Project Report

CISSAN
Collective intelligence supported by security aware nodes

D6.1 CISSAN platform and solutions for the project use cases

Editor: Ilgin Safak, University of Jyväskylä

Abstract

The present report aims to describe the platform-based solution approaches developed and implemented for the five project use cases, namely, transportation, smart grids, tunnel construction, manufacturing execution environments, and automated disaster recovery. The document aims to show the capability of the project platform to provide secure, reliable, and coordinated operation in a wide range of IoT and OT environments. The present document also aims to describe the ways in which the fundamental capabilities of the project platform, such as distributed detection, collective intelligence, automated protection, and coordinated response, are realized and adapted to meet the unique operational and security needs of each respective domain. The use cases presented in this document aim to demonstrate the flexibility, scalability, and operational value of the project platform in providing secure operation for critical and industrial environments, as well as its applicability to multiple domains.

Project CISSAN

Public

April 2026

Participants in project CISSAN are:

- University of Jyväskylä (coordinator)
- Affärsverken Karlskrona AB
- Arctos Labs AB
- Bittium Wireless Ltd
- Bittium Biosignals 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

D6.1 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

Executive Summary

This report describes the platform-based solutions that have been developed and showcased across the five project use cases: transportation, smart grids, tunnel construction, manufacturing execution environment, and the joint use case. It also presents how the project contributes to the ability of Europe to protect its critical and industrial systems through collective, automated, and interoperable cybersecurity solutions. The CISSAN platform enables distributed detection, collective intelligence (CI), automated protection, and response across heterogeneous IoT and OT environments, thus directly addressing the current fragmentation, response time, and reliance on external security services that hinder current cyber resilience capabilities.

The project showcases the potential for reusing and scaling up European Union (EU) developed and standards-aligned cybersecurity solutions across multiple domains by deploying a common platform architecture. The use cases also provide tangible evidence of the impact of the solutions on the ability to detect and respond to cyber threats and security incidents more rapidly, ensuring continuous operations, minimizing recovery times, and increasing trust in the digital environment. In particular, the automated disaster recovery use case showcases the potential for large-scale, secure, and coordinated recovery under adverse and high-pressure scenarios.

Overall, the use cases provide robust evidence that the platform contributes to the achievement of EU digital sovereignty by reducing reliance on non-EU cybersecurity services, enabling secure cross-organizational collaboration, and embedding European standards and security principles directly into operational systems. The results also demonstrate the potential for the platform to be used in real-world environments and its potential to contribute to the achievement of EU policy goals related to strategic autonomy and the secure and trusted digital transformation of critical infrastructures.

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

List of Authors

In alphabetic order by partner name:

- Jari Partanen, Bittium
- Anders Liden, Clavister
- Rodrigo Martinez, Councilbox
- Klaus Chmelina, Geodata
- Ilgin Safak, University of Jyväskylä
- Mikko Lehkonen, University of Jyväskylä
- Stella Palenius, University of Jyväskylä
- Veikko Markkanen, University of Jyväskylä
- Teemu Kemppainen, Mattersoft
- Ann Sjökvist, Mint Security
- Niko Candelin, Netox
- Jyrki Portin, Scopesensor
- Oliver Bölin, Techinova

Table of Contents

Abbreviations

ACL	Access Control List
AI	Artificial Intelligence
API	Application Programming Interface
AVL	Automatic Vehicle Location
BFT	Byzantine Fault Tolerant
BKVS	Blockchain Key Value Store
BMES	Bittium Manufacturing Execution System
CAD	Computer-Aided Dispatch
CEF	Common Event Format
CI	Collective Intelligence
CISSAN	Collective Intelligence Supported by Security Aware Nodes
CTI	Cyber Threat Intelligence
DB	Database
EU	European Union
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HITL	Human-in-the-Loop
HTTP	Hypertext Transfer Protocol
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
OT	Operational Technology
PCAP	Packet Capture
PQC	Post-Quantum Cryptography
RADIUS	Remote Authentication Dial-In User Service
REST	Representational State Transfer
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
TAP	Test Access Points
TI	Threat Intelligence
UC	Use Case
UI	User Interface
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 purpose of this report is to clarify how the CISSAN platform is utilized for its use case solutions, thus showing the relevance of the platform in a wide range of Internet of Things (IoT) and Operational Technology (OT) scenarios. The focus is on the integration of the CISSAN platform in the use case systems, the deployment of the CISSAN platform, and the benefits in terms of security and operation. Five use cases are considered in this report: transportation, smart grids, tunnel construction, manufacturing execution environments, and joint use case. A detailed description of the CISSAN architecture and implementation is provided in the D2.3 report, where this report focuses on solution descriptions, integration, and use case-specific instantiations of the CISSAN platform.

1.2 Document Structure

This report is organized as follows. Section 1 introduces the report. Section 2 provides an overview of the CISSAN platform and describes how it is used for representing multiple use cases. Sections 3 through 7 provide an overview of each of the CISSAN use cases, including transportation, smart grids, tunnel construction, manufacturing execution environments, and joint use case. Section 8 highlights the main lessons learned, including the potential for reuse of the CISSAN platform and its solutions. Finally, Section 9 concludes this report.

1.3 Relation to Other Deliverables

This report builds on the platform architecture outlined in work package (WP) 2, presenting the structural design, distributed system components, and their interfaces of the project platform. The architecture provides the basis for the implementation and instantiation of the project platform in the use case solutions presented in this document. The solutions presented in WP4 and WP5 instantiate the components and functionalities of the architecture presented in WP2, including the collective intelligence (CI) mechanisms, security services, and integration interfaces, and deploy and configure the solutions to meet the operational needs of the use cases. WP2 focuses on the definition of the project platform architecture and implementation model, while this document illustrates the operationalization of the architectural components and solutions presented in WP2 to achieve the use case solutions.

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 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. Through ongoing engagement with partners, WP3 helped identify Key Exploitable Results, clarify partner-specific opportunities, and support consortium-wide maturity in security-by-design, privacy-by-design, and governance practices. 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" (see CISSAN D3.1 report) — continues to hold strong, as demonstrated in this CISSAN D6.1 deliverable.

1.4 Overview of the Five Use Cases

Use Case 1 (UC1) focuses on Global Positioning System (GPS)-based positioning used in public transport systems such as buses and trams. Position information originating from satellite navigation systems is processed by onboard equipment and transmitted through operational transport telemetry systems. Within the CISSAN platform, these positioning data streams are analysed to identify anomalies that may indicate Global Navigation Satellite System (GNSS) spoofing, jamming, or other irregular behaviour affecting positioning-dependent services. The objective of the use case is to demonstrate how CI and monitoring mechanisms can improve the resilience and trustworthiness of positioning services used in public transport operations, thereby supporting reliable and sustainable transport services.

Use Case 2 (UC2) is related to smart power grids. Smart power grids can collect large amounts of sensor data in each substation to monitor the health and quality of the power grid. When a cyber-attack or operational fault occurs, the challenge is to quickly detect it, classify it, and identify its root cause. The objective of this use case is to ensure that cyber protection for the smart grid can automatically detect any potential cyber-attack or effects of attacks in the grid of substations. This means that the substation components are monitored to detect potentially malicious behaviours in terms of local processing behaviours, network communication behaviours or operational grid health. Locally detected events are correlated, helping operators mitigate faults faster and restore grid operation.

Use Case 3 (UC3) is related to tunnel construction. The domain is characterized by numerous monitoring sensors installed in and above a tunnel under excavation that are used for construction process control (e.g., the control of tunnelling machinery) and manifold decision making on site (e.g., for assessing the safety of the tunnel and existing structures above). The permanent availability of high-quality monitoring data is therefore of utmost importance for the safe and economic execution of a tunnel project. The use case now is a data tampering attack affecting this availability where the data is manipulated to reach certain goals (e.g., suppressing alarms for saving costly counteractions, avoiding costly measuring effort by inventing data instead of measuring). Therefore, required counteractions are either missing or unnecessary actions carried out causing problems like delays, stop of works, damages, injuries, etc.

Use Case 4 (UC4) is related to a virtual Manufacturing Execution System (MES), namely the Bittium MES (BMES). The use case is characterized by virtual MES environment which controls the manufacturing of products and devices throughout the life cycle until the maintenance phase of the products. The manufacturing itself is executed by manufacturing partners. The planned system will be used by for the life-cycle management of customers. The full system is containerized and able to be scaled up to consisting of several hundreds of containers, one per manufacturing partner. The idea is to develop security functions for the BMES in cooperation with the CISSAN partners, Bittium and Netox using both real and simulated scenarios and data, and to distribute them to the various nodes within the system (security aware nodes). The use case security functions include e.g. local anomaly detection as well as system level anomaly detection. The databases are based on Microsoft (MS) Structured Query Language (SQL) server and microservices architecture. Applications are based on React and business services are exposed as Representational State Transfer (REST) Application Programming Interfaces (APIs) for client applications. Anomaly detection on incoming of transferred commands and sensor data; if an entry deviates from historical baselines or rule thresholds, it quarantines the information, reverts to the last safe schedule, and alerts the operator.

Use Case 5 (UC5) aims to demonstrate the CISSAN platform functionalities and showcase CI with a prototype in the JYU CISSAN lab leveraging existing use cases. In this setup, WebAssembly Modules (WASMs) from transportation and tunnel construction—together with trust-scoring components—operate across a shared network to simulate a multi-domain environment. The core of the demo is how the platform's CI detects signs of a threat or ongoing attack by correlating unusual behaviour across distributed nodes. When the system identifies a device outage linked to this incident, CISSAN reacts automatically and identifies the failure, evaluates its impact, and redistributes tasks to other available nodes to maintain operational continuity. This demonstrates the system's ability to adapt to disruptions, sustain critical functions, and support resilient, cross-sector

operations without manual intervention. The Councilbox Eventchain system provides infrastructure to record device lifecycle events to a Byzantine Fault Tolerant (BFT) blockchain designed to enable cross-organisational trust without relying on a central authority in production deployments.

2 CISSAN Platform Deployment Model for Use Case Solutions

2.1 Overview of CISSAN Platform

The CISSAN platform is a segmented cybersecurity research and experimentation environment designed to integrate Industrial Control Systems (ICS), Internet of Things (IoT) networks, CI-driven orchestration services, artificial intelligence (AI) edge devices and security testing domains within a unified but logically isolated architecture. The platform is implemented in the CISSAN Lab using Virtual Local Area Network (VLAN)-based network segmentation, centralized authentication, secure remote access mechanisms, and virtualization infrastructure to enable controlled experimentation, monitoring, and resilience testing.

At the architectural level, the CISSAN platform is structured around multiple security zones, each mapped to a dedicated VLAN. These zones include: (i) a Management domain for centralized administration and virtualization services; (ii) an ICS domain hosting Remote Terminal Units (RTUs) and Supervisory Control and Data Acquisition (SCADA) systems for industrial process control; (iii) an IoT domain comprising distributed sensor and edge devices; (iv) a Security Testing domain for engineering workstations and controlled attack simulations; (v) an CI orchestration domain; and (vi) a dedicated CISSAN tools domain for cybersecurity services and research components. Inter-zone communication is governed through controlled routing policies, firewall rules, and access control mechanisms to enforce segmentation and minimize lateral movement.

CISSAN platform components are described in CISSAN D2.3 report for CISSAN architecture.

2.2 Mapping of Use Cases to Platform Instances

UC2 representative assets are in the ICS Zone of the CISSAN platform. The ICS Zone focus is on simulation, development of security solutions and protocol testing for ICS Networks. The core assets are three production grade RTUs, and the associated Windows virtual machine running SCADA software. In addition to these ICS Zone specific assets, there are shared assets located within the management zone, that have responsibilities overlapping the Zone borders that play a crucial role in supporting the ICS centric CISSAN solutions. These assets include a switch for L2 VLAN trunking and segmentation, an industrial router which functions as the primary edge router/firewall and internal Message Queuing Telemetry Transport (MQTT) broker for the lab, leveraged by the ICS centric security solutions, and the CISSAN Management Server which plays a crucial role in aggregating CISSAN solution specific data for further analysis and actions. Also, there are shared assets in one of the Management zones. A key instance is the Security Incident and Event Management SIEM server, which is set up to enable the human operator to observe the functions of the underlaying ICS-centric solutions. The Management Zone also hosts further supporting infrastructure for remote access and access management, critical for enabling secure access to the various segments of the CISSAN platform.

UC3 operational environment (= a tunnel under construction) is characterized by various (often hundreds of) devices, including sensors, loggers, and gateways, communicating data via different protocols and media to a cloud-based control and data management centre. In CISSAN, the main challenge addressed is the detection of data tampering attacks and preventing 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 in tunnelling. The CISSAN platform can be integrated in different ways in the use case. One way is to establish the data exchange (via 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 relevant CISSAN platform components related to this use case include the CISSAN management server, CISSAN Orchestrator, Raspberry Pis, the switch, the data quality verification WASMs and the anomaly detection WASM.

The core physical assets for UC1 and UC3 reside in the IoT zone of the CISSAN platform. The main assets are the five Raspberry Pi devices and a commercial router acting as the router for the IoT zone. The Raspberry Pis represent IoT devices for both use cases. There are also shared assets located in the two Management zones and the Orchestration zone. The switch for L2 VLAN is used for trunking and segmentation, while the industrial router is the primary edge router/firewall. The CISSAN Orchestrator server in the Orchestrator zone is used to coordinate the execution of the WASM modules used in both use cases to calculate anomaly risk scores, believability scores and trust scores on the Raspberry Pis. The input data for the Data Quality Verification module in UC3 is obtained from the SIEM while the data for the AnomalyDetection module is received from the external Mattersoft system via MQTT. The CISSAN Management Server is used for aggregating the generated security data of the different WASM modules. Lastly, the supporting management infrastructure allows for remote access and access management to the CISSAN platform environment.

In addition, the ICS zone is also connected to external systems via APIs. One such external system includes a simulated power distribution grid comprising a primary station and three substations was set up and used for conducting AI-based experiments, with the purpose of detecting cyberattacks, faults and failures (e.g., relay faults), by applying local behavioural-based anomaly detection. While the analysis was performed locally, a correlation engine was used to correlate the locally generated events and create higher-level events containing metadata describing affected substations and fault origin. These higher-level events are then transmitted to the CISSAN platform via MQTT protocol. Furthermore, a machine learning (ML) based fault detector, namely NodeEye, is an external system integrated with the CISSAN platform using MQTT communications. NodeEye is a CISSAN developed embedded real-time fault detection and classification system designed to run directly on an RTU-class microcontroller based on the Techinova’s hardware platform. It acts as an intelligent edge node for 3-phase feeder monitoring, continuously analysing operational electrical signals and reporting abnormal behaviour with minimal latency and without reliance on cloud processing.

The CISSAN platform does not introduce separate, new physical assets for the implementation of UC5. Instead, UC5 is realized by integrating and orchestrating the already-existing systems used in UC1, UC2 and UC3, which collectively represent the heterogeneous, cross-domain environment described in UC5. These systems are connected and coordinated through the shared resources provided by the CISSAN Management Server and the CISSAN Orchestrator, enabling the combined cross-domain data visibility, anomaly detection, trust scoring, and automated response capabilities required for UC5.

3 Use Case 1: Transportation

3.1 Operational Context and Challenges

Public transport systems constitute a critical component of national infrastructure, supporting economic activity, societal continuity, and public safety. Their operation increasingly depends on satellite-based positioning to enable functions such as Computer-Aided Dispatch and Automatic Vehicle Location (CAD/AVL), traffic signal priorities, real-time passenger information, and service planning.

GNSS signals are inherently vulnerable to interference, including spoofing and jamming attacks that can be executed with relatively low-cost equipment. Manipulated positioning data may degrade service reliability, disrupt operational decision-making, and propagate across multiple dependent digital services. Detecting such anomalies is particularly challenging because individual vehicles typically lack sufficient contextual awareness to distinguish malicious manipulation from natural signal degradation.

This use case therefore explores how CI can improve the detection of positioning anomalies across fleets, strengthening the resilience of digitally enabled public transport environments. Public transport cybersecurity is increasingly recognised as a prerequisite for resilient and sustainable smart cities.

3.2 CISSAN Platform Integration and Setup

The CISSAN platform is integrated with a public transport data environment providing near real-time GNSS location data from actual operating vehicles from a city in Finland (Tampere). Positioning data and operational context are securely transmitted through authenticated interfaces into the platform, enabling fleet-level observation without requiring modifications to operational transport systems.

The upstream data pipeline — including acquisition, processing, and transmission up to the MQTT broker — operating under an International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001-certified information security management system. Established controls for secure communications, access management, risk handling, and operational monitoring support the reliability of the ingested data.

Within the CISSAN platform, the CISSAN management server and anomaly detection WASMs deployed on Raspberry Pis analyse aggregated positioning behaviour. This allows the CISSAN platform to function as an external intelligence layer focused on detecting abnormal patterns while remaining isolated from production infrastructure.

3.3 Security and Intelligence Mechanisms

The transportation use case applies a layered security approach that combines standards-aligned data protection with distributed intelligence capabilities.

Vehicle positioning data is transmitted via authenticated and encrypted channels, supporting confidentiality and integrity during transfer. Operational monitoring and incident management practices are implemented for the upstream environment, enabling the identification of events that may affect data reliability.

The CISSAN platform performs distributed anomaly detection by correlating positioning data across multiple vehicles, improving the ability to identify patterns indicative of GNSS spoofing or jamming that might remain undetected at the individual node level. Data quality verification mechanisms evaluate plausibility and consistency, while trust-oriented evaluation concepts assist in distinguishing potentially compromised data sources from normal operational deviations.

Structured threat information sharing using Structured Threat Information eXpression (STIX) enhances situational awareness among participating entities. Certain advanced capabilities,

including automated threat intelligence exchange and post-quantum cryptography (PQC), are being evaluated within the project context and represent potential extensions for future operational deployments.

3.4 Expected or Observed Benefits

Applying collective anomaly detection to positioning data is expected to strengthen the dependability and continuity of public transport services. Earlier identification of interference supports faster operational response, helping maintain accurate passenger information and coordinated fleet operations.

Greater service reliability can increase public trust in transport systems and encourage a shift from private vehicles toward public transport. Such modal changes contribute to reduced congestion, lower urban emissions, improved air quality, and progress toward climate objectives.

From a security perspective, the CISSAN platform introduces an intelligence-driven observation layer that complements existing technologies without requiring significant architectural changes. The use case therefore demonstrates how collective cybersecurity capabilities can enhance infrastructure resilience while supporting broader societal and sustainability goals.

4 Use Case 2: Smart Grids

4.1 Operational Context and Challenges

The use case operates on the CISSAN platform that mimics a smart-grid field layer: RTUs receive supervisory control from a SCADA system and publish telemetry and trust-related evidence over a separate MQTT security overlay. The infrastructure is segmented so that the SCADA–RTU control loop stays within the ICS segment while the MQTT overlay, and management plane are reachable only over defined paths following IEC 62443 guidance. Actors include the field devices (RTUs), the CISSAN Management Server (coordination and aggregation), the CISSAN Orchestrator (deployment and module lifecycle), and the blacklister (port-level isolation), with operators using the CISSAN Management Server GUI and, where applicable, a SIEM for monitoring and investigation. The environment is treated as operationally sensitive while also being labour intensive: devices participate in distributed trust scoring and automated response, so incorrect or delayed isolation of a compromised unit can affect the integrity of CI decisions and the effectiveness of mitigation. The main challenges are securing a distributed, resource-constrained edge layer and enforcing a clear security boundary without redesigning the OT control protocols. RTUs are attractive targets (limited hardening, often shared networks) and may be compromised or misbehaving; the CISSAN platform must detect deteriorating trust or anomaly signals and act on them quickly. At the same time, isolation must be constrained and reversible: only designated ports are allowed to be blocked, and restoration to a specific VLAN must be possible so that legitimate devices are not permanently disconnected.

4.2 CISSAN Platform Integration and Setup

The UC2 segment in the CISSAN platform was established to provide a realistic environment for integrating and validating IIoT centric CISSAN platform solutions. The purpose of building a dedicated ICS/OT zone is to test the solutions under constraints that shape real deployments: resource-constrained field devices, segmented OT networking, remote access requirements, and safety-driven operational expectations. The CISSAN platform was designed to mirror essential elements of a power distribution automation and remote monitoring/control system, while remaining manageable for iterative development and experimentation.

From an integration standpoint, the lab follows a substation-style deployment model. Multiple RTU-class field devices connect to a layer 2 switch and communicate with a SCADA environment hosted on a server platform. Normal operational traffic is emulated by generating process-like signals on the RTUs and transmitting them to the SCADA server using an industry-standard SCADA protocol, providing a realistic baseline for integration and validation. CISSAN platform capabilities are integrated as an overlay to this baseline system rather than replacing operational functions. Field devices retain their process-facing roles, while platform components are deployed where they fit best: on-device functions on RTUs for local observation and participation in distributed security tasks, a management/server layer for aggregation and system-level state, and gateway/agent roles at the OT boundary and server environment for controlled remote access and monitoring integration. This structure reflects how a real use case system can be extended with security awareness and cooperative security functions without restructuring the underlying OT workflow.

Deployment on the CISSAN platform can be summarized as follows. In the OT/ICS field layer, three RTUs represent the primary use case devices and participate in the CISSAN platform’s distributed workflows. In the server/virtualization layer, a hypervisor hosts the SCADA server VM and supporting VMs (e.g., engineering workstation and remote access/VPN services), while centrally reachable CISSAN platform services are placed here to avoid burdening constrained field devices. At the OT/WAN interface, a dedicated router provides separation and controlled connectivity between the OT segment and external access networks, enabling realistic administration patterns (e.g., remote maintenance) without collapsing OT segmentation.

Operationally, the CISSAN platform is accessed using standard remote administration practices: remote sessions to RTUs, remote access to virtual machines, and web-based management interfaces for network equipment. To keep the environment controllable, the CISSAN platform also uses intentional abstractions (simplified redundancy, no IT pipeline and limited auxiliary IIoT subsystems) while preserving the essential characteristics needed for CISSAN: segmented OT

connectivity, constrained endpoints, involvement of realistic operational traffic, and a practical surface for validating distributed and cooperative security mechanisms.

4.3 Security and Intelligence Mechanisms

In UC2, the CISSAN platform applies security mechanisms that are compatible with OT constraints while still enabling collaborative defence, essentially extending cybersecurity to protect the operational environment from within. A central capability is distributed security features at the device layer, where field endpoints generate security-relevant observations. This approach is used because many OT threats unfold “inside the perimeter” (e.g., credential misuse or living-off-the-land activity) and therefore require visibility that is closer to the process and devices than centralized monitoring alone typically provides.

CI is then realized through novel AI solutions, peer-to-peer security intelligence exchange and data quality verification via cross-checking. For example, the CISSAN platform can employ lightweight, process-level monitoring that learns a baseline behavioural profile for each device and then continuously tracks its temporal evolution to detect anomalous deviations from the baseline that are indicative of potential compromise. Devices share their observations with peers and use agreement or divergence to assess whether behaviour is consistent with the segment’s expected operating conditions. On top of this, the platform applies trust scoring as a governance mechanism: trust provides a continuously updated measure of device reliability that reduces dependency on single reports and limits the influence of misconfiguration, noise, or compromised nodes. Global trust is derived through aggregation of peer assessments, enabling system-level decisions about whether a device should remain eligible to participate in communication.

As a natural extension, the CISSAN platform supports structured intelligence outputs for human oversight and potential external sharing. Security-relevant events and trust-related outcomes can be mirrored to centralized monitoring for operator visibility, and the project prototypes STIX-based threat intelligence sharing to represent high-value CISSAN security events in an interoperable Collective Threat Intelligence (CTI) format. This is particularly relevant where trust-related events (e.g., loss of reliability leading to isolation) should be communicated beyond the local segment to support partner triage, correlation, and response workflows.

In addition to the distributed security and trust mechanisms described above, the Smart Grid use case integrates a NodeEye as a process-level fault and anomaly detector operating at the control/device layer. It continuously monitors three-phase abnormal voltage behaviour in real time and, using tiny machine learning algorithms and neural networks it finds anomalies in the three phase voltage data. When these anomalies are found it reports it to the CISSAN Management Server and then uses other algorithms to analyse the three-phase current data that was observed during the anomalous window. If this is classified as a type of electrical fault, it will indicate this to the CISSAN Management Server as well. By performing this intelligence locally on a constrained RTU or fault detector hardware, it can share its results collectively and reduces detection latency. Moreover, multiple NodeEye deployments could indicate more significantly where the fault is in the grid, depending on how the anomaly on the voltage compares to how the classification of the current fault results in over multiple NodeEye deployments.

4.4 Expected or Observed Benefits

In this use case, one of the primary expected benefits is improved detection depth and earlier visibility into malicious and faulty behaviour on OT endpoints, and naturally, within the protected network. By shifting part of the security responsibility to the device layer the platform can surface abnormal activity that may not be visible through perimeter controls or centralized monitoring alone, especially when anomalous instances occur through legitimate channels. This strengthens situational awareness in the ICS segment without requiring heavyweight analytics on constrained devices.

A second major benefit is faster, more resilient response through collective reasoning. Peer sharing and comparison reduce uncertainty by allowing multiple nodes to corroborate observations and build

confidence in what is occurring, while trust scoring provides a structured way to translate distributed observations into network-level confidence. This reduces the risk that a single faulty or compromised node dominates security conclusions, and it supports containment actions, such as constraining participation in communication, based on aggregated assessments rather than isolated alerts.

Benefits are also gained through coordination and interoperability. Central aggregation and structured outputs provide a unified view for operators and enable integration with monitoring and intelligence workflows, improving stakeholder coordination during incidents. Where CTI export is applied, intelligence becomes easier to communicate across tools and organizational boundaries, supporting more rapid triage, evidence-driven investigation, and consistent reporting practices.

5 Use Case 3: Tunnel Construction

5.1 Operational Context and Challenges

UC3 is in the tunnel construction domain where numerous monitoring sensors are operated to measure manifold physical parameters relevant for the control of construction processes and machines. To guarantee correct decisions and an efficient control of processes and machines on site, the availability of high-quality data is paramount. Thus, any cyberattack disturbing the acquisition and transfer of data from the sensors to the central control and data management system as well as any data tampering or operational causes influencing the data quality might have severe impacts on the tunnel project.

The use case's operational environment (= a tunnel under construction) is characterized by various (often hundreds of) devices (sensors, loggers, gateways) communicating data via different protocols and media to a cloud-based control and data management centre. From there, the data is provided to various automatic services, and numerous (often hundreds of) users access the data through web clients to make decisions. The heterogeneity and high number of devices, protocols, media, involved actors, Information Technology (IT) systems, etc. makes the operational environment highly fragmented, complex, and difficult to secure. In CISSAN, the main challenge addressed is the detection of data tampering attacks and to prevent their impact. The CI-methods provided by the CISSAN platform, especially their capability to alarm, quarantine, isolate and blacklist affected devices and data are seen as a step forward to increase security in tunnelling.

5.2 CISSAN Platform Integration and Setup

The CISSAN platform can be integrated in different ways in the use case. One way is to establish the data exchange (via 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 corresponding believability scores can be returned. The main CISSAN platform components used include the CISSAN Management Server, CISSAN Orchestrator, Raspberry Pis, the data quality verification WASMs and the Councilbox Eventchain System.

Another way is to connect devices that provide sufficient processing power (or that first need to be upgraded to provide the needed processing power) for being trust monitored, scored, and, in case, blacklisted and/or even deactivated.

Additionally, a PQC tool may potentially be leveraged by the CISSAN platform post-project for executing its code in devices that, as above, provide sufficient processing power (or that first need to be upgraded to provide the needed processing power) to securely transfer data between devices, servers and users.

5.3 Security and Intelligence Mechanisms

Different security and intelligence mechanisms can be used in the use case. The mechanisms considered most beneficial are data quality verification and anomaly detection as they aim for detecting data tampering attacks which are considered most critical/impactful.

Trust scoring and blacklisting of devices like sensors and gateways are considered also beneficial. The devices in most cases do not automatically/directly affect tunnelling operations but are used for decision making on these operations. It is valuable to know when they are attacked and to indicate/flag/deactivate the use of the data they deliver; stopping their operation/deactivating them might not be required.

The potential use of a PQC tool by the CISSAN platform for providing high-level encryption of data is seen relevant, especially for sensor data communication in future.

The use of STIX is considered important for future exchange of threat information with the outside world (other tunnel projects, other domains) to allow for precautionary measures and preventive actions.

5.4 Expected or Observed Benefits

The use of the CISSAN platform is expected to significantly improve the detection of data tampering attacks on tunnel monitoring data, and the detection of operational issues. It will reduce the probability of incorrect or missed detections derived from tampered data and enable faster responses to such attacks, as a result, tunnelling will become safer.

6 Use Case 4: Bittium Manufacturing Execution Environment

6.1 Operational Context and Challenges

Bittium is currently developing a virtual MES environment which controls the manufacturing of Bittium products and devices throughout the life cycle until the maintenance phase of the products. The manufacturing itself is executed by manufacturing partners. The planned system will be used by Bittium for the life-cycle management of Bittium customers. The full system is containerized and able to be scaled up to consisting of several hundreds of containers, one per manufacturing partner (see Figure 1). There is a built-in secure architecture available in UC4 that follows the CISSAN development approaches. See more detailed description, e.g., from the CISSAN D4.3 report.

Netox-led cybersecurity architecture design for CISSAN is validated and tested it in the Bittium BMES Use Case. The objective was to realize *security-aware nodes* and distributed detection across IoT/OT, edge, and IT platform layers, leveraging *Microsoft Defender for IoT* sensor for passive network telemetry with Sentinel as the SIEM plane and Security Operations Centre (SOC) Radar for external Threat Feeds. These choices follow the current CISSAN architecture and the guidance to focus on concrete components and interfaces. The implementation is defined through Bittium use case.

6.2 CISSAN Platform Integration and Setup

The developed security functions for the BMES in cooperation with the CISSAN partner Netox using both real and simulated scenarios and data, and to distributed them to the various nodes within the system (security aware nodes). The security functions include, e.g., local anomaly detection as well as system level anomaly detection. The databases are based on MS SQL server and microservices architecture. Applications are based on React and business services are exposed as REST APIs for client applications. Postgres SQL has been selected as a basis for operative data storages. Operating environment follows the following Digital Twin Architecture.

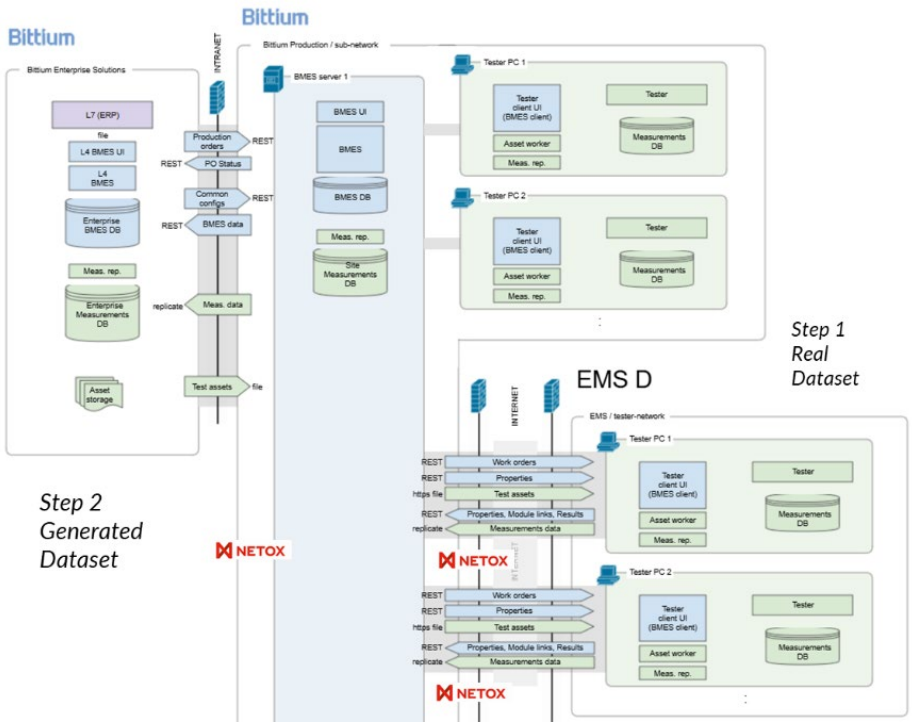

Figure 1. BMES system architecture

Following the CISSAN architecture, Netox designed positions of Defender for IoT sensors at Bittium BMES network vantage points NGINX (SPAN/TAP) to perform asset discovery, vulnerability

exposure mapping, and threat detection on east-west and north-south traffic, forwarding normalized telemetry and alerts to the cloud management plane and Microsoft Sentinel for correlation, hunting, and automated response. The architecture also anticipates certificate-based device authentication, remote attestation, and secure boot/protocol primitives in the device/edge layer where available via BMES capabilities. The architecture provided by Netox is described in D2.3 (see Figure 2, page 15).

Systems Integration within BMES ↔NETOX are the following:

- Network telemetry: SPAN/TAP → Defender for IoT sensors (virtual appliances). Sensor-to-cloud uses secure outbound connection; incidents stream to Sentinel.
- SIEM/Security Orchestration, Automation and Response (SOAR): Ingests Defender for IoT alerts plus BMES logs (API gateway, container runtime, orchestration, database (DB)). Playbooks orchestrate containment (e.g., network Access Control List (ACL) updates, service isolation).
- Threat Intelligence (TI): Cloud-based TI and ML/AI analytics augment detections and with supervised learning logic.

Data Exchange Formats and Protocols.

- Traffic capture: Packet Capture (PCAP) (Switch Port Analyzer (SPAN)/ Test Access Point (TAP)) for sensor ingestion.
- Security events: Defender for IoT → Sentinel via native connector (JavaScript Object Notation (JSON)).

Application logs: JSON/ Common Event Format (CEF) common schema to Sentinel

- The design directly implements CISSAN's security-aware nodes concept by distributing detection and response across nodes and layers and supports CI by sharing local insights (sensor analytics) into a central reasoning plane for fused, cross-node decisions.

6.3 Security and Intelligence Mechanisms

The following security and intelligence elements were applied.

Distributed System Elements and Interfaces

A. Device & Edge layer

- IoT/OT devices: BMES use-case endpoints (manufacturing-related device fleet represented by the Bittium dataset) and site infrastructure components that generate operational telemetry (dataset-based representation for development/validation).
- Gateways/edge nodes: Network elements that forward traffic; vantage points for passive sensors.
- Security sensors: Defender for IoT on-premises sensors (virtual appliance form factor) receiving mirrored traffic; sensors extract metadata/features locally and forward findings to the cloud management plane.

B. Bittium BMES Application Layer

- Microservices: Containerized (Docker) services (hundreds at scale) providing business capabilities via REST endpoints.
- Data services: MS SQL Server for relational back-office/state; PostgreSQL for operative stores.
- User Interface (UI) layer: React front ends invoking service APIs.

C. Netox Security & Management Layer

- Defender for IoT Cloud, Management of sensors, Threat analytics, CTI feeds, and ML/AI-enhanced detections. Hunting querys-

- Microsoft Sentinel for alert ingestion, correlation, case management, and automation playbooks.
- Bittium device control for secure device-to-control communications where the use case requires command/control alongside passive monitoring.

D. Device, Edge, and Agent Layers

- Device layer: Sensors/actuators in the manufacturing lifecycle; modelled by Bittium's 1,000-device dataset for development and test.
- Edge layer: Gateways and virtual switches enabling SPAN/TAP; Defender for IoT sensors run as virtual appliances adjacent to BMES traffic paths.
- Agent layer: Where applicable, lightweight agents for endpoint/host telemetry complement network-centric detection, with events fused in Sentinel.

The above componentization conforms with CISSAN's secure platform vision, and the security-aware nodes rationale as introduced in the project description documents.

Interfaces, integrations and protocols

As BMES is a microservices-based system (React front end, REST services, MS SQL Server & PostgreSQL back ends) designed to scale to hundreds of containers, often one per manufacturing partner. Interfaces and protocols are the contract that keeps this scale from devolving into brittle point-to-point coupling (see Figure 2).

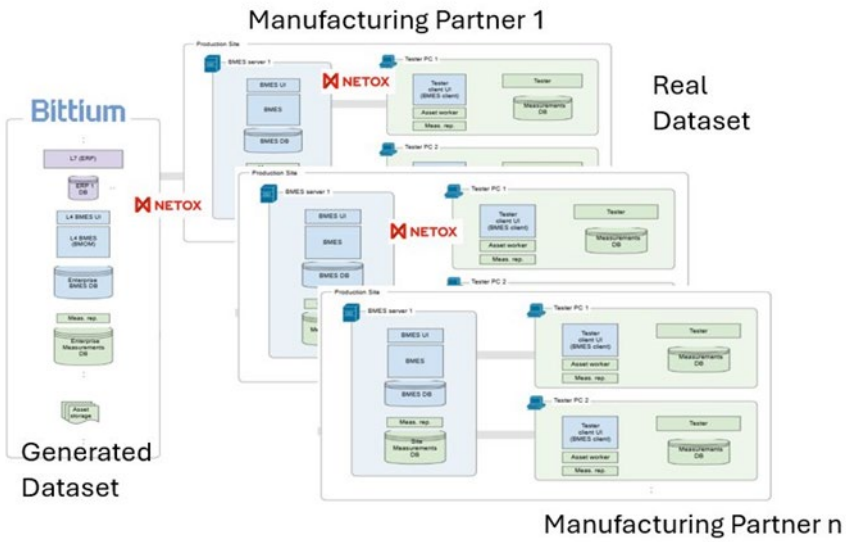

Figure 2. Overview of the UC4 virtual MES setup

Netox's stack relies on Defender for IoT sensors (passive network visibility) feeding Sentinel (SIEM) and D3 (Security Orchestration, Automation and Response (SOAR)). Unless you pin down the exact feeds, schemas, auth patterns, and network placements, detections and automated response cannot be guaranteed or audited. Also considering human-in-the-loop (HITL) in BMES use case is important.

Internal Service Interfaces.

- *BMES Service APIs*: REST endpoints consumed by the React UI and partner services (Security: OAuth2/OpenID Connect recommended; API gateway logging to SIEM).
- *Data access*: App-to-DB over segmented virtual networks to MS SQL Server/PostgreSQL (DB audit to SIEM).

IoT and OT Device Interfaces

- Device telemetry/control via site networks and gateways; Bittium “IoT Hub” is available for secure device-to-cloud messaging when used; device trust reinforced by certificate-based authentication, remote attestation, and secure boot.

Systems Integration (BMES ↔NETOX)

- *Network telemetry*: SPAN/TAP → Defender for IoT sensors (virtual appliances). Sensor-to-cloud uses secure outbound connection; incidents stream to Sentinel.
- *SIEM/SOAR*: ingests Defender for IoT alerts plus BMES logs (API gateway, container runtime, orchestration, DB). Playbooks orchestrate containment (e.g., network ACL updates, service isolation).
- *Threat Intelligence*: Cloud-based TI and ML/AI analytics augment detections and with *supervised learning* logic.

Data Exchange Formats and Protocols.

- *Traffic capture*: PCAP (SPAN/TAP) for sensor ingestion.
- *Security events*: Defender for IoT → Sentinel via native connector (JSON).
- *Application logs*: JSON/CEF common schema to Sentinel

The design directly implements CISSAN’s security-aware nodes concept—distributing detection and response across nodes and layers—and supports CI by sharing local insights (sensor analytics) into a central reasoning plane for fused, cross-node decisions.

Distributed Network Traffic Monitoring & Threat Detection

Passive, out-of-band network monitoring using Defender for IoT sensors provide L2–L7 visibility without requiring intrusive instrumentation inside BMES containers. Sensors extract metadata and behavioural features locally, enabling both local anomaly detection and system-level analytics through the CISSAN plane.

Sensor placement

- Primary taps on BMES container fabric ingress/egress and service-mesh/inter-service segments using SPAN/TAP on the virtualized host switches or container network overlays.
- Optional taps at partner-link edges where BMES instances per partner terminate.
- Where encrypted traffic limits inspection, relies on metadata (SNI, JA3/JA4, flow behaviour) and control-plane logs for context; use of selective decryption only in the zones approved by Bittium security.

Telemetry pipeline

1. PCAP/SPAN mirrors feed Defender for IoT sensors.
2. Sensors perform asset discovery, vulnerability posture inference, protocol parsing, and threat analytics, and export findings to Defender cloud; enriched incidents stream to Microsoft Sentinel for correlation with identity, endpoint, and *cloud signals.*
3. BMES service and infrastructure logs (API gateway, container runtime, DB audit) are forwarded to Sentinel via connectors for fused detections and playbooks.

Security Management

- Defender for IoT deployment: Provision virtual sensors sized to BMES throughput; register with Defender portal; define zones aligned to BMES network segments; enable cloud analytics and TI feeds.
- Sensor connectivity: Outbound-only management plane; no inbound exposure required. (Meets BMES security constraints.)

Orchestration & Automated Response (presented method)

- Implementation of analytics rules tuned to BMES protocols and flows; automate triage/containment (e.g., block indicators, isolate services, open incident with context to BMES operators).
- CI signals (e.g., distributed anomaly scores) are shared to reinforce detections across nodes.

6.4 Expected or Observed Benefits

The system functionality has been validated with two datasets. In December 2024, the first system data example provided several anomalies within the use case functionality. These observations were compared to available example dataset´s in Github. During the second phase, the BMES security functions were already in place and based on the second phase dataset obtained in December 2025, the identified vulnerabilities with a truly large dataset were very low.

7 Use Case 5: Automated Disaster Recovery (Joint Use Case)

7.1 Operational Context and Challenges

The CISSAN joint use case demonstration is based on a multi-domain critical infrastructure attack mitigation scenario, leveraging the previous use cases. In this use case, transportation, smart grids and tunnel construction systems are all connected and simultaneously attacked by a cyber-attack. As a result, data produced by the previous use cases is at risk of exposure, and critical systems face an increased risk of service outage.

In distributed environments, individual anomalies may appear as isolated technical issues, while their combined effect can indicate a coordinated cyber-attack. A unified platform provides centralized visibility and enables correlation of signals across devices and services, supporting more effective incident detection and analysis. As system size and complexity increase, manual monitoring and recovery become difficult to manage and prone to delays or inconsistencies. Automated disaster recovery helps address these challenges by enabling timely and coordinated restoration of system operation, thereby supporting reliable and secure operation.

7.2 CISSAN Platform Integration and Setup

The CISSAN Management Server acts as the central platform component coordinating the CISSAN platform. It serves as the integration point through which different services and platform components are connected. This central deployment enables unified visibility of system status, cross-domain event correlation, and coordinated response actions during simultaneous cyber-attacks.

Councilbox Eventchain is deployed in CISSAN as containerized services via Docker Compose: one master node and two hub nodes, each running the full stack (Events API, Blockchain API, Blockchain Key Value Store (BKVS), and Blockchain Explorer).

The primary integration point with the CISSAN platform is the Metadata API, a stateless REST service that abstracts blockchain operations behind standard Hypertext Transfer Protocol (HTTP)/JSON interfaces. The CISSAN Management Server records device lifecycle events (registration, trust score updates, anomaly detections, and blacklisting) without direct blockchain interaction. All events are signed, stored as BKVS transactions, and included in blocks that undergo BFT consensus validation across all nodes.

The integration flow: the CISSAN Management Server issues authenticated REST calls to the Metadata API, which dispatches signed transactions to the consensus pipeline. The master node assembles transactions into Merkle trees, creates blocks, and broadcasts them to hub nodes. Consensus is achieved when at least 51% of nodes provide verified validations.

The Blockchain Explorer provides a web-based interface for inspecting blocks, transactions, and consensus status in real time, supporting operational oversight and audit during use case execution.

7.3 Security and Intelligence Mechanisms

The CISSAN platform uses a combination of security and CI mechanisms to build a shared understanding of the system’s security state. Data quality verification checks the reliability of incoming information, helping to filter out manipulated or misleading data before it influences decisions. Believability scoring and blockchain-based trust mechanisms add another layer by evaluating how dependable each device and data source has been over time.

Anomaly detection and risk scoring run across multiple devices and network points, identifying unusual behaviour in traffic patterns, device activity or operational processes. These findings are combined through multi-agent coordination, which allows security tasks—such as malware pattern matching, routing decisions or distributed disaster recovery—to be shared across the network rather than handled by a single component. Threat intelligence from external sources is incorporated through structured formats such as STIX, and communication between components is protected

using post-quantum cryptography. Together, these mechanisms create a defence model where devices support each other and respond collectively to emerging threats.

Eventchain contributes to the automated disaster recovery use case as an immutable recording and query layer for device governance decisions.

Trust management. Every trust score change issued by the management server is recorded as a consensus-validated blockchain transaction, creating a tamper-proof audit trail of trust evolution. The BKVS provides $O(1)$ retrieval of the latest device state and the full history of events for any given key, enabling operators and automated processes to assess device reliability based on verifiable history.

Device governance. The management server records the complete device lifecycle on the blockchain through the Metadata API: registration, trust score updates, anomaly detection events, and blacklisting. Eventchain stores them through BFT consensus, ensuring that no single component can unilaterally alter the governance record.

External immutability. The blockchain periodically anchors its state to Bitcoin via OP_RETURN transactions, providing an independently verifiable proof of the ledger state at each epoch boundary.

7.4 Expected or Observed Benefits

Using the CISSAN platform in this joint use case brings several practical advantages. By combining information from different domains, the CISSAN platform can detect coordinated attacks earlier and with greater confidence. Automated response capabilities help restore normal operation more quickly, reducing the time systems remain disrupted. The use of trust scoring and distributed detection improves resilience by ensuring that the system can continue functioning even when individual components are compromised or unreliable.

Stakeholders gain a clearer view of what is happening across the entire environment, which supports more informed decision-making during incidents. The coordinated approach also reduces operational risk by preventing isolated responses that might conflict with each other. Overall, the platform strengthens the continuity and security of interconnected critical infrastructure by enabling faster detection, more consistent recovery and better cooperation between the involved systems.

Integrating Eventchain into the joint use case delivers several tangible benefits.

- **Immutable audit trail.** Every governance event is permanently recorded and validated through BFT consensus, ensuring that the operational history of every device can be reconstructed and verified for post-incident analysis and compliance reporting.
- **Cross-organizational trust.** All nodes independently validate each block, enabling organizations operating different infrastructure segments to rely on a common, verified record. In production deployments with multi-organizational nodes, this shared trust layer is designed to reduce the coordination overhead typical of multi-stakeholder disaster recovery.
- **Interoperability.** Standard REST/JSON interfaces enable integration with other CISSAN components without requiring blockchain expertise, lowering the integration barrier.
- **Byzantine fault resilience.** BFT consensus ensures correct operation even when a minority of nodes behave unexpectedly, a property particularly valuable in disaster recovery contexts where infrastructure integrity cannot be assumed.

8 Lessons Learned and Reuse Potential

8.1 Key Lessons Learned from Use Case Implementation

UC1: Public transport positioning data proved suitable for demonstrating anomaly detection concepts within the CISSAN platform. The use case showed that existing operational telemetry streams can be reused for security monitoring without modifying the underlying transport systems. The use of standardized interfaces and messaging mechanisms simplified integration and allowed the platform to scale to multiple data sources. In addition, the separation between operational transport systems and the CISSAN analysis environment ensured that experiments could be conducted without affecting operational continuity, highlighting the importance of gateway-based architectures when integrating OT environments with cybersecurity platforms.

UC2: The smart-grid OT/ICS deployment demonstrated that CI security mechanisms can be integrated into a realistic control environment without disrupting the operational loop, provided that monitoring remains lightweight and communications are cleanly separated from control traffic. A key lesson was that RTU-class devices can contribute meaningful security visibility when outputs are standardized and shared, while centralized aggregation simplifies operator oversight and enforcement actions such as isolation. The implementation also highlighted the importance of careful segmentation, scheduling, and configuration management to keep resource use predictable and to avoid cross-interference in a constrained lab setting, which improves reuse potential across similar OT environments.

UC3: The Data Quality Verification module is implemented based on code from Geodata. Due to data coming in different forms from different use cases, we performed data preprocessing to unify all dataset from different cases into Geodata format. However, experimental results obtained for other use cases do not display as high performance as that obtained using the Geodata dataset. By further investigation, it is inferred that the data pattern is the main cause of poor generalization results. Dataset (voltage and GPS) from smart grids and public transportation are not linearly distributed. Linear regression-based data quality verification is not suitable for these datasets. As for similarity-based methods, unlike neighbouring sensor readings from Geodata, there are no similar features in other use cases. A potential solution is to extract normal time series data from historical dataset as a reference to compare it with.

UC4: The vulnerability and anomaly detection system functionality has been validated now with two datasets. In the initial system data, several anomalies were provided within use case functionality, where these observations were compared to the sample dataset available in GitHub. During the second phase, the BMES security functions were already in place, where the identified vulnerabilities and anomalies were very low in a massive dataset, which indicates that improvements were made during the CISSAN development. What was learned during the process that after the first dataset, how thorough the security functions should be in the case of scalable number of nodes considered which was indicated after the first iteration. For the second iteration all these were installed with help of Netox as they identified the key improvements. Similarly, we identified improvements that we should do for the software component testing for the BMES, which are still on-going.

UC5: One of the key lessons learned in the process of the UC5 implementation on the CISSAN platform is that integration is a critical aspect to consider when multiple parties are involved in a project. Different server infrastructures, architectural design, and configuration methods need to be considered in integrations. This posed a challenge in the compatibility and ability of the servers to communicate and exchange data effectively. However, this problem was addressed by standardizing all interface specifications and key configuration parameters, as well as creating a consistent API structure. This significantly improved compatibility and stability of all server environments. Abstracting blockchain complexity behind a standard REST API proved critical for adoption: integration through familiar HTTP/JSON patterns without requiring blockchain expertise. The BKVS design, which provides both current state and full historical queries for any key, proved essential for the CISSAN management server to make trust-based decisions efficiently. The clear separation between decision-making (CISSAN Management Server) and recording (Councilbox Eventchain System) simplified integration and ensured that the governance record remains an independent verification artifact.

8.2 Reuse and Replication Potential

Most of the developed data quality verification and anomaly detection methods provided by the CISSAN platform focus on analysing sensor data. Therefore, they can be used in practically all domains and operational environments where sensors are used. Sensors are used in various industries and business areas to transform physical data into informed decisions. Examples of areas where the CISSAN platform could be used, even real-time decisions must be made and cybersecurity has become of great concern, are:

- Industry & Manufacturing (Industry 4.0): Sensors monitor parameters to, for example, enable predictive maintenance before costly breakdowns occur.
- Agriculture (smart farming): Soil moisture and weather sensors help farmers make precise decisions about irrigation and fertilization, maximizing yields and conserving resources.
- Logistics & supply chains: GPS and acceleration sensors track locations and transport conditions (e.g., cold chain for vaccines) to optimize routes and guarantee product quality.
- Healthcare: Wearables record vital signs (heart rate, oxygen saturation), enabling medical staff to monitor patients remotely and make faster diagnoses.
- Energy & smart buildings: Presence and light sensors automatically control HVAC systems (heating, ventilation, air conditioning) and lighting to reduce energy consumption based on actual room usage.
- Retail: Sensors for measuring customer traffic help optimize store layouts and allocate staff more efficiently.
- Construction: Sensors monitor the strength of hardening concrete or the utilization of heavy machinery to minimize project delays.

The trust scoring mechanism and Councilbox Eventchain system is designed for reuse across IoT and OT environments beyond CISSAN. The Councilbox Eventchain system has a Docker-based containerized architecture that enables the rapid deployment with minimal configuration. The BKVS provides a generic key-value store on top of the blockchain, adaptable to any domain requiring immutable state management, including critical infrastructure protection, supply chain integrity, and industrial IoT. The Metadata API built for CISSAN demonstrates how a domain-specific REST interface can be layered on top of the BKVS for a particular use case. The modular design (consensus layer, key-value store, and REST API as separate components) allows individual parts to be reused or extended independently.

The CISSAN Orchestrator has significant potential for reuse and replication in use case domains beyond CISSAN for disaster recovery automation, security task orchestration, and the use of standardized integration mechanisms, thanks to its modular architecture. It helps devices coordinate data, perform routing and task provisioning autonomously, thereby enabling collective intelligence and transforming centralized, legacy systems into decentralized ones. This helps enhance the cybersecurity of IoT/OT networks by creating automated workflows for the processing of threat intelligence and the response processes. This, therefore, creates the potential for it to be adapted to different organizational settings, mainly because of the need for such cybersecurity processes. It is anticipated to be particularly useful for applications in environments with high availability and continuity of operational requirements of OT networks and IIoT environments such as manufacturing.

9 Conclusion

The CISSAN platform and its use case solutions demonstrate the feasibility of a collectively intelligent cybersecurity infrastructure that facilitates information sharing, automation, and response. With the integration of various system components such as the CISSAN Management Server, CISSAN Orchestrator, Councilbox Eventchain System, use case partner systems, and other related services, it has been evident that the CISSAN platform has been instrumental in improving information sharing among various organizations regarding cybersecurity. In addition, various use cases were developed to demonstrate how the CISSAN platform would be instrumental in supporting various scenarios through improved awareness, response to incidents, and automation of cybersecurity processes including disaster recovery, trust management and access control.

During the project, various lessons were learned, one of which is regarding interoperability, especially when dealing with various organizations with diverse server infrastructures and system architectures. The importance of interface standardization, configuration alignment, and monitoring, thus improving the reliability of the CISSAN platform has been established. Other lessons learned include the importance of careful segmentation, scheduling, and configuration management to keep resource use predictable and to avoid cross-interference in a constrained platform setting. Another important lesson learned is that not all data quality verification methods can be applied to any data, as data patterns may vary significantly, which may lead to poor generalization. A potential solution is to extract normal time series data from historical dataset as a reference to compare it with.

The results of the CISSAN project demonstrate that it is possible to create a platform that is instrumental in improving cybersecurity collaboration across various organizations. With its modularity and integration with various standards, it is evident that there is an opportunity to improve the CISSAN platform and its solutions beyond this study through replication and reuse. In particular, the data quality verification and anomaly detection methods provided by the CISSAN platform focus on analysing sensor data, which can be used in any domain and operational environment where sensors are used. The trust scoring mechanism and Councilbox Eventchain system is also designed for potential reuse across IoT and OT environments beyond CISSAN with its containerized architecture that enables the rapid deployment with minimal configuration. The CISSAN Orchestrator also has significant potential for reuse and replication in use case domains beyond CISSAN for disaster recovery automation, security task orchestration, and the use of standardized integration mechanisms, thanks to its modular architecture, where it is anticipated to be particularly useful for applications in environments with high availability and continuity of operational requirements of OT networks and IIoT environments.