E-CORRIDOR
Edge Enabled Privacy & Security Platform For Multi Modal Transport

D 4.1

Requirements for the ISAC Pilot.

WP4 – ISAC Pilot

E-CORRIDOR

Edge enabled Privacy and Security Platform for Multi Modal Transport

Due date of deliverable: 30/11/2020
Actual submission date: 30/11/2020

30/11/2020
Version 1.0

Responsible partner: MISE
Editor: Sandro Mari
E-mail address: sandro.mari@mise.gov.it

Project co-funded by the European Union within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

The E-CORRIDOR Project is supported by funding under the Horizon 2020 Framework Program of the European Union DS-2018-2019-2020, GA #883135

Authors: Giacomo Giorgi (CNR), Sandro Mari (MISE), Veronica Elena Bocci (DIG), Roland Rieke (FC).

Approved by: Stefano Sebastio (UTRC), Riccardo Orizio (UTRC), Thanh Hai Nguyen (CEA)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	27-Jul-2020	G. Giorgi, M. Manea, S. Mari	HPE, MISE	Initial ToC
0.2	17-Sept-2020	G. Giorgi, S. Mari	CNR, MISE	First requirements, Scenario, Stakeholders
0.3	09-Nov-2020	G. Giorgi, S. Mari, V. Bocci	CNR, MISE, DIG	Defined User stories, use cases
0.4	12-Nov-2020	G. Giorgi, S. Mari	CNR, MISE	Defined non-functional requirements, objective
0.5	19-Nov-2020	G. Giorgi, S. Mari, V. Bocci	CNR, MISE, DIG	Defined storyboards, completed UC, US for railway sector
0.6	20 Nov-2020	G. Giorgi, S. Mari	CNR, MISE	Internal review revision
1.0	29 Nov-2020	G. Giorgi, S. Mari	CNR, MISE	Final Revision

Executive Summary

The Information Sharing and Analysis Centre (ISAC) Pilot of the E-CORRIDOR project focuses on producing a prototype implementation of a multi-tenanted managed security analytics platform integrating E-CORRIDOR technology to allow controlled sharing/pooling of security data belonging to different prosumers (i.e., information producer and consumer). Furthermore, the prototype platform will be used to evaluate and validate the E-CORRIDOR approach, architecture, and technology in the context of a security information sharing and analytics service provided to multimodal transport enterprises and users.

This document describes the main stakeholders involved in the ISAC pilot and their different expectations in the adoption of E-CORRIDOR contributions to achieve the pilot's goals. It also describes several crucial use cases for the scenario, and Non-Functional requirements, combining existing Pilot functionalities with those of E-CORRIDOR.

Table of contents

1. High Level Requirements

The ISAC pilot studies application of the E-CORRIDOR concept to a multimodal transportation (MMT) ecosystem that includes air, automotive and train sectors. The pilot aims at providing a multi-tenanted security analytics platform that allows to share data between the transportation sectors specifying the Data Sharing Agreements (DSAs) to protect, regulate and guarantee a privacy level of the data shared. Furthermore, the pilot aims to guarantee a collaborative analysis of the data coming from each transportation sector and the data collected from public sources to identify new threats, vulnerabilities, and anomaly events.

This section is organised to describe the high-level requirements for the ISAC pilot by presenting in Section 1.1 an overview of the current scenario, and the identification of the main stakeholders in Section 1.2. Then, Section 1.3 describes the current practice and how adopting the E-CORRIDOR framework can improve it. In Section 1.4 are reported the user stories, whereas their relevance for the E-CORRIDOR objectives are remarked in Section 1.5. In Section 1.6 are reported some questions that will guide the pilot evaluation.

Use cases and non-functional requirements for the ISAC pilot are reported in Section 2 and Section 3. The document concludes in Section 4.

1.1. Scenario

Interconnected Transportation Systems (automotive, aviation, railway) produce and consume a large amount of data. These pieces of information concerns both the operative side of the transports themselves and of their users. Being a critical sector, motivation of attackers in targeting this is rising for several reasons, such as accessing private user information, causing denial of service with the intention of tampering reputation of rival companies, or even attempt to perform terrorist actions. To prevent such attacks, it is required to have systems that can timely notify known vulnerabilities and strategies to address them, while keeping the privacy/control of shared information. Privacy is of great importance. If ones share the information on a vulnerability or an attack s(he) might either compromise the reputation of a company or expose involuntarily a company to attacks due to disclosure of an existing vulnerability. A system able to convey information on vulnerability and attacks, across different transportation systems (multi-modal) in a timely manner by preserving data privacy is needed. To this end the Information Sharing and Analysis Center (ISAC) can help critical transportation infrastructure owners and operators to protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyse and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. The ISAC can involve multiple transportation sector in the sharing and analysing process to the end to increase the overall picture of vulnerabilities and attacks of the whole transportation ecosystem and provide a notification system to timely react to possible cyber-attacks.

Through the E-CORRIDOR framework it is easier to gather and share data in a controlled manner, by leveraging purpose-specific Data Sharing Agreements, and thus possibly control the analytics functions that can be applied on the shared data to discover possible cyber threats or anomaly events. This will allow transport services and infrastructures to exchange, retrieve and analyse in a privacy preserving manner information on vulnerabilities, attacks, safety issues, incident reports and other relevant data.

The ISAC pilot is instantiated by means of a hybrid infrastructure which enables edge-based and cloud-based operations. Information can be easily fed to the information sharing system, after specifying its sharing policy, which states where the data can be moved, stored, used and

which level of privacy must be reached for each operation via anonymization. Data can be anonymized either locally or in ISAC's premises. Analysis is generally performed in ISAC's premises on data anonymized or homomorphic encrypted according to provider policies and results are automatically delivered by the ISAC to all interested parties, for a timely notification on new threats, attacks or vulnerabilities that can affect their systems. However, thanks to the E-CORRIDOR framework each transportation sector can run locally their own analytics on their system (vehicle, railway, airport), and also choose to share with the ISAC initial/partial results computed with the set of information that is available locally, specifying through the Data Sharing Agreement (DSA) with whom to share the data.

In addition, the interested stakeholder can receive information on course of actions to fix vulnerabilities, to mitigate or to stop ongoing attacks and/or to recover the system functionalities, after a successful attack. Thus, both the ISAC and the stakeholders registered with the ISAC install an instance of the sharing infrastructure, which manages publishing of information of vulnerabilities and threats in a privacy-preserving way. The ISAC receives that information from different stakeholders, which are aggregated in a collaborative manner and gives a global view of the whole multi-modal transport system, for both the vehicles and the infrastructure. The correlated information will eventually provide a complete and timely view of the systems that might be affected by a vulnerability, or potential victim of a threat. Then, the interested stakeholders are immediately notified, while maintaining the privacy, if desired, of the initial provider of information. Figure 1: ISAC-MMT architecture shows the ISAC multimodal transportation (ISAC-MMT) architecture.

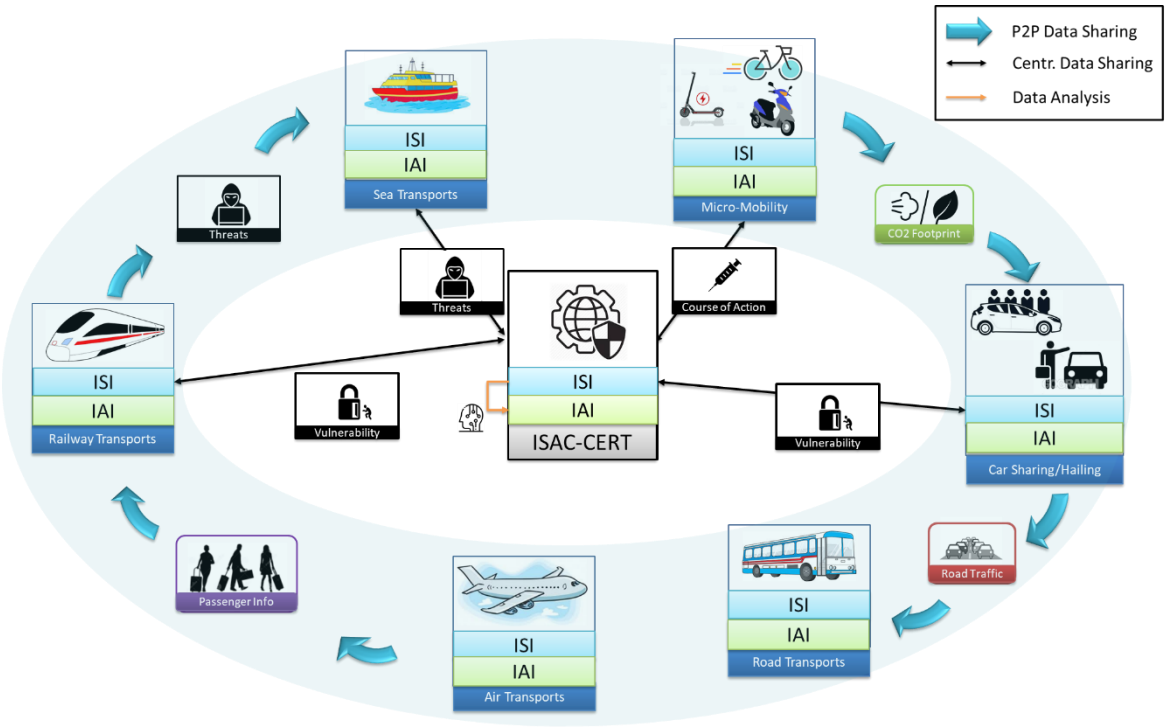

Figure 1: ISAC-MMT architecture

1.2. Stakeholders

Starting from the scenario described in Section 1.1, it is possible to identify stakeholders that differently participate to the processes of gathering, communicating and consuming shared cyber-security information through the ISAC.

The list of stakeholders that interact with the ISAC in the E-CORRIDOR framework and the different roles is here listed:

Stakeholder	**Role**
ISAC Multi Modal Transportation (ISAC-MMT)	• Data collector Analytic infrastructure • Sharing infrastructure
Small and Medium Enterprises (SMEs)	Car sharing, aerospace, railway companies
Large Enterprises	• Aviation enterprise a. Airport Managing Body (AMB) • Automotive enterprise a. Original Equipment Manufacturer (OEM) b. Suppliers c. Vehicle • Railway enterprise
Transportation ISACs	CTI provider
Institutional and not-profit organisations	Public CTI provider

Table 1: Role of stakeholders

Figure 2 depicts the stakeholders involved in the scenario.

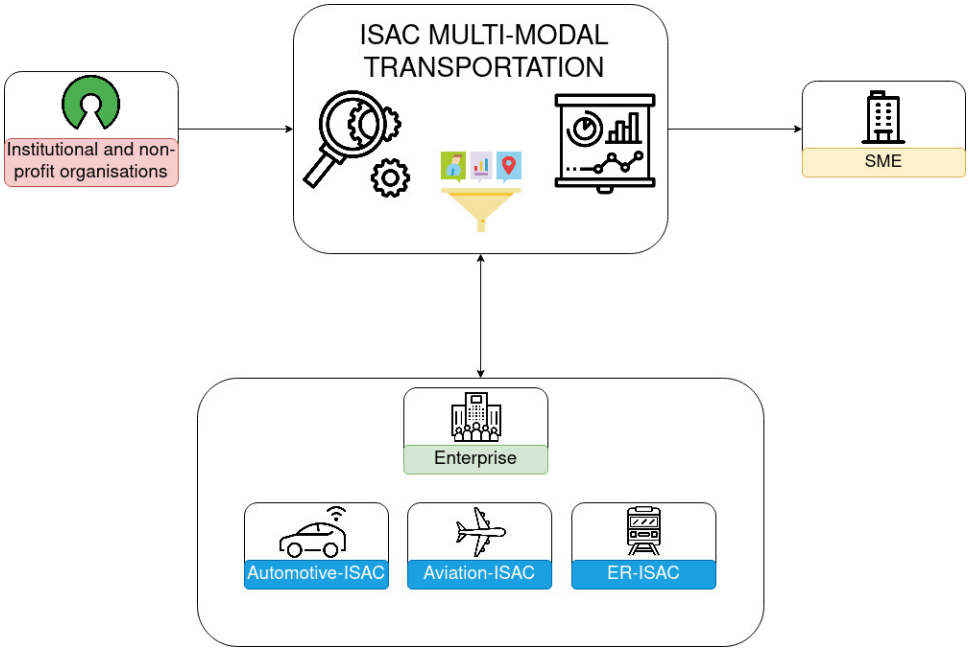

Figure 2: ISAC stakeholders

ISAC MMT

The first stakeholder identified is the **ISAC multi modal transportation**, which is interested in *receiving shared* information from several transportation sectors and in collecting information from public sources. It can be seen as an aggregator and information sharing hub among all other pilots in the E-CORRIDOR project. The shared information can be provided by the sector specific ISACs or by other E-CORRIDOR partners. It is composed of the **data collector** used to gather public cyber-threat information, the **analytic infrastructure** that offers security service analytics offered to each organisation registered to the ISAC and the **sharing infrastructure** exploited by each transportation organisation to share its collected information or analytic results.

SME

Small and Medium Enterprises represent companies that generally do not have internal cyber-security teams and outsource this service to other parties. The increase in cybercrime has hit particularly the SMEs unlike large organisations, these enterprises often struggle due to a lack of awareness, expertise, and resources[1]. For this reason, SMEs might heavily rely on the services of a Community Emergency Response Team (CERT) for early detection of vulnerabilities, and at the same time, they can provide several information about incidents, since they are likely targets for cyber-attacks.

Large Enterprises

Enterprises represent large companies which generally have their own cyber-security infrastructure and defence team. Since usually penetrating such defence mechanisms requires a bigger effort for the attacker, large enterprises generally face larger scale attack, compared to SMEs, which might have serious consequences not only to the company directly, but also to customers and other related stakeholders. The enterprises involved in the E-CORRIDOR project include the three main transportation sectors, e.g., automotive, aviation and railway. In the **automotive field**, a vehicle, an original equipment manufacturer or an automotive supplier can play a role of stakeholder sharing its own security information or can benefit of the services offered by the ISAC-MMT. In the **airport field**, an Airport Managing Body that administers and manages the airport facilities and it is in charge of ensuring security, can be seen as an ISAC stakeholder that can share information collected by the sensors distributed and connected in the airport. In the **railway field** each enterprise involved in the railway transportation can share different types of information that can be related to physical damage to crucial railway infrastructure such as the signalling equipment or related to the information system attacks due, for example, to denial of services.

Institutional and non-profit organisation

Institutional and non-profit organisation are referred to each security entity that make public security information such as exploits, vulnerabilities, threats and mitigations over the most common platforms in order to raise awareness and prevent cyber-attacks. Within the list of

[1] Renaud, Karen. "How smaller businesses struggle with security advice." *Computer Fraud & Security* 2016.8 (2016): 10-18.

institutional organisations that offers such service one of the most important is the National Institute of Standards and Technology (NIST[2]) that provides the National Vulnerabilities Database (NVD)[3], e.g., U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

Another similar organisation is the MITRE corporation[4] is an American not-for-profit organization that manages federally funded research and development centres supporting several U.S. government agencies. It, through the MITRE ATT&CK project[5] provides a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

Another non-profit project is represented by the Exploit Database maintained by Offensive Security[6] an information security training company that provides various Information Security Certifications as well as high end penetration testing services. The Exploit Database is a Common Vulnerabilities Enumeration (CVE) compliant archive of public exploits and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

Transportation ISACs

In the pilot scenario also an ISAC that works for a specific transportation sector can be seen as a stakeholder that offers intelligence and security information to share and to create collaborative analysis. An overview of existent ISAC in each transportation field that could be exploited as sources of the ISAC-MMT is listed below.

Table 2 shows the ISAC for each transportation sector.

Transport Stakeholders	**Sector**
Auto-ISAC	Automotive
Aviation-ISAC	Aviation
Railway-ISAC	Railway
ST-ISAC	Surface Transportation
PT-ISAC	Public Transportation

[2] https://www.nist.gov/

[3] https://nvd.nist.gov/

[4] https://www.mitre.org/

[5] https://attack.mitre.org/

[6] https://www.exploit-db.com/

Table 2: Transportation ISACs

- Auto-ISAC

The Auto-ISAC provides an industry-wide forum for companies of the automotive sector to share and analyse intelligence about emerging cyber-security risks to the vehicle, and to collectively enhance vehicle cyber-security capabilities across the global automotive industry, including light- and heavy-duty vehicle Original Equipment Manufacturer (OEMs), suppliers and the commercial vehicle sectors. Collaboration is aimed to enhance cyber-security protections in automotive systems through many types of actions, including implementing security feature in every stage of the vehicle lifecycle. The most critical information in vehicular network is collected from the Controlled Area Network (CAN) that is the vehicle bus standard designed to allow Electronic Control Units (ECUs) to communicate with each other's applications without a host computer. Such information can be analysed by Intrusion Protection System (IPS) able to prevent possible Reply or Fuzzing attacks among different partition of the CAN bus network. The results of the IPS or directly the collected messages exchanged through the CAN bus can be shared to the end to enhance cyber-security protections in automotive systems.

Other methods are represented by the definition of best practices for securing the vehicle ecosystem, and provision of guidance to implement the guidelines.

Members gain access to a secure portal that enables anonymous information sharing, houses real-time cyber-security intelligence reports and analysis, and facilitates live interaction among members. Members also engage in Standing Committees and Working Groups, receive early access to Best Practice Guides, and participate in exercises and workshops.

- Aviation-ISAC

The Aviation ISAC is a unique focal point for security information sharing across the aviation sector. It enhances the ability of the aviation sector to prepare for threats, vulnerabilities, and incidents so that businesses operating in the aviation industry can best manage their risks.

In the airport context, Industrial Internet of Things unites (IIoT) perform sensing, monitoring and smart automatic coordination ensuring worker, passenger and aircraft safety decreasing the risk of human error. Edge based IIoT, relies on a large amount of edge devices with a decentralized data interaction that makes it easy to experience data leakage, manipulation, and other network attacks. The Airport Managing Body (AMB) administers and manages the airport facilities and it is in charge of ensuring that security checks on passengers and baggage. It can be in charge to ensure also security of the IIoT network exploiting Intrusion Detection System (IDS) designed for detecting anomalies in the network traffic[7]. The sharing of timely and actionable information related to IIoT network traffic, network anomalies, threats, vulnerabilities, incidents, potential protective measures, and best practices, enhances the analyses information to validate accuracy and severity and recommend mitigation strategies.

[7] Yao, Haipeng, et al. "Hybrid Intrusion Detection System for Edge-Based IIoT Relying on Machine-Learning-Aided Detection." *IEEE Network* 33.5 (2019): 75-81.

- Railway-ISAC

The railway ISAC aims to monitor relevant activities related to cybersecurity in the railway context, cover safety requirements of the rail system, e.g., the assessment of safety consequences originated by cybersecurity threats and reflect the above in Technical Specifications for Interoperability and Common Safety Methods. There are many different types of cyber-threats that could adversely affect rail transport systems. Some attacks may result in physical damage to crucial railway infrastructure such as the signalling equipment, while others might not even be focused specifically on the rail system (e.g., viruses and malware). Moreover, due to the complex landscape of potential threats, anticipatory measures are often difficult to develop and put in place. The European Railway ISAC (ER-ISAC), founded in June 2019 under the lead of Infrastructure Managers (IM) and Railway Undertakings (RU), provides an inclusive platform for them to collectively exchange information on and tackle cyber-security threats also through sharing of best practices, discussion of common vulnerabilities, influencing regulation and standardisation.

- ST-ISAC

Surface transportation is related to the transport of people or goods by road, train, or ship, rather than by plane. The ST-ISAC collects, analyses and distributes critical security and threat information from worldwide resources to protect its members' vital information and information technology systems from attack. ST-ISAC services are specifically tailored to meet the security demands of each one of its members.

The ST-ISAC is a secure reporting and analytical capability that, in addition to transmitting critical alerts, advisories and solutions, also provides a vehicle for the anonymous or attributable sharing of incident, threat, and vulnerability data among the members.

ST-ISAC members also have access to information and analytical reporting provided by other sources, such as foreign governments; law enforcement agencies, technology providers and international computer emergency response teams (CERTs).

- PT-ISAC (Public Transit ISAC)

Public Transit ISAC, collects, analyses and reports critical and physical security and threat information from different sources including:

- Private infrastructures.
- Intelligent community.
- Government.
- Military.

It enables the transmission of critical alerts and advisories as well as the collection, analysis and report of security information for transit agencies across the territory.

1.3. Comparison to current practice

Currently, ISAC are used to collect, analyse and share information related to cyber-threats in specific sectors. Even if ISACs are collecting information from public data sources and can be connected in consortiums to share a subset of information, each ISAC has a partial view of the whole picture of vulnerabilities and attacks of the whole ecosystem. Existing transportation ISACs target specific transportation sectors, such as automotive[8], railways[9], marine[10] and aviation[11]. ISACs are generally private/public organizations or consortia of organizations willing to share information among the participating partners. The typical situation is of sectorial ISAC. This is because the trust is more easily established in communities with common knowledge and experience. Nowadays transportation is multimodal, then the main lack of the existent sectorial ISACs is the overall view of the transportation that can increase the CTI knowledge. Some of these ISACs are mainly communities that manually share information on cyber-threats related to their systems without having automated systems for data collection and analysis.

Most of ISACs are currently in the US. Some ISACs are instead public and government entities such as the Italian public ISAC, which is located at the Italian Ministry of Economic Development[12]. It is the main reference point at the national level for the prevention and countermeasures against cyber-security attacks. Differently from transportation ISACs, the public ISACs have a more organized system to handle a broader set of information, related or relatable to CTI, processing thus network logs, email files, database contents, etc. National ISACs are targeting enterprises, both large and small to medium, with different business. Critical infrastructures, including transports, up to now, have only been marginally affected by them.

The ISAC-MMT proposes a collaboration of each transportation sector in sharing local information related to threats, vulnerabilities, incident reports, local security analysis results providing an overall view of the transportation scenario through which it is possible perform an automated collaborative analysis to enhance the security level of each transportation sector in a privacy preserving way.

[8] https://automotiveisac.com

[9]https://www.enisa.europa.eu/events/enisa-maritime-cybersecurity-workshop/Good_practices_from_European_Rail_ISAC.pdf/

[10] https://www.mtsisac.org/

[11] https://www.a-isac.com/

[12] https://csirt.gov.it/

1.4. User Stories

1.4.1. ISAC-US-01: Public cyber-threat information collection

As a

ISAC-MMT data collector

I want to

Collect cyber-threat information from public sources

So that

I can increase cyber-threat knowledge at global level including such information in the cyber-analytic tools with the end to improve security analytics.

1.4.1.1. Discussion

Main Stakeholders:

- ISAC-MMT
- Institutional and not-profit organisations

Cyber-threat information (CTI) is any kind of information that can help to identify, assess, monitor, and respond to cyber-threats. Examples of CTI include indicators (system artifacts or observables associated with an attack), Tactics, Techniques and Procedures (TTPs), security alerts, threat intelligence reports, and recommended security tool configurations. Most of such information is public and it is provided through news feeds or structured databases daily updated by governmental organization[13] to make public security issues and its countermeasures.

Gathering intelligence from disparate sources has the potential to increase the accuracy of a security system, both for a predictive and reactive approach and to timely respond to security attack. The vast amount of data being produced by consumers, hackers, newsmakers, and bloggers every single day is a precious free source information that can be exploited to discover new security issues.

The ISAC-MMT, through the data collector module, will be able to gather public CTI data related to the known software and hardware vulnerabilities from the various security news feeds, social media sources, institutional web pages and available online databases, exploiting crawlers in conjunction with parsers to extract relevant CTI.

13 https://www.nist.gov/cyberframework

1.4.1.2. Acceptance test

- The ISAC-MMT is able to receive automatically and periodically public cyber-threat information.
- The ISAC-MMT is able to make the data received accessible from the external public.

1.4.2. ISAC-US-02: Private transportation sector data collection

As a

Specific transportation sector organization

I want to

Collect information from the transportation environment useful for the security threat detection

So that

I can increase cyber-threat knowledge useful to perform security analysis on the transportation environment.

1.4.2.1. Discussion

Main Stakeholders:

- Automotive enterprise
- Aviation enterprise
- Railway enterprise

The key point of an information sharing system is to identify potential source of information useful to detect and prevent threats. Every transportation sector organization deploys tools and sensors to acquire threat information both from the internal system and from external threat information feeds or repositories. In large organizations, this inventory process is also a mean of discovering information that is being collected and analysed in business units across the organization. The process of identifying threat information sources includes the identification of sensors, tools, data feeds, and repositories that produce threat information, and making sure that the information is produced at a frequency, precision, and accuracy to support cyber-security decision-making.

In the transportation field, each organization will exploit its knowledge to collect data from its environment sensors (CAN bus, IIoT sensors) and from its private repositories. The data will be converted in a standard format to share them with other partners and adapt them to the security analytics.

1.4.2.2. Acceptance test

- The private transportation sector can collect periodically information from its transportation environment (CAN bus, IIoT sensors, external sources).
- The private transportation sector can adapt collected data to its security analytic functions.

1.4.3. ISAC-US-03: ISAC-MMT cyber-threat information analysis

As a

ISAC-MMT

I want to

Infer and aggregate automatically useful information about incident and vulnerabilities from large amounts of heterogeneous data provided by different sources

So that

I can discover new threats, vulnerabilities, and anomalies to improve the detection of security issues in each transportation sector.

1.4.3.1. Discussion

Main Stakeholders:

- ISAC-MMT

Analysis on shared data is one of the biggest challenges for the ISAC. The heterogeneous information shared by different sources could make the analysis not easy to do. Nevertheless, standardizing the sharing information, data provided by different sources can offer different views of the same data applied on different context, where exploiting aggregating functions would enable to learn new knowledge that with a view on a single mode of transportation would not be possible.

In the ISAC-MMT the sharing analytics are fundamental to aggregate information provided by different transportation sectors and collected by public sources to discover new threats, vulnerabilities and attack patterns.

In addition, the ISAC-MMT can guarantee more computational capabilities to run analytics that would not be available if run locally.

1.4.3.2. Acceptance test

- A vulnerability, an attack pattern or a threat are discovered aggregating information provided by entities belonging to different mode of transportation.
- A security detection system is improved by being trained on data shared by each transportation sector.
- The ISAC-MMT can run a security analytic that would not be possible to run locally due to the computational limits.

1.4.4. ISAC-US-04: ISAC-MMT cyber-threat notification

As a

ISAC-MMT

I want to

Notify enterprises from disparate sectors about (or anyone who requested the analysis) discovered threat, vulnerabilities with a set of corresponding mitigations

So that

I can inform each sector about new possible threats and give them the possibility to take countermeasures.

1.4.4.1. Discussion

Main Stakeholders:

- ISAC-MMT

Referenced Stakeholders:

- Aviation enterprise
- Automotive enterprise
- Railway enterprise
- SME

One of the objectives of the ISAC-MMT is to provide both predictive and reactive approach and to timely respond to the security attack. The basis of this approach is to inform each transportation enterprise about new threats and vulnerabilities discovered and provides a corresponding countermeasure to mitigate a possible or an ongoing attack. The ISAC-MMT can offer a CTI notification service where a transportation enterprise can subscribe by informing the ISAC-MMT about its preferences (software, hardware, sector). When the ISAC-MMT analyser discovers a new threat or vulnerabilities notify each subscriber respect to its preferences.

1.4.4.2. Acceptance test

- A discovered vulnerability, attack pattern or threat must be notified to the specific sector that requires the analysis and all the sectors interested in such analysis.
- Threats events are presented to the stakeholders with respect to the subjective relevance.

1.4.5. ISAC-US-05: ISAC-MMT cyber-threat visualization

As a

ISAC-MMT

I want to

Provides a MMT web portal containing transportation information organized in private and public sections.

So that

I can disseminate awareness to the interested parties and provide additional information to private/registered stakeholders according to the sharing agreement.

1.4.5.1. Discussion

Main Stakeholders:

- ISAC-MMT
- Referenced Stakeholders:
- SME
- Aviation enterprise
- Automotive enterprise
- Railway enterprise

The ISAC-MMT allow each E-CORRIDOR entity to share its own data according to a Data Sharing Agreement, tacking the advantages to increase the transportation knowledge and improve the security analytics. Such information can be public (accessible to everyone) or private (accessible to a single entity or a set of entities). The ISAC-MMT should provide a MMT web portal able to allow the access and the visualization of the data according to the data sharing agreement of each shared data.

The public section should contain the new public vulnerabilities, threats and mitigations discovered, and all the data provided and made public by each transportation sector. The section will also provide statistics and aggregated results obtained from the analytics of the public data collected.

The private section is related to each registered entity (transportation enterprises) where they can access with its own credentials and can see the data section, containing its own data and the data shared with them, and the results section, containing the analytic results performed on its data or the analytic results shared with them.

1.4.5.2. Acceptance test

- The ISAC-MMT must provide a MMT web portal.
- The portal must have a public section where the public threats and vulnerabilities discovered with the corresponding mitigations are shown.
- The portal must have a private section where each E-CORRIDOR partner can access with its credentials and visualizes the (i) data section containing its private data or the data shared with them and (ii) the results section containing the results of the performed security analytics.

1.4.6. ISAC-US-06: Automotive cyber-threat information analysis

As a

Vehicle of an automotive enterprise

I want to

Run either edge analytics on the data collected from the CAN bus or exploiting the analytic tools offered by the ISAC-MMT that performs a collaborative analysis on the shared information

So that

I can discover new threats, vulnerabilities or anomalies and the corresponding mitigation to actuate.

1.4.6.1. Discussion

Main Stakeholders:

- Vehicle
- Automotive enterprise
- ISAC-MMT

Modern cars contain mini-computer devices called Electronic Control Units (ECUs) that control all the automobile's system including transmission, steering, and electrical peripheral devices. Such devices are connected with the Controller Area Network (CAN) that is a robust vehicle bus standard designed to allow microcontrollers and devices to communicate with each other's applications without a host computer. Multiple devices embedded in the modern cars have access to the internet. The OBD-II port provides open access to all a vehicle's CAN buses, which could be manipulated by hackers putting the driver's life at risk[14]. For this reason, it is necessary to identify and react to a possible attack analyzing the traffic of the CAN bus. An intrusion detection system based on machine learning approach can be used to analyze and identify anomalies in the CAN bus traffic. In the E-CORRIDOR scenario, a vehicle can perform an intrusion detection analysis locally with its limited computational capabilities or

[14] G. Costantino and I. Matteucci, "CANDY CREAM - Hacking Infotainment Android Systems to Command Instrument Cluster via Can Data Frame," *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, New York, NY, USA, 2019, pp. 476-481.

exploits the computational capabilities and the intrusion detection system tools offered by the ISAC-MMT.

1.4.6.2. Acceptance test

- A vehicle can run locally an intrusion detection system analyzing CAN bus data.
- The automotive enterprise can detect novel complex threat events that would not be able to identify locally connecting to the analytic tool offered by the ISAC-MMT.

1.4.7. ISAC-US-07: Sharing automotive cyber-threat information

As a

Vehicle of an automotive enterprise

I want to

Share either the CAN bus information or the analytic results provided by the vehicle security analytic tools, according to a customized security policy

So that

I can share my knowledge with other specific sectors, make them public or exploiting it for security analysis.

1.4.7.1. Discussion

Main Stakeholders:

- Vehicle
- Automotive enterprise
- OEM
- ISAC-MMT

Information sharing enable organizations to increase the collective knowledge, experience, and analytic capabilities of the sharing entities. In the security field, sharing information permits to enhance the defensive capabilities and even a single contribution, e.g., a different observation of an event, can increase the awareness and security of the entire community.

In each transportation sector field, sharing cyber-information is fundamental to increase its security knowledge and prevent security issues. In the automotive field, vehicles, OEM (Original Equipment Manufacturer), suppliers, collaborate to share information related to vulnerabilities, threat feeds, research, best practices, intelligence, trends, forecasts and data provided directly from the vehicle (CAN bus).

The ISAC-MMT will permit to share both low level information extracted directly from the vehicle CAN bus and more high-level information as the security analytic results performed analysing the CAN bus logs. Each automotive entity can decide

to make public its data or protect the access and the distribution of the data to share by specifying the authorization, obligation, and prohibition policies.

1.4.7.2. Acceptance test

- The ISAC-MMT provides the function to share data
- The ISAC-MMT receives from the automotive sector:
  - Data provided by the CAN bus logs
  - Analytic results of an automotive IDS
  - Exploits and vulnerabilities related to the automotive sector

1.4.8. ISAC-US-08: Aviation cyber-threat information analysis

As a

AMB

I want to

Run either locally a continuous security monitoring system with anomaly detection on the data collected from the airport or exploiting the analytic tools offered by the ISAC-MMT that performs an analysis on the shared information.

So that

I can identify new cyber-, physical- and cyber-physical threats.

1.4.8.1. Discussion

Main Stakeholders:

- AMB
- ISAC-MMT

Referenced Stakeholders:

- Railway enterprise

Several activities are carried out in the airport. Thanks to novel analytic services, the AMB improves the airport security while providing both aviation (e.g., provision, maintenance and operation of equipment, and technologies required by the air carrier and handling services) and non-aviation services (e.g., commercial activities and business lounges).

Event log from the Industrial Internet of Things (IIoT), cloud and integrated systems deployed in the airport are collected. After the establishment of multi-party or Peer to Peer (P2P) agreements, information from carriers (e.g., air and train carriers) and passengers are collectively analysed to improve the confidence level of the detection. Events contextual, internal and external to the airport are properly correlated and analysed.

To aim for advanced detection services the analysis should include operation, system and network events. Cyber-, physical- and cyber-physical threats must be identified and predicted through a continuous security monitoring system with anomaly detection. Once the analysis is concluded, the security analytic services of the AMB distribute the

results to all the stakeholders according to the relative relevance. At the reception of such results, each stakeholder is then able to apply at runtime any novel security model/policy that should be needed, and timely stop any attempt of breaking the identification management services. Mitigation actions are potentially performed proactively. Both data and analytics results have attached DSAs.

1.4.8.2. Acceptance test

- The AMB can detect novel complex threat events that would not be able to identify otherwise.
- All the stakeholders can increase the knowledge about the threats, and to improve and adapt their own security tools.

1.4.8.3. Cross-pilot user-story: reference D2.1 AT-US-04: Advanced Security Analytic Services

In the deliverable D2.1, the AT pilot (AT) presents the user story AT-US-04 that describes the AMB willing to enhance the security analytics tools in order to improve the security for all passengers visiting my airport, the hosted airline companies, other carriers reaching the airport (e.g., train or car sharing) and the airport itself, and be less vulnerable to novel (cyber) security attacks.

1.4.9. ISAC-US-09: Aviation cyber-threat information sharing

As a

AMB

I want to

Share, according to a customized security policy, either the monitored information extracted from the airport sensors or the analytic results provided by the monitoring system (e.g., Anomaly detection).

So that

I can distribute my knowledge with other transportation enterprise, make them public or using it in a private way for a security analysis.

1.4.9.1. Discussion

Main Stakeholders:

- Airport Managing bodies (AMB)
- ISAC-MMT

In terms of airport security, the AMB provides advanced detection services to identify Cyber-, physical- and cyber-physical threats through a continuous security monitoring system with anomaly detection. The results of the analysis are distributed and shared with all the stakeholders according to the relative relevance to mitigate and timely stop the discovered attack. In addition, several activities are carried out in the airport and different information provided by the Industrial Internet of Things (IIoT) are collected in form of event logs that can

be shared with other carriers and take advantages of the data collaboration to enhance the anomaly detection.

The ISAC-MMT will permit to share both low level information extracted directly from the airport sensors (event logs) and more high-level information as the security analytic results performed by the anomaly detection systems that analyse the airport sensor data. The AMB can decide to make public its data or protect their access and distribution specifying the authorization, obligation, and prohibition policies.

1.4.9.2. Acceptance test

- The ISAC-MMT provides the function to share data
- The ISAC-MMT receives from the aviation sector:
  - Event log from the systems deployed in the airport
  - Cyber-, physical- and cyber-physical threats identified by the anomaly detection system
  - Exploits and vulnerabilities related to the aviation sector

1.4.9.3. Cross-pilot user-story: reference D2.1 AT-US-04: Advanced Security Analytic Services

In the deliverable D2.1, the AT pilot (AT) presents the user story AT-US-04 that describes the AMB willing to enhance the security analytics tools in order to improve the security for all passengers visiting my airport, the hosted airline companies, other carriers reaching the airport (e.g., train or car sharing) and the airport itself, and be less vulnerable to novel (cyber) security attacks. The sharing of airport information provides a collaborative analysis that can improve the security of the airport environment.

1.4.10. ISAC-US-10: Railway cyber-threat information sharing

As a

Railway enterprise

I want to

Share, according to a customized security policy, the monitored information extracted from the railway stations or the vulnerabilities/threats discovered in the railway system.

So that

I can distribute my knowledge with enterprises belonging the same sector or to other transportation sector to disseminate awareness about such vulnerability.

1.4.10.1. Discussion

Main Stakeholders:

- Railway enterprise
- ISAC-MMT

The security teams of the railway enterprises monitor relevant activities related to cybersecurity in the railway context and cover safety requirements of the rail system, e.g., the assessment of safety consequences originated by cybersecurity threats. There are many different types of cyber-threats that could adversely affect rail transport systems. Some attacks may result in physical damage to crucial railway infrastructure such as the signalling equipment, while others might not even be focused specifically on the rail system (e.g., viruses and malware).

The ISAC-MMT will permit to share with other railway enterprises the discovered vulnerabilities and the possible countermeasures to adopt in order to mitigate a possible attack on the railway system.

1.4.10.2. Acceptance test

- The ISAC-MMT provides the function to share data
- The ISAC-MMT receives from the railway sector:
  - Event log from the systems deployed in the railway station.
  - Exploits and vulnerabilities related to the railway sector.

1.5. Relevance to E-CORRIDOR objectives

The objectives of the ISAC pilot are to produce a prototype implementation of a multi-tenanted managed security analytics platform integrating the E-CORRIDOR technology to allow controlled sharing/pooling of security data belonging to different prosumers. By using this prototype platform it would be possible to evaluate and validate the E-CORRIDOR approach, architecture and technology in the context of a security information sharing and analytics services provided to different multimodal transportation enterprises. The user stories discussed in the previous sections represent different facets of the pilot, and are relevant to the E-CORRIDOR objectives and in some aspects related to the Car Sharing (S2C) and Airport and Train (AT) pilots.

In particular the ISAC pilot focuses on the information sharing and collaborative analysis of data provided by different transportation sector, given a particular attention to the privacy requirements for both users and companies involved in multi-modal transportation sharing and therefore contribute to the following E-CORRIDOR objectives (here reported for the sake of completeness):

- Objective 1: E-CORRIDOR will build a flexible, confidential and privacy-preserving framework for managing data sharing, for several purposes, by different prosumers (i.e., information producer and consumer).
- Objective 2: E-CORRIDOR will define edge-enabled data analytics and prediction services in a collaborative, distributed and confidential way.
- Objective 3: E-CORRIDOR will define a secure and robust platform in holistic manner to keep the communication platform safe from cyber-attacks and ensure service continuity.
- Objective 4: E-CORRIDOR will improve, mature and integrate several existing tools provided by E-CORRIDOR partners and will tailor those to the specific needs of the E-CORRIDOR platform and Pilots.
- Objective 5: the framework and the services developed will be used to deliver a pilot product for Centre of information sharing for multimodal transportation (ISAC).

The correlation between the User Stories presented in Section 1.4 and the above-mentioned E-CORRIDOR objectives are as follow.

The *ISAC-US-07: Sharing automotive cyber-threat information*, *ISAC-US-09: Aviation cyber-threat information sharing*, *ISAC-US-10: Railway cyber-threat information sharing* are related to the *Objective 1* of the project. The data are shared in a privacy preserving way between all the entities envolved in the ISAC. The data are shared specifying a DSA that regulates the authorization, obligation, and prohibition policies to protect the access and the distribution of the data to share.

The *ISAC-US-03: ISAC-MMT cyber-threat information analysis*, *ISAC-US-06: Automotive cyber-threat information analysis*, *ISAC-US-08: Aviation cyber-threat information analysis* are linked to the *Objective 2* of the project. Each transportation sector can analyze its data in a local

way exploiting its local analytics or in a collaborative way exploiting the security analytic tools offered by the ISAC-MMT

that perform the analysis on the shared data in a privacy preserving way.

The *ISAC-US-4: ISAC-MMT cyber-threat notification*, *ISAC-US-07: Sharing automotive cyber-threat information*, *ISAC-US-09: Aviation cyber-threat information sharing*, *ISAC-US-10: Railway cyber-threat information sharing* are linked to the *Objective 3* of the project. Each transportation sector is exposed to a security issues and cyber-attacks. The security analytic tools offered by the ISAC-MMT will permit to discover new threats and vulnerabilities in each transportation sector and notify them with the discovered event and the possible countermeasures needed to its mitigation.

The *ISAC-US-03: ISAC-MMT cyber-threat information analysis*, *ISAC-US-07: Sharing automotive cyber-threat information*, *ISAC-US-09: Aviation cyber-threat information sharing*, *ISAC-US-10: Railway cyber-threat information sharing*, are linked to the *Objective 4* of the project. Security analytics offered by each transportation sector will improve thanks to the data sharing and the collaborative analysis. The ISAC offers both data to increase knowledge and thus improve analytic tools (e.g., classification, detection services) as well as security analytic tools that exploits the shared knowledge.

The *ISAC-US-01: Public cyber-threat information collection*, *ISAC-US-02: Private transportation sector data collection*, *ISAC-US-03:* I*SAC-MMT cyber-threat information analysis*, *ISAC-US-05: ISAC-MMT cyber-threat visualization*, *ISAC-US-06: Automotive cyber-threat information analysis*, *ISAC-US-08: Aviation cyber-threat information analysis* are linked to the *Objective 5* of the project. Security analytics and cyber-threat visualization will be used by the other E-Corridor pilot to reach its security objectives.

User Stories	**Objective 1**	**Objective 2**	**Objective 3**	**Objective 4**	**Objective 5**
ISAC-US-1					✓
ISAC-US-2					✓
ISAC-US-3		✓		✓	✓
ISAC-US-4			✓		
ISAC-US-5					✓
ISAC-US-6		✓			✓
ISAC-US-7	✓		✓	✓	
ISAC-US-8		✓			✓
ISAC-US-9	✓		✓	✓	
ISAC-US-10	✓		✓	✓	

Table 3: User stories to objectives mapping

1.6. Pilot Evaluation

The evaluation of the ISAC pilot, is a relevant phase to contribute to the success of this pilot.

The user stories introduced in the Section 1.4 define actions and operations that the ISAC pilot should integrate. Integration, execution, and evaluation of the pilot scenarios in the E-CORRIDOR framework will follow the acceptance tests defined at the end of each user story. To this purpose, we will provide hereafter some questions that will help to understand and to find gaps from what is designed and what should be also considered.

Question 1: Will a transportation sector perceive a benefit in performing collaborative analysis in terms of mitigation or prevention of possible cyber-attacks?

Question 2: Will a transportation sector perceive a benefit in running a security analytics on the ISAC-MMT?

Question 3: Will the publication of the security analysis on the shared data disseminate awareness on cyber-security field?

Question 4: Will the data sharing by each transportation sector improve the security analytics offered to discover specific-sector threats/vulnerabilities?

Question 5: Will the sanitisation measures, such as anonymisation, homomorphic encryption, guarantee to each transportation sector that their data will be treated as they want/hope?

Question 6: Will the Data Sharing Agreement be a solution to allow each transportation sector to express their hopes in terms of data privacy-preserving and data distribution?

Question 7: What response capabilities do ISACs have?

In Table 4: Questions to objectives mapping is reported the mapping between the E-Corridor objectives described in Section 1.5 and the pilot evaluation questions.

	Objective 1	**Objective 2**	**Objective 3**	**Objective 4**	**Objective 5**
Question 1		✓			✓
Question 2		✓		✓	✓
Question 3					✓
Question 4				✓	✓
Question 5	✓		✓		✓
Question 6	✓		✓		✓
Question 7	✓	✓	✓	✓	✓

Table 4: Questions to objectives mapping

2. Use Cases

In this section are described the use cases for the ISAC pilot. Section 2.1 offers a representation of the use case diagram, that are discussed in details in Section 2.2. These use cases have a priority assigned according to the MoSCoW (Must have, Should have, Could have, and Won't have but would like) method and give a description of the event flow. A matching of the use cases with the user stories is reported in Section 2.3. To give a visual representation of the most important user stories and use cases, Section 2.4 reports the storyboards.

2.1. Use Case Diagram

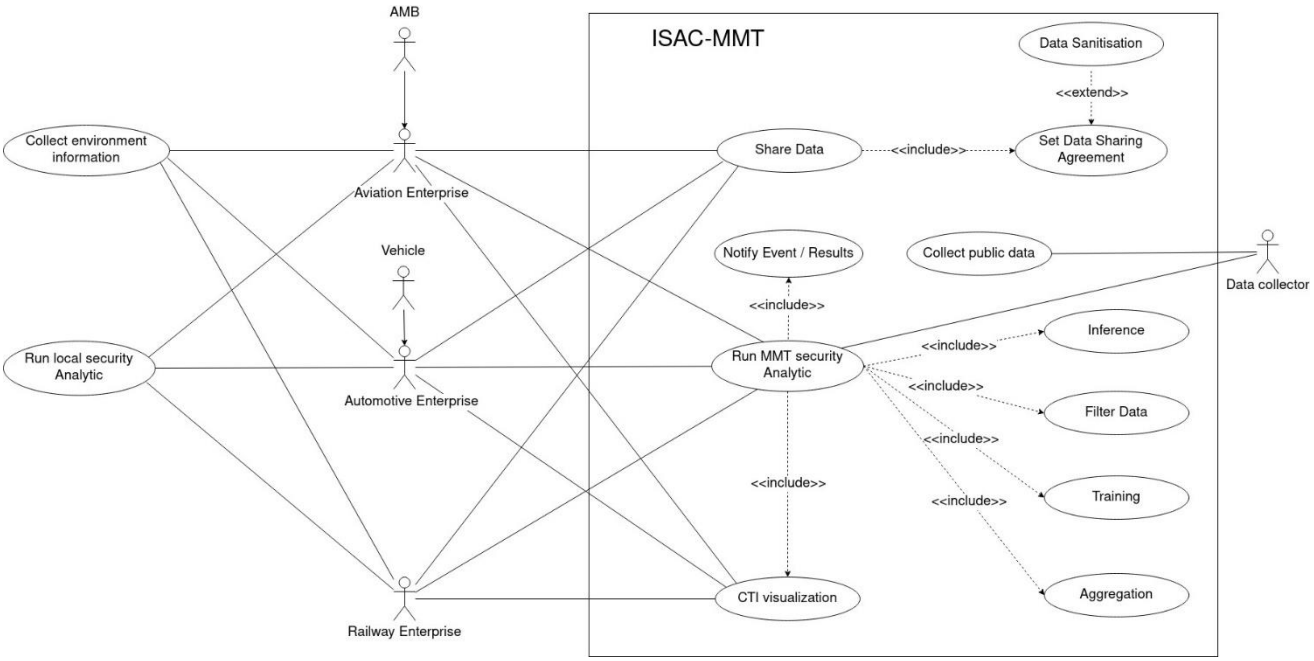

Figure 3: Use case diagram

2.2. Use Case Descriptions

2.2.1. ISAC-UC-01: Public CTI data collection

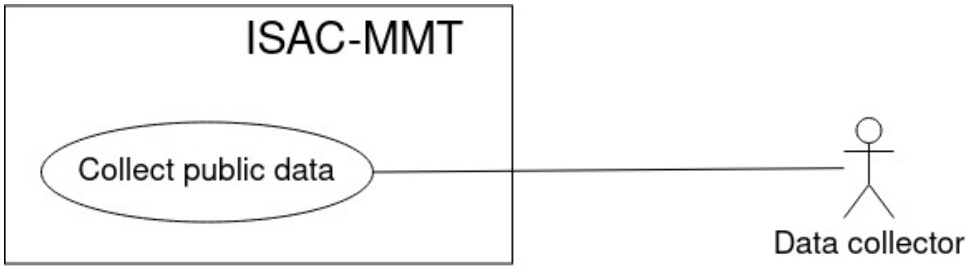

Figure 4: ISAC-UC-01 Public CTI data collection UC

Use Case Name	Public CTI data collection
Participating actors	ISAC-MMT data collector
Purpose	Collect risks, vulnerabilities, threats, attack patterns, exploits and mitigations from public cyber-information sources.
Priority	MUST
Flow of events: Normal flow	1. The ISAC-MMT data collector downloads every day from public cyber-threat information sources: vulnerabilities, exploits, attack patterns and mitigations related to known hardware and software. 2. The ISAC-MMT data collector processes the collected information to be converted in a standard format. 3. The ISAC-MMT data collector append to the collected information, a Data Sharing Agreement (DSA) to make it accessible to every stakeholder. 4. The ISAC-MMT data collector stores the collected information in a standard format to be processed by the data analyzer.
Flow of events: Alternative flow	The ISAC-MMT perform on the collected data pre-processing operations regarding (i) anonymisation, if necessary and (ii) data format conversion.
Pre-condition	• Storage space for collected information. • Existence of a standard for information communication would ease the analysis process.
Post-condition	The ISAC-MMT has acquired additional knowledge about public risks, vulnerabilities, threats, attack patterns, exploits and mitigations related to known hardware and software.

Table 5: ISAC-UC-01 Public CTI data collection

2.2.2. ISAC-UC-02: ISAC-MMT sharing data

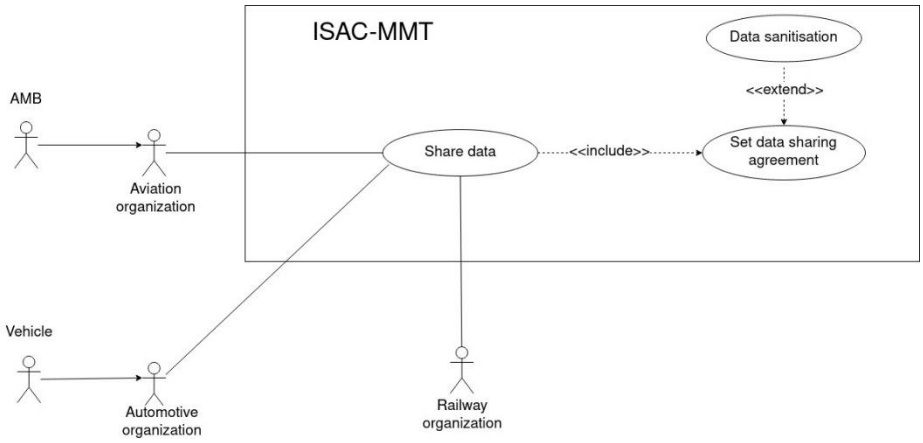

Figure 5: ISAC-UC-02 ISAC-MMT sharing data

Use Case Name	ISAC-MMT sharing data
Participating actors	ISAC-MMT • AMB • Vehicle • Aviation enterprise • Automotive enterprise • Railway enterprise
Purpose	A transportation enterprise or directly the systems managed by the transportation sectors can share its collected data or security analytic results in a privacy-preserving way.
Priority	MUST
Flow of events: Normal flow	1. The transportation enterprise or the system managed by the transportation sector (AMB, vehicle) exploits the ISAC-MMT to share its information. 2. The ISAC-MMT stores the shared information in a sharing space. 3. The ISAC-MMT ISI makes the shared data accessible to the entities as specified in the DSA.
Flow of events: Alternative flow:	The ISAC-MMT perform on the collected data pre-processing operations specified in the DSA regarding (i) anonymisation, (ii) data encryption and (iii) data format conversion.

Pre-condition	• The entity that wants to share data defines a DSA to associate to the data (ISAC-UC-03).
Post-condition	The ISAC-MMT has acquired new knowledge exploitable for data analysis. • Data are shared with other entities as described in the DSA.

Table 6 : ISAC-UC-02 ISAC-MMT sharing data

2.2.3. ISAC-UC-03: Data sharing agreement

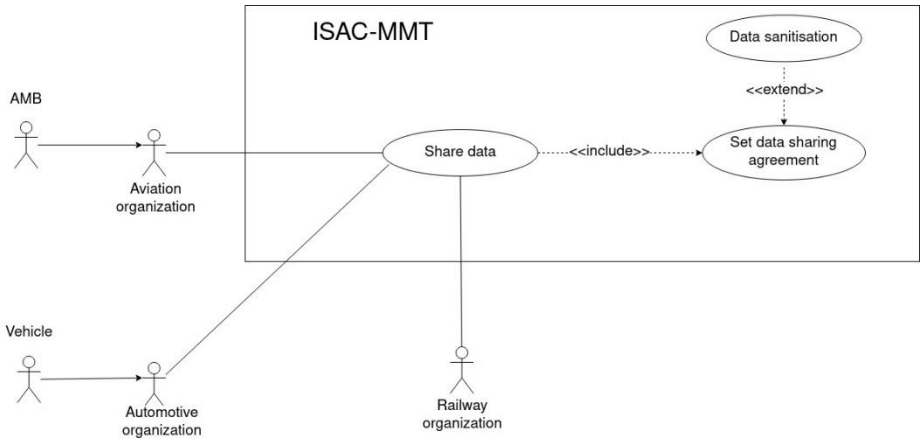

Figure 6: ISAC-UC-03 Data sharing agreement

Use Case Name	Data sharing agreement
Participating actors	• ISAC-MMT ISI • Aviation enterprise Automotive enterprise AMB Railway enterprise Vehicle
Purpose	A private transportation enterprise creates a new Data Sharing Agreement (DSA) to specify authorization, obligation, and

	prohibition policies to protect the access and the distribution of the data to share.
Priority	MUST
Flow of events: Normal flow	1. The transportation enterprise selects a policy for the authorization. 2. The transportation enterprise selects a policy for the obligation. 3. The transportation enterprise selects the sanitisation procedure: a. No sanitisation b. Data anonymisation c. Data encryption
Pre-condition	• A list of authorization, obligation, and sanitisation to be applied exist.
Post-condition	• The DSA is available to be attached to the data to share.

Table 7: ISAC-UC-03 Data sharing agreement

2.2.4. ISAC-UC-04: Run ISAC-MMT security analysis

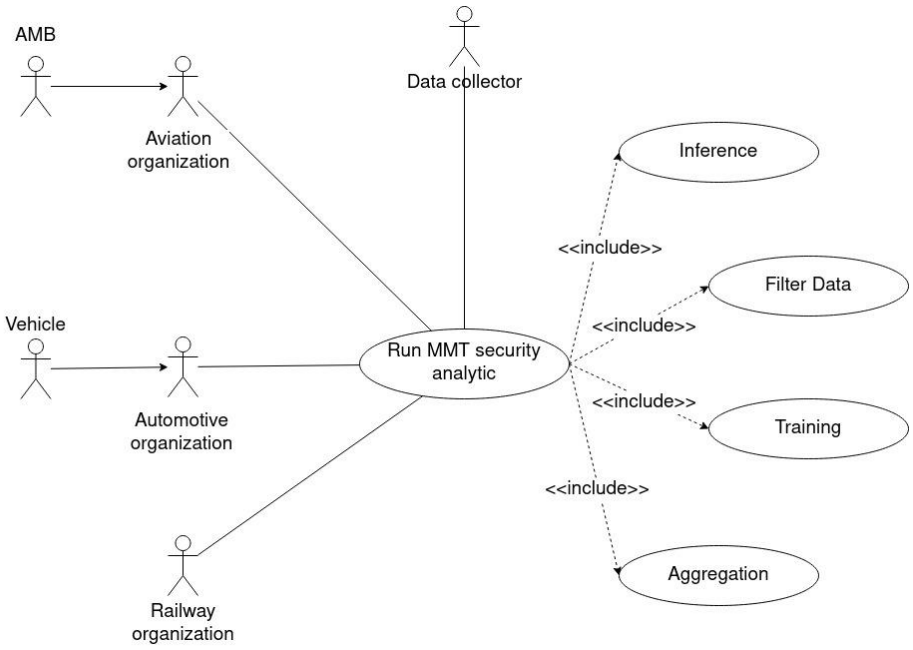

Figure 7: ISAC-UC-04: Run ISAC-MMT security analysis

Use Case Name	Run ISAC-MMT security analysis
Participating actors	• Automotive organization • Aviation organization • Railway organization • AMB • Vehicle • Data collector ISAC-MMT
Purpose	Run analysis on the shared data or on the public data collected.
Priority	MUST
Flow of events: Normal flow	The private transportation enterprise can run through the ISAC-MMT the following analytics: • Inference analytic: classification/detection analysis on the data. • Aggregation analytic: combination of cyber-threat information. • Filter analytic: data filtering function based on specific criteria.
Flow of events: Alternative flow 1	The data collector run the aggregation security analytic exploiting the ISAC-MMT to combine the public data collected.
Flow of events: Alternative flow 2	The private transportation enterprise can run a training activity on a classifier offered by the ISAC.
Pre-condition	• The analytic functions must be deployed on the ISAC-MMT server. • The training data must be uploaded on the ISAC-MMT server.

Post-condition	• The analytic results performed by the ISAC-MMT security analytic service are available for the notification (ISAC-UC-05). • The analytic results performed by the ISAC-MMT security analytic service are available in the ISAC-MMT web portal (ISAC-UC-08).

Table 8: ISAC-UC-04: Run ISAC-MMT security analysis

2.2.5. ISAC-UC-05: Cyber-threat notification

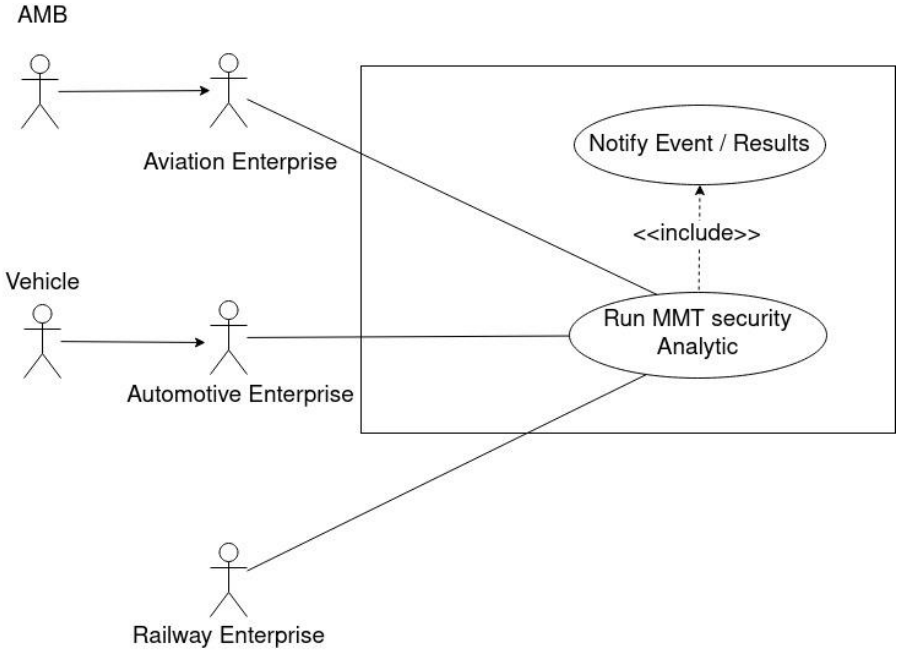

Figure 8: ISAC-UC-05: Cyber-threat notification

Use Case Name	Cyber-threat notification
Participating actors	• ISAC-MMT Automotive enterprise Aviation enterprise Railway enterprise AMB Vehicle
Purpose	To timely notify relevant information about threat and vulnerabilities within the related mitigation or an analytic result.

Priority	MUST
Flow of events: Normal flow	• A stakeholder specifies its own interests (transportation sector, keywords, list of software and hardware). • Public vulnerabilities/exploits are divided by class of sectors. • Information is sent to the interested stakeholders periodically.
Pre-condition	• Interests for receiving stakeholders and their sector is known. • Vulnerability/threat information has been already analyzed and classified.
Post-condition	Information on threats, vulnerabilities and mitigations are delivered to the interested stakeholder periodically.

Table 9: ISAC-UC-05: Cyber-threat notification

2.2.6. ISAC-UC-06: Specific transportation sector data collection

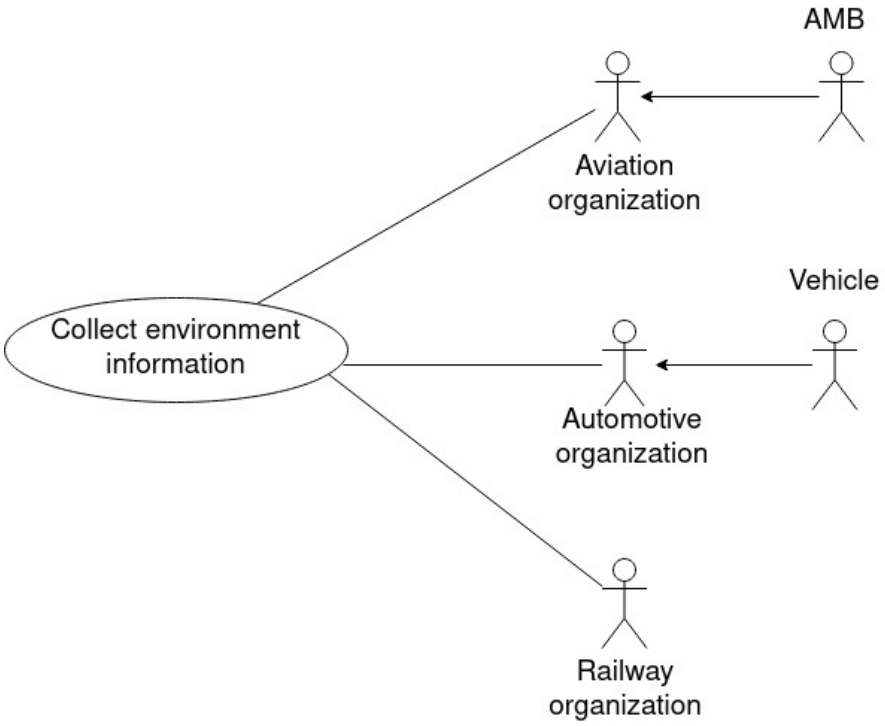

Figure 9: ISAC-UC-06: Specific transportation sector data collection

Use Case Name	Specific transportation sector data collection
Participating actors	• Automotive organization • Aviation organization • Railway organization • AMB • Vehicle
Purpose	Collect specific sector information to run security analytics and increase its own cyber-threat knowledge or share them for a collaborative analysis.
Priority	MUST
Flow of events: Normal flow	1. The specific sector data collector gathers information from its own environment: a. Automotive sector: CAN bus logs directly from the vehicle, OEM information related to

	vulnerabilities, threat feeds, research, best practices, intelligence, trends, forecasts. b. Aviation sector: sensors distributed in the airport used to monitor the airport environment (IIoT sensors logs). c. Railway sector: vulnerability report provided by the railway enterprise. 2. The data are converted in a standard data format and stored in a local space.
Pre-condition	• Each sector must have sensors distributed in its own environment from which can be possible to extract useful data for security analysis. • A local storage is required.
Post-condition	• Data are collected from the transportation sector environment, converted in a standard data format and stored in a local space.

Table 10: ISAC-UC-06: Specific transportation sector data collection

2.2.7. ISAC-UC-07: Run local analytic

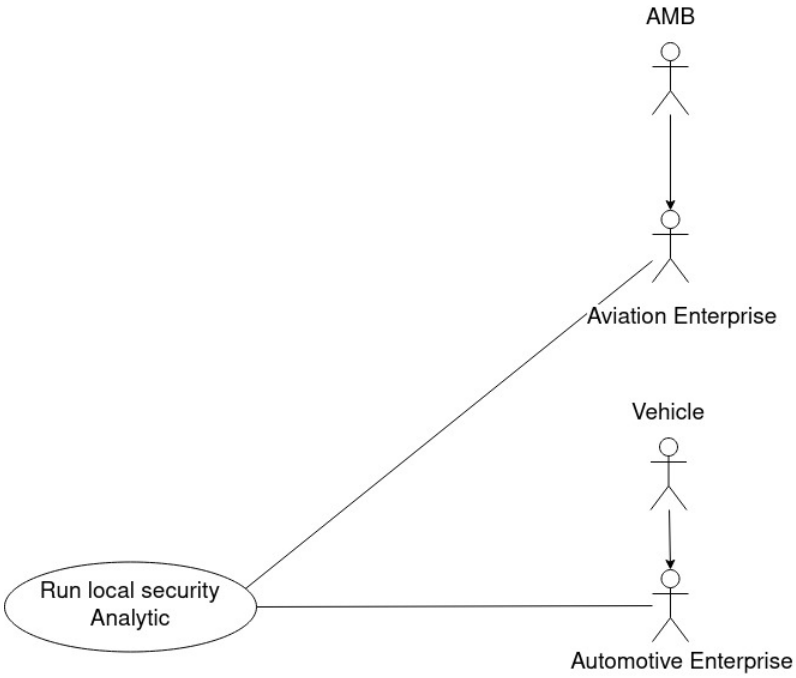

Figure 10: ISAC-UC-07: Run local analytic

Use Case Name	Run local analytic
Participating actors	Automotive enterprise Aviation enterprise • AMB Vehicle
Purpose	Running locally a security analytic to detect anomalies on the data collected.
Priority	MUST
Flow of events: Normal flow	Run a local analysis of data collected in the specific sector environment: 1. Automotive analysis: Intrusion detection system on the CAN bus data. 2. Aviation analysis: Anomaly detection system on the airport sensor data.
Pre-condition	• Data must be collected and stored locally (ISAC-UC-6).

Post-condition	• Detection of anomalies, threats, vulnerabilities on the transportation sector behavior.

Table 11: ISAC-UC-07: Run local analytic

2.2.8. ISAC-UC-08: CTI visualization

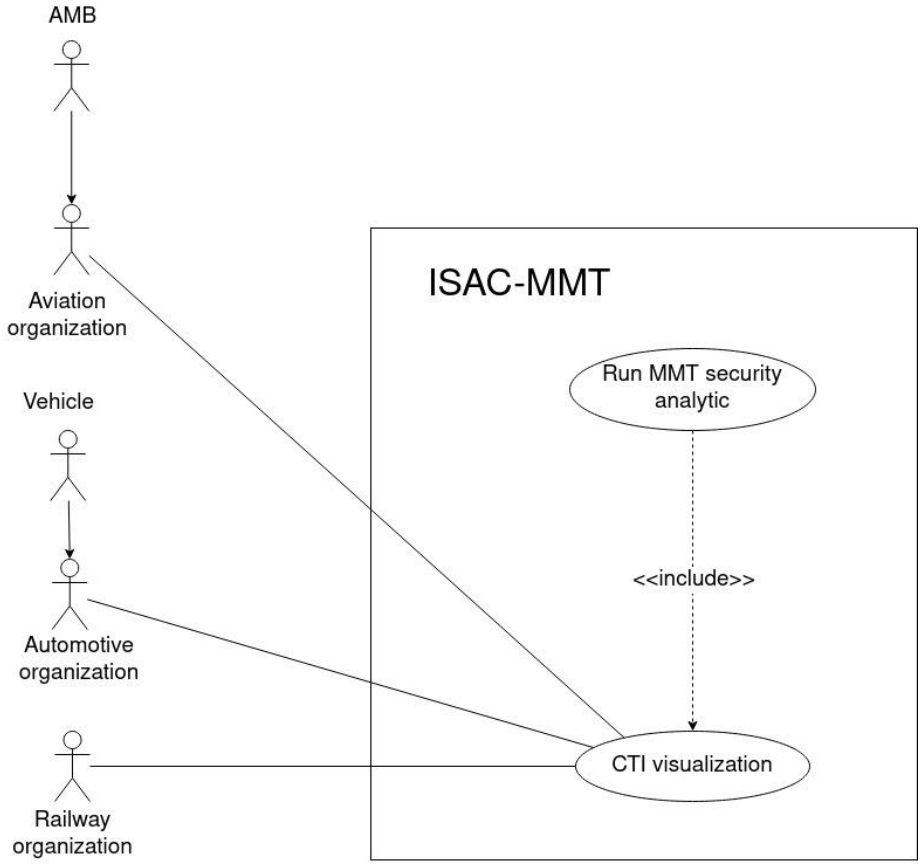

Figure 11: ISAC-UC-08: CTI visualization

Use Case Name	CTI visualization
Participating actors	Aviation organization AMB Automotive organization Vehicle • Railway organization • External entities • ISAC-MMT

Purpose	Provide a web portal to show CTI statistics, aggregated results from the analysis performed on the transportation shared data.
Priority	MUST
Flow of events: Normal flow	1. An external entity (not belonging to the sharing system) accesses to public section of the transportation web portal. 2. The entity can access the analytic results section that shows the aggregated results performed by the analytics on the public data.
Flow of events: Alternative flow	1. A transportation organization (belonging to the sharing system) logs in to the transportation web portal. 2. The organization can access the public section (public CTI and analytic results on public data). 3. The organization can see the data section containing its own data and the data shared with them. 4. The organization can access the result section containing the analytics results performed by the organization on its data and the analytic results shared with them by other organization.
Pre-condition	• Data must be already collected from public and private sources. • Aggregating analysis must be already performed by the ISAC-MMT.
Post-condition	A web portal that provides: (i) a public access to see the aggregated public security analytic results on the transportation information and a private access; (ii) a private view about shared data and private analytic results.

Table 12: ISAC-UC-08: CTI visualization

2.3. Catalogue of Use Cases

Use Case	User Stories
ISAC-UC-01	ISAC-US-01
ISAC-UC-02	ISAC-US-07 ISAC-US-09 ISAC-US-10
ISAC-UC-03	ISAC-US-07 ISAC-US-09 ISAC-US-10
ISAC-UC-04	ISAC-US-03
ISAC-UC-05	ISAC-US-04
ISAC-UC-06	ISAC-US-02
ISAC-UC-07	ISAC-US-06 ISAC-US-08
ISAC-UC-08	ISAC-US-05

Table 13: Mapping of Use Cases to User Stories

2.4. Storyboard

The following storyboards recall some of the user stories and use cases introduced in Section 1.4 and Section 2. They describe the main scenarios offered by the ISAC pilot: the *ISAC-SB-01: Subscription to the security notification service* to prevent and react promptly to a cyber-attack, the *ISAC-SB-02: Running analytic on the ISAC-MMT*, to exploit the powerful of the ISAC-MMT analytics benefiting of the collaborative analysis (ISAC-SB-02), and the *ISAC-SB-03: Running local analytic and sharing information* to improve the CTI knowledge at global level.

2.4.1. ISAC-SB-01: Subscription to the security notification service

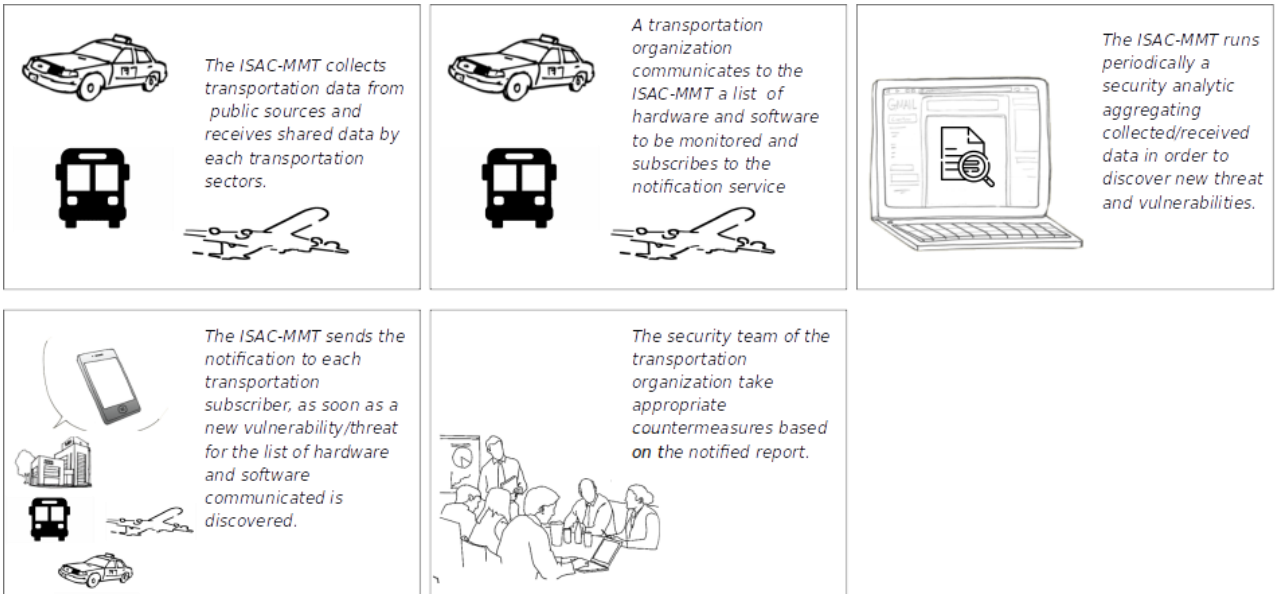

Figure 12: ISAC-SB-01: Subscription to the security notification service

The storyboard in Figure 12: ISAC-SB-01: Subscription to the security notification service represents the subscription of a transportation sector to the security notification service offered by the ISAC-MMT (ISAC-US-05, ISAC-UC-05).

2.4.2. ISAC-SB-02: Running analytic on the ISAC-MMT

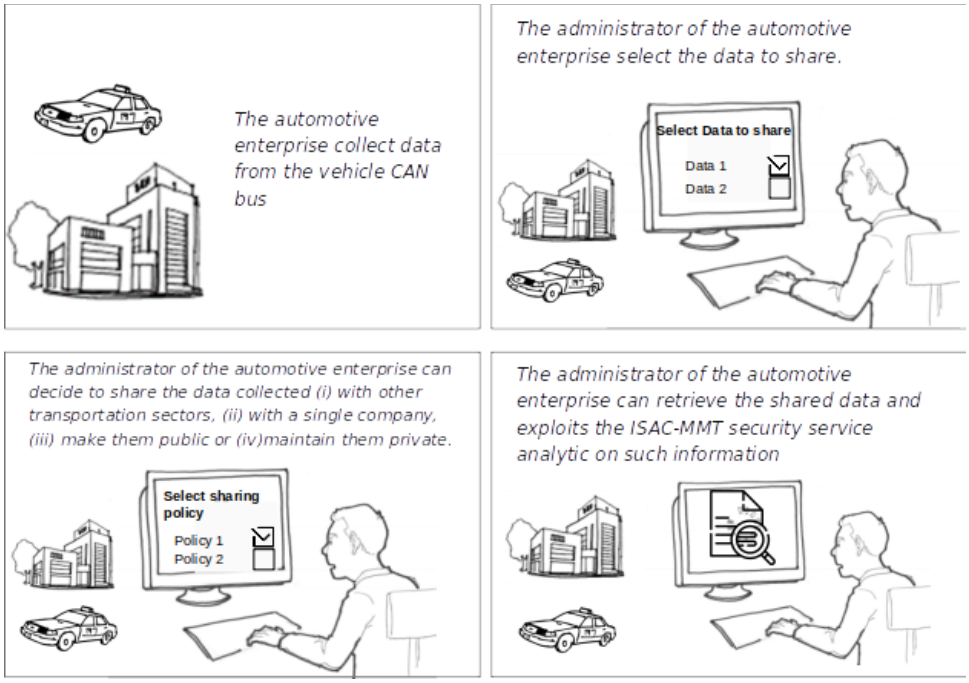

Figure 13: ISAC-SB-02: Running analytic on the ISAC-MMT

The storyboard in Figure 13: ISAC-SB-02: Running analytic on the ISAC-MMT represents the exploitation of an automotive analytic offered by the ISAC-MMT on the shared data (ISAC-UC-04, ISAC-US-06).

2.4.3. ISAC-SB-03: Running local analytic and Sharing information

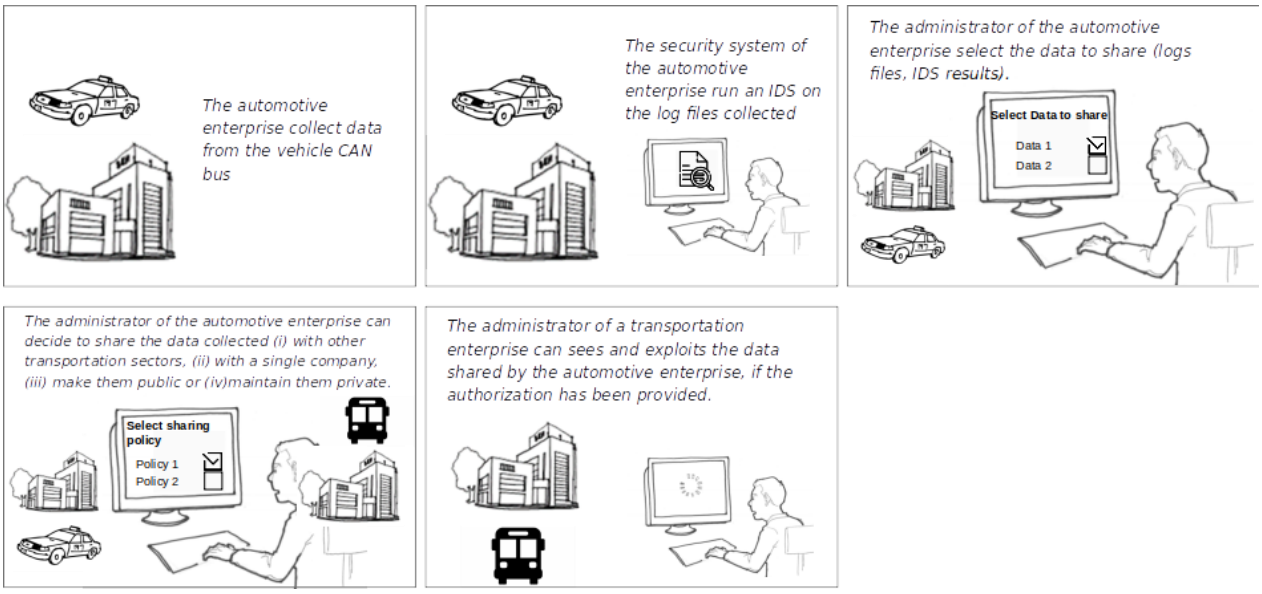

Figure 14: ISAC-SB-03: Running local analytic and Sharing information

The storyboard in Figure 14 represents the automotive data collection (ISAC-UC-06, ISAC-US-02), the security analytic performed locally (ISAC-UC-07) and the sharing of the collected

information or the analytic result with other sector-specific companies, other sectors or make them public (ISAC-UC-02, ISAC-UC-03).

3. Non-functional Requirements

In the following section is reported the list of non-functional requirements divided into *security*, *operational*, *performance*, *reliability*, and *usability* classes.

3.1. Security

ISAC-NFR-01	The ISAC-MMT sharing system should guarantee *confidentiality* using the Transportation Layer Security (TLS) protocol.
ISAC-NFR-02	The ISAC-MMT sharing system should guarantee *integrity* of the message exchanged during the communication between the ISAC-MMT and the transportation sectors.
ISAC-NFR-03	Collected data from the transportation environment should be stored in encrypted format and anonymized.

3.2. Operational

ISAC-NFR-04	The security analytics deployed in the ISAC-MMT should be run asynchronously and the result should be provided to the user once the job is completed.
ISAC-NFR-05	Sharing information should match a standard format that is compliant with the analytic tools.
ISAC-NFR-06	The sharing system should permit to upload large amount of data in order to train a ML security analytic.
ISAC-NFR-07	Data and analysis results are shared on a need-to-know basis.

3.3. Performance

ISAC-NFR-08	The ISAC-MMT should be able to run a Machine Learning (ML) security analytic, for predicting purposes.
ISAC-NFR-09	The response time of the ISAC-MMT anomaly detection analytics should be as low as possible to timely notify an anomaly event to the transportation enterprises and thus avoid or promptly mitigate the attack in progress.
ISAC-NFR-10	The capacity of the ISAC-MMT server should be high as possible, and should allow to run many sessions at the same time.

3.4. Reliability

ISAC-NFR-11	The ISAC-MMT security anomaly detection analytics based on ML techniques do not provide measurable reliability, nevertheless, it is tolerated a high False Positive Rate (normal event detected as anomaly) respect to the False Negative Rate (anomaly event detected as normal).

3.5. Usability

ISAC-NFR-12	The sharing system should be easy to use. A user should be able to easily share data with a linked DSA, see its accessible data and run security analytics on the data by accessing a web portal through a user-friendly interface.

4. Conclusions

This document describes an Information Sharing and Analytic Center (ISAC) between multiple transportation sectors, highlighting the challenges and the benefits of such proposal. To explain the goals of this pilot, an overview of the ISAC scenario is given comparing it with the current practices and presenting its improvements in terms of sharing information and collaborative analysis thanks to the E-CORRIDOR framework. Some relevant user stories and use cases are described to detect functional and non-functional requirements.

The main objective of the pilot is to guarantee a flexible, confidential and privacy-preserving framework used to share data provided by different transportation sector and offer an edge-enabled data analytics and prediction services in a collaborative, distributed and confidential way. Such sharing and collaborative analysis will permit to discover new threats and vulnerabilities with a cross-sectorial view and will allow to prevent or promptly react to cyber-attack in each transportation field.

5. Appendix

5.1. Resource Types

Resource ID	Data Type Class	Data Format	Standard	Use Case	Used for Sharing	Used for Analysis	Used for DMO
ISAC-R-1	CTI	STIX (vulnerabilities, CAPEC, CPE, exploits, attack pattern)	Open standard	ISAC-US-01 ISAC-US-03 ISAC-US-04 ISAC-UC-01 ISAC-UC-04	✓	✓	
ISAC-R-2	CAN bus	CAN Frame	Standard ISO 11898-1	ISAC-US-02 ISAC-US-06 ISAC-US-07 ISAC-UC-02 ISAC-UC-03 ISAC-UC-04 ISAC-UC-07	✓	✓	✓
ISAC-R-3	Event log	CEF	Open standard	ISAC-US-02 ISAC-US-03 ISAC-US-08 ISAC-US-09 ISAC-UC-02 ISAC-UC-03 ISAC-UC-04 ISAC-UC-06 ISAC-UC-07	✓	✓	✓
ISAC-R-4	Network log	syslog-ng	Open Standard	ISAC-US-02 ISAC-US-03 ISAC-US-08 ISAC-US-09 ISAC-UC-02 ISAC-UC-03 ISAC-UC-04 ISAC-UC-06 ISAC-UC-07	✓	✓	✓
ISAC-R-5	IDS results	JSON	Open Standard	ISAC-US-06 ISAC-US-07 ISAC-US-08 ISAC-US-09 ISAC-UC-07	✓	✓	✓

Table 14: Resource types

5.2. Definitions and Abbreviations

Term	Meaning
AMB	Airport Managing bodies
AT	Airport and Train
CAN	Controlled Area Network
CERT	Community Emergency Response Team
CTI	Cyber-Threat Intelligence
CVE	Common Vulnerability Enumeration
DMO	Data Manipulation Object
DSA	Data Sharing Agreement
ECU	Electronic Controlled Unit
ER-ISAC	European Railway ISAC
IDS	Intrusion Detection System
IIOT	Industrial Internet of Things
IM	Infrastructure Managers
IPS	Intrusion Prevention System
ISAC	Information Sharing Analysis Centre
ISAC-MMT	Information Sharing Analysis Centre Multi Modal Transportation
ML	Machine Learning
MoSCoW	Must have, Should have, Could have, and Won't have but would like
NFR	Non-Functional Requirement
NIST	National Institute of Standards and Technology
NVD	National Vulnerabilities Database
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
P2P	Peer-to-Peer
PT-ISAC	Public Transportation ISAC
RU	Railway Undertakings
SCAP	Security Content Automation Protocol
SME	Small And Medium Enterprise
ST-ISAC	Surface Transportation ISAC
TLS	Transport Layer Security
TTP	Tactics, Techniques and Procedures

Table 15: Definitions and Abbreviations

5.3. Requirements elicitation process

The pilot requirements collected in this document are the results of several (web call) discussions with all the E-CORRIDOR partners and in particular with the partners involved in the ISAC pilot (MISE, CNR, DIG, FG, HPE and AMTU). Parts of the work has been done in conjunction with ADP regarding the aviation sector, DIG for the railway sector and CLEM for the automotive.