Project Report

CISSAN

Collective intelligence supported by security aware nodes

D6.3 Joint use case demonstration and CISSAN framework

Editor: Ilgin Safak, University of Jyväskylä

Abstract

This report presents the joint use case demonstration that was carried out within the CISSAN project, as well as the way in which the CISSAN framework facilitates the joint use case validation for coordinated cybersecurity activities in various sectors. The joint use case focuses on the mitigation of a multi-domain critical infrastructure attack, where the cascading effect of the attack is mitigated through automated disaster recovery, collective intelligence, and collaborative defence mechanisms. Three use cases—transportation, smart grids, and tunnel construction—were incorporated into the CISSAN framework to represent realistic cross-sectoral dependencies for the joint use case scenario. This report presents the choreography of the joint use case scenario, highlighting the way in which heterogeneous components, use case-specific systems, and security services interact with one another through well-defined interfaces and shared intelligence to address the cyber-attack scenario in real time. Furthermore, this report presents the way in which the CISSAN framework facilitates the joint use case scenario, highlighting the way in which common services are provided for the joint use case scenario to operate autonomously while providing a unified cyber defence mechanism against the cyber-attack scenario.

Project **CISSAN**

Public

April 2026

Participants in project CISSAN are (in alphabet order with the 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

D6.3 CISSAN platform and solutions for the project use cases

Editor: Ilgin Safak, University of Jyväskylä

Project coordinator: Ilgin Safak, University of Jyväskylä

CELTIC published project result

2026 CELTIC-NEXT participants in project CISSAN

Executive Summary

This report presents a joint use case demonstration of the CISSAN project, highlighting its capabilities in facilitating joint, cross-sector cybersecurity operations through collective intelligence, disaster recovery, and defence. The joint use case focuses on a multi-domain critical infrastructure cyber-attack scenario that affects transportation, smart grids and tunnel construction infrastructures, where the cascading effects of such a cyber-attack propagate through interconnected critical infrastructures, requiring immediate, automated, and trusted coordination of diverse platforms and entities.

This report presents a detailed description of the choreography of the joint use case, including how security information, trust information and threat intelligence are shared, and automated disaster recovery is performed, and incidence response is coordinated among the three use cases through the CISSAN platform. The shared services provided through the CISSAN framework, including Structured Threat Information eXpression (STIX) based sharing of threat intelligence, trust score evaluation, secure communication, and joint decision support, facilitate independent execution of each use case while providing a joint defence and disaster recovery process. This choreography of joint execution demonstrates how a set of distributed systems, such as those involved in the joint use case, can collaboratively detect, analyse, and respond to complex cyber-attacks in real-time, even in a state of partial failure.

This joint execution demonstrates the effectiveness of the CISSAN framework in a real-world environment, showcasing its potential in strengthening cyber resilience in the European Union, reducing response times in critical infrastructure cyber-attacks, and facilitating future joint execution of collective intelligence-based cyber defence solutions in IoT and OT domains.

Our initial value proposition —"Securing Tomorrow's Connected World" (D3.1) — continues to hold strong, as demonstrated in WP6.

List of Authors

In alphabetic order by partner name:

- Lars-Göran Magnusson, Arctos Labs
- Anders Liden, Clavister
- Rodrigo Martinez, Councilbox
- Klaus Chmelina, Geodata
- Ilgin Safak, University of Jyväskylä
- Stella Palenius, University of Jyväskylä
- Mikko Lehkonen, University of Jyväskylä
- Veikko Markkanen, University of Jyväskylä
- Pasi Tapanainen, University of Jyväskylä
- Xiaobang Sun, University of Jyväskylä
- Palvi Shelke, University of Jyväskylä
- Teemu Kemppainen, Mattersoft
- Ann Sjökvist, Mint Security
- Oliver Bölin, Techinova

Table of Contents

Abbreviations

API	Application Programming Interface
CER	Critical Entities Resilience
CI	Collective Intelligence
CTI	Cyber Threat Intelligence
CISSAN	Collective Intelligence Supported by Security Aware Nodes
DTW	Dynamic Time Warping
EU	European Union
GPS	Global Positioning System
GUI	Graphical User Interface
ICS	Industrial Control Systems
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
JSON	JavaScript Object Notation
MES	Manufacturing Execution System
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MS SQL	MicroSoft Structured Query Language
NIS	Network and Information Systems
NIST	National Institute of Standards and Technology
OT	Operational Technology
PQC	Post-Quantum Cryptography
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Incident and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Centre
SPAN	Switch Port Analyzer
STIX	Structured Threat Information eXpression
UC	Use Case
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
WAN	Wide Area Network
WASM	WebAssembly Module
WP	Work Package

1 Introduction

1.1 Purpose and Scope

The aim of this report is to describe the joint use case (automated disaster recovery) that has been implemented within the CISSAN project, showcasing how the collective intelligence (CI) mechanisms developed in CISSAN and the CISSAN platform facilitates joint cybersecurity operations across sectors through CI, disaster recovery, and collaborative defence capabilities. The scope of this report includes the choreography, execution, and results of the mitigation of a multi-domain critical infrastructure attack scenario, where transportation, smart grid, and tunnel construction infrastructures are represented on the CISSAN platform. This report highlights how the CISSAN platform services help in achieving interoperability between heterogeneous Internet of Things (IoT) and Operational Technology (OT) devices through joint cybersecurity operations. This report focuses on the orchestration, integration, and results of the CISSAN joint use case.

1.2 Document Structure

The report is structured as follows. Section 1 introduces the report. In Section 2, an overview of the joint use case is presented, including the multi-domain critical infrastructure attack scenario and the use cases involved in the joint use case demo. In Section 3, the role of the CISSAN platform in supporting the joint use case choreography for different sectors is presented, including the shared services used for this purpose. In Section 4, an overview of the execution of the joint use case is presented, including actions taken, CI mechanisms used, and disaster recovery flows executed. In Section 5, an overview of the results achieved from executing the joint use case is presented, including key observations and lessons learned from this experience. In Section 6, key findings from this experience are presented, including recommendations for future deployment and research in this area.

1.3 Relation to Other Deliverables

The joint use case leverages the CISSAN platform, which has an architecture outlined in WP2. The architecture provides the basis for the implementation and deployment of the CISSAN platform in the use case solutions that are represented in the joint use case. The solutions presented in WP4 and WP5 deliver the components and functionalities for the joint use case demo, including the CI mechanisms, security services. The joint use case has been developed to address the value proposition of the joint user story developed in WP3.

In parallel to the technical development, WP3 has played a critical role in ensuring that these architectural and implementation efforts translate into meaningful business value, governance of readiness, and long-term exploitability. Throughout the project, WP3 worked closely with the technical work packages to align business interpretations with demonstrated system behaviour. This collaboration ensured that the evolving platform capabilities—such as distributed anomaly detection, trust scoring, coordinated recovery, and secure intelligence sharing—were aligned with sector-specific value propositions, earning-model pathways, and governance considerations.

WP3 also developed a structured approach to bridging technology with market reality. This included refining earning-model classifications, constructing the Joint User Story and Joint Use Case business interpretation, and introducing the D6.3 → D3.3 traceability matrix to transparently link technical outputs with their business implications. These activities ensure that the architectural and technical solutions presented in this document are not only feasible, but also viable, compliant, and strategically aligned for real-world adoption.

Together, the outcomes of WP2, WP3, WP4, and WP5 demonstrate how CISSAN progresses from platform architecture to applied technical solutions and further into actionable business and governance frameworks. D6.1, in combination with D3.3 therefore reflects both the operationalization of the project platform and the broader ecosystem thinking necessary for its sustained impact across critical-infrastructure sectors. Our initial value proposition —"Securing Tomorrow's Connected World" (D3.1) — continues to hold strong, as demonstrated in this CISSAN_D6.1 deliverable

2 Overview of the CISSAN Joint Use Case

2.1 Joint User Story Description: a coordinated response to a multi-domain cyber incident

On a typical working day, operators across transportation, energy, and tunnel construction focus on keeping their own systems running safety and reliable. Public transportation depends on accurate positioning and real-time data. Smart grids rely on trusted monitoring and control of operational technology. Tunnel construction sites continuously collect sensor data to control construction processes, protect structural integrity and worker safety. Each domain functions independently, guided by its own operational priorities and responsibilities.

At the same time, these infrastructures are no longer isolated. Digitalization has created practical and physical dependencies between systems. Data is shared, services overlap, and failures rarely main contained. While this interconnection brings efficiency, it also means that disruptions in one domain can quickly affect others. In day-to-day operations, however, security monitoring and incident response are still largely handled within domain boundaries.

The Joint User Story begins when unusual behaviour appears almost simultaneously across multiple domains. Transportation operators notice inconsistency in vehicle positioning and service coordination. Energy operators detect irregular patterns in grid monitoring and control systems. Meanwhile, tunnel construction systems begin reporting sensor readings that no longer align with expected physical conditions. On their own, each signal could be interpreted as a technical fault or a localized issue. Taken together, they point to something more serious.

At this moment, the central challenge is not detection alone. Operators must determine whether the events are connected, which systems and data can be trusted, and how to respond without triggering further disruptions. Acting in isolation risks slow reactions, incomplete understanding, or decisions that unintentionally worsen the situation across interconnected infrastructures.

Through the CISSAN platform, security-relevant observations from the different domains are brought together. Each system contributes its local perspective—anomalies, trust assessments, and contextual information—into a shared CI layer. This does not replace local control. Instead, it allows operators to form a common view of the situation and recognize how developments in one domain relate to others.

As the situation evolves, trust and data quality assessments help identify compromised components and unreliable data sources. Coordinated containment measures can then be applied where needed, such as isolating affected devices or limiting their influence on shared processes. At the same time, threat intelligence is exchanged in a standardized manner, ensuring that lessons learned in one domain are immediately available to others.

Once the immediate risk is under control, attention shifts to recovery and ensuring societal and business continuity. Rather than restoring services in isolation, recovery actions are coordinated across systems. Where possible, automated disaster recovery processes are triggered, guided by trust levels, operational priorities, and available resources. This approach supports a gradual return to normal operations while reducing the risk of further cascading effects.

By the end of the scenario, services across all domains are stabilized. The outcome is the result of multiple independent actors working together through shared intelligence and coordinated decision-making, and a strengthened centralized authority. The Joint Use Case demonstrates how the CISSAN framework supports this shift—from isolated responses toward a collective, cross-sector approach to cyber defence and recovery that better reflects the realities of modern critical infrastructure.

Our initial value proposition —"Securing Tomorrow's Connected World" (D3.1) — continues to hold strong, as demonstrated in the Joint Use Case.

2.2 Multi–Domain Critical Infrastructure Attack Scenario

The CISSAN joint use case (automated disaster recovery) demonstration is based on a multi-domain critical infrastructure attack mitigation scenario, where transportation, smart grids, tunnelling construction systems are simultaneously attacked by a cyber-attack, leading to the cascading failure of the interconnected infrastructure services and domains and are mitigated using the CI mechanisms in the CISSAN platform. The joint use case demonstration is an accurate representation of the realistic dependencies between the CISSAN use cases' domains, where the disruption of one domain results in the cascading effect on other domains, thereby increasing the risk of operation and safety. In the joint use case demonstration, the automated disaster recovery of the device outages and service disruptions is showcased on the CISSAN platform using CI and collaborative defence mechanisms developed in the project, including distributed anomaly detection, trust management, device management, security task orchestration, incidence response and distributed disaster recovery.

2.3 Participating Use Cases

2.3.1 Transportation

The CISSAN transportation use case, represented by Mattersoft primarily focuses on securing public transport information and control systems used in fleet monitoring, real-time passenger information, traffic signal prioritization, traffic flow analysis, and traffic data management. The use case involves in-vehicle and roadside devices that rely on highly centralized data processing, analysis, and decision-making architectures, making it a significant issue in the context of cybersecurity. The introduction of Network and Information Systems (NIS) 2 requirements makes the issue even more pressing in the context of improving the security mechanisms. The use case primarily deals with the analysis of Global Positioning System (GPS) data to identify issues such as jamming, spoofing, and device failures, creating a basis for CI-based detection and response to cyber threats.

2.3.2 Smart Grids

The CISSAN smart grids use case, represented by Affärsverken, Clavister and Techinova, focuses on cybersecurity for energy grid monitoring and control systems, with emphasis on operational technology such as Supervisory Control and Data Acquisition (SCADA) and Remote Terminal Unit (RTU) environments. These systems are traditionally monitored and analysed using centralized security functions, yet they belong to a highly critical sector and operate under strong availability and safety constraints, while also being subject to regulatory and resilience requirements such as the Critical Entities Resilience Directive and NIS2. Within CISSAN, the use case explores local and hybrid AI-based anomaly detection over both network telemetry and physical sensor/process data to identify cyber-attacks, faults, and abnormal operating states, and to enable run-time collaboration between nodes for a more resilient and cooperative cybersecurity approach, including local anomaly detection and correlation to support software-based relay protection.

2.3.3 Tunnel Construction

The tunnel construction use case, represented by Geodata, is focused on ensuring the security of IoT-based monitoring systems used during construction, where geotechnical sensors are used to provide critical physical data for safety and operational decision-making. This is a risky use case, given that it involves various stakeholders and data consumers, and hence poses a significant risk of data manipulation, misuse, and breach of operational rules. The use of the monitoring services is for critical infrastructure, and hence it is important to ensure that it meets the NIS2 cybersecurity requirements. In the CISSAN project, the use case is focused on ensuring sensor data believability to identify potential attacks, faults, and abuse, while ensuring data integrity through blockchain and security chips for signing sensor data.

2.4 Objectives of the Joint Use Case Demonstration

The objective of the joint use case demonstration is to validate the CISSAN platform's ability to facilitate coordinated and cross-sector cybersecurity operations in the context of complex and multi-domain cyber-attack scenarios against critical infrastructures. It aims to validate the CISSAN platform's ability to facilitate the choreography of CI, disaster recovery, and collaborative defence strategies in the context of IoT and OT environments that are heterogeneous and representative of transportation infrastructures, smart grid infrastructures, and tunnel construction systems. It also showcases the interoperability of the CISSAN framework in the context of multiple and heterogeneous IoT and OT environments and its ability to facilitate the choreography of threat detection, threat intelligence sharing, and decision coordination using Structured Threat Information eXpression (STIX)-based threat intelligence sharing and communication services.

2.5 Role of the CISSAN Platform

The CISSAN platform plays an important role in the joint use case demonstration scenario in that the CISSAN platform allows for the implementation and evaluation of the security concepts and collective intelligence mechanisms developed in the project for its use case systems and domains. The CISSAN platform, which has been developed based on the updated CISSAN architecture defined in the CISSAN D2.3 report, allows for the structured representation of the CISSAN use case systems that have been included in the joint use case demonstration. This includes the representation of the key use case system components and their interactions with relevant components in the CISSAN platform. The aim is to enable the CISSAN partners to connect their use case systems and test the functionality of the collective intelligence mechanisms including data quality verification, anomaly detection, trust scoring, and threat information sharing. The CISSAN platform, therefore, allows partners to execute and test the joint use case scenario in a safe environment that does not impact any of the operational systems of any of the participating partners. Partners can thus test and understand how events that are locally detected can be correlated and acted upon in other domains through collective intelligence and collaborative defence. In a sense, it is not only a technical integration platform that is offered to partners, as it also acts as a tool that can be used to validate and test the feasibility and benefits of the approaches that have been proposed. It is also critical to note that it offers a means through which partners of the project can test and validate the potential benefits that can be derived if these mechanisms are adopted in their environment. Therefore, it acts as a tool that bridges the gap between research and implementation, allowing partners to understand how collective intelligence can be used to improve their environment. Hence, it offers a means through which partners can explore and understand how these benefits can be derived and how these benefits can be exploited beyond the scope of the project.

2.6 Collective Intelligence Mechanisms Used in the Demo

2.6.1 Orchestration

In the demonstration, orchestration is used to coordinate the deployment and execution of distributed tasks across the available devices. Based on the task distribution template produced by the Arctos Labs Optimization Solver and delivered via the CISSAN Management Server, the CISSAN Orchestrator provisions the tasks to the selected devices and ensures that the required software components are available before execution is initiated. The role of orchestration in the demo is to demonstrate how an optimized task distribution can be automatically realized in a distributed environment with minimal manual intervention.

2.6.2 Security task distribution

CISSAN seeks to transform traditional centralised security systems to distributed ones by distributing security tasks so that devices can collaborate with each other in performing tasks as a means of enabling CI. For this purpose, security tasks are distributed across networked devices in the CISSAN platform instead of being solely performed a central server. Arctos Labs' Optimisation Solver was used to calculate the optimal task distribution considering various factors such as device capabilities,

task dependencies, quality-of-service considerations, disaster recovery requirements, as well as the impact of task distribution on the devices' performances and the network security. Consequently, tasks are distributed and deployed automatically by the CISSAN Orchestrator depending on the output generated by the optimization solver. By achieving this goal, security-related tasks are distributed across various devices, enabling CI in the CISSAN platform.

2.6.3 Trust scoring

Trust scoring is used in the CISSAN platform as a cross-cutting mechanism for turning distributed security observations into a single, actionable control signal. Local components and participating devices produce trust-related assessments based on their own evidence and peer comparisons, while a central trust management function on the management server aggregates these inputs into a global trust score per unit. In the demos, differences in observed behaviour, captured by the participating CISSAN solutions, translate into changes in these global trust scores, which serve as the primary trigger for risk mitigation actions. In essence, trust scoring provides the high-level rationale for constraining or isolating units that appear unreliable, compromised, or inconsistent with the rest of the system.

Within the CI enabled threat hunting and automatic threat mitigation framework (Rotor), trust scoring is derived from peer consistency**.** When the simulated attack generates anomalous observations on one RTU, that device's report diverges from the peer group's expected state. Peers therefore compare received observations against their own local snapshot and produce a consistency outcome, which is used to update their trust assessment of the affected unit over successive cycles. Because only one RTU exhibits genuinely abnormal behaviour in the scenario, peer evaluations converge toward reduced confidence in that unit, causing its aggregated trust score to decline rapidly. Once the score crosses the configured threshold, the platform treats the unit as untrusted and isolates it to contain risk and prevent further impact. Trust scoring flow as part of the Rotor framework is explained in more detail in the CISSAN D5.4 report.

In the IoT network, trust scoring is handled by distributing security functions in the form of WebAssembly modules (WASMs) to the IoT devices depending on their available resources and executing these modules in succession. Trust scores for the devices in the network are calculated based on trust data, including anomaly risk scores, believability scores, and device responsiveness, as observed by the device executing the scoring. Derived scores are stored locally and shared with the CISSAN Management Server. If the scores are below an acceptable threshold, blacklisting is initiated to remove the devices with low scores from the rest of the network. A detailed description of the different WASMs and trust scoring model can be found in CISSAN D5.4 report.

2.6.4 Data quality verification

The purpose of the Data Quality Verification module is to calculate the local believability scores using the trust scores of nodes in the CISSAN server. The module also calculates an overall believability score to validate the results. If a discrepancy is identified, the module triggers anomaly detection to the "Distributed Monitoring and Threat Detection" module. If the believability score of data is identified as low (below a pre-defined threshold), anomaly detection is performed on the data at the CISSAN server using the aggregated data obtained from the Security Incident and Event Management (SIEM) server. We adopt variance-based and similarity-based methods in data quality verification. Variance-based method can detect anomalies using local linear regression within a sliding window. Similarity-based method uses Dynamic Time Warping (DTW) to measure similarity between two time series data from neighbouring sensors.

In CISSAN, the main challenge addressed is the detection of data tampering attacks and to prevent their impact. The anomaly detection methods provided by the CISSAN platform and its capability to alarm, quarantine, isolate and blacklist affected devices and data are seen as a step forward to increase security. The CISSAN platform can be integrated in different ways in the use case. One way is to establish the data exchange (via Application Programming Interface (API)) with the central control and data management centre of the tunnel project. In this way, sensor data can be transferred to the CISSAN platform for advanced data quality verification and anomaly detection, and corresponding detection results (believability scores, anomalies) can be returned. The main platform component used is the CISSAN management server providing the Data Quality Verification and the AnomalyDetection modules.

2.6.5 Distributed anomaly detection

Distributed anomaly detection in the smart grid use case places detection capabilities close to where relevant signals originate, enabling low-latency identification of abnormal behaviour with awareness of the local operational context. In a software-based relay protection setting, anomalies may manifest both in physical/process measurements and in the cyber layer (e.g., manipulation or abnormal communication behaviour). The distributed approach therefore relies on local analysis at substations or nodes to detect faults, abnormal operating states, and potential cyber-attacks without depending solely on centralized detection.

To provide outputs that are directly usable and interpretable, the local detections are forwarded for central correlation, where related observations from multiple substations are consolidated into a single correlated anomaly/fault event. This centrally produced event describes what happened, identifies the originating location (where it was first observed), and lists other substations that observed the same event in order. As a result, consumers receive already correlated intelligence with clear fault description and location, rather than having to reconstruct meaning from multiple independent local alerts.

2.6.6 Threat intelligence sharing (STIX)

As part of the demonstration, STIX is used to showcase how a major security state change in the network can be translated into standardized, shareable cyber threat intelligence. The practical application in this effort lies within the Industrial Control Systems (ICS) Zone of the network. When a compromised unit is blacklisted due to a trust-threshold violation, the management server automatically generates a STIX bundle that captures the event and its supporting evidence. The generator runs centrally, using the aggregated context already available there: peer-driven trust outcomes and the anomaly traces produced during the incident, with the Rotor monitor acting as the primary contributor of evidence in this scenario. The result is a machine-readable STIX report in JavaScript Object Notation (JSON) format, demonstrating that trust-based decisions can be packaged together with the observations that led to them in a portable Cyber Threat Intelligence (CTI) representation. For the purposes of the demo, validation focuses on confirming that STIX generation is triggered correctly by the blacklisting event and that the exported bundle contains the expected incident context and evidence entries.

2.6.7 Automated disaster recovery

Automated disaster recovery is used to maintain continuous task execution in the presence of device failures. During runtime, the system detects failures of participating devices and automatically replaces affected tasks using pre-selected failover devices, allowing the demonstration to proceed without manual intervention. Automation is essential in this context, as the system is designed to scale to environments with many devices and concurrently running tasks. Manually identifying failures and restoring operation would be impractical and error-prone for a security or system manager, particularly under time-critical conditions. The demonstration illustrates how automated disaster recovery helps reduce manual operational effort while supporting reliable execution of distributed tasks.

2.6.8 Incidence response and decision coordination

In the demo, incident response is implemented as a CI workflow in which distributed observations are converted into coordinated, network-level decisions during runtime. Rather than relying on a single detection point or manual escalation, participating nodes share security-relevant signals and contribute to a common assessment of whether behaviour is consistent with expected operating conditions. This enables coordinated response decisions while retaining centralized visibility for operators.

Providing an example of this concept, the Rotor framework drives coordination by combining lightweight monitoring cycles (demonstrated manually) with intelligent event-driven peer validation. RTUs execute Rotor periodically to maintain baseline visibility, but when anomalous activity is detected on any unit, the CI logic initiates automated incident-response sequence: the detecting node publishes its report to peers, listening peers initiate a comparison against their local state, and trust

updates are produced based on agreement or divergence. As detailed in D5.4, these device-level trust updates provide an immediate collective view of network security status and are then aggregated at the management server into a global trust perspective. The coordinated outcome determines whether the alert source remains within tolerable risk limits or is deemed too risky to be treated as benign, which in turn governs containment actions such as blacklisting and isolation. In this way, Rotor's incident response and decision coordination are inseparable from its CI and trust-scoring mechanisms, spanning both device-level evaluation and centralized aggregation.

2.7 Logical Choreography of the CISSAN Joint Use Case

This section provides an overview of the logical choreography of the CISSAN joint use case (UC5), which explains how different use case domains and CISSAN services work together in detecting, analysing, and mitigating a coordinated multi-domain cyber-attack against transportation, smart grids and tunnel construction critical infrastructures represented on the CISSAN platform. It provides a series of high-level actions and information exchanges that facilitate CI, collaborative defence, and disaster recovery, from initial anomaly detection to coordinated execution of disaster recovery tasks. It will not delve into technical details, but rather provide a clear overview of how events, decisions, and responses are choreographed across the transportation, smart grids, and tunnel construction systems using the CISSAN platform.

In Use Case 5 - Joint Use Case, the principal sequence of high-level interactions and information exchanges are described in Table 1:

Table 1. Principal sequence of high-level interactions and information exchanges in the UC5 - joint use case

Step #	Trigger / Event	Actor(s)	Action	CISSAN Service Used	Output
1	Anomaly detected	Use case 1 actors: • GPS sensors • Mattersoft backend server • MQTT broker • CISSAN Lab Use case 2 actors: • RTUs • SCADA server • MQTT broker Use case 3 actors: • Tunnel sensor and security chip • Geodata gateway • Geodata blockchain-based data transfer	Use case 1: 1. GPS sensors in buses/trams calculate their positions. This information is passed through Mattersoft backend and MQTT broker over to CISSAN Lab. 2. Positions of vehicles are shown on OpenStreetMap. 3. When the anomaly detection algorithms notice suspicious positions, those are indicated by different colors on the map.	• Management • Data quality verification • Anomaly detection	Anomaly event (believability scores and anomaly risk scores)

		system (Lightning Network nodes) • GeodataHub CISSAN platform actors: • CISSAN Management Server • Raspberry Pis • Data Quality Verification WASMs • AnomalyDetection WASM • SIEM server	Use case 2: 1. The normal state of the smart-grid OT network is visualised through the management interfaces. 2. Local monitoring is performed alongside regular operation: Rotor monitors cyber-related anomalies, while PASAD and NodeEye monitor operational anomalies and process behaviour. 3. When suspicious activity or abnormal behaviour is detected, the respective component generates an alert or report based on local evidence. 4. OT alerts are analysed via machine learning features by the respective solutions and visualised in their respective interfaces 5. Cyber alerts and supporting evidence are shared with peer units through the collective intelligence overlay, while also mirroring them into the		

			SIEM for centralized situational awareness and investigation. 6. Peer units compare the received cyber related report against their own local observations and produce trust assessments for the reporting unit. 7. Trust assessments are aggregated at network level to form a collective view of the reporting unit's trustworthiness. 8. If the aggregated trust score falls below the defined threshold, the compromised or suspicious unit is isolated from the rest of the network. 9. The updated state of the network including alerts from Rotor, NodeEye, and PASAD, trust status, and possible isolation of affected units, is visualised to the operator. Use case 3: 1. Tunnel sensor generates monitoring data		

			2. Security chip signs monitoring data 3. Gateway verifies signature, transfers data to Lightning Network 4. Gateway performs multi-route/multi-channel transfer of data to GeodataHub 5. Gateway verifies signatures, verifies identity of data coming from different routes, provides data to CISSAN Management Server 6. CISSAN Management Server requests performing data quality verification by triggering the execution of Data Quality Verification WASMs at Raspberry Pis 7. Raspberry Pis perform data quality verification to calculate believability scores and send results to CISSAN Management Server. Attack or fault detected, if believability score is below a certain threshold.		
2	Event generated	CISSAN platform components: • Wazuh SIEM server	Correlate local evidence	Correlation service at SIEM server	Correlated event

		Use case components: • Use case analytics systems			
3	Trust threshold violated	CISSAN platform components: • CISSAN Management Server trust management module • Councilbox Eventchain System	Compute global trust score at CISSAN Management Server using local trust scores obtained from Raspberry Pis and RTUs	Trust assessment at CISSAN Management Server	Blacklisting event
4	Blacklisting	CISSAN platform components: • CISSAN Management server trust management module • Switch • Councilbox Eventchain System • CISSAN Orchestrator Server	• Generate STIX bundle • Isolate device at switch • Mark device as blacklisted at CISSAN Orchestrator device list • Update Device ledger to mark device as blacklisted	• STIX service • Blacklisting • Access control	Extended STIX report
5	Topology change	CISSAN platform components: • CISSAN Management server • Arctos Labs Optimization Solver • CISSAN Orchestrator	• Recalculate optimal deployment after device removal • Reassign tasks to available nodes • Push new deployment to the network	• Management • Optimization • Orchestration	New optimized deployment
5	STIX ready	CISSAN platform components: • CISSAN Management server STIX services	Share intelligence cross-domain	• CTI exchange • Management	Shared threat context
6	Shared threat	CISSAN platform components: • CISSAN Management Server trust	Assess impact & priorities	• Trust management • Management	Recovery strategy

		management module			
7	Device becomes unreachable	Use case 1: • GPS sensors Use case 2: • RTUs Use case 3: • Tunnel sensors Represented with CISSAN platform component: • Raspberry Pis	Use case 1: • No location data on the map for the bus Use case 2: • Device is tagged as unresponsive in the SCADA server • Rotor is unreachable Use case 3: • GeoDataHub sends a warning that data is missing (no data sent by sensors) CISSAN platform: • A Raspberry Pi hosting active tasks is unplugged	• Data quality verification	Device failure condition initiated
8	Missed heartbeat detected	CISSAN platform components: • CISSAN Orchestrator • Raspberry Pis • WASMs	Performs periodic health checks, identifies non-responsive node	Health Monitoring	Device inactive event
9	Device inactive event received	CISSAN platform components: • CISSAN Management Server	Visually marks the failed device to inactive state and failed tasks in red to indicate loss of availability	GUI Rendering	User-visible failure indication
10	Disaster recovery triggered	CISSAN platform components: • CISSAN Orchestrator • Raspberry Pis	Starts automated disaster recovery workflow, selects healthy failover nodes for task reallocation	Disaster Recovery	Updated deployment
11	Deployment updated	CISSAN platform components: • CISSAN Management Server	Shows updated task allocation on the failover devices	GUI Rendering	User-visible failover task

					activation
12	System in stable state	CISSAN platform components: • CISSAN Management Server • CISSAN Orchestrator • Raspberry Pis	Run execution again to verify functionality	Task execution	Execution successful

3 CISSAN Joint Use Case Execution

This section discusses the execution of the CISSAN joint use case demonstration, with special emphasis placed on how a coordinated cyber-attack targeting different domains of critical infrastructure is detected, analysed, and mitigated via the CISSAN framework. It defines the operation assumptions, logical interactions between different systems and framework services participating in the CISSAN joint use case demonstration, as well as the disaster recovery and collective defence actions undertaken during the execution of the CISSAN joint use case demonstration. It mainly focuses on the orchestration of cross-domain actions rather than implementation details.

3.1 Initial Conditions and Assumptions

It is assumed that transportation, smart grids, and tunnel construction systems are running under normal operating conditions, and all the monitoring, communication, and security services are enabled in all the participating domains. The use case platforms are connected to the CISSAN platform through their interfaces defined in D6.2. It is assumed that the basic trust relationships, identity, and access control are established, and the services offered by the framework, such as the exchange of threat intelligence, trust assessment, orchestration, and communication, are available. It is also assumed that the use case platforms are running heterogeneous devices and systems, such as legacy systems, which is a realistic assumption. Human intervention is limited to actions explicitly required for scenario execution, such as deliberately simulating a device outage. The initial conditions and assumptions are summarized in Table 2.

Table 2. Initial conditions and assumptions

Aspect	**Assumption**
System state	Normal operation prior to attack
Connectivity	Cross-domain communication enabled
Security services	Monitoring, trust assessment, orchestration active
Trust baseline	Initial trust scores above threshold
Automation level	Recovery actions enabled
Human involvement	Simulating an attack by causing a device outage

3.2 Step-by-Step Choreography

The CISSAN joint use case execution process follows a structured sequence of interactions in various domains and framework services. Initially, detection of local anomalies and attacks in one or more use cases is achieved in the domains, which are then correlated and enriched with analytics and trust services, resulting in the detection of untrusted components in the system. Threat intelligence sharing in the STIX format facilitates a common situational awareness, and decisions are made regarding mitigation and recovery, which are then executed in the system through task distribution and orchestration services. This process continues iteratively, enabling the system to adapt dynamically in a changing environment.

The run-time choreography begins by first displaying the existing network, providing a clear view of the current system topology and available devices. Once this baseline has been established, the optimized deployment solution is presented, showing how the system has distributed the modules and resources. After reviewing this optimized configuration, the deployment is executed. As the system begins operating, it displays the collected data in real time, allowing observers to monitor how the deployed components behave in the live environment (see Figure 1).

Figure 1. Device view showing the active task in green together with its anomaly, believability, and trust values

As the system continues running, the real-time data stream reveals abnormal patterns indicating one or more anomalies within the operational environment. These anomaly signals are automatically fed into the trust-management pipeline. Each affected device's trust score begins to decline as the anomalous behaviour accumulates, reflecting a reduced confidence in its operational integrity. Once the global trust score for a device drops below the predefined threshold, the platform initiates an automated blacklisting sequence. The device is isolated at the switch level, removed from the active deployment configuration, marked as blacklisted in the CISSAN Orchestrator, and an associated STIX-formatted intelligence report is generated. Blacklisting triggers the automated resilience mechanisms, which causes the device's assigned tasks to be highlighted visually in red (see Figure 2), indicating a loss of availability, and the disaster-recovery workflow is activated to redistribute tasks to healthy devices. Since the topology changed due to blacklisting, it automatically triggers the Optimization Solver for a new optimal task placement.

Figure 2. Task highlighted in red indicating a failed or unavailable state

To further demonstrate the system's resilience, one of the devices is then intentionally turned off, simulating a sudden failure. The system automatically detects the non-responsive node and initiates recovery procedures. Modules are migrated to alternative devices, and the updated configuration becomes active without manual intervention. The system continues to operate on the remaining devices. The execution is run again to verify that all functions remain available on the new deployment configuration, demonstrating the platform's ability to maintain service continuity under disruptions.

3.3 Automated Disaster Recovery Flow

The automated disaster recovery workflow in Figure 3 illustrates how the system responds to a device failure during runtime. In the demo scenario, the CISSAN Management Server GUI initially displays the system operating in normal conditions, showing all active devices and their assigned tasks. When executed tasks detect anomalies, the trust score updates automatically. When the trust score of a device drops below threshold, the device gets blacklisted. The CISSAN Management Server GUI automatically highlights failed tasks in colour red. The CISSAN Orchestrator starts disaster recovery and migrates tasks to healthy failover nodes. When they are executed and management server detects the task was executed on the failover device, the task migrates on GUI and is visualized with colour violet. The CISSAN Management Server then resumes to normal operation.

When one of the Raspberry Pi devices is intentionally unplugged, the CISSAN Orchestrator continues to perform periodic health checks, sent every 15 seconds. After five consecutive checks are missed, the device is automatically marked as offline. At that moment, the GUI visually highlights the affected tasks in red, indicating a loss of availability. Simultaneously, the CISSAN Orchestrator

triggers the disaster recovery mechanism, which evaluates alternative devices and migrates the failed tasks to healthy nodes. The updated task placement is then shown in the GUI as the new deployment becomes active. Finally, the execution is run again to verify that all functions remain available, demonstrating the platform's ability to maintain service continuity despite the disruption.

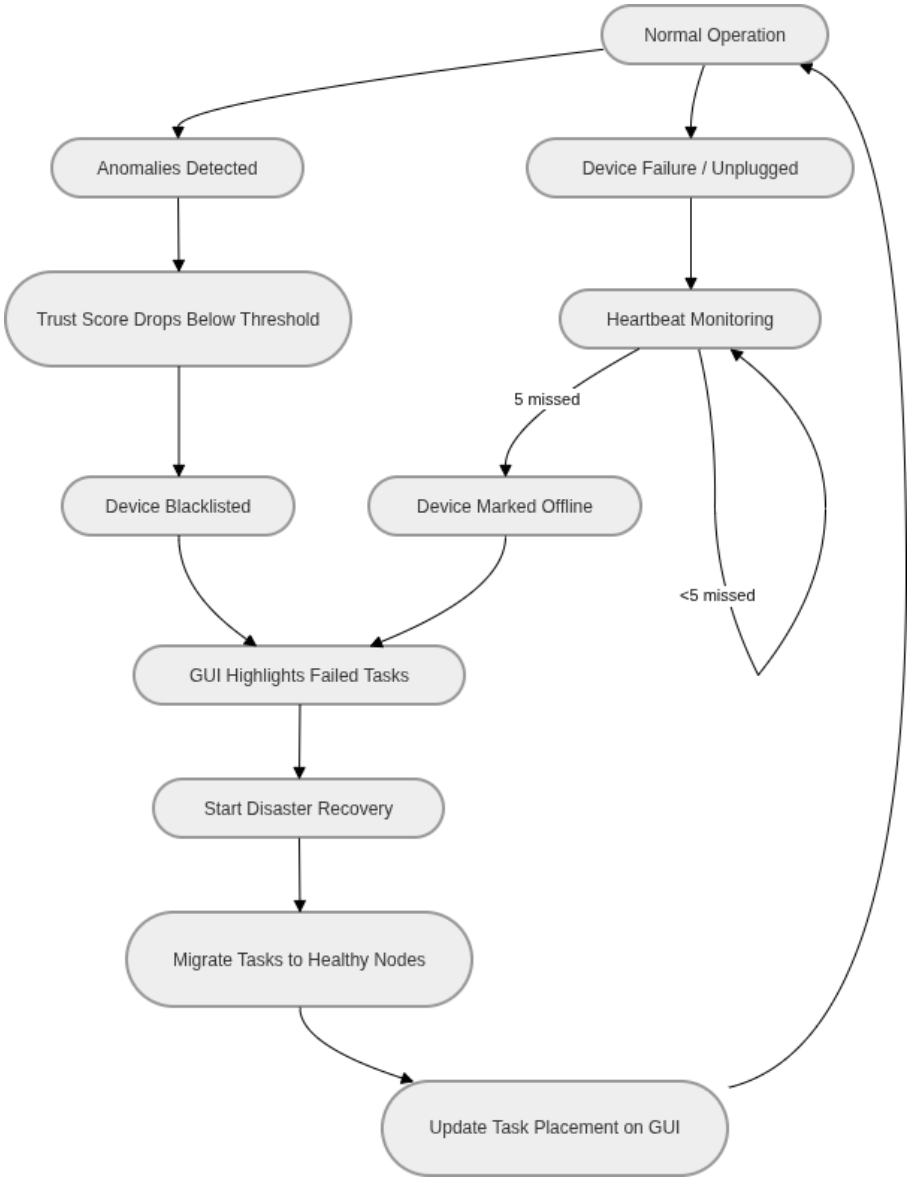

Figure 3. Automated disaster recovery workflow demonstrating system response to blacklisting and a device failure during the demo

3.4 Collective Intelligence and Collaborative Defence Actions

Rotor is used in the demo to illustrate CI and collaborative defence as runtime capabilities within the CISSAN platform. The scenario simulates an OT intrusion targeting Smart Grid control units (RTUs) in the ICS Zone, with the goal of detecting adversary traces early, propagating awareness across the segment, and containing risk by isolating the affected unit. Rotor supports this by combining device-level security visibility with peer cooperation, allowing abnormal behaviour observed on one device to influence the defensive posture of the wider network.

At runtime, the execution flow begins with local monitoring on the targeted RTU, which produces security observations when anomalous behaviour is detected. The unit publishes a report to its peers, triggering the CI layer: participating RTUs receive the report and compare it against their own local

snapshot to determine whether the observed behaviour is consistent with the segment's expected operating conditions. The comparison produces a consistency outcome that is converted into trust updates, which peers publish to the trust management component. The CISSAN Management Server aggregates these peer inputs into global trust scores, maintains a consolidated view of device reliability, and forwards the anomaly context to the SIEM for operator visibility and downstream analysis.

Collaborative defence is demonstrated when the aggregated trust score for the affected unit drops below the configured threshold. The unit is then blacklisted and isolated to prevent further impact and contain the incident within the ICS segment. The incident is observable through both operational interfaces: anomaly and timeline views in the SIEM, and trust/network status in the management view. The same trust-triggered state change also initiates automatic STIX report generation, demonstrating how collaborative defence outcomes and their supporting evidence can be packaged as standardized CTI for potential sharing beyond the local environment. Collectively, these steps demonstrate how CI-based peer validation and aggregated trust reasoning strengthen situational awareness and enable coordinated containment of active risk during runtime.

Figure 4 outlines the execution flow of the Rotor components as part of the demonstration.

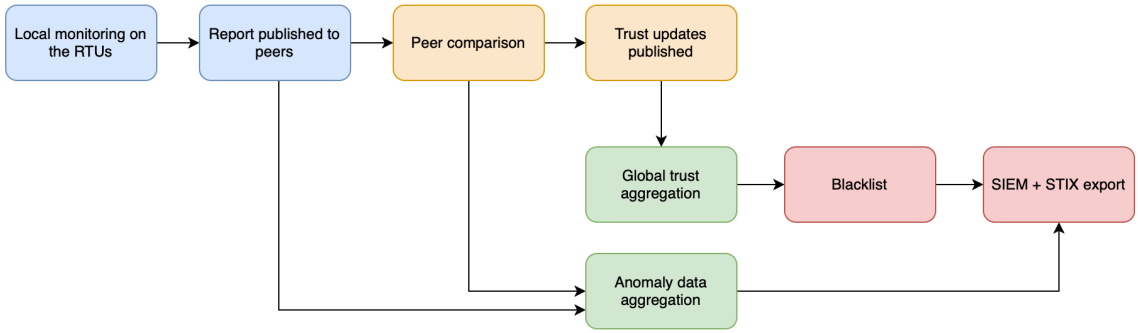

Figure 4. Outline of Rotor CI and Collaborative defence flow as part of the demonstration

Local trust scoring of IoT devices is initiated by the TrustScoring module once the WASM-modules distributed in the network for calculating anomaly/believability scores have finished their execution providing input for the TrustScoring module. The module first checks for peer device responsiveness. Based on the results and available anomaly/believability scores, the module calculates a trust score for its peer devices. The trust scores are aggregated at the management server where they are used to calculate global trust scores and are presented in the management view of the network. Devices falling below the threshold of acceptable trust are blacklisted from the IoT network to contain potential attacks to individual devices. This blacklisting can be observed in the management view and is traceable from the blockchain system where device status is recorded for auditing. After blacklisting, the responsibility of executing the blacklisted device's the WASM-modules is given to the failover devices, ensuring that the collective intelligence operations continue to operate.

4 Results and Observations

4.1 Achieved Outcomes

The CISSAN joint use case demonstration has been successful in validating the potential of the proposed CISSAN platform to facilitate the operation of coordinated cybersecurity services across various critical infrastructure domains, based on a realistic model of a multi-domain attack scenario. The integration of the transportation, smart grids, and tunnel construction use cases has enabled the validation of the potential of collective intelligence services, disaster recovery services, and collaborative defence services to be orchestrated in a timely manner. The validation has confirmed the potential of distributed detection, STIX-based generation of threat intelligence, secure communication, and automated orchestration of tasks to operate in a manner that mitigates the likelihood of cascading failures.

The ability to coordinate cybersecurity activities across different areas of critical infrastructure has been demonstrated as proof that organisations within the EU can significantly limit the cost and impact of large-scale cyber security incidents through collective intelligence and automation. The ability to detect and recover from security incidents more quickly translates directly into business operations continuity, reduced downtime, and lower business losses for organisations delivering critical services.

4.2 Interoperability and Automation Benefits

The CISSAN joint use case demonstration underscored the considerable benefits of interoperability and automation that could be achieved by leveraging the CISSAN platform, especially in the context of the adoption of cybersecurity standards. For instance, the application of STIX 2.1 for structured exchange of threat intelligence information can facilitate heterogeneous systems from the transportation, smart grids, and tunnel construction sectors to exchange security information. Moreover, the inclusion of post-quantum cryptography (PQC) mechanisms can facilitate the secure and future-proof exchange of recovery commands and information in accordance with the National Institute of Standards and Technology (NIST) PQC recommendations and the NIS implementation roadmap. Furthermore, the application of CISSAN mechanisms in accordance with established cybersecurity standards, regulations and best practices for the security of CI, such as NIS2, Critical Entities Resilience (CER) Directive, International Electrotechnical Commission (IEC) 62443, and International Organization for Standardization (ISO)/IEC 27001, can facilitate the seamless integration of heterogeneous IoT and OT systems.

The ability for different systems, partners, and suppliers to interact with each other through standards like STIX and PQC helps organisations operating in the EU become more flexible and avoid being locked into any supplier, thus increasing investment protection. The automation of security and recovery processes helps organisations avoid the scarcity of cybersecurity skills and reduces operational costs, thereby making it easier for organisations of different sizes to benefit from advanced security solutions.

4.3 Limitations and Lessons Learned

Although the CISSAN joint use case demonstration was successful in validating the feasibility and utility of the CISSAN platform, it was also identified that certain limitations may have a bearing on future work. In this regard, it was noted that compliance with PQC was not facilitated across all use case partners. In addition, full compliance with the extended STIX-based threat intelligence exchange was noted to vary depending on system maturity levels. In other words, certain use cases were found to rely on transitional mechanisms rather than fully standardized mechanisms. The implications of these limitations are that, although the CISSAN platform has been found to have significant potential as a tool that enables interoperability with other security solutions that are expected to emerge in the future, full compliance with standardized security mechanisms would require additional integration beyond the project's lifespan. In other words, full compliance with post-quantum cryptography and STIX would require a gradual migration process. The fact that the PQC and the STIX protocols have been partially adopted in the partnerships demonstrates the challenges involved in migrating legacy systems to new security protocols, which has cost, planning, and organizational implications for EU organizations. It is therefore critical for EU organizations to plan

for the migration of legacy systems to emerging security protocols in order to be in full compliance in the near future. This will enable them to be competitive in a highly regulated environment.

Moreover, a single global threshold was used in determining when a device was considered untrusted, triggering isolation at the switch, STIX bundle generation, and orchestration updates. However, domains differ in their expected variability for instance, physical sensors in tunnelling may legitimately experience fluctuations, whereas ICS units may produce steady patterns except during faults. In several cases, natural variability brought certain devices closer to the threshold faster than others. The lesson learned was that a static global threshold simplifies orchestration but does not fully reflect domain specific behaviour. Future work may include exploring dynamic baselining and trust thresholding strategies that account for typical data variability patterns within each domain, while still ensuring consistent triggers for containment, STIX generation, and disaster recovery workflows.

Another issue identified is related to device health checks, which are used to determine the device liveness and to trigger recovery workflows. Since device responsiveness is a part of the trust score calculation, communication jitter or short-lived connectivity issues may occasionally resemble genuine non-responsiveness, interacting with trust updates and leading to uncertainty about the device's true state. The lesson learned is that short-term communication instability needs to be better isolated from trust related interpretations of behaviour. As part of future work, incorporating communication quality indicators or adaptive responsiveness checks could help reduce the likelihood that temporary network conditions are treated as security relevant anomalies. Also, adding intermediate state indicators or event ordering cues across trust management, CTI generation, and orchestration processes could help operators follow system behaviour more clearly during containment and recovery.

5 Conclusions

This report provides the CISSAN joint use case demonstration on the CISSAN platform, which validated the effectiveness of the CISSAN platform and use case solutions in providing the necessary support for the joint operation of various critical infrastructure domains with CI, collaborative defence, and disaster recovery. The integration of the transportation, smart grid, and tunnel construction use cases within the platform provided the necessary validation for the potential effectiveness of heterogeneous IoTs and OTs in providing collaborative solutions to complex cyber-attacks against critical infrastructure domains.

The CISSAN joint use case demonstration provided the necessary validation that the CISSAN platform can provide the necessary support for the effective operation of IoTs and OTs within critical infrastructure domains using standardised threat intelligence sharing, secure communication, trust assessment, and task orchestration. Although the joint use case demonstration highlighted some challenges with the use of emerging standards such as PQC and STIX within the CISSAN platform, such challenges are realistic and provided the necessary guidance towards the potential use of the CISSAN framework within the EU.