CELTIC-NEXT
Eureka Cluster

Project Report

CISSAN

Collective intelligence supported by security aware nodes

D7.2 Coordination of the Standardization Related Issues in other WPs

Editors: Ilgin Safak, University of Jyväskylä and Kurt Tutschku, Blekinge Tekniska Högskolan

Abstract

This report describes standardization-related activities across CISSAN work packages, as per the CISSAN Standardization Action Plan defined in D7.1. It describes the design and implementation of the five project use cases, transportation, smart grids, tunnelling construction, manufacturing execution systems, and automated disaster recovery, and their compliance with industry standards, regulations, and best practices. The report explains CISSAN's contribution to standards with the adoption and expansion of the STIX threat report format to facilitate standardization, interoperable, and machine-readable threat intelligence and runtime collective intelligence sharing in IoT and OT environments. It also describes CISSAN's plans for the potential compliance of the CISSAN platform with NIST post-quantum cryptography (PQC) standards and NIS PQC implementation roadmap post-project to ensure a long-term, cryptographic resilience for the security-critical communications. The report overall demonstrates the spanning, domain, and standards use to optimize interoperability, security, and the practical applicability of CISSAN's technical outcomes.

Project CISSAN

Public Report

October 2025

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

- University of Jyväskylä (coordinator)
- Affärsverken Karlskrona AB
- Arctos Labs Scandinavia AB
- 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

D7.2 Coordination of the Standardization Related Issues in other WPs

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

Project coordinator: Ilgin Safak, University of Jyväskylä

CELTIC published project result

Executive Summary

This report provides a structured overview of the efforts required to coordinate the standardization of the project's work packages. To ensure the project follows best practices, industry standards, and regulatory frameworks, these activities were conducted in accordance with the CISSAN Standardization Action Plan defined in D7.1. The design and implementation of the five project use cases, namely transportation, smart grids, tunnelling construction, manufacturing execution systems, and joint use case (automated disaster recovery), have been done with a rigorous emphasis on adherence to standards to enhance their utility in the industry, ensure their safety, and facilitate interoperability with other systems. In particular, the project has both adopted and contributed to standardization by extending the Structured Threat Information eXpression (STIX) threat report format, enabling enhanced support for runtime collective intelligence, trust assessment, and automated response in Internet of Things (IoT) and Operational Technology (OT) environments. This has been achieved while maintaining interoperability with existing STIX-based ecosystems.

Parallel to this, the project has investigated the implementation of National Institute of Standards and Technology (NIST) post-quantum cryptography (PQC) standards and Network and Information Systems (NIS) PQC roadmap to guarantee the long-term cryptographic resilience and regulatory alignment of security-critical communications with its potential compliance post-project.

Through the execution of the CISSAN Standardization Action Plan in D7.2, the CISSAN project guarantees and ensures that its technical outputs are interoperable, future-proofed, and directly applicable to real-world industrial deployments by coordinating these activities across work packages and use cases. Additionally, it contributes to European leadership in secure and trustworthy critical infrastructures.

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

- Jari Partanen, Bittium
- Kurt Tutschku, BTH
- Anders Liden, Clavister
- Klaus Chmelina, GeoData
- Teemu Kemppainen, Mattersoft
- Oliver Bölin, Techinova
- Kristian Kratschmer, Techinova
- Veikko Markkanen, University of Jyväskylä (JYU)
- Ilgin Safak, University of Jyväskylä (JYU)

Table of Contents

Abbreviations

AES	Advanced Encryption Standard
AI	Artificial intelligence
CISSAN	Collective intelligence supported by security aware nodes
CER	Critical Entities' Resilience
CLI	Command-Line Interface
CRA	Cyber Resiliency Act
CRYSTALS	Cryptographic Suite for Algebraic Lattices
CSA	Cybersecurity Act
CSF	Cybersecurity Framework
CTI	Cyber Threat Intelligence
ECC	Elliptic Curve Cryptography
EN	European Standard
EMC	Electromagnetic Compatibility
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
IACS	Industrial Automation and Control Systems
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
ISGs	Industry Specification Groups
ISO	International Organization for Standardization
IT	Information Technology
ITxPT	Information Technology for Public Transport
JSON	JavaScript Object Notation
JSONL	JSON Lines
KATAKRI	Kansallinen Turvallisuusauditointikriteeristö
MES	Manufacturing Execution System
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
OASIS	Organization for the Advancement of Structured Information Standards
OT	Operational Technology

PQC	Post-Quantum Cryptography
RED	Radio Equipment Directive
RSA	Rivest Shamir Adelman
SCADA	Supervisory Control and Data Acquisition
SCO	STIX Cyber-observable Object
SDO	STIX Domain Object
SIEM	Security Information and Event Management
SP	Special Publications
STIX	Structured Threat Information eXpression
UC	Use Case
VPN	Virtual Private Network
WP	Work Package

1 Introduction

The CISSAN project aims to support the design of its platform by providing guidance through a concise process that verifies the platform's compliance with current security standards and directives, and by contributing to standards.

This report provides a structured overview of efforts to coordinate and implement standardization across the project's platform design work packages (WPs). These activities were conducted in accordance with the CISSAN Standardization Action Plan, as defined in the CISSAN deliverable D7.1 report, which ensures that the CISSAN project follows best practices, industry standards, and security regulatory frameworks. The standardization-related phases for new standards (or enhancements to existing ones) in the CISSAN standards activity plan are depicted in Table 1. The tables also list activities for these phases and the two foci areas of Structured Threat Information eXpression (STIX) and Post-Quantum Cryptography (PQC), as prioritized by the standardization gap analysis in D7.1. D7.2 describes the execution and results of the three (out of four) that are marked by grey-shaded boxes. The "Assign Ownership and Governance" is described in the CISSAN deliverable D7.1 report.

The first phase, which was conducted and documented in the CISSAN deliverable D7.1 report, is the "Define Standardization Action" phase. This involves the plans for identifying possible technical enhancements to the STIX threat report standard as means to contributing to standards and the potential compliance of the CISSAN platform with National Institute of Standards and Technology (NIST) PQC standards and Network and Information Systems (NIS) PQC roadmap post-project.

The second phase, which is part of this CISSAN deliverable, D7.2, is the "Coordinate with work packages" phase. It details the activities conducted in the work packages for enabling the CISSAN platform and its use case solutions to comply with relevant security standards. It also presents potential approaches for implementing the STIX standard enhancement in its use cases.

The third phase discussed here is the "Engage with Standardization" phase. It describes the interactions and communications achieved and planned by the CISSAN project with the relevant standard defining organizations.

Table 1. Activities in the Standardization Action Plan for CISSAN

Phases of the Standardization Action Plan framework (see Figure 1)	**Activity**	
	STIX	**PQC**
Define Standardization Action	Detail current STIX capabilities and suggest enhancements for collaborative intelligence in cybersecurity using distributed AI	Detail discussion with CISSAN platform design specific current PQC 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

1.1 Structure of this Document

After this introduction, D7.2 outlines in Section 2 the platform's compliance with existing standards and applies the use cases to make this description auditable.

Section 3 discusses the contribution to relevant security standards. This entails a suggestion for extending the STIX threat report format for the exchange of cybersecurity threat information. It is explained how STIX is used in CISSAN, the interactions with the WPs on the STIX implementation in the CISSAN platform, and the planned interaction with the standard defining organization responsible for STIX.

Section 4 addresses CISSAN's potential compliance with the NIST PQC standards and NIS PQC roadmap post-project. The section briefly outlines the PQC standards considered, a feasibility analysis for the potential integration of PQC in the CISSAN platform and next steps for the potential compliance of the CISSAN platform with the relevant PQC standards.

Lastly, Section 5 provides the conclusions of the report.

2 Compliance of the CISSAN Platform and Use Cases with Standards

Compliance with relevant technical standards is crucial to realizing the goals of interoperability, security, and scalability within a complex digital platform. The CISSAN has considered the relevant international standards and best practices governing data exchange, security, and system interoperability, among other factors as described in the CISSAN deliverable D2.3 report. The alignment of the CISSAN platform and its use case solutions with the relevant standards and best practices helps to realize the goals of the platform, including the ability to work with other systems and infrastructures within the diverse deployment environments. This section analyses the conformity of the design and implementation of the CISSAN platform and its use case solutions with the relevant standards and regulations defined in the CISSAN Standardization Action Plan in the CISSAN deliverable D7.1 report.

2.1.1 Compliance of Use Case 1 with Standards

Use case 1 system aligns with five main standardization and regulatory frameworks:

- Information Technology for Public Transport (ITxPT) Global Navigation Satellite System (GNSS) v2.2.0
- International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) 27001:2022 (selected Annex A controls)
- NIST Special Publications (SP) 800-53 (selected controls for monitoring, logging and access control)
- NIS2 Directive (Article 21 security measures)

Use case 1 partners implemented a GNSS data integration and anomaly detection pipeline. Real-time vehicle positioning data is transmitted over authenticated and encrypted Message Queuing Telemetry Transport (MQTT) channels and basic integrity and plausibility checks are applied before ingestion by the anomaly detection module. Logging and monitoring of events are partially implemented to support system observability. Compliance has been assessed through interface testing and configuration reviews. The implementation relates primarily to WP2, WP4 and WP5.

2.1.2 Compliance of Use Case 2 with Standards

CISSAN use case 2 aligns with IEC 62443 requirements for secure Industrial Automation and Control Systems (IACS) architectures and complements IEC 62351 communication security by introducing AI-based distributed anomaly detection within secured grid communication channels. Furthermore, it supports NIS2 obligations for risk management and incident detection for operators of essential energy services.

In detail, the use case should strive to comply with the following standards.

At regulatory and governance levels:

- NIS2 directive
- Critical Entities' Resilience (CER) directive
- ISO27K, where ISO27019 regarding energy production and distribution is of special importance

At the Operational Technology (OT)/ Industrial Control Systems (ICS) level:

- IEC62443, specifically 3-3 to 4-2 regarding cybersecurity and networking.
- IEC60870-5-104 for any ICS data between edge devices and Supervisory Control and Data Acquisition (SCADA). For substation automation, compliance with IEC61850. These should further be compliant with IEC62351 to enhance the security.
- IEEE2030 provides guidance for smart grid architecture and integration that aligns with the scope of the use case.
- European Standard (EN) 17927 is a more recent framework that is highly relevant in the use case. This will further provide conformance with EU Cyber Resilience Act (CRA) and IEC62443.

For any hardware developed that intended to sit at substation level, the following standards apply:

- Electromagnetic Compatibility (EMC) IEC61000,
- Environment robustness (IEC60068)
- For wireless devices, compliance with the EU Radio Equipment Directive (RED) is mandatory

2.1.3 Compliance of Use Case 3 with Standards

At current stage, the developed use case 3 systems (= Data Quality Verification System, Blockchain-based Data Transfer System, Security Chip-based Data Signing System) are regarded as compliant with the following security-related regulatory framework:

- General Data Protection Regulation (GDPR)

Compliance with the following further security-related standards and regulations have been considered but not implemented (only some of the related processes are implemented):

- ISO 27001, ISO42001, NIS2, NIST PQC, CRA, Cybersecurity Act (CSA), AI Act, STIX

Use case 3 partners developed the requirements and architectures of the above mentioned 3 systems in WP2, and their prototypes in WP4 and WP5.

2.1.4 Compliance of Use Case 4 with Standards

The standards the use case 4 system is compliant with are as follows:

- ISO/IEC 27001:2022 (selected controls applicable to system) - Subject to continuous evaluation
- NIST SP 800-53 (selected controls for monitoring, logging and access control)
- Kansallinen Turvallisuusauditointikriteeristö (KATAKRI) 2020 (Finnish regulation)
- GDPR
- NIS2 Directive (Article 21 security measures)
- Relevant security encryption standards compliancy (Advanced Encryption Standard (AES)-256),
- Later also related PQC standard (NIST PQC). Bittium has in its possession Bittium SafeMove Virtual Private Network (VPN) products that are already compliant with PQC, but are also subject to further enhancements.

At the moment, the use case 4 system is under the Verification phase.

2.1.5 Compliance of Use Case 5 and the CISSAN Platform with Standards

In use case 5, CISSAN addresses the need to secure and scale automated disaster recovery across diverse systems and infrastructures from cross-domain critical infrastructure threats, including future quantum computing threats. This requires collaboration, speed, automation, and trust among diverse systems and infrastructures, which makes it extremely vulnerable to sophisticated and high-level risks related to weak cryptography and security protocols and mechanisms. To address these concerns, the CISSAN platform has been implemented to comply with the security standards identified in the CISSAN Standardization Action plan in D7.1 as follows:

- IEC 62443 and ISO/IEC 27001 for the SCADA server
- ISO/IEC 27001 and NIS2 for the CISSAN Management Server
- ISO/IEC 27001 and NIS2 for the CISSAN Orchestration Server
- ISO/IEC 27001 and NIS2 for the Security Information and Event Management (SIEM) Server
- ISO/IEC 27001 for the Arctos Labs Optimization Solver connected to the CISSAN Management Server
- ISO/IEC 27001 and NIS2 for the Councilbox Blockchain System connected to the CISSAN Management Server
- ITxPT GNSS, ISO/IEC 27001, and NIS2 for the Mattersoft Global Positioning System (GPS) system connected to the CISSAN Management Server
- ISO 27001 for the Clavister PASAD system connected to the CISSAN Management Server

Additionally, all CISSAN platform components are compliant with GDPR. The CISSAN Management Server is designed and implemented to support an extended version of the STIX threat report format for threat information sharing, including the proposed new trust object (see Section 3 for details).

Additionally, the CISSAN platform is intended to comply with NIST PQC standards and NIS PQC roadmap post-project (see Section 4 for details).

3 Contribution to Standards: STIX – A Data Structure and Protocol for the Exchange of Cybersecurity Threat Information for Collaborative Intelligence in Cybersecurity

3.1 Introduction to STIX

The Structured Threat Information Expression (STIX) is an open standard, maintained by Organization for the Advancement of Structured Information Standards (OASIS), originally developed by MITRE, for representing and exchanging Cyber Threat Intelligence (CTI). STIX defines a common data model and serialization syntax, typically expressed in JavaScript Object Notation (JSON), that allows diverse systems to describe cyber threats in a structured and machine-readable way. By supporting concepts such as threat actors, indicators, attack patterns, and the relationships between them, STIX enables interoperability among security platforms and organizations. Its openly published specification and broad adoption make it a widely used format for CTI exchange, particularly valuable for organizations with limited resources seeking to participate in collaborative CTI sharing networks alongside larger institutions. A more detailed explanation of the standard is provided in the CISSAN deliverable D5.4 report.

3.2 Potential Usage of STIX in CISSAN

Within the CISSAN project, the focus lies in distributing security responsibilities across network participants to enhance overall resilience. CTI sharing represents a natural extension of this approach: it allows nodes to exchange local knowledge, transforming isolated observations into shared situational awareness. In this context, adopting STIX as a representation format aligns with CISSAN's vision of resource-efficient, cooperative, and proactive cybersecurity, empowering even constrained devices or organizations to contribute to, and benefit from, a broader intelligence ecosystem.

STIX is therefore intended to serve as a standardized representation layer for enabling the exportation of selected security outcomes. Two requirements drive this choice. First, the format must be widely recognized to maximize interoperability and adoption. The value of intelligence sharing increases when more participants can ingest and interpret it. Second, the format must be extensible, because CISSAN generates security concepts that are not always represented directly in conventional CTI models.

In practise, the CISSAN platform leverages the concept of trust for security governance. Trust related events are not naturally represented by STIX. However, this is a major analyst level concept, and a status change in the system, which should be recorded and shared with interested parties to gain further insight into security incidents. It is also a forward-looking approach: if CISSAN concepts transition into production use and see wider adoption, a standardized mechanism for representing and sharing trust-based security events becomes essential for integrating these outcomes into established CTI sharing workflows.

Considering the adoption of STIX provides value to both consortium partners and the wider industry by enabling interoperable CTI exchange and supporting increased cybersecurity maturity across connected systems.

To support interoperability beyond the project, the consortium has initiated contact with the relevant STIX standardisation bodies at OASIS to communicate the project's observations regarding trust-related data modelling. The objective is to communicate implementation experience from the project and contribute these observations to the wider standards discussion. The formal communication process through the appropriate OASIS channels is ongoing.

3.3 Implemented or Foreseen Activities in the Work Packages STIX

CISSAN prototypes automated STIX report generation as an export mechanism that transforms selected platform outputs into STIX 2.1 bundles. The detailed technical workflow is described in the dedicated implementation documentation (D5.4). At a high level, STIX bundle generation is designed to be triggered by significant trust-related security events. This approach keeps CTI output high-signal and operationally meaningful, while maintaining traceability to supporting evidence.

From a use-case perspective, the implementation is evaluated under Use Case 2, where constrained devices and centrally managed telemetry make it an appropriate environment for prototyping trust-triggered CTI export. Selecting this use case is also strategically efficient: the STIX generation is performed on the CISSAN Management Server, and the exported bundles depend primarily on the availability of standardized JSON Lines (JSONL) telemetry and trust events rather than on use-case-specific OT processes. As a result, once the pipeline and object mappings are validated in the most constrained setting, the approach can be extended to other CISSAN use cases that expose comparable report formats and trust evaluations, without requiring changes to the underlying STIX generation logic. This choice is also practically feasible: it minimizes dependencies on parallel development activities and enables implementation and validation within the project timeframe.

Use Case 1: Public transportation

STIX integration has been considered in Use Case 1. The overarching goal of achieving a unified, secure, and automated monitoring system, requires a method to deliver observed anomalies to relevant parties. STIX is a suitable candidate for achieving these goals.

In UC1, the focus is GNSS-related security anomalies. The project implements a layered architecture to detect, report, and respond to these types of anomalies in public transportation. The detected anomalies encapsulate movement metadata, anomaly scores, geolocation, and references a location object. While currently, the anomalies are handled within the system, STIX can be used to extend the approach by parsing this information into a standardized format, for sharing with the relevant CTI channels. This also enables further integration into existing SIEM systems.

The key challenge, similar to UC2, is that many attributes are not recognized by standard STIX types. In UC2, the custom elements are proposed as extensions to the format: the main extension being the trust score STIX domain object (SDO), but also project-specific STIX cyber-observable objects (SCOs) produced by pre-publication tools. These are referred to using the “x-” prefix, as custom elements typically are addressed in STIX. In UC1, a different approach is used. Instead of creating complete STIX bundles, the anomalies are represented as individual observed-data SDOs, and the use-case-specific elements are embedded under properties. While this is readable, properties is not a standard STIX 2.1 field for observed data.

Despite the observed limitation, a theoretical implementation was considered. Similar to UC2, a parser is required to generate the report from source data. The proposed integration treats STIX observed data as the entry point: the parser extracts labels to identify the device and anomaly status, and if properties exist, parses them into structured fields for enrichment. Alerting can then be triggered when labels include “anomaly” or when anomaly-score fields exceed thresholds. For operational context, latitude/longitude are used for geospatial mapping, and trip/route identifiers are used to correlate with other telemetry and route metadata. Finally, object_refs can be used to link to additional STIX objects so that anomalies can be shared beyond the local system and aggregated over time to detect patterns. The following structure represents the complete STIX payload structure projected for sharing in UC1 context:

```
{
  "type": "observed-data",
  "id": "observed-data--<UUID>",
  "created": "<ISO 8601 UTC timestamp>",
  "modified": "<ISO 8601 UTC timestamp>",
  "first_observed": "<ISO 8601 UTC timestamp>",
  "last_observed": "<ISO 8601 UTC timestamp>",
  "number_observed": <integer>,
  "labels": ["gnss", "anomaly", "<device_id>"],
  "object_refs": ["location--<UUID>"],
  "description": "GNSS anomaly: original payload included.",
  "properties": {
    "device_id": "<string>",
    "latitude": <float>,
    "longitude": <float>,
    "created_at": "<timestamp with timezone>",
    "speed": <float>,
    "bearing": <float>,
    "movement_type": "<string>",
    "short_trip_id": <integer>,
    "is_near_stop": <boolean>,
    "shape_id": "<string>",
    "current_stop": <integer|null>,
    "distance_to_path": <float>,
    "time_diff": <float>,
    "distance": <float>,
    "acceleration": <float>,
    "distance_growth": <float>,
    "bearing_speed": <float>,
    "anomaly_score_iforest": <float>,
    "is_anomaly_iforest": <boolean>,
    "anomaly_score_lof": <float>,
    "is_anomaly_lof": <boolean>,
    "timestamp": "<ISO 8601 timestamp>"
  }
}
```

Use Case 2: Smart Grids

UC2 is the primary implementation context for the custom STIX integration, which is described in detail in the CISSAN deliverable D5.4 report.

To overview this effort, a custom parser is created to leverage the standardized JSONL output from UC2 tools. This parser is triggered upon significant trust related state change within the OT segment, resulting in the creation of a custom Trust SDO. Trust SDO is connected to the Observed Object SDO's, which aggregates the relevant evidence regarding the major state change. The result is a custom STIX 2.1 bundle (JSON file), which can later be pushed to appropriate CTI sharing channels. The following structure represents the complete STIX payload structure generated in UC2 context:

```
{
  "type": "bundle",
  "id": "bundle--<UUID>",
  "spec_version": "2.1",
  "objects": [
    {
      "type": "identity",
      "spec_version": "2.1",
      "id": "identity--<RTU_UUID>",
      "created": "<ISO 8601 UTC timestamp>",
      "modified": "<ISO 8601 UTC timestamp>",
      "name": "<rtu_id>",
      "identity_class": "device"
    },
    {
      "type": "observed-data",
      "spec_version": "2.1",
      "id": "observed-data--<UUID>",
      "created": "<ISO 8601 UTC timestamp>",
      "modified": "<ISO 8601 UTC timestamp>",
      "first_observed": "<ISO 8601 UTC timestamp>",
      "last_observed": "<ISO 8601 UTC timestamp>",
      "number_observed": 1,
      "objects": {
        "0": {
          "type": "x-rotor-event",
          "event_type": "<string>",
          "subtype": "<string>",
          "source": "<string>",
          "source_rtu": "<string>",
          "severity": <integer>,
          "timestamp_unix": <integer>,
          "message": "<string>",
          "metadata": { "<key>": "<value>" }
        }
      }
    },
    {
      "type": "x-cissan-trust-score",
      "spec_version": "2.1",
      "id": "x-cissan-trust-score--<UUID>",
      "created": "<ISO 8601 UTC timestamp>",
      "modified": "<ISO 8601 UTC timestamp>",
      "target_ref": "identity--<RTU_UUID>",
      "score_value": <float>,
      "score_threshold": <float>,
      "is_below_threshold": <boolean>,
      "calculation_method": "<string>",
      "basis_refs": ["observed-data--<UUID>"],
      "explanation": "<string>"
    }
  ]
}
```

Use Case 3: Tunnel Construction

STIX has been identified as a useful standard to report and exchange data on threats like data tampering attacks that are detected by the data quality verification system developed. The potential adoption of STIX for use case 3 systems will be considered post-project, based on, e.g., customer requirements.

Use Case 4: Bittium Manufacturing Execution System

The use of the suggested STIX threat report format to document threats could potentially be applied to the Bittium virtual manufacturing execution system (MES) for documenting and exchanging information about cyber security-related incidents that take place within interconnected manufacturing processes. By making use of STIX objects to model assets and processes as well as detected anomalies, it would allow for more standardized and interoperable reporting within the manufacturing environment. The potential adoption of STIX for MES will be considered post-project, based on, e.g., customer requirements.

Use Case 5: Joint Use Case

As part of WP5 work on collective intelligence, it was identified that there is a need for using a standard format for sharing collective intelligence in IoT/OT networks, where the STIX standard was selected. As the STIX threat report format currently does not support sharing of the collective intelligence mechanisms developed in the project, it has been extended to include trust scores and anomaly risk scores. The CISSAN management server implementation work has been conducted to support the extended STIX standard.

Work Packages

The STIX-related effort primarily supports WP7 and WP5. WP7 addresses standardization-related activities and requires the project to consider and contribute to relevant security standards. In this context, the adoption of STIX, and particularly the proposed extension for representing trust-related events, directly advances the project's standardization objectives by demonstrating how CISSAN outputs can be modelled and exported in a recognized CTI format. In parallel, using STIX aligns CISSAN with established CTI exchange practices and improves interoperability with existing security tooling, which supports broader collaboration and strengthens collective security across the sector. The same activity also aligns with WP5, as it provides a concrete mechanism for extending CISSAN's collective-intelligence approach beyond local detection and internal coordination. By enabling CISSAN security outputs to be packaged and shared using an industry-recognized CTI format, STIX supports higher cyber maturity by facilitating future integration with SIEM/CTI platforms and enabling external stakeholders to consume and act on project-generated intelligence. While WP7 and WP5 form the core linkage, the work also interfaces with other efforts in CISSAN, including architectural integration and proof-of-concept validation, since standardized export requires consistent data modelling, clear trigger conditions, and repeatable generation workflows.

WP4

Use Case 3: Tunnel Construction

The use of STIX has been analysed and the technical efforts required to implement the standard have been explored. Decision on and further steps towards its implementation are post-project.

WP6

Use Case 5: Joint Use Case

STIX 2.1 (JSON) has been adopted as a standard cyber threat intelligence format for representing and exchanging machine-readable threat, anomaly, and trust-related data in use case 5, where the following activities have been conducted:

- Implemented automated STIX bundles on the CISSAN Management Server, which is initiated by trust score threshold violation events that lead to blacklisting of components that are either compromised or not trustworthy.
- Extended the data model with a custom data structure called 'Trust Score Structured Data Object,' with the identifier 'x-cissan-trust-score,' for representing dynamic trust assessments of devices, services, and segments of the network.
- Linked Trust Score with supporting anomaly evidence, providing contextualized reports that combine trust scores with indicators, alerts, and observed information.

- Made enhancements to improve correlation of events and pieces of evidence in time, providing more accurate, interpretable, and relevant STIX reports.

- Facilitated the automated consumption of enriched STIX bundles by platform components to enable real-time disaster recovery activities across distributed systems and stakeholders.

4 Future Compliance: Post-Quantum Cryptography

4.1 Introduction to PQC

PQC refers to a group of cryptographic algorithms that have the capability to provide the highest level of security against any kind of cyberattack from classical as well as quantum computers [1]. The development of quantum computers is a major threat to the widespread use of classical cryptographic techniques like Rivest Shamir Adelman (RSA) [2] and Elliptic Curve Cryptography (ECC) [3]. These cryptographic techniques use mathematical problems that can easily be solved by the quantum computers using Shor's algorithm. On the contrary, the PQC algorithms use different mathematical problems that cannot be easily solved by the classical or quantum computers. These mathematical problems include lattice-based cryptography, hash-based cryptography, code-based cryptography, and multivariate polynomial-based cryptography. The development of quantum computers is in the early stages, and the NIST has initiated the standardization of PQC algorithms.

It is very important to adopt the PQC standards to ensure interoperability of the system. By adopting the PQC standards, the system will be able to achieve compatibility with the upcoming digital infrastructure. Moreover, the use of PQC standards will provide long-term benefits to the system. The system will be able to protect the data from the “harvest now, decrypt later” threat. The data stored in the system will be safe from the upcoming quantum computers. The PQC standards will provide long-term benefits to the system. The system will be able to adapt to the changes in the upcoming days. Moreover, the system will provide the highest level of security to the data.

4.2 Potential Usage of PQC in CISSAN

The PQC command-line interface (CLI) tool developed by JYU outside of the CISSAN project was customized for CISSAN as part of collaboration between the CISSAN and AIQUSEC projects. It enables quantum-resistant data encryption, data decryption, and data signing of the payload data for ensuring compliance with the NIST PQC standards and NIS PQC implementation roadmap. ML-DSA [4], formerly known as CRYSTALS-Dilithium, is used as a signature scheme for secure signing of commands, threat reports, and recovery instructions. ML-KEM [5] (previously referred to as CRYSTAL-Kyber) is used as the key encapsulation mechanism to offer 32-byte quantum-resistant data encryption. The tool also provides tunable levels of security with the PQC tool by offering support for Dilithium2, Dilithium3, and Dilithium5 for signatures and Kyber512, Kyber786, and Kyber1024 for key encapsulation in various configurations. The aim is to ensure the sustainability of the CISSAN project results by future proofing the CISSAN platform’s security stance against quantum attacks by protecting sensitive information exchanged between the CISSAN Management Server and external parties.

4.3 Foreseen Activities in the Work Packages for PQC Related Standardization Activities

WP1

As part of WP1 work, quantum computing was identified to pose a threat to the sustainability of project results post project. As a result, a standardization gap was identified for the project and was agreed upon during the Standardization meeting on May 9, 2025, by the consortium to ensure the compliance of the CISSAN platform, including the CISSAN server and connecting external systems, with NIST PQC standard and NIS PQC implementation roadmap to future proof the CISSAN platform against quantum attacks. This led to a need for collaboration between the CISSAN and AIQUSEC projects, where the PQC tool developed by JYU has been customized for CISSAN. The aim is to

determine the suitability of using such a PQC tool for ensuring the compliance of the CISSAN platform and its use case solutions with NIST PQC standards post-project.

WP6

The following activities were performed in WP6 in relation to UC5:

- Meetings were held with the AIQUSEC project team to determine the most economically and technically feasible approach for integrating PQC into the CISSAN platform and its use case solutions.
- The need for developing and integrating a PQC tool to secure and decrypt use case data, allowing the CISSAN management server and CISSAN platform entity elements to secure all payloads was identified.
- The PQC CLI tool developed by JYU outside of the CISSAN project was customized to ensure the compatibility of the tool with all use cases.
- The PQC CLI tool was analysed to determine the feasibility of integrating it with the CISSAN Management Server and connecting external systems, including the Councilbox Blockchain System, the Arctos Labs Optimization Solver, the Clavister PASAD system and the Mattersoft GPS system.
- The PQC CLI tool is aimed to be integrated post-project will be delivered as a compiled binary executable to enable portability, performance, and ease of use for heterogeneous architectures. Configuration capabilities within the PQC tool are to be provided for generation of cryptographic assets, key management, and loading of runtime parameters.

5 Conclusion

This report provides an overview of the coordination of the standardization activities carried out within the CISSAN project across the different work packages to carry out the actions defined in the CISSAN deliverable D7.1 CISSAN Standardization Action Plan to enable an auditable, security standards compliant CISSAN platform. This involves three main standardization activities within the CISSAN project: a) the CISSAN platform's and its use case systems' compliance with existing standards (auditability feature), b) the contribution to existing standards by developing a suggestion for extending the STIX threat report format, and c) the potential future compliance with post-quantum cryptography (PQC) standards for the sustainability of the CISSAN platform.

As part of the activities related to the compliance with standards, the CISSAN consortium has ensured the compliance of the CISSAN platform and its use case solutions with the standards defined in the D7.1 Standardization Action Plan including ETSI, ISO, IEEE, and IETF standards that relate to interoperability, cybersecurity, and distributed systems architecture. By ensuring the compliance of the CISSAN platform with relevant security standards and regulations, the CISSAN project has ensured the interoperability of CISSAN platform with larger digital ecosystems.

Regarding activities related to contributing to standards, the consortium proposed an extension to the Structured Threat Information eXpression (STIX) threat reporting format with the aim of enabling the relevant threat reporting requirements for the CISSAN use cases to support trust management. The consortium also contacted the STIX authorities for the proposed extension.

Additionally, as part of future compliance of the CISSAN platform with PQC, the consortium collaborated with the AIQUSEC project to determine the most technically and economically feasible approach and conducted a preliminary analysis of a PQC tool for its potential integration with the CISSAN platform and connecting use case systems. Compliance with PQC standards will be relevant for the long-term sustainability of the CISSAN platform's security.

At the same time, the CISSAN project seeks to develop new architectures and approaches to improve the state of the art, especially regarding the concept of collective intelligence and collaborative cybersecurity infrastructures. However, the inclusion of standardization activities within the context of innovation-oriented approaches to research and development might raise some challenges, especially because standards are often developed after the relevant technologies have become mature enough to support the development of standards around them. An important lesson learned from the context of the CISSAN project is the necessity to develop structured mechanisms to facilitate the interaction between research and standardization communities.

In this context, greater collaboration with standardization communities and collaborative specification approaches, such as ETSI Industry Specification Groups, might enhance the association between research and standardization communities and activities. Consequently, the coordination of standardization activities within the context of the project has enabled the development of the CISSAN platform to align with the relevant standards, while at the same time identifying opportunities to make contributions to the relevant standards in the future.

References

[1] D. J. Bernstein, J. Buchmann and E. Dahmen, Post-Quantum Cryptography, Berlin, Germany: Springer, 2009.

[2] J. Katz and Y. Lindell, Introduction to Modern Cryptography, 2 ed., Boca Raton, FL, USA: CRC Press, 2014.

[3] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, New York, NY, USA: Springer, 2004.

[4] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Digital Signature Standard (ML-DSA). FIPS PUB 204," NIST, Gaithersburg, MD, 2024.

[5] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM). FIPS PUB 203," NIST, Gaithersburg, MD, 2024.