with relevant security regulations and best practices while remaining adaptable to future technological and regulatory developments.

First, the document identifies and reviews key international cybersecurity standards and regulatory frameworks relevant to the project. These include general cybersecurity management frameworks, IoT and industrial control system security standards, artificial intelligence governance frameworks, sensor data standards, communication protocols, and emerging post-quantum cryptography (PQC) standards. Major standardization bodies considered include National Institute of Standards and Technology (NIST), International Organization of Standardization (ISO)/ International Electrotechnical Commission (IEC), European Telecommunications Standards Institute (ETSI), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), and International Telecommunication Union-Telecommunication Standardization Sector (ITU-T). The plan also evaluates how these standards apply to the architecture and components of the CISSAN platform and its use cases.

To guide the standardization effort, the report analyses five representative CISSAN use cases: transportation systems with Global Navigation Satellite System (GNSS) anomaly detection, smart energy grids, tunnel construction, manufacturing execution systems, and a joint multi-domain scenario involving coordinated cyber-defence across Internet of Things (IoT) and Operational Technology (OT) environments. These use cases illustrate how the platform can detect anomalies, secure sensor data, enable distributed security monitoring, and support coordinated incident response across heterogeneous infrastructures.

A compliance assessment and gap analysis were conducted to evaluate the alignment of the CISSAN platform components with relevant standards. The analysis shows that many components already follow widely accepted cybersecurity frameworks such as ISO/IEC 27001, IEC 62443, and the Network and Information Systems (NIS) 2 directive. However, some components remain at the prototype stage and will require further hardening, certification, or extended compliance activities before deployment in operational environments.

Based on this gap analysis, the standardization action plan identifies two strategic areas for future development. First, the project explores the use of Structured Threat Information eXpression (STIX) for standardized sharing of cybersecurity threat intelligence across distributed systems. Second, the project assesses the feasibility of integrating PQC mechanisms to ensure long-term cryptographic resilience for IoT and OT systems with long operational lifetimes.

The plan also defines governance mechanisms and responsibilities for standardization activities across the project consortium, ensuring coordinated contributions to relevant standards and alignment between research outcomes and industry practices.

List of Authors (in alphabetical order according to partner name)

- Jari Partanen, Bittium
- Jianguo Ding, BTH
- Kurt Tutschku, BTH
- Anders Liden, Clavister
- Rodrigo Martinez, Councilbox
- Klaus Chmelina, GeoData
- Teemu Kemppainen, Mattersoft
- Ann Sjökvist, Mint Security
- Oliver Bölin, Techinova
- Kristian Kratschmer, Techinova
- Ilgin Safak, University of Jyväskylä

Table of Contents

Abbreviations

AI	Artificial intelligence
ANSI	American National Standards Institute
CIA	Confidentiality, Integrity and Availability
CISSAN	Collective intelligence supported by security aware nodes
CoAP	Constrained Application Protocol
CRA	Cyber Resiliency Act
CRYSTALS	Cryptographic Suite for Algebraic Lattices
CSA	Cybersecurity Act
CSF	Cybersecurity Framework
DevSecOps	Development, Security, and Operations
DLT	Distributed Ledger Technology
DRM	Digital Rights Management
ETSI	European Telecommunications Standards Institute
ETSI EN	ETSI European Standard
FIPS	Federal Information Processing Standards
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human-Machine Interface
HTTP	Hypertext Transfer Protocol
IAM	Integrated Access Management
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKEv2	Internet Key Exchange version 2
IoT	Internet of Things
IP	Internet Protocol
ISG QSC	Industry Specification Group on Quantum-Safe Cryptography
ISA	International Society of Automation
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector
ITxP	Information Technology for Public Transport
JTC	Joint Technical Committee
LTE	Long-Term Evolution
ML-DSA	Module-Lattice-Based Digital Signature Algorithm
ML-KEM	Module-Lattice Key Encapsulation Mechanism

MQTT	Message Queuing Telemetry Transport
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
NISTIR	NIST Internal Report
OGC	Open Geospatial Consortium
O&M	Observations & Measurements
OTN	Optical Transport Network
PASAD	Process Aware Stealthy Attack Detection
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PQC	Post Quantum Cryptography
RACI	Responsible Accountable Consulted Informed
REST	Representational State Transfer
RFC	Request for Comments
RTU	Remote Terminal Unit
SC	Subcommittee
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SLH-DSA	Stateless Hash-Based Digital Signature Algorithm
SOAR	Security Orchestration, Automation, and Response
SPHINCS	Stateless Practical Hash-based Incredibly Nice Cryptographic Signature
SSL	Secure Sockets Layer
STIX	Structured Threat Information eXpression
SWE	Sensor Web Enablement
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
TRL	Technical Readiness Level
TS	Technical Specification
UC	Use Case
UDP	User Datagram Protocol
VDSL	Very-high-bit-rate Digital Subscriber Line
VLAN	Virtual Local Access Network
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WP	Work Package
3GPP	3rd Generation Partnership Project

1 Introduction

Security standards aim to protect data, systems, and users while managing risk and ensuring compliance in a consistent, auditable manner.

Furthermore, in general, standards aim at interoperability and the sustainability of systems. Different parts and functions of a system can interact through standardized communication. Thus, parts are becoming interoperable because of their functionality and behaviour are being well-defined. In addition, standards enable parts of a system to be implemented by different vendors, implying that these implementations produce the same results.

The ambition of the work package 7 (WP7) is to support the design of the CISSAN platform by facilitating a concise process that identifies the platform's compliance to current security standards and directives as well as the contribution of new parts of existing standards or even the creation of new standards at large. This support is obtained by the specification of a *standardization activity plan* for managing compliance and for creating new standards or standard parts.

A major challenge in organizing and managing standardization activities in the CISSAN, however, is the project's fundamental ambition to develop novel structures and solutions that advance the state of the art, e.g., in collective intelligence. Hence, an early structuring of the part into parts, functions, or architectural roles is typically not readily available. Furthermore, different design processes, e.g., agile or waterfall, require different implementation time scales.

In order to achieve the CISSAN ambition to guide the system design with respect to standards, the WP7 has three aims: a) provide a structured list of current security standards and directives that are addressed in the CISSAN platform*, b)* defined a "standardization activity plan" base on the understanding of what kind of standards are addressed ye by the CISSAN architecture and based on a gap analysis expect for the novel part of the CISSAN system, and, finally, *c)* provide a concise follow up on the activity plan for the different CISSAN work packages.

The deliverable D7.1 implements the first two steps of the above-mentioned process. In the first step, the D7.1 identifies and discusses the current security standards and directives available in the platform and required by the use cases. Hereby, D7.1 lays major focus on the *security gap analysis* of CISSAN platform components for data collection (WP4), distributed security intelligence (WP5) and foundational CISSAN functions and architecture features (WP2 and WP6). The second step comprises the specification *standardization activity plan*.

This document is structured as follows:

- Section 2 provides, in Section 2.1, a brief overview of the general objectives of security standards. Section 2.2 structures the area of security standards relevant to CISSAN, and Section 2.3 specifies the CISSAN project's process to derive a standardization action plan.

- Section 3 discusses, in Section 3.1, the security objectives and area of security concern of the CISSAN use case and architecture. Section 3.2 lists the compliance of the CISSAN systems with security standards and provides a gap analysis for identifying the required actions in the action plan for technologies in CISSAN

- Section 4 specifies the CISSAN Standardization Action Plan

- Finally, Section 5 provides the conclusions of the report.

2 Cybersecurity Standards Engineering for the CISSAN Platform

The CISSAN standardization action plan outlines important standardization activities in the CISSAN platform and its use case solutions. The activities comprise design and implementation tasks that include a) CISSAN technologies that are compliant to current security standards, and b) also activities that enhance CISSAN technologies to be compliant with future security requirement. To facilitate these activities, it is important to understand the general aims and categories of security design objective and processes. In this section, we detail the importance of cybersecurity standards in the design.

2.1 Building a Standardization Action Plan

2.1.1 Objectives of Security Standards and Regulations

In general, the objectives of security standards in information technology (IT) systems are to protect information, systems, and users in a consistent, reliable, and measurable way. Typically, these characteristics comprises three area of security concerns in IT systems: a) detailing the information security attributes, i.e. techniques enabling the consistent consideration security features like the Confidentiality, Integrity, and Availability (CIA) triad, b) the concept for security-by-design, i.e. the application of design pattern and techniques to avoid or reduce the risk of security vulnerabilities, and c) the generation of trust and confidence into the system by providing measurable and observables security features or certifications.

In practice, they focus on three core objectives:

A) Security Features:

1. **Protect confidentiality:** Ensure that information is only accessible to authorized users (e.g., access controls, encryption).

2. **Maintain integrity:** Prevent unauthorized modification or destruction of data, and ensure information remains accurate and trustworthy.

3. **Ensure availability:** Make sure systems and data are accessible to authorized users when needed (e.g., redundancy, backups, disaster recovery).

B) Security Design Concepts and Patterns:

4. **Reduce risk and vulnerabilities:** Provide software pattern, best practices or to identify, assess, and mitigate security risks systematically.

5. **Establish consistency and best practice:** Create a common framework so organizations implement security controls in a standardized and proven way rather than ad hoc solutions.

6. **Enable continuous improvement:** Encourage regular review, monitoring, and updating of security controls as threats and technologies evolve.

C) Measurability and Verification of Security Compliance

7. **Support legal and regulatory compliance:** Help organizations meet laws and regulations (such as data protection, privacy, and industry-specific requirements).

8. **Improve trust and confidence:** Demonstrate to customers, partners, and stakeholders that security is taken seriously and managed professionally.

In short, security standards aim to protect data, systems, and users while managing risk and ensuring compliance in a consistent, auditable manner.

2.1.2 Deriving the CISSAN Standardization Action Plan

The identification of security requirements and of security standards, is general a challenging task. The engineering process typically depends on the system's function, the system's architecture, the system's use case, and the threads to the systems. The use of the security design concepts such as security-by-design [1] and Development, Security, and Operations (DevSecOps) [2] are desirable. However, their execution and implementation in the context of the CISSAN use cases are not trivial. Moreover, security concepts should be implemented throughout every element of the CISSAN platform. Moreover, this generalized "everywhere" approach would entail a likely significant amount of implementation effort, which may divert work from CISSAN platform development.

The concrete security requirements and their compliance mapping, derived from CISSAN use-cases' security requirement specifications provided in the annexes of the CISSAN deliverable D2.3 report, are presented in Section 3.

Challenges in CISSAN Security Requirements Engineering and Standards

The challenges on these concepts arise from the CISSAN project's ambition to implement a *continuous design* process through the lifetime of the project to obtain a *generalizable CISSAN platform.*

The CISSAN platform has the ambition to be reusable, relevant for real-world challenges, and to address the diversity of the CISSAN use cases. All these use cases (public transportation, smart grids, tunnel construction, Bittium manufacturing execution system and automated disaster recovery/joint use case) are of high technical readiness level (TRL), however still may differ in the details and TRL.

An extensive security-by-design approach for security engineering for the whole platform, e.g., using the waterfall design model considering the many uses cases may be inefficient [3]. Although Github is used for version control, full DevSecOps practices have not yet been adopted since the CISSAN platform is not yet production-ready.

Another challenge is the characteristic that Internet of Things (IoT) security standards, regulations and best practices are typically defined by a very large number of stakeholders. These stakeholders comprise standardization-defining organizations, denoted as SDOs, such as National Institute of Standards and Technology (NIST), Internet Engineering Task Force (IETF), European Telecommunications Standards Institute (ETSI), and International Organization for Standardization (ISO). However, de facto standards and best practices are often also created by industrial players such as Pivot Point Security, SecuriThings, Mint Security, or Bittium. This large number of players and standards makes it difficult to identify the relevant ones a-priori, i.e., not exclude important ones.

Finally, IoT standards may need to address the unique challenges of IoT system like limited resources and vast scale. Hence, they focus on a few specific security functions, such as authentication, encryption, software updates, data locality for privacy, and trusted execution environments. Moreover, only a few comprehensive IoT standardization frameworks exist, such as ETSI Technical Specification (TS) 103645 for consumer IoT, NIST frameworks for federal use, and the ISO / International Electrotechnical Commission (IEC) 27400:2022 for IoT security and privacy. However, an inspection of these frameworks reveals, as for the case of ISO/IEC 27400:2022, that they are mainly applicable for IoT devices only (see Annex A of ISO/IEC 27400:2022) rather than for the security design of IoT systems or platforms.

The above discussion outlines that typical security design processes, i.e., ones using the waterfall model or processes based on the DevSecOps concept have their own rights but are of limited use for the CISSAN project. The project has high ambitions on platform capabilities, cybersecurity and in the diversity in security needs, while being realistic in achieving relevant results. All in all, it can be stated that a clear choice for a security design process is not yet available.

The Process for Security Engineering and Security Standards of the CISSAN Platform

The CISSAN uses case are highly detailed, and their security requirements are defined clearly. Further, the representation of the use cases on the CISSAN platform bear the opportunity to demonstrate the commonality of functions and their security needs, including their security requirements, e.g., for decision making, trust management, orchestration, or encryption. Although certain regulations and security standards in the CISSAN use cases are complex and extensive, their diversity enables the CISSAN project to identify the most relevant requirements to address.

2.2 Considered Areas of Security Standards and Regulations

This section provides an overview of the international standards landscape considered in developing the CISSAN Standardization Action Plan. Please see Annex A for more details on standards and standardization organizations relevant to CISSAN.

The standards and regulatory frameworks reviewed for CISSAN span eight technical domains: general cybersecurity, IoT security, industrial control systems (ICS), distributed ledger technology (DLT), artificial intelligence (AI), sensor data, post-quantum cryptography (PQC), and data communications. The review covers publications from the world's leading standardization bodies, including ETSI, NIST, IEEE, ISO/IEC, IETF, ITU-T (International Telecommunication Union - Telecommunication Standardization Sector), American National Standards Institute (ANSI), and Open Geospatial Consortium (OGC). An important practical distinction is that NIST, IETF, and ETSI publications are freely accessible, while ISO/IEC, IEEE, and ANSI standards typically require purchase.

2.2.1 General Cybersecurity Frameworks

The foundation of the standards landscape is formed by a set of broadly applicable cybersecurity frameworks and management standards. The NIST Cybersecurity Framework (CSF) 2.0 is widely regarded as the most influential global risk management tool, structured around the core functions of Govern, Identify, Protect, Detect, Respond, and Recover. It is complemented by NIST SP 800-53, a comprehensive catalog of security and privacy controls for information systems, and NIST SP 800-63, which provides guidelines for digital identity, authentication, and federation.

On the international side, ISO/IEC 27001 defines requirements for an Information Security Management System (ISMS), with ISO/IEC 27002 providing accompanying security controls and ISO/IEC 27005 addressing information security risk management. ISO/IEC 15408 (Common Criteria) offers a globally recognized framework for the security evaluation of IT products and systems. Together, these standards establish the compliance of the backbone upon which more specialized domain-specific frameworks are built.

2.2.2 IoT and Industrial Control Systems Security

The security of connected devices and operational technology environments requires standards tailored to their specific constraints and risk profiles. For consumer and industrial IoT, ETSI European Standard (EN) 303 645 establishes 13 baseline security provisions, including prohibiting the use of default passwords and mandating vulnerability disclosure mechanisms, and forms the basis for numerous national and regional IoT certification schemes. NIST Internal Report (NISTIR) 8259 provides complementary guidance for IoT device manufacturers on foundational cybersecurity activities across the device lifecycle. ISO/IEC 27400 and the forthcoming ISO/IEC 27030 extend these principles to cover security and privacy in IoT systems more broadly. At the protocol level, IETF Request for Comments (RFC) 9019 defines a manifest format for secure firmware updates on constrained IoT devices.

For ICS operating in critical infrastructure, including power grids, water treatment facilities, and manufacturing environments, the ISA/IEC 62443 series is the most comprehensive internationally recognized standard. It addresses security across four dimensions: general concepts and models, security management policies and procedures, system-level risk assessment and design, and component-level technical requirements for devices such as Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Human-Machine Interfaces (HMIs). NIST SP 800-82 provides a dedicated ICS/SCADA security guide, and IEEE 1711.2 specifies cryptographic protection for serial communications in electrical substations.

2.2.3 Distributed Ledger Technologies, and Artificial Intelligence

In the domain of DLT, ISO/TC 307 leads international standardization with foundational publications covering vocabulary (ISO 22739), reference architecture (ISO 23257), smart contract interactions (ISO/TR 23455), and security management for digital asset custodians (ISO/Technical Report (TR) 23576). IEEE standards address blockchain consensus processes (IEEE 2140.1) and Digital Rights Management (DRM) frameworks (IEEE 2144.1). ITU-T's X.1400 series covers DLT security frameworks and privacy protection, while NIST contributes research reports on blockchain technology (NISTIR 8202) and cross-chain interoperability (NISTIR 8401).

AI standardization is led by ISO/IEC JTC 1/SC 42, which has produced the landmark ISO/IEC 42001:2023, the world's first AI Management System standard, analogous in scope to ISO 27001 for information security. Complementary standards address AI concepts and terminology (ISO/IEC 22989), ML system frameworks (ISO/IEC 23053), bias mitigation (ISO/IEC TR 24027), trustworthiness (ISO/IEC TR 24028), and AI-specific risk management (ISO/IEC 23894). NIST's AI Risk Management Framework (AI RMF 1.0) is one of the most widely adopted global tools for governing AI risk. IEEE provides engineering-based guidance on ethical AI design (IEEE 7000) and well-being impact assessment (IEEE 7010), while ETSI's Industry Specification Group on Securing AI (ISG SAI) addresses data supply chain security for AI systems.

2.2.4 Sensor Data Standards

Sensor data standardization addresses performance characterization, device interoperability, and secure data transmission. IEEE 2700 defines common performance parameters and units for a wide range of sensor types, enabling consistent comparison across vendors. The IEEE 1451 family of standards specifies smart transducer interfaces, allowing sensors and actuators to be connected to networks and instrumentation systems through standardized communication protocols and electronic data sheets (TEDS).

For data transmission in IoT environments, IETF RFC 8428 (SenML) provides a lightweight and efficient data model for encoding sensor measurements in Representational State Transfer (REST) APIs, while RFC 7252 (CoAP) defines a purpose-built application protocol for constrained devices operating over low-bandwidth networks. The OGC's Sensor Web Enablement (SWE) suite, including SensorML for describing sensor systems and the Observations & Measurements (O&M) model for encoding sensor output, supports discoverability and web accessibility of sensor data, which is particularly relevant for geospatial and environmental monitoring applications.

2.2.5 Post-Quantum Cryptography

PQC represents one of the most critical and rapidly advancing areas of current standardization activity, driven by the long-term threat that quantum computing poses to widely deployed public-key cryptographic systems. NIST's multi-year PQC Standardization Project has concluded its selection process and is finalizing three Federal Information Processing Standards: Federal Information Processing Standards (FIPS) 204 (Module-Lattice Key Encapsulation Mechanism (ML-KEM), based on Cryptographic Suite for Algebraic Lattices (CRYSTALS)-Kyber) for key encapsulation, FIPS 203 (Module-Lattice-Based Digital Signature Algorithm (ML-DSA), based on CRYSTALS-Dilithium) for digital signatures, and FIPS 205 (Stateless Hash-Based Digital Signature Algorithm (SLH-DSA), based on Stateless Practical Hash-based Incredibly Nice Cryptographic Signature (SPHINCS+)) as a stateless hash-based signature alternative.

ISO/IEC Joint Technical Committee (JTC) 1/ Subcommittee (SC) 27 is amending existing cryptography standards (ISO/IEC 14888-3 and ISO/IEC 18033-2) to incorporate the NIST-selected algorithms, and new standalone standards for additional algorithms are under development. ETSI's Industry Specification Group on Quantum-Safe Cryptography (ISG QSC) is producing migration guidance to support organizations in transitioning from classical to quantum-safe cryptographic solutions. The IETF is actively integrating PQC into core internet protocols, including specifications for hybrid key exchange in Transport Layer Security (TLS) 1.3 and PQC algorithm identifiers for X.509 certificates.

2.2.6 Data Communication Standards

Data communication standards provide the technical infrastructure upon which all networked systems depend. The IETF's Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite — encompassing IP (RFC 791), TCP (RFC 793), UDP (RFC 768), HTTP/1.1 and HTTP/2, and TLS 1.3 (RFC 8446), defines the foundational protocols of the internet. At the physical and data link layers,

IEEE 802.3 (Ethernet) and IEEE 802.11 (Wireless Fidelity (Wi-Fi)) govern wired and wireless local area networking, while IEEE 802.1Q (Virtual Local Access Networks (VLANs)) and 802.1X (network access control) provide network management and authentication capabilities.

ITU-T's G-series standards cover global optical and digital transport infrastructure, including the Optical Transport Network (OTN, G.709) and Very-high-bit-rate Digital Subscriber Line 2 (VDSL2) (G.993.2), while the X-series includes X.509, the foundational standard for public key infrastructure (PKI) and digital certificates used to secure TLS/Secure Sockets Layer (SSL) communications. ETSI supports the 3GPP-defined mobile communication standards for LTE and 5G networks. For government and security-sensitive applications, NIST FIPS 140-3 mandates security requirements for cryptographic modules, and NIST SP 800-52 provides guidance on TLS implementation to ensure secure data communications in federal information systems.

2.3 Creating a Standardization Action Plan

A standardization action plan identifies activities to be conducted in a project to ensure that the generated solution or platform complies with current and future standards. While compliance with existing standards is typically a verification process, the platform's readiness for future standards is difficult to assess in practice: the future standards are typically not yet defined (as per their definition), and parts of the system that should implement these systems are not yet designed. Hence, it is more likely that enhancements to current standards replace the ambition to comply with new standards. For this purpose, two main approaches are planned to be followed in the creation process of a standardization action plan for the CISSAN project:

- Ensure the compliance of the platform towards existing standards (“current view”)
- Assess the capability of current security standards leading to new standards (“future view”)

This involves the following activities for the platform architecture, elements and use cases in the CISSAN project: a) identifying relevant standards and the requirements, b) elaborating the rationale and origin of the requirements (”anchoring”, ”threat model”), and c) identifying gaps by performing a gap analysis and prioritizing standardization activities with the highest risk reduction and impact

In CISSAN, the so-called “current view” targets well-defined security objectives, threat assumptions, and regulatory context for each use case and provide a concrete baseline for aligning platform components with applicable standards such as ISO/IEC 27001:2022, IEC/ISA 62443, NIS 2, and ITxP. The “current” standardization activities and requirements are therefore real-world-driven and use-case-focused, ensuring traceability between operational security needs and selected standards. The “future” view is based on hypotheses and projections into future capabilities of the CISSAN platform.

The detailed steps involved in carrying out the standardization action plan is summarized in Figure 1.

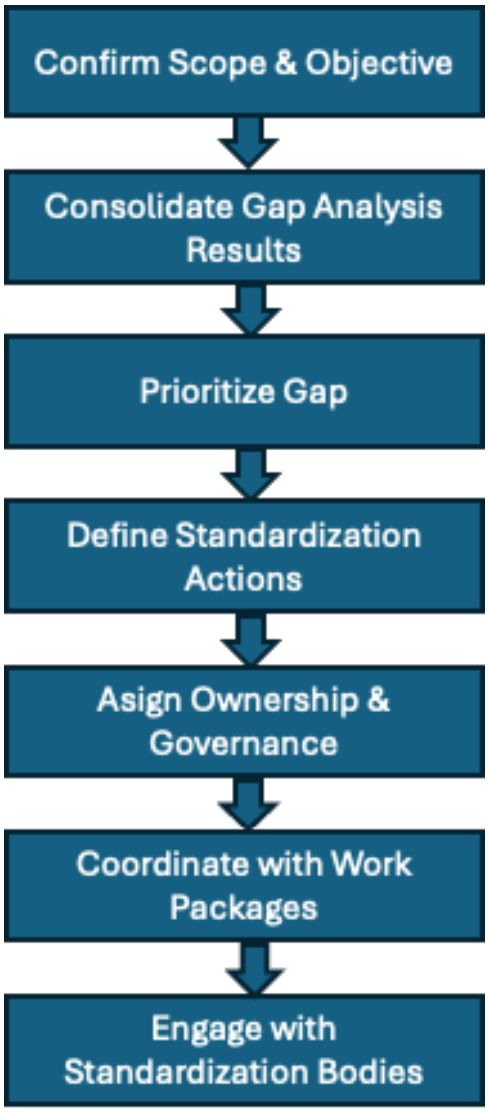

Figure 1. Frame and Phases of the Standardization Action Plan

3 CISSAN's Security Standards Compliance, and Gap Analysis

In this section, the compliance of the CISSAN platform and its use case solutions with applicable security standards and regulations are assessed. This allows the identification of applicable security regulations, security requirements for the secure deployment and operation of the CISSAN platform and its use case solutions. The gap analysis with the applicable security standards and regulations is performed, which ensures the identification of gaps in the proposed system in comparison with the best practices in the field. This will enable the secure deployment of the system in critical infrastructures, which requires compliance with the applicable security regulations and regulations in the EU.

3.1 Security Standards and Requirements of the Platform and Use Cases

3.1.1 The CISSAN Platform and its Use Cases

3.1.1.1 Use Case 1 - Transportation

Use Case 1 (UC1) focuses on detecting Global Navigation Satellite System (GNSS) anomalies in public transport environments. Due to practical reasons, the focus is on GPS (Global Positioning System). The use case demonstrates how positioning data from public transport vehicles can be analysed to detect spoofing, jamming, or inconsistent GNSS behaviour. The goal is to improve resilience and situational awareness for positioning-dependent services used in transport operations.

Within the CISSAN platform, the transport use case combines onboard GNSS positioning data, backend analysis components, and secure communication interfaces for anomaly reporting. GNSS data streams are analysed for irregular patterns, such as unrealistic position jumps or signal loss, and anomaly alerts are transmitted through the platform using MQTT-based messaging.

The main components involved in the use case include onboard GNSS receivers in vehicles, backend processing and anomaly detection logic, logging and monitoring systems, and secure communication interfaces used for telemetry and alerting. The security requirements and compliance considerations therefore apply to networked transport devices, backend services, communication interfaces, and monitoring components of the CISSAN platform.

3.1.1.2 Use Case 2 – Smart grids

Context

Smart energy grids are classified as critical infrastructure in Europe and are subject to strict cybersecurity and resilience requirements.

Use Case 2 aligns with:

- NIS2 directive: *Requires energy operators to implement cybersecurity risk management, incident detection, and reporting*

  → CISSAN supports early detection of cyber threats in grid environments through AI-based anomaly detection

- EU CER (Critical Entities Resilience) directive: *Strengthens resilience obligations for essential services, including energy transmission and distribution*

  → CISSAN enhances resilience by enabling distributed, security-aware monitoring across grid nodes

Impact: The project contributes directly to Europe's objectives for protecting essential energy services against cyber threats

Societal Impact: Secure and resilient energy systems

Electric power grids form the backbone of modern society. Healthcare, transportation, water supply, communications, and industry all depend on the availability of reliable electric energy. As energy systems become increasingly digitalized and interconnected, they also become more exposed to cyber threats.

CISSAN Use case 2 contributes to societal resilience by:

- Improving early detection of cyber incidents in smart energy grids
- Supporting faster response to disruptions
- Reducing risk of large-scale power outages
- Increasing trust in digitalized energy infrastructure

By strengthening monitoring and protection capabilities in line with European cybersecurity requirements such as the NIS2 Directive, the project directly supports the continuity of essential services for citizens and businesses.

In practical terms, this means fewer disruptions, reduced economic impact, and improved public safety in the event of cyber incidents targeting critical infrastructure.

Strategic contribution to European digital sovereignty

The protection of energy infrastructure is closely linked to Europe's digital sovereignty and strategic autonomy. As smart grids evolve, they rely increasingly on AI, distributed systems, and interoperable technologies.

CISSAN contributes strategically by:

- Advancing European expertise in AI-driven cybersecurity for critical infrastructure
- Supporting implementation of standards such as IEC62443 and ISO27019
- Strengthening Europe's capability to secure its own critical digital and energy ecosystems
- Supporting harmonized regulatory compliance under frameworks such as Critical Entities Resilience Directive

By aligning technological innovation with European regulatory frameworks and industrial standards, the project reinforces Europe's capacity to develop secure, trustworthy, and resilient energy systems without over-reliance on non-European security solutions.

OT (Operational Technology) security standards

Modern energy grids rely on industrial control systems and substation automation technologies. These are governed by internationally recognized standards.

- IEC62443: *Global standard for securing industrial automation and control systems*
  - → CISSAN supports this framework by adding intelligent detection capabilities within secure grid architectures
- IEC62351: *Defines cybersecurity measures for power system communications*
  - → CISSAN complements these protections by detecting abnormal communication patterns even when traffic is secured.

Impact: The project strengthens practical implementation of established OT security standards.

Security governance in the energy sector

Energy utilities commonly implement sector-specific information security controls.

- ISO27001: *Information Security Management System standard*
- ISO27019: *Tailored security controls for energy generation, transmission, and distribution*

CISSAN provides monitoring and detection capabilities that support continuous risk management and compliance within these frameworks

Interoperability and automation within smart grids

Smart grids depend on standardized communication and automation protocols.

- IEC61850: *Core standard for substation communication and automation*
- IEEE2030: *Framework for interoperability across smart grid systems*

CISSAN contributes by enabling secure and intelligent monitoring across interoperable grid components.

Summary of overall contribution to standardisation in use case 2

CISSAN use case 2 does not replace existing standards. Instead, it:

- Reinforces compliance with European cybersecurity regulation
- Enhances resilience of critical energy infrastructure
- Supports implementation of internationally recognized OT security standards
- Contributes to future evolution of AI-enabled protection mechanisms within smart grids

In summary, the project strengthens Europe's ability to protect energy systems in line with current regulatory and standardization frameworks.

CISSAN use case 2 strengthens the cybersecurity and resilience of European smart energy grids by integrating AI-based, distributed anomaly detection into critical infrastructure environments. The approach complements established industrial standards such as IEC62443 and sector-specific governance frameworks like ISO27019, while supporting regulatory obligations under the NIS2 directive and the Critical Entities Resilience directive.

By enhancing early threat detection and enabling security-aware collaboration between grid nodes, the project contributes to the protection of essential energy services, reduces the risk of large-scale disruptions, and reinforces Europe's strategic capability to secure its critical digital infrastructure.

In summary, CISSAN demonstrates how advanced European research in collective intelligence and AI can directly support regulatory compliance, industrial standards implementation, and long-term societal resilience in the energy sector.

3.1.1.3 Use Case 3 – Tunnel Construction

In use case 3 (UC3) it is shown how a data tampering attack on tunnel monitoring data (sensor time series data) is detected and the affected data excluded from further decision making and processing. Detection is based on a data quality verification method that continuously calculates believability scores of data quality parameters (e.g., accuracy, noise, timeliness, frequency, trend similarity, completeness) and alerts any conflict with believability thresholds. Such conflicts are assumed to be signs of either data tampering attacks or operational issues. A second attack detection method uses the Lightning Network for enabling a parallel, multi-party/multi-channel transfer of data from a tunnel monitoring sensor to the central data management server. The thus established redundant data transfer allows for checking that data has not been tampered during transfer/along their route from sensor to server. The method also allows for the permanent anchoring and proof of evidence of monitoring data and attack events in the Bitcoin Blockchain. Finally, a data signing method has been developed that uses security chips to sign data already at creation/at the sensor and to verify the signature before data use.

The system components in the CISSAN platform relevant to UC3 are listed below.

- Networked Devices
- Management Server
- Orchestration Server
- Security Information and Event Management (SIEM) Server
- Councilbox Blockchain System

The relevant system components in the UC3 system include the following:

- Geodata Data Quality Verification System
- Geodata Blockchain System (based on Lightning Network)
- Geodata Data Signing System (based on Infineon Security Chips)

3.1.1.4 Use Case 4 – Manufacturing Execution System

In use case 4 (UC4), security functions are distributed within the Bittium manufacturing execution system (BMES) system, its interoperability partners and part manufacturers. The manufacturing itself is executed by manufacturing partners. The full system is containerized and able to be scaled up to consisting of several hundreds of containers, one per manufacturing partner. BMES has a built-in secure architecture following CISSAN development approaches described in D2.3. The architecture is based on inputs of another EU project (Cyberfactory #1) and further inputs from CISSAN.

The security functions for BMES were developed in cooperation with the CISSAN partner Netox using both real and simulated scenarios and data, and to distribute them to the various nodes within the system to achieve security aware nodes. Security functions include, e.g., local anomaly detection as well as system level anomaly detection. Business services are exposed as REST APIs for client applications. Anomaly detection is based on transferred commands and sensor data; if an entry deviates from historical baselines or rule thresholds, it will be quarantined, reverted to the last safe schedule, and alerted to the operator.

The applied methods are Virtual Private Network (VPN) and Integrated Access Management (IAM) throughout the user chain. As IAM only accesses one-layer using authentication, the anomaly source can be isolated. As a result of the transmitted alert, anomalies related to an order are detected and quarantined. The result is followed up by the SIEM used at the hosting company (Bittium).

The CISSAN BMES VPN tool is planned to be updated post-project to support PQC post-project using Bittium SafeMove Mobile VPN [4], which supports the standardized ML-KEM algorithm for multiple key exchanges in Internet Key Exchange version 2 (IKEv2).

The system as well as security components in the CISSAN platform relevant to UC4 are listed below.

- Networked Devices

- CISSAN Management Server
- CISSAN Orchestration Server
- IAM (Integrated Access Management)
- Security Information and Event Management (SIEM) Server
- VPN (to be upgraded to Bittium SafeMove Mobile VPN for PQC support post-project)

3.1.1.5 Use Case 5 – Joint Use Case

Use case 5 (UC5) highlights how a multi-domain cyber-attack on IoT and OT networks can be mitigated by collective intelligence and collective defence mechanisms for the CISSAN transportation, smart grids and tunnelling construction use cases. In UC5, security tasks are distributed across the IoT and OT networks, where low quality data is identified using data quality verification and anomalies are detected using machine learning based anomaly detection by distributed devices, which are correlated in real-time at the SIEM and used to perform trust and device management via the Councilbox blockchain system. Trust information is shared as Structured Threat Information eXpression (STIX)-based threat intelligence, which enables interoperable and machine-readable information exchange between heterogeneous IoT and OT domains and organisational boundaries. By collective intelligence, it is possible to identify the propagation paths of attacks, track trust degradation, blacklist and isolate devices and take coordinated disaster recovery actions. At the same time, PQC is envisioned to be supported to secure all data exchanges between the CISSAN management server with all external systems connected to it, ensuring confidentiality, integrity, and authenticity of disaster recovery operations in the face of advanced threat scenarios. By using collective intelligence, STIX-based information exchange, and potentially PQC, this use case demonstrates how standardised and automated mechanisms can be used to achieve automated and distributed disaster recovery in a multi-domain infrastructure attack scenario.

The system components in the CISSAN platform relevant to use case 5 are listed below.

- Networked Devices
- SCADA Server
- CISSAN Management Server
- CISSAN Orchestration Server
- SIEM Server
- Councilbox Blockchain System
- Arctos Labs Optimization Solver
- Mattersoft GPS system
- Clavister Process Aware Stealthy Attack Detection (PASAD) system

3.1.2 Security Requirements

3.1.2.1 Security Requirements of Use Case 1 – Transportation

Use Case 1 focuses on GNSS-based positioning in public transport vehicles and the detection of GNSS spoofing, jamming, or inconsistent positioning behaviour. The objective is to demonstrate how GNSS data streams can be analyzed under operational conditions and how detected anomalies can be surfaced to operators and research stakeholders through the CISSAN platform.

The use case combines onboard GNSS positioning inputs, operational context from public transport systems, backend analysis components, and an MQTT-based interface for transmitting anomaly alerts. The implementation used in CISSAN demonstrations represents a research and prototype environment, meaning that not all security controls are implemented at full production maturity. Instead, the focus is on demonstrating realistic detection scenarios, secure data flows, and traceability to relevant standards and security requirements.

The main security objective of the transport use case is ensuring the **integrity, authenticity, and auditability** of positioning data and anomaly detection outcomes. Since public transport vehicle positions are typically public operational data, confidentiality is not the primary concern.

The security requirements defined for UC1 include detection of anomalous GNSS behaviour (REQ-1), logging and auditability of anomaly events (REQ-2), secure communication of alerts via MQTT (REQ-3), controlled access to anomaly detection configuration (REQ-4), fallback positioning behaviour when GNSS anomalies are detected (REQ-5), and validation of software and component integrity within the supply chain (REQ-6).

The security requirements for Use Case 1 are summarized per system component and interface involved in Table 1.

Table 1. Security requirements of use case 1

Req. ID	Requirement Summary	Architecture Component(s)	Interface(s) involved
REQ-1	Detect inconsistent GNSS behaviour and spoofing/jamming anomalies	GNSS Receiver, Onboard Systems, CISSAN Lab / Backend	GNSS → CISSAN
REQ-2	Log anomaly detection events and retain audit records	Backend, Logging Subsystem	Backend
REQ-3	Trigger anomaly alerts via secure MQTT communication	CISSAN Lab, MQTT Broker	CISSAN → MQTT
REQ-4	Restrict access to anomaly detection configuration and control functions	Backend, Access Control System	User → Backend
REQ-5	Switch to fallback positioning (if available) when GNSS anomalies are detected	CISSAN Lab, Onboard Sensors	CISSAN ↔ Sensors
REQ-6	Ensure integrity and security validation of third-party components and software supply chain	All components	All interfaces

3.1.2.2 Security Requirements of Use Case 2 – Smart Grids

The security requirements for use case 2 (UC2) are summarized per system component and interface involved in Table 2.

Table 2. UC2 security requirements

Req. ID	Requirement Summary	Architecture Component(s)	Interface(s) involved
REQ-1	Detect anomalies in grid communication and operational data	Monitoring Node, AI Detection Engine, Backend	Grid Device/RTUs → Node → Backend
REQ-2	Collect and forward monitoring data securely	Monitoring Agents, Edge Gateways	CISSAN → MQTT / Rotor gateway
REQ-3	Generate security alerts on detected anomalies	Detection Engine, Alert Service, Dashboard	Device → Alert Service → SIEM

REQ-4	Log anomalies and system events	Backend Logging Subsystem, SIEM	Backend and device → SIEM
REQ-5	Use encrypted communication between components	Monitoring Node, Secure Gateway, Backend	Node ↔ Backend
REQ-6	Restrict access to system configuration	Access Control System, Admin Interface	Admin → System
REQ-7	Share anomaly information across nodes	Monitoring Nodes, Backend Platform	Node ↔ Backend
REQ-8	Verify integrity of software components	Deployment System, Component Repository	Repository → System

3.1.2.3 Security Requirements of Use case 3 – Tunnel Construction

The security requirements for use case 3 (UC3) are summarized per system component and interface involved in Table 3.

Table 3. UC3 security standards

Req. ID	Requirement Summary	Architecture Component(s)	Interface(s) involved
REQ-1	Detect tampered tunnel monitoring data	Sensor, Gateway, Data Mgt Server	Sensor → Gateway → CISSAN
REQ-2	Trigger alerts via MQTT	CISSAN Lab, MQTT Broker	CISSAN → MQTT
REQ-3	Log anomalies for audit	Backend, Logging Subsystem	Backend

3.1.2.4 Security Requirements of Use case 4 – Manufacturing Execution System

The security requirements for use case 4 (UC4) are summarized per system component and interface involved in Table 5.

Table 4. UC4 security requirements

Req. ID	Requirement Summary	Architecture Component(s)	Interface(s) involved
REQ-1	Detect inconsistent IAM data	Sensor, Gateway, Data Mgt Server	Sensor → Gateway
REQ-2	Log anomalies for audit	Backend, Logging Subsystem	Backend

3.1.2.4 Security Requirements of Use case 5 and the CISSAN platform

The security requirements for use case 5 (UC5) and the CISSAN platform are summarized per system component and interface involved in Table 5.

Table 5. UC5 security standards

Req. ID	Requirement Summary	Architecture Component(s)	Interface(s) involved
REQ-1	Detect inconsistent GNSS data	GNSS Receiver, CISSAN Lab	GNSS → CISSAN
REQ-2	Correlate onboard sensor data with backend telemetry	CISSAN Lab, Mattersoft Backend	CISSAN ↔ Backend

REQ-3	Trigger alerts via MQTT	CISSAN Lab, MQTT Broker	CISSAN → MQTT
REQ-4	Log anomalies for audit	Backend, Logging Subsystem	Backend
REQ-5	Switch to backup positioning	CISSAN Lab, Onboard Sensors	CISSAN ↔ Sensors
REQ-6	Supply Chain risk	All components	All interfaces

3.2 Compliance with Standards and Gap Analysis

This section discusses the alignment of the CISSAN platform and its use case solutions with relevant security standards and regulations. Based on the security requirements and the CISSAN architecture, this section will discuss the appropriate security standards and regulations that are applicable to the CISSAN use case solutions and provide the standardization gap analysis.

3.2.1 List of Standards and Regulations Addressed by the CISSAN Platform

The list of the relevant security standards and regulations considered in the CISSAN project is provided for each use case below. This will provide the foundation in determining the appropriate compliance and identifying the standardization gaps that may be addressed in the development of the CISSAN platform and its use case solutions.

3.2.1.1 Security Standards in Use Case 1 - Transportation

Table 6. UC1 security standards

Component	Security Standards	Justification for Compliance
Networked Devices (GNSS receivers / onboard systems)	I TxPT GNSS v2.2.0, ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
Backend / Management Server	ISO/IEC 27001, NIS2, NIST SP 800-53	• Security requirements • Industrial practice
MQTT Broker / Communication Interface	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
Logging and Monitoring Components	ISO/IEC 27001, NIST SP 800-53	• Security requirements • Industrial practice

3.2.1.2 Security Standards in Use Case 2

Table 7. UC2 security standards

Component	Security Standards	Justification for Compliance

Networked Devices	ISO/IEC 27001, NIS2, General Data Protection Regulation (GDPR)	• Security requirements • Industrial practice
SCADA Server	IEC 62443, ISO/IEC 27001	• Security requirements • Industrial practice
SIEM Server	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
RTU	IEC 62443, ISO/IEC 27001	• Security requirements • Industrial practice

3.2.1.1 Security Standards in Use Case 3

Table 8. UC3 security standards

Component	Security Standards	Justification for Compliance
Networked Devices	ISO/IEC 27001, NIS2, General Data Protection Regulation (GDPR)	• Security requirements • Industrial practice
SCADA Server	IEC 62443, ISO/IEC 27001	• Security requirements • Industrial practice
Management Server	ISO/IEC 27001, NIS2, PQC, STIX	• Security requirements • Industrial practice
Orchestration Server	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
SIEM Server	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
Geodata Data Quality Verification System	ISO/IEC 27001, ISO/IEC 42001, NIS2, GDPR, PQC, Cyber Resilience Act (CRA), Cybersecurity Act (CSA), STIX, AI act	• Security requirements • Industrial practice
Geodata Blockchain System	ISO/IEC 27001, ISO/IEC 42001, NIS2, PQC, CRA, CSA	• Security requirements • Industrial practice
Geodata Data Signing System	ISO/IEC 27001, ISO/IEC 42001, NIS2, PQC, CRA, CSA	• Security requirements • Industrial practice

3.2.1.1 Security Standards in Use Case 4

Table 9. UC4 security standards

Component	Security Standards	Justification for Compliance
Integrated Access and Management (IAM)	ISO/IEC 27001, NIS2, GDPR	• Security requirements • Industrial practice

SIEM Server	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
Bittium VPN solution	ISO/IEC 27001, ISO/IEC 42001, NIS2, PQC, CRA, CSA	• Security requirements • Industrial practice

3.2.1.1 Security Standards in Use Case 5 and the CISSAN Platform

Table 10. UC5 and CISSAN platform security standards

Component	Security Standards	Justification for Compliance
Networked Devices	ISO/IEC 27001, NIS2, GDPR	• Security requirements • Industrial practice
SCADA Server	IEC 62443, ISO/IEC 27001	• Security requirements • Industrial practice
Management Server	ISO/IEC 27001, NIS2, PQC, STIX	• Security requirements • Industrial practice
Orchestration Server	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
SIEM Server	ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
Councilbox Blockchain System	ISO/IEC 27001, NIS2, GDPR	• Security requirements • Industrial practice
Arctos Labs Optimization Solver	ISO/IEC 27001	• Security requirements • Industrial practice
Mattersoft GPS system	ITxPT GNSS, ISO/IEC 27001, NIS2	• Security requirements • Industrial practice
Clavister PASAD system	ISO 27001	• Security requirements • Industrial practice

3.2.2 Standards Gap Analysis

This subsection will present the gap analysis that was carried out to assess the level of compliance that the CISSAN platform has with the established standards in the field of cybersecurity. This gap analysis is based on the list of standards that are applicable in the field of cybersecurity, as well as the security requirements that the CISSAN platform has. This will help in the identification of the areas that the CISSAN platform is already in compliance within terms of the established guidelines.

For each use case, please mention the gaps determined in the Standardization Gap Analysis Workshop presentation and how you plan to address them now or post-project in this section.

3.2.2.1 Security Standards Gaps in Use Case 1

Table 11. Security standards gaps in UC1

Component	Security Standards	Gap
Networked Devices (GNSS receivers)	ITxPT GNSS, ISO/IEC 27001, NIS2	No major gaps identified in the research prototype environment. Full compliance with operational transport system requirements may require additional hardware-based security and certified validation mechanisms in production deployments.
Backend / Management Server	ISO/IEC 27001, NIS2, NIST SP 800-53	Logging and monitoring capabilities are implemented at prototype level. Full compliance with operational security governance and certification frameworks would require additional hardening and formal security management processes
MQTT Communication Interface	ISO/IEC 27001, NIS2	Secure communication can be implemented using TLS and authenticated messaging. Comprehensive enforcement of broker-level authorization policies and full production-grade monitoring remain possible post-project development tasks.
Logging and Monitoring Components	ISO/IEC 27001, NIST SP 800-53	Logging is implemented for demonstration and traceability of anomaly events. Tamper-evident log storage and long-term retention policies are considered part of possible future operational deployment.

3.2.2.1 Security Standards Gaps in Use Case 2

Table 12. Security standards gaps in UC2

Component	Security Standards	Gap
CISSAN Lab OT Network	IEC 62443-3-3 & 3-2, NIS2	Network implemented at reseach and laboration level of IEC 62443 with no specific Security Level (SL). Networks are segmented as good as possible but no hardware redundancy or high availability done.

Techinova AI Fault Detector	IEC 62443-4-2 & 4-3	Not fully compliant with IEC 62443 since it is at a prototype level.
Logging, monitoring, SIEM	ISO/IEC 27001, NIS2	Compliant
OT Software Components / OT Hardware Components	IEC 62443, NIS2, IEC 60870, IEC 61850	Component documentation and inventory available. Vulnerability testing has been done multiple times on OT devices. Compliant with IEC 62443, 60870, 61850

3.2.2.2 Security Standards Gaps in Use case 3

As a result of the standards gap analysis conducted for UC3, the gaps indicated in Table 15 were identified.

Table 13. Security standards gaps in UC3

Component	**Security Standards**	**Gap**
Networked Devices	ISO/IEC 27001, NIS2, GDPR	None
SCADA Server	IEC 62443, ISO/IEC 27001	None
Management Server	ISO/IEC 27001, NIS2, NIST PQC and NIS PQC roadmap, STIX	None
Orchestration Server	ISO/IEC 27001, NIS2	None
SIEM Server	ISO/IEC 27001, NIS2	None
Geodata Data Quality Verification System	ISO/IEC 27001, ISO/IEC 42001, NIS2, GDPR, PQC, CRA, CSA, STIX, AI act	Only compliant with GDPR. Compliancy considered post-project.
Geodata Blockchain System	ISO/IEC 27001, ISO/IEC 42001, NIS2, PQC, CRA, CSA	Not compliant. Compliancy considered post-project.
Geodata Data Signing System	ISO/IEC 27001, ISO/IEC 42001, NIS2, PQC, CRA, CSA	Not compliant. Compliancy considered post-project.

3.2.2.3 Security Standards Gaps in Use Case 4

As a result of the standards gap analysis conducted for UC4, the gaps indicated in Table 14 were identified.

Table 14. Security standards gaps in UC4

Component	**Security Standards**	**Gap**
Integrated Access and Management (IAM)	ISO/IEC 27001, NIS2, GDPR	• None
SIEM Server	ISO/IEC 27001, NIS2	• Compliant

Bittium VPN solution	ISO/IEC 27001,NIS2, PQC, CRA, CSA	• Compliant with mentioned standards • PQC standard – based solution published 11.2025

3.2.2.4 Security Standards Gaps in Use case 5 / CISSAN Platform

As a result of the standards gap analysis conducted for UC5 and the CISSAN platform, the gaps indicated in Table 15 were identified.

Table 15. Security standards gaps in UC5 and CISSAN platform

Component	**Security Standards**	**Gap**
Networked Devices	ISO/IEC 27001, NIS2, GDPR	None
SCADA Server	IEC 62443, ISO/IEC 27001	None
Management Server	ISO/IEC 27001, NIS2, NIST PQC and NIS PQC roadmap, STIX	None
Orchestration Server	ISO/IEC 27001, NIS2	None
SIEM Server	ISO/IEC 27001, NIS2	None
Councilbox Blockchain System	ISO/IEC 27001, NIS2, GDPR, NIST PQC and NIS PQC roadmap	Not compliant with NIST PQC and NIS PQC roadmap. Planned to be compliant post-project
Arctos Labs Optimization Solver	ISO/IEC 27001, NIST PQC and NIS PQC roadmap	Not compliant with NIST PQC and NIS PQC roadmap. Planned to be compliant post-project
Mattersoft GPS system	ITxPT GNSS, ISO/IEC 27001, NIS2, NIST PQC and NIS PQC roadmap	Not compliant with NIST PQC and NIS PQC roadmap. Planned to be compliant post-project
Clavister PASAD system	ISO 27001, NIST PQC and NIS PQC roadmap	Not compliant with NIST PQC and NIS PQC roadmap. Planned to be compliant post-project

4 Standardization Action Plan

The CISSAN standardization action plan is based on the above-discussed compliance and gap analyses of the CISSAN platform and its use cases, as well as projections of its future capabilities. Considering this gap analysis, two areas emerge for major consideration in the CISSAN standardization action plan: a) STIX [5], the data structure and protocol for exchanging cybersecurity threat Information and its enhancement of collaborative intelligence in cybersecurity, and b) the potential use of PQC in the CISSAN platform.

The project considers the potential use of STIX for the support of the standardized representation and exchange of cybersecurity threat intelligence within the CISSAN platform and its use case solutions. Although the full integration of STIX with the CISSAN use case solutions is not within the scope of the current project due to time and resource constraints, the action plan includes the extension of the STIX data model to better support the representation of various cybersecurity threats and security events associated with the security of IoT and OT environments. The extended STIX data model will be used for the structured representation and reporting of various security events associated with the security of devices connected to the platform, as well as the representation of various security threats and vulnerabilities associated with the devices. After the design of the extensions, the support for the extended STIX data model will be developed within the CISSAN platform for the evaluation of the feasibility of the extended STIX data model for the representation and sharing of various security threats and security events associated with the security of the networked devices in the CISSAN platform for the use case systems they represent.

Although it is recognized as a major step forward in ensuring long-term cryptographic robustness, the complete integration of PQC into the CISSAN platform is not within the scope of the current project due to time and budget constraints. However, it is recognized that quantum-resistant security features will become increasingly important for IoT and OT systems, especially considering that such systems are expected to have long lifetimes. The project aims to undertake a preliminary feasibility analysis of incorporating PQC into the CISSAN platform and its use case solutions. This would involve examining the potential impact of PQC-based algorithms on system performance, computational demands, and communication overheads, especially for resource-constrained IoT and OT domains. This would enable identifying potential cryptographic components, such as key exchange and digital signatures, which could potentially be replaced or supplemented with PQC-based solutions. The preliminary feasibility evaluation of PQC adoption and its potential impact on the overall CISSAN platform architecture would potentially lay the groundwork for future implementation and evaluation activities beyond the scope of the proposed project. As part of the post-project plan, it is envisaged that the integration of PQC algorithms, especially those currently being standardized by NIST, will be assessed for key CISSAN platform components such as device authentication, secure communication protocols, and trust management techniques. The initial step will be to evaluate the computational overhead and latency of PQC schemes in constrained IoT systems. To support this activity, it is planned that follow-on funding will be sought from national and international research programs and collaborations with industry and standardization organizations. This will be done to extend the CISSAN platform with quantum-resistant cryptographic features while ensuring interoperability, performance, and compatibility with existing security frameworks and protocols.

Table 16 lists the suggested activities for the different steps in standardization action plan (refer to Figure 1 for the steps of a standardization action plan).

Table 16. Activities in Standardization Action Plan for CISSAN

Phases from Standardization Action Plan framework (see Figure 1)	**Activity**	
	STIX	**PQC**
Define Standardization Action	Detail current STIX capabilities and suggest enhancements for	Detail discussion with CISSAN platform design specific current PQC

	collaborative intelligence in cybersecurity using distributed AI	capabilities and implementation opportunities
Assign Ownership and Governance	Discuss with use cases who can be owner for governance and compliance verification	Discuss with platform implementors (WP5) who can be owner for compliance verification
Coordinate with work packages	Discuss the implementation of parts of STIX and STIX enhancement in the WP2, WP4, and WP5 (hereby consider relation to each use case)	Discuss the potential and feasibility of implementing PQC in parts of the CISSAN systems in WP5
Engage with Standardization	Provide suggestions for enhancement of the existing STIX standard	If time permits: provide feedback for existing PQC standardization projects on implementation challenges

5 Ownership and Governance

A RACI matrix is created to identify ownership and governance of the CISSAN standardization activities with clear roles and responsibilities. The acronym RACI stands for Responsible, which indicates the roles or people performing the task; Accountable, which indicates the roles or people with final authority and decision-making; Consulted, which indicates roles or people with expertise in the activity; and Informed, which indicates roles or people to be updated regularly on activities in the project. The RACI matrix (see Table 17) was created based on the key activities identified in the standardization action plan, where project partners involved in each activity were identified according to their level of involvement in each activity.

Table 17. RACI matrix for carrying out CISSAN standardization action plan

Activity	**Standardization Lead (BTH / JYU)**	**WP Leads**	**Project Coordinator (JYU)**	**Consortium Partners**
Identify relevant standards	**R**	C	A	C
Perform gap analysis for compliance	**R**	**R**	A	C
Prioritize identified gaps	**R**	C	A	C
Coordinate with technical WPs	**R**	**R**	A	I
Contact standards bodies / authorities	**R**	C	A	I

R: Responsible, A: Accountable, C: Consulted, I: Informed

The organizational structure for the CISSAN project's standardization activities depicted in Figure 2 has been conceived with a view to providing clear leadership, collaborative work, and transparency in decision-making, as can be inferred from the RACI matrix. The role of the Standardization Lead is critical and mainly entails providing leadership and coordination for standardization-related work packages, including standard identification, gap analysis, and prioritization of standard compliance gaps, and liaison with relevant authorities and standardization bodies. The role of the Work Package (WP) Leads is to provide technical expertise and ensure that project development is aligned with existing and emerging standards. Finally, the role of the Project Coordinator is to ensure that standardization work is aligned with project objectives, timelines, and reporting requirements. The role of the Consortium partners is to provide domain expertise and be consulted whenever their expertise is deemed relevant, and to be kept informed of key developments. This structure has been conceived with a view to facilitating collaborative work among consortium partners and enabling effective communication between technical and strategic roles.

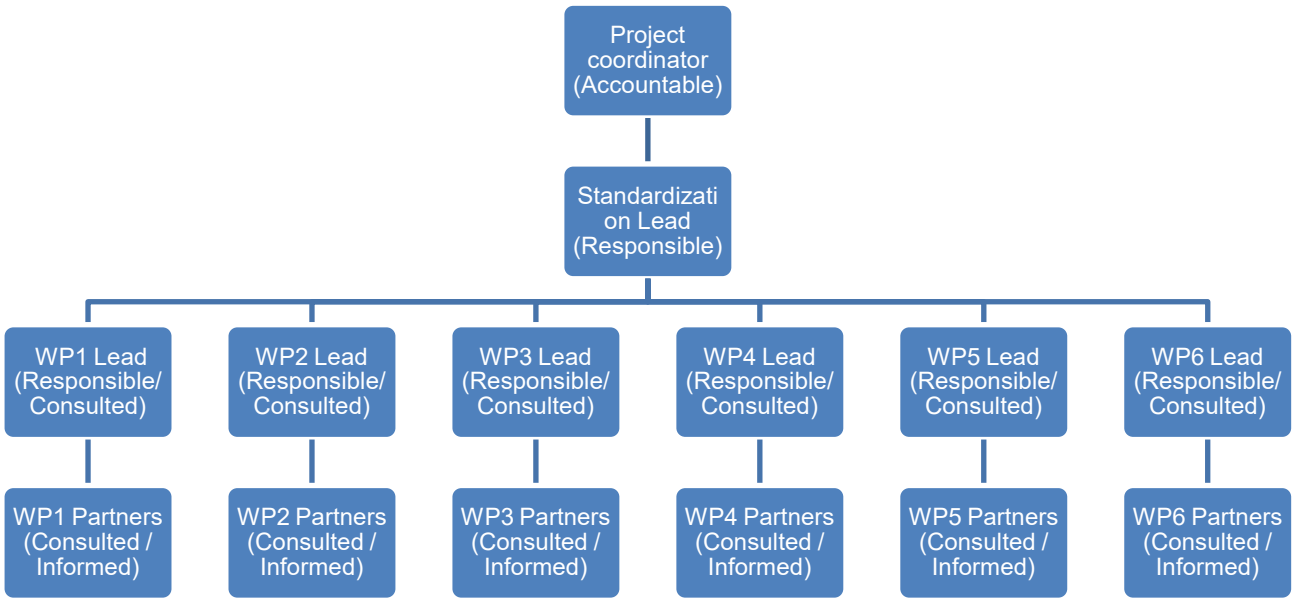

Figure 2. Organizational structure of CISSAN standardization activities

6 Conclusion

This report provides the CISSAN standardization action plan, including the ownership and governance for standardization activities. The CISSAN security requirements defined in CISSAN deliverable D2.3 confidential annexes have been analysed in line with relevant cybersecurity standards and regulations. A standardization gap analysis of the compliance of the CISSAN platform and its use cases has been performed to align it with relevant cybersecurity standards and regulations. Based on the standardization gap analysis, the CISSAN standardization action plan has been defined, including the relevant ownership and governance structure to align the project in relevant work packages. Standardization gaps identified are to be prioritized based on the highest risk reduction and impact as part of activities to be carried out in work packages.

The CISSAN standardization action plan has identified the opportunities for CISSAN to 1) improve their interoperability and security by ensuring compliance with existing standards, 2) contribute to standards and 3) plan potential future compliance with standards to ensure the sustainability of the CISSAN platform and its use case solutions post-project.

CISSAN plans to contribute to standards with the extension, implementation and testing of the STIX threat report format for the representation and exchange of security-related information generated by the CISSAN platform, including security events from devices and threats.

CISSAN also plans the potential future compliance with NIST PQC standards within its standardization action plan. This includes performing a preliminary feasibility analysis of integrating the PQC mechanisms to improve the cryptographic security of the CISSAN platform and its use case solutions. These activities will provide the basis for the future development in potential new projects.

The results of the CISSAN standardization action plan also have implications for broader European goals in terms of cybersecurity, digital resilience, and technological sovereignty. The promotion of the adoption of interoperable security standards and the exploration of more advanced mechanisms such as STIX-based threat intelligence sharing and PQC can all help to improve the security and resilience of critical digital infrastructures in Europe.

References

[1] A. J. Masys, Security by design. Innovative Perspectives on Complex Problems, Springer, 2018.

[2] T. H.-C. Hsu, Hands-On Security in DevOps: Ensure continuous security, deployment, and delivery with DevSecOps, Packt Publishing Ltd., 2018.

[3] A.-M. Väyrynen and E. Räisänen, *Secure Software Design and Development: Towards Practical Models for Implementing Information Security into the Requirements Engineering Process,* Jyväskylä: University of Jyväskylä, 2020.

[4] Bittium, “Bittium SafeMove Mobile VPN - Highly Secure and Seamless Connectivity for Government and Authority Use,” Bittium, Oulu, Finland, 2025.

[5] S. Barnum, “Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™),” MITRE, 2014.

Annex A Standardization Related to CISSAN

This appendix provides a larger list of details on standards and standardization organizations relevant to the CISSAN platform. It complements the summary provided in Section 2.3 of this report.

A.1 Overview of the Standard Organizations

- **ETSI:** European Telecommunications Standards Institute - Focuses on ICT, including cybersecurity for telecommunications and critical infrastructure.
- **NIST:** National Institute of Standards and Technology (U.S.) - Develops widely influential standards, frameworks, and guidelines, especially for the U.S. federal government.
- **IEEE:** Institute of Electrical and Electronics Engineers - Focuses on networking, communications, and hardware-level security.
- **ISO/IEC:** International Organization for Standardization / International Electrotechnical Commission - The world's leading developers of international standards. They often publish joint standards (e.g., ISO/IEC 27001).
- **ANSI:** American National Standards Institute - The official U.S. representative to ISO and IEC. They *accredit* standards developed by other organizations (like NIST and IEEE) as American National Standards (ANS) but do not write them.
- **IETF:** Internet Engineering Task Force - Develops the foundational standards (RFCs) that make the internet work, including many core security protocols.
- **ITU:** International Telecommunication Union - A UN agency specializing in information and communication technologies, with a focus on global infrastructure and policy.
- **OGC (Open Geospatial Consortium)** The OGC specializes in standards for geospatial/location data, which is fundamental for any sensor with a location (e.g., environmental sensors, vehicle sensors).

A.2 Important Note on Access

- **Free Access:** Standards from **NIST, IETF, and ETSI** are almost always freely available for download.
- **Purchase Required:** Standards from **ISO, IEC, IEEE, and ANSI** are typically **not free**. The links provided often lead to informational pages or abstracts. To obtain the full standard, you must purchase it from the organization's webstore.

A.3 Cybersecurity in General Standards

A.3.1 ETSI (European Telecommunications Standards Institute)

- **ETSI EN 303 645 (Cyber Security for Consumer Internet of Things)**
  - **Description:** A foundational standard for cybersecurity in consumer IoT devices, outlining 13 provisions for secure design and development.
  - **Link:** https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- **ETSI TS 103 701 (CYBER; Middlebox Security Protocol)**
  - **Description:** Specifies a protocol to securely expose the functions of middleboxes (like firewalls) without breaking encryption.
  - **Link:** https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
- **ETSI GS NFV-SEC (Network Functions Virtualisation - Security)**
  - **Description:** A series of documents addressing security best practices and specifications for NFV environments.

- **Link:** https://www.etsi.org/committee/1429-nfv#specifications

A.3.2 NIST (National Institute of Standards and Technology)

- **NIST Cybersecurity Framework (CSF)**
  - **Description:** A voluntary framework consisting of standards, guidelines, and best practices to manage cybersecurity risk. It is arguably the most influential cybersecurity framework globally.
  - **Link:** https://www.nist.gov/cyberframework
- **NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations)**
  - **Description:** A comprehensive catalog of security and privacy controls for all U.S. federal information systems. It is the basis for many compliance regimes worldwide.
  - **Link:** https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- **NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)**
  - **Description:** Specifies requirements for protecting sensitive U.S. government information (CUI) held by contractors and non-federal organizations.
  - **Link:** https://csrc.nist.gov/pubs/sp/800/171/r3/final
- **NIST SP 800-63 (Digital Identity Guidelines)**
  - **Description:** Provides guidelines for implementing digital identity services, including identity proofing, authentication, and federation (e.g., for passwords and multi-factor authentication).
  - **Link:** https://pages.nist.gov/800-63-3/

A.3.3 IEEE (Institute of Electrical and Electronics Engineers)

- **IEEE 802.1X (Port-Based Network Access Control)**
  - **Description:** A standard for authenticating devices connecting to a LAN or WLAN, providing a mechanism for network access control.
  - **Link:** https://standards.ieee.org/ieee/802.1X/1029/
- **IEEE 1609.2 (Security Services for Wireless Access in Vehicular Environments)**
  - **Description:** Defines security services for WAVE (Wireless Access in Vehicular Environments) networks, including secure message formats and processing.
  - **Link:** https://standards.ieee.org/ieee/1609.2/1041/

A.3.4 ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

- **ISO/IEC 27001 (Information Security Management Systems - Requirements)**
  - **Description:** The international benchmark for an Information Security Management System (ISMS). It specifies the requirements for establishing, implementing, maintaining, and continually improving an ISMS.
  - **Link:** https://www.iso.org/isoiec-27001-information-security.html
- **ISO/IEC 27002 (Information security, cybersecurity and privacy protection — Information security controls)**
  - **Description:** A code of practice that provides a reference set of generic information security controls and implementation guidance. It is the companion to ISO/IEC 27001.
  - **Link:** https://www.iso.org/standard/75652.html
- **ISO/IEC 27005 (Information security risk management)**

- **Description:** Provides guidelines for information security risk management, supporting the requirements of ISO/IEC 27001.
- **Link:** https://www.iso.org/standard/75281.html

- **ISO/IEC 15408 (Common Criteria for Information Technology Security Evaluation)**
  - **Description:** Provides a framework for evaluating the security properties of IT products and systems (e.g., hardware, software, firmware).
  - **Link:** https://www.commoncriteriaportal.org/ (The official portal for the Common Criteria)
- **NIS 2 Directive**
  - **Description:** ***The NIS2 Directive establishes a unified legal framework to uphold cybersecurity in 18 critical sectors across the EU.***
  - **Link:** https://eur-lex.europa.eu/eli/dir/2022/2555

A.4 IoT Security Standards

A.4.1 Overview of the Domain

- **IoT Security:** Focuses on the unique challenges of securing constrained, connected devices, their data, and the networks they form.

A.4.2 ETSI (European Telecommunications Standards Institute)

ETSI is a leader in IoT security standardization, particularly for consumer devices.

- **ETSI EN 303 645** - **Cyber Security for Consumer Internet of Things**
  - **Description:** The globally recognized baseline for consumer IoT security. It outlines 13 provisions for secure design, including no default passwords, vulnerability disclosure, and secure update mechanisms. It forms the basis for many global IoT certification schemes.
  - **Link:** https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
- **ETSI TS 103 701** - **CYBER; Middlebox Security Protocol**
  - **Description:** While not exclusively IoT, this is crucial for IoT environments that use middleboxes (like firewalls and NATs), ensuring they don't break end-to-end encryption.
  - **Link:** https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf

A.4.3 NIST (National Institute of Standards and Technology)

NIST provides foundational cybersecurity frameworks and specific IoT guidance.

- **NISTIR 8259** - **Foundational Cybersecurity Activities for IoT Device Manufacturers**
  - **Description:** Provides core cybersecurity activities IoT device manufacturers should perform, including device documentation, interface protection, and software update capabilities. This is the core of the NIST IoT cybersecurity guidance.
  - **Link:** https://csrc.nist.gov/publications/detail/nistir/8259/final
- **NIST Cybersecurity Framework (CSF) 2.0**
  - **Description:** While not IoT-specific, this is the premier risk management framework used globally. Its "Govern," "Identify," "Protect," "Detect," "Respond," and "Recover" functions can be directly applied to IoT ecosystems.
  - **Link:** https://www.nist.gov/cyberframework
- **NIST SP 1800-15** - **Securing Small-Business and Home Internet of Things (IoT) Devices**
  - **Description:** An example implementation showing how to apply cybersecurity technologies and practices to protect IoT devices in a home/small business setting.

- **Link:** https://www.nccoe.nist.gov/projects/use-cases/iot-devices

A.4.4 ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

ISO/IEC standards provide internationally agreed-upon best practices.

- **ISO/IEC 27400** - **Cybersecurity — IoT security and privacy — Guidelines**
  - **Description:** Provides guidelines on IoT security and privacy risks, principles, and controls for stakeholders throughout the IoT device lifecycle.
  - **Link:** https://www.iso.org/standard/44373.html (Purchase required)
- **ISO/IEC 27030** - **Information security, cybersecurity and privacy protection — Guidelines for security and privacy in Internet of Things (IoT) systems**
  - **Description:** Offers guidelines for addressing security and privacy aspects in the design, implementation, and operation of IoT systems.
  - **Link:** https://www.iso.org/standard/81270.html (Under development, link to preview)

A.4.5 IETF (Internet Engineering Task Force)

IETF standards focus on the protocols that make the Internet (and IoT) work.

- **RFC 8576** - **Internet of Things (IoT) Security: State of the Art and Challenges**
  - **Description:** An informational RFC that provides a great overview of the IoT security landscape, its challenges, and relevant IETF protocols.
  - **Link:** https://www.rfc-editor.org/rfc/rfc8576.html
- **RFC 9019** - **Software Updates for Internet of Things (SUIT) Manifest**
  - **Description:** A critical standard for IoT security, defining a manifest format that describes how to install and verify firmware updates on constrained devices.
  - **Link:** https://www.rfc-editor.org/rfc/rfc9019.html

A.5 ICS/SCADA Security Standards

A.5.1 Overview of the Domain

- **ICS/SCADA Security:** Focuses on the operational technology (OT) environments that run critical infrastructure (power grids, water treatment, manufacturing). Priorities are safety and reliability, which sometimes differ from IT security priorities.

A.5.2 ISA / IEC (International Society of Automation / International Electrotechnical Commission)

The **ISA/IEC 62443** series is the most comprehensive and internationally recognized set of standards for ICS/SCADA security.

- **ISA/IEC 62443 Series** - **Security for Industrial Automation and Control Systems**
  - **Description:** A multi-part standard covering all aspects of ICS security.
    - **General (62443-1):** Concepts and models.
    - **Policies & Procedures (62443-2):** Establishing an IACS security program (e.g., 62443-2-1: Requirements for an IACS security management system).
    - **System Level (62443-3):** Risk assessment, system design, and security requirements.
    - **Component Level (62443-4):** Technical security requirements for products like PLCs, RTUs, and HMIs.

- **Link (ISA Page):** https://www.isa.org/standards-and-publications/isa-standards/isa-62443-series-of-standards
- **Link (IEC Page):** https://www.iec.ch/blog/cybersecurity-industrial-automation-and-control-ensuring-safety-and-reliability-critical-infrastructures

A.5.3 NIST (National Institute of Standards and Technology)

NIST provides tailored frameworks and guides for the OT environment.

- **NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security**
  - **Description:** The definitive guide from NIST on securing ICS, including SCADA systems, DCS, and PLCs. It provides an overview of ICS, identifies threats and vulnerabilities, and recommends security safeguards.
  - **Link:** https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **NIST Cybersecurity Framework (CSF) 2.0 - ICS Profile**
  - **Description:** A "profile" that tailors the broader NIST CSF to the specific needs, terminology, and risks of Industrial Control Systems.
  - **Link (Example Profile):** https://www.nist.gov/system/files/documents/2020/07/21/ICS%20Profile%20Version%201.1%20Final.pdf

A.5.4 IEEE (Institute of Electrical and Electronics Engineers)

- **IEEE 1711.2 - Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links**
  - **Description:** Specifically for the power industry, this standard provides a protocol for encrypting and authenticating serial communications in electrical substations, a critical part of the grid.
  - **Link:** https://standards.ieee.org/ieee/1711.2/1029/

A.6 Blockchain/DLT Standards

A.6.1 ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission)

The joint technical committee **ISO/TC 307** is the primary developer of international blockchain and DLT standards.

- **ISO 22739:2020 - Blockchain and distributed ledger technologies — Vocabulary**
  - **Description:** Provides a foundational set of terms and definitions for blockchain and DLT. This is critical for ensuring consistent understanding across the industry and different standards.
  - **Link:** https://www.iso.org/standard/73758.html (Purchase required)
- **ISO 23257:2022 - Blockchain and distributed ledger technologies — Reference architecture**
  - **Description:** Defines a common framework and set of views (e.g., functional, operational) to describe blockchain systems. It promotes interoperability and a common understanding of system components.
  - **Link:** https://www.iso.org/standard/75093.html (Purchase required)
- **ISO/TR 23455:2019 - Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems**
  - **Description:** A technical report that provides an overview of smart contracts and how they interact within DLT systems.
  - **Link:** https://www.iso.org/standard/77444.html (Purchase required)

- **ISO/TR 23576:2023** - **Blockchain and distributed ledger technologies — Security management of digital asset custodians**
  - **Description:** Provides guidance on security management for organizations that custody digital assets, a critical area for the cryptocurrency industry.
  - **Link:** https://www.iso.org/standard/81193.html (Purchase required)

A.6.2 IEEE (Institute of Electrical and Electronics Engineers)

IEEE standards often focus on the architectural and interoperability layers.

- **IEEE 2140.1-2020** - **Standard for General Process of Blockchain Consensus**
  - **Description:** Defines a general process for blockchain consensus, breaking it down into stages like transaction submission, block generation, verification, and chaining.
  - **Link:** https://standards.ieee.org/ieee/2140.1/10416/ (Purchase required)
- **IEEE 2144.1-2020** - **Standard for Blockchain-Based Digital Rights Management**
  - **Description:** Specifies a framework for using blockchain for digital rights management (DRM), covering content registration, license issuance, and access control.
  - **Link:** https://standards.ieee.org/ieee/2144.1/10418/ (Purchase required)
- **IEEE P2418.1** - **Standard for the Framework of Blockchain Use in Internet of Things (IoT)**
  - **Description:** (Under Development) Aims to define a framework for using blockchain to enhance IoT security and functionality, covering data integrity, device identity, and automated transactions.
  - **Link:** https://standards.ieee.org/ieee/2418.1/10780/ (Project page)

A.6.3 ITU-T (International Telecommunication Union - Telecommunication Standardization Sector)

ITU-T focuses on the application of DLT in telecommunications and infrastructure.

- **ITU-T F.751.1** - **Assessment criteria for distributed ledger technology (DLT) platforms for financial applications**
  - **Description:** Provides criteria for assessing the suitability of DLT platforms for various financial applications.
  - **Link:** https://www.itu.int/rec/T-REC-F.751.1-202212-I
- **ITU-T X.1400 series** - **Security standards for Distributed Ledger Technology**
  - **Description:** A series of recommendations covering security threats, security frameworks, and personal identifiable information protection for DLT.
  - **Link (Overview):** https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/security-dlt.aspx
  - **Example: ITU-T X.1401:** Security framework for DLT: https://www.itu.int/rec/T-REC-X.1401

A.6.4 ETSI (European Telecommunications Standards Institute)

ETSI's work is organized under the Industry Specification Group for Permissioned Distributed Ledgers (ISG PDL).

- **ETSI GR PDL 001** - **Permissioned Distributed Ledgers (PDL); Report on Operational and Legal Challenges**
  - **Description:** A group report identifying key challenges and potential solutions for deploying permissioned DLTs.
  - **Link:** https://www.etsi.org/deliver/etsi_gr/PDL/001_099/001/01.01.01_60/gr_pdl001v010101p.pdf

- **ETSI GR PDL 002** - **Permissioned Distributed Ledgers (PDL); Use Cases**
  - **Description:** Documents a variety of use cases for permissioned DLTs across different industries.
  - **Link:** https://www.etsi.org/deliver/etsi_gr/PDL/001_099/002/01.01.01_60/gr_pdl002v010101p.pdf

A.6.5 NIST (National Institute of Standards and Technology)

NIST's role is to provide foundational research, cybersecurity guidance, and reports rather than prescriptive standards.

- **NISTIR 8202** - **Blockchain Technology Overview**
  - **Description:** An excellent introductory report explaining how blockchain works, its key characteristics, and its consensus models.
  - **Link:** https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf
- **NISTIR 8301 (Upd.)** - **Usage of Blockchain in Healthcare: A Tutorial**
  - **Description:** A report exploring the potential benefits and challenges of using blockchain technology for healthcare applications and data.
  - **Link:** https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8301.upd.pdf
- **NIST.IR 8401** - **Interoperability for Blockchain and Distributed Ledger Technologies: Review of the State of the Art and Perspectives**
  - **Description:** A detailed analysis of the interoperability challenges between different blockchain systems and approaches to solving them.
  - **Link:** https://nvlpubs.nist.gov/nistpubs/ir/2023/NIST.IR.8401.pdf

A.6.6 IETF (Internet Engineering Task Force)

The IETF's work is focused on the core protocols that would enable blockchain/DLT systems to interoperate at the network level.

- **Blockchain Overlays (BLOCO)** - **Working Group**
  - **Description:** This group works on standards for running overlay networks on top of existing blockchains to enable interoperability and new functionalities. Their work is ongoing, and no RFCs have been published yet.
  - **Link (Working Group Page):** https://datatracker.ietf.org/wg/bloco/about/

A.6.7 ANSI (American National Standards Institute)

As an accreditor, ANSI's role is to approve standards developed by other bodies (like IEEE) as American National Standards (ANS). For example, many of the **IEEE blockchain standards** listed above are also ANSI-accredited.

A.7 AI Standards

A.7.1 ISO/IEC JTC 1/SC 42 (Artificial Intelligence)

This is the **primary and most important joint committee** between ISO and IEC dedicated to AI standardization. It covers the entire AI ecosystem.

- **ISO/IEC 22989:2022** - **Information technology — Artificial intelligence — Artificial intelligence concepts and terminology**
  - **Description:** Provides a foundational set of terms and definitions for AI, which is critical for ensuring consistent understanding across the industry and other standards.
  - **Link:** https://www.iso.org/standard/74296.html (Purchase required)

- **ISO/IEC 23053:2022** - **Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML)**
  - **Description:** Defines a framework for AI systems using machine learning, including typical components and functions. It's a key architectural standard.
  - **Link:** https://www.iso.org/standard/74438.html (Purchase required)
- **ISO/IEC 42001:2023** - **Information technology — Artificial intelligence — Management system**
  - **Description:** The world's first international standard for an AI Management System (AIMS). It provides requirements for establishing, implementing, maintaining, and continually improving an AI management system within organizations. This is a landmark standard, analogous to ISO 27001 for security.
  - **Link:** https://www.iso.org/standard/81230.html (Purchase required)
- **ISO/IEC TR 24027:2021** - **Information technology — Artificial intelligence (AI) — Bias in AI systems and AI aided decision making**
  - **Description:** A technical report that provides guidance on identifying, assessing, and mitigating bias in AI systems throughout the machine learning lifecycle.
  - **Link:** https://www.iso.org/standard/77607.html (Purchase required)
- **ISO/IEC TR 24028:2020** - **Information technology — Artificial intelligence — Overview of trustworthiness in artificial intelligence**
  - **Description:** Provides an overview of trustworthiness aspects in AI, including robustness, reliability, reproducibility, explainability, and fairness.
  - **Link:** https://www.iso.org/standard/77608.html (Purchase required)
- **ISO/IEC 23894:2023** - **Information technology — Artificial intelligence — Guidance on risk management**
  - **Description:** Provides guidance for organizations on managing risks related to AI systems, intended to be used in conjunction with the overall risk management process described in ISO 31000.
  - **Link:** https://www.iso.org/standard/77304.html (Purchase required)

A.7.2 NIST (National Institute of Standards and Technology)

NIST's role is to develop foundational research, risk management frameworks, and technical guidelines, often in response to U.S. government executive orders.

- **NIST AI Risk Management Framework (AI RMF 1.0)**
  - **Description:** A voluntary framework to better manage risks to individuals, organizations, and society associated with AI. It provides guidance on governing, mapping, measuring, and managing AI risk. This is one of the most influential documents globally.
  - **Link:** https://www.nist.gov/itl/ai-risk-management-framework
- **NIST Special Publication 1270** - **Towards a Standard for Identifying and Managing Bias in Artificial Intelligence**
  - **Description:** Provides a detailed study of bias in AI and recommends approaches for identifying and managing it.
  - **Link:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270.pdf
- **NIST Trustworthy and Responsible AI Resource Center**
  - **Description:** Not a single standard, but a portal for all of NIST's AI work, including the AI RMF Playbook, metrics and evaluations, and news on upcoming publications.
  - **Link:** https://airc.nist.gov/

A.7.3 IEEE (Institute of Electrical and Electronics Engineers)

IEEE standards often focus on ethical considerations, algorithmic bias, and technical processes for implementing trustworthy AI.

- **IEEE 7000-2021 - Standard Model Process for Addressing Ethical Concerns during System Design**
  - **Description:** Provides a practical, engineering-based process for identifying and addressing ethical concerns in the design of autonomous and intelligent systems.
  - **Link:** https://standards.ieee.org/ieee/7000/6780/ (Purchase required)
- **IEEE 7010-2020 - IEEE Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being**
  - **Description:** Provides guidance on how to measure and assess the impact of A/IS on human well-being.
  - **Link:** https://standards.ieee.org/ieee/7010/6080/ (Purchase required)
- **IEEE Ethically Aligned Design (EAD) - A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems**
  - **Description:** Not a standard itself, but a foundational document that has influenced much of IEEE's and the world's work on AI ethics. It provides recommendations for creating standards.
  - **Link:** https://standards.ieee.org/content/ieee-standards/en/industry-connections/ec/autonomous-systems.html

A.7.4 ITU-T (International Telecommunication Union)

ITU-T focuses on the application of AI in telecommunications and networks.

- **ITU-T Y.3172 - Architectural framework for machine learning in future networks including IMT-2020**
  - **Description:** Defines an architectural framework for deploying machine learning in future networks (like 5G/6G).
  - **Link:** https://www.itu.int/rec/T-REC-Y.3172
- **ITU-T Y.3xxx series - AI for Good and other applications**
  - **Description:** ITU has a large portfolio of standards and initiatives under its "AI for Good" umbrella, focusing on using AI to meet sustainable development goals.
  - **Link (Overview):** https://www.itu.int/en/ITU-T/AI/Pages/default.aspx

A.7.5 ETSI (European Telecommunications Standards Institute)

ETSI has a group focused on securing AI and its use in cybersecurity.

- **ETSI GR SAI 005 - Securing Artificial Intelligence (SAI); Data Supply Chain Security**
  - **Description:** A group report addressing security issues in the data supply chain for AI, including data collection, storage, and processing.
  - **Link:** https://www.etsi.org/deliver/etsi_gr/SAI/005_099/005/01.01.01_60/gr_sai005v010101p.pdf
- **ETSI ISG SAI - Industry Specification Group on Securing Artificial Intelligence**
  - **Description:** The main page for all of ETSI's work on AI security, including published reports and ongoing work.
  - **Link:** https://www.etsi.org/committee/1420-sai

A.7.6 ANSI (American National Standards Institute)

As an accreditor, ANSI's role is to approve standards developed by other bodies (like NIST or IEEE) as American National Standards (ANS). For example, the **NIST AI RMF** is a key U.S. guidance document.

- **ANSI Website on AI:** https://www.ansi.org/standards-activity/emerging-technologies/artificial-intelligence

A.7.7 IETF (Internet Engineering Task Force)

The IETF's work related to AI is typically focused on how AI/ML is used to **manage networks** rather than standardizing AI itself.

- **Work on AI/ML for Networking:** Research and proposed standards often appear in the **IRTF (Internet Research Task Force)** or working groups like **NWGM (Network Working Group)**. There are no core AI protocol standards from IETF akin to those from ISO or IEEE.

A.8 Sensor Data Standards

A.8.1 IEEE (Institute of Electrical and Electronics Engineers)

IEEE has some of the most fundamental standards for sensors themselves, defining how their performance is measured and described.

- **IEEE 2700-2017** - **IEEE Standard for Sensor Performance Parameter Definitions**
  - **Description:** This is a critical standard that provides common definitions, units, conditions, and mathematical relationships for a wide set of performance parameters used in sensor specifications (e.g., for accelerometers, magnetometers, gyros). It enables comparison between different sensors.
  - **Link:** https://standards.ieee.org/ieee/2700/5915/ (Purchase required)
- **IEEE 1451** - **Standard for a Smart Transducer Interface for Sensors and Actuators**
  - **Description:** A family of standards that defines a set of common communication interfaces for connecting transducers (sensors or actuators) to microprocessors, instrumentation systems, and networks. Key parts include:
    - **IEEE 1451.0:** Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats.
    - **IEEE 1451.1:** Network Capable Application Processor (NCAP) Information Model.
  - **Link (Overview):** https://standards.ieee.org/ieee/1451/4519/ (Purchase required for individual parts)

A.8.2 ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission)

ISO and IEC standards often focus on the application layer, data representation, and system-level integration of sensor data.

- **ISO/IEC 30128:2014** - **Information technology — Sensor networks: Generic Sensor Network Application Interface**
  - **Description:** Specifies a generic application interface for sensor networks, facilitating interoperability at the application level.
  - **Link:** https://www.iso.org/standard/53248.html https://www.iso.org/standard/53200.html (Purchase required)
- **IEC 62714** - **Engineering data exchange format for use in industrial automation systems engineering - AutomationML**

- **Description:** AutomationML is a data format based on XML for storing and exchanging engineering data, including plant layout, kinematics, and logic. It is widely used to describe sensors and their data points within a manufacturing system.
- **Link (Part 1):** https://webstore.iec.ch/en/publication/65493 (Purchase required)

- **IEC 61850 - Communication networks and systems for power utility automation**
  - **Description:** While specific to the electrical power industry, this is a crucial standard for sensor data in substations. It defines abstract data models and services for communication between intelligent electronic devices (IEDs) like sensors and control systems.
  - **Link (Overview):** https://iec61850.dvl.iec.ch/

A.8.3 IETF (Internet Engineering Task Force)

The IETF develops the core protocols that enable sensor data to be transmitted over IP networks, which is the foundation of the Internet of Things (IoT).

- **RFC 8428 - Sensor Measurement Lists (SenML)**
  - **Description:** A simple, efficient, and lightweight data model for representing sensor measurements and device parameters. It defines a media type for SenML (application/senml+json) and is a cornerstone for RESTful IoT APIs.
  - **Link:** https://www.rfc-editor.org/rfc/rfc8428.html
- **CoAP (Constrained Application Protocol) - RFC 7252**
  - **Description:** A specialized web transfer protocol for use with constrained nodes and constrained networks. It is designed for machine-to-machine (M2M) applications and is commonly used by sensors to send data over the internet in a RESTful way, similar to HTTP but much lighter.
  - **Link:** https://www.rfc-editor.org/rfc/rfc7252.html

A.8.4 OGC (Open Geospatial Consortium)

The OGC specializes in standards for geospatial/location data, which is fundamental for any sensor with a location (e.g., environmental sensors, vehicle sensors).

- **Sensor Web Enablement (SWE) Suite**
  - **Description:** A suite of standards that enables developers to make all types of sensors, transducers, and sensor data repositories discoverable, accessible, and usable via the Web.
    - **SensorML:** Standard models and XML schema for describing sensor systems and processes.
    - **Observations & Measurements (O&M):** Conceptual model and XML schema for encoding observations and measurements from sensors.
    - **PUCK Protocol:** A protocol for retrieving a sensor's XML metadata directly from the device itself.
  - **Link:** https://www.ogc.org/standards/swe

A.8.5 NIST (National Institute of Standards and Technology)

NIST provides guidelines and frameworks for managing and securing sensor data, particularly in the context of IoT and cyber-physical systems.

- **NIST SP 800-183 - Networks of 'Things'**
  - **Description:** Provides a foundational model for understanding the complex relationships and data flows within networks of things, which are fundamentally built on sensor data.
  - **Link:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
- **NIST Cybersecurity for IoT Program**

- **Description:** While not a single standard, this program page provides links to all of NIST's work on IoT security, which is directly applicable to securing the data generated by sensors (e.g., NISTIR 8259 series).
- **Link:** https://www.nist.gov/programs-projects/cybersecurity-iot-program

A.8.6 ETSI (European Telecommunications Standards Institute)

ETSI's work on IoT (e.g., ETSI EN 303 645 for consumer IoT security) indirectly governs how sensor data from those devices should be protected. Their SmartM2M group also works on standards for IoT, including data aspects.

- **ETSI SmartM2M:** https://www.etsi.org/committee/1420-smartm2m

A.8.7 ITU-T (International Telecommunication Union)

ITU-T focuses on the networking and infrastructure aspects of transmitting sensor data, particularly for smart cities and utilities.

- **ITU-T Y.4000 / Y.2060 - Overview of the Internet of things**
  - **Description:** Provides a framework and definition for the IoT, which is the primary context for large-scale sensor data applications.
  - **Link:** https://www.itu.int/rec/T-REC-Y.2060

A.8.8 ANSI (American National Standards Institute)

As an accreditor, ANSI's role is to approve standards developed by other bodies (like IEEE or ISA) as American National Standards (ANS). For example, the **IEEE 1451** and **ISA100.11a** (wireless systems for automation) standards are also ANSI-accredited.

A.9 PQC Standards

A.9.1 NIST (National Institute of Standards and Technology)

NIST's PQC Standardization Project is the **central and most influential effort** globally. It has selected algorithms and is now in the process of publishing them as formal standards.

- **NIST PQC Standardization Project**
  - **Description:** The multi-year process to select and standardize quantum-resistant public-key cryptographic algorithms. It has concluded its third round, selecting algorithms for standardization and for further study.
  - **Link (Main Project Page):** https://csrc.nist.gov/projects/post-quantum-cryptography
- **Selected Algorithms for Standardization (FIPS)**
  - **FIPS 203 (Draft) - Module-Lattice-Based Digital Signature Standard (ML-DSA)**: Based on CRYSTALS-Dilithium.
    - **Link:** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf
  - **FIPS 204 (Draft) - Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)**: Based on CRYSTALS-Kyber.
    - **Link:** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf
  - **FIPS 205 (Draft) - Stateless Hash-Based Digital Signature Standard (SLH-DSA)**: Based on SPHINCS+.
    - **Link:** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.205.ipd.pdf
- **Additional Algorithms for Further Study (NISTIRs)**
  - **NISTIR 8413 - Status Report on the Third Round of the NIST PQC Standardization Process**

- **Description:** Details the results of the third round, including the selections and recommendations.
- **Link:** https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8413.pdf

- The algorithms **BIKE**, **Classic McEliece**, **HQC**, and **SIKE** are covered in separate NIST Internal Reports (NISTIRs) as candidates for future standardization.

A.9.2 ETSI (European Telecommunications Standards Institute)

ETSI has a dedicated group working on the practical implementation and migration aspects of PQC.

- **ETSI ISG QSC (Quantum-Safe Cryptography)**
  - **Description:** This Industry Specification Group produces reports and specifications to help industry and regulators migrate to quantum-safe cryptographic solutions. Their work includes use cases, implementation guidance, and testing requirements.
  - **Link (Main Group Page):** https://www.etsi.org/committee/1430-qsc
- **ETSI GR QSC 005 - Quantum-Safe Migration Recommendations and Guidance**
  - **Description:** A comprehensive report providing guidance on how to plan and execute a migration from current cryptography to quantum-safe alternatives.
  - **Link:** https://www.etsi.org/deliver/etsi_gr/QSC/001_099/005/01.01.01_60/gr_QSC005v010101p.pdf

A.9.3 IETF (Internet Engineering Task Force)

The IETF is working to integrate PQC algorithms into the core protocols that secure the Internet.

- **PQC in TLS (Transport Layer Security)**
  - **draft-ietf-tls-hybrid-design** - **Hybrid key exchange in TLS 1.3**
    - **Description:** An Internet-Draft defining how to combine classical and post-quantum key exchange algorithms in TLS to provide a transitional security layer.
    - **Link:** https://datatracker.ietf.org/doc/draft-ietf-tls-hybrid-design/
  - **draft-ietf-tls-pquip-pqc-engine** - **A PQC KEM for TLS 1.3**
    - **Description:** An Internet-Draft specifying how to use a post-quantum KEM (like Kyber) in TLS 1.3.
    - **Link:** https://datatracker.ietf.org/doc/draft-ietf-tls-pquip-pqc-engine/
- **PQC in X.509 Certificates and PKIX**
  - **draft-ietf-lamps-kyber-certificates** - **Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Kyber**
    - **Description:** Defines algorithm identifiers for the use of Kyber in Internet X.509 certificates and CRLs.
    - **Link:** https://datatracker.ietf.org/doc/draft-ietf-lamps-kyber-certificates/

A.9.4 ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

The joint technical committee **JTC 1/SC 27** is responsible for international security standards, including cryptography. They are working to adopt the NIST-selected algorithms as international standards.

- **ISO/IEC 14888-3:2018 (Under Amendment)** - **Information security — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms**
  - **Description:** This standard is being amended to include the lattice-based signature scheme **CRYSTALS-Dilithium** (ML-DSA).
  - **Link (Base Standard):** https://www.iso.org/standard/76382.html (Purchase required)

- **ISO/IEC 18033-2:2006 (Under Amendment) - Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers**
  - **Description:** This standard is being amended to include the key encapsulation mechanism **CRYSTALS-Kyber** (ML-KEM).
  - **Link (Base Standard):** https://www.iso.org/standard/38770.html (Purchase required)
- **New Work Items:** New standalone standards for the other NIST-selected algorithms (e.g., **Falcon**, **SPHINCS+**) are also in development within SC 27.

A.9.5 ITU-T (International Telecommunication Union)

ITU-T's Study Group 17 focuses on security and has recommendations related to PQC.

- **ITU-T X.1705 - Quantum key distribution network – Key management**
  - **Description:** While focused on Quantum Key Distribution (QKD), this shows ITU-T's work on quantum-safe security. Work on pure PQC algorithms often aligns with or references the work of NIST and ISO.
  - **Link:** https://www.itu.int/rec/T-REC-X.1705

A.9.6 ANSI (American National Standards Institute)

As an accreditor, ANSI's role will be to approve the final **NIST FIPS 203, 204, and 205** as American National Standards (ANS) once they are finalized.

A.9.7 IEEE (Institute of Electrical and Electronics Engineers)

While not leading the algorithm selection, IEEE has standards and projects related to the broader category of quantum-safe security.

- **IEEE P1363 - Standard for Public-Key Cryptography**
  - **Description:** This established standard specifies common public-key cryptography techniques. It is likely that future revisions or additions will incorporate post-quantum algorithms.
  - **Link:** https://standards.ieee.org/ieee/1363/2046/

A.10 Data Communication Standards

A.10.1 IETF (Internet Engineering Task Force)

The IETF is arguably the most important organization for data communication, as it creates the standards (RFCs) that form the core of the Internet.

- **TCP/IP Protocol Suite**
  - **RFC 791 - Internet Protocol (IP):** Defines the fundamental addressing and routing system of the internet.
    - **Link:** https://www.rfc-editor.org/rfc/rfc791
  - **RFC 793 - Transmission Control Protocol (TCP):** Provides reliable, ordered, and error-checked delivery of a stream of data between applications.
    - **Link:** https://www.rfc-editor.org/rfc/rfc793
  - **RFC 768 - User Datagram Protocol (UDP):** Provides a simpler, connectionless communication model without guarantees.
    - **Link:** https://www.rfc-editor.org/rfc/rfc768
- **Application Layer Protocols**
  - **RFC 2616 (Obsolete) / RFC 9110 - Hypertext Transfer Protocol (HTTP/1.1):** The foundation of data communication for the World Wide Web.
    - **Link (HTTP Semantics):** https://www.rfc-editor.org/rfc/rfc9110

- **RFC 7540 - Hypertext Transfer Protocol Version 2 (HTTP/2):** Major revision of HTTP for improved performance.
  - **Link:** https://www.rfc-editor.org/rfc/rfc7540
- **RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3:** The primary protocol for securing communications over a computer network (encryption, authentication).
  - **Link:** https://www.rfc-editor.org/rfc/rfc8446

- **Network Management**
  - **RFC 1157 - Simple Network Management Protocol (SNMP):** A protocol for managing devices on IP networks.
    - **Link:** https://www.rfc-editor.org/rfc/rfc1157

A.10.2 IEEE (Institute of Electrical and Electronics Engineers)

IEEE standards dominate the **Physical and Data Link layers** (Layers 1 & 2 of the OSI model), defining how data is framed and transmitted over physical media.

- **IEEE 802.3** - **Ethernet**
  - **Description:** The definitive standard for wired LAN (Local Area Network) technology. It defines the physical layer and the MAC (Media Access Control) layer for Ethernet.
  - **Link (Working Group):** https://standards.ieee.org/ieee/802.3/10495/ (Purchase required for full standard)
- **IEEE 802.11** - **Wireless LAN (Wi-Fi)**
  - **Description:** The set of standards for wireless local area networking (e.g., 802.11a/b/g/n/ac/ax). It defines the over-the-air interface.
  - **Link (Working Group):** https://standards.ieee.org/ieee/802.11/10590/ (Purchase required for full standard)
- **IEEE 802.1** - **Bridging and Network Management**
  - **Description:** Includes crucial standards like **802.1Q (VLANs)** and **802.1X (Port-Based Network Access Control)** for authentication on wired and wireless networks.
  - **Link (Working Group):** https://standards.ieee.org/ieee/802.1/10489/

A.10.3 ITU-T (International Telecommunication Union)

ITU-T standards are fundamental for global telecommunications infrastructure, including wide-area networks and optical transport.

- **ITU-T G Series** - **Transmission systems and media, digital systems and networks**
  - **Description:** Includes critical standards for digital transport, such as:
    - **G.709 (OTN):** Optical Transport Network (OTN) standard.
    - **G.993.2 (VDSL2):** Very-high-bit-rate digital subscriber line 2.
    - **G.hn:** A standard for home networking over coaxial cable, phone lines, and power lines.
  - **Link (G Series List):** https://www.itu.int/rec/T-REC-G/en
- **ITU-T X Series** - **Data networks, open system communications and security**
  - **Description:** Covers data networks, including:
    - **X.509:** The standard for public key infrastructure (PKI) and digital certificates, which is foundational for TLS/SSL.
    - **X.25:** An older packet-switching protocol, historically important.
  - **Link (X Series List):** https://www.itu.int/rec/T-REC-X/en

- **ITU-T H Series - Audiovisual and multimedia systems**
  - **Description:** Includes codecs for multimedia communication, e.g., **H.264 (AVC)**, **H.265 (HEVC)** for video, and **H.323** for VoIP.
  - **Link (H Series List):** https://www.itu.int/rec/T-REC-H/en

A.10.4 ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)

ISO/IEC often adopts and formalizes technologies into international standards and works on higher-layer protocols.

- **ISO/IEC 7498-1:1994 - The Basic Reference Model for Open Systems Interconnection (OSI Model)**
  - **Description:** The famous 7-layer conceptual model that describes the functions of a telecommunication or networking system.
  - **Link:** https://www.iso.org/standard/20269.html (Purchase required)
- **ISO/IEC 11801 - Information technology — Generic cabling for customer premises**
  - **Description:** Defines standards for structured cabling systems (e.g., for Ethernet) in buildings and campuses.
  - **Link:** https://www.iso.org/standard/70375.html (Purchase required)

A.10.5 ETSI (European Telecommunications Standards Institute)

ETSI standards are critical for European and global telecommunications, particularly for radio and mobile communications.

- **ETSI GSM, 3GPP (LTE, 5G)**
  - **Description:** While 3GPP now leads mobile communication standards (LTE, 5G), ETSI was a founding partner and hosts many of the key specifications.
  - **Link (3GPP Portal):** https://www.3gpp.org/
  - **Link (ETSI Mobile Standards):** https://www.etsi.org/technologies/mobile
- **ETSI EN 300 328 - Wideband transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band**
  - **Description:** A critical standard for regulating access to the 2.4 GHz band, which is used by Wi-Fi (IEEE 802.11), Bluetooth, and other devices in Europe.
  - **Link:** https://www.etsi.org/deliver/etsi_en/300300_300399/300328/02.02.01_60/en_300328v020201p.pdf

A.10.6 NIST (National Institute of Standards and Technology)

NIST provides guidelines, frameworks, and specific technical recommendations, often for U.S. government use.

- **NIST FIPS 140-3 - Security Requirements for Cryptographic Modules**
  - **Description:** Mandatory for U.S. federal agencies, this standard defines the security requirements for cryptographic modules used to protect sensitive information. It is critical for secure data communication.
  - **Link:** https://csrc.nist.gov/pubs/fips/140-3/final
- **NIST SP 800-52 - Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations**
  - **Description:** Provides guidance on properly using TLS to protect data communications.
  - **Link:** https://csrc.nist.gov/pubs/sp/800/52/r2/final