Artificial Intelligence Threat Reporting and Incident Response System

D2.1 – Vision scenarios and use cases definition

Project Title:	Artificial Intelligence Threat Reporting and Incident Response System
Project Acronym:	IRIS
Deliverable Identifier:	D2.1
Deliverable Due Date:	31/12/2021
Deliverable Submission Date:	30/12/2021
Deliverable Version:	V1.2
Main author(s) and Organisation:	René Serral-Gracià (UPC)
Work Package:	WP2 – System Co-Design
Task:	Task 2.1 – Use cases and application scenarios definition
Dissemination Level:	PU: Public

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Quality Control

	Name	Organisation	Date
Editor	René Serral	UPC	28/12/2021
Peer Review 1	Sofia Tsekeridou	INTRA	29/12/2021
Peer Review 2	Gonçalo Cadete	INOV	29/12/2021
Submitted by (Project Coordinator)	Nelson Escravana	INOV	30/12/2021
Resubmitted by (Project Coordinator)	Gonçalo Cadete	INOV	30/06/2023

Contributors

Organisation
UPC
Taltech
FVH
Cisco

Document History

Version	Date	Modification	Partner
0.1	15/10/2021	Creation of Initial Document	UPC
0.2	01/12/2021	Contributions for PUC descriptions	FVH, Taltech, UPC, Cisco, IMI
1.0	29/12/2021	Final version, reviewed	INTRA, INOV
1.1	12/05/2023	Revision after Mid/review	UPC
1.2	22/06/2023	Enhanced PUC1	UPC

Legal Disclaimer

Contents

1 Introduction 9
1.1 Deliverable purpose 9
2 Scenario definition 10
2.1 Generic scenario specification template 10
3 Pilot Use Case 1: Tramway Monitoring 12
3.1 Scenario overview 12
3.2 Covered stakeholders' needs 14
3.3 Involved actors 14
3.4 Technical Assets 14
3.5 Data in transit or in use 15
3.6 Risk of the scenario 15
3.7 IRIS platform involvement 15
3.8 IRIS platform benefits 16
3.9 User story 1: Enhancing safety of vulnerable road users 17
3.10 User story 2: Protecting the confidentiality, integrity and privacy of the video feed system 18
4 Pilot Use Case 2: Autonomous Transportation System 20
4.1 Scenario overview 20
4.2 Covered stakeholders' needs 21
4.3 Involved actors 22
4.4 Technical assets 22
4.5 Data in transit or in use 23
4.6 Risk of the scenario 24
4.7 IRIS platform involvement 24
4.8 IRIS platform benefits 24
4.9 User story 25
4.9.1 User story 1 25
4.9.2 User story 2 26
5 Pilot Use Case 3: SmartGRID system 27
5.1 Scenario overview 27
5.2 Covered stakeholders' needs 29

5.3 Involved actors 29
5.4 Technical assets 29
5.5 Data in transit or in use 31
5.6 Risk of the scenario 31
5.7 IRIS platform involvement and benefits 31
5.8 User story 32
5.8.1 User story 1 32
5.8.2 User story 2 32
5.8.3 User story 3 33
6 Stakeholders Feedback 34
6.1 Stakeholders questionnaire 34
6.1.1 Introductory questions 34
6.1.2 PUC particular questions 34
6.1.3 Final remarks 35
6.2 Questionnaire results 35
6.2.1 Introductory questions 35
6.2.2 PUC 1 Questions 35
6.2.2.1 Question: Opinion regarding the use-case 35
6.2.2.2 Question: Do you think the scenario is vulnerable to other type of attacks? 36
6.2.2.3 Question: Which aspects of the use case would you improve? 36
6.2.2.4 Question: Would you involve another city infrastructure to the use case? 37
6.2.2.5 Question: Do you think this scenario, once deployed, will be beneficial for the city 37
6.2.2.6 Question: Provide a possible alternative use case for this Pilot 37
6.2.3 PUC 2 Questions 37
6.2.3.1 Question: Opinion regarding the use-case 37
6.2.3.2 Question: Do you think the scenario is vulnerable to other type of attacks? 38
6.2.3.3 Question: Which aspects of the use case would you improve? 38
6.2.3.4 Question: Would you involve another city infrastructure to the use case? 39

6.2.3.5 Question: Do you think this scenario, once deployed, will be beneficial for the city 39
6.2.3.6 Question: Provide a possible alternative use case for this Pilot 39
6.2.4 PUC 3 Questions 40
6.2.4.1 Question: Opinion regarding the use-case 40
6.2.4.2 Question: Do you think the scenario is vulnerable to other types of attacks? 40
6.2.4.3 Question: Which aspects of the use case would you improve? 40
6.2.4.4 Question: Would you involve another city infrastructure to the use case? 41
6.2.4.5 Question: Do you think this scenario, once deployed, will be beneficial for the city 41
6.2.4.6 Question: Provide a possible alternative use case for this Pilot 42
6.2.5 Final remarks 42
6.2.5.1 Question: How could IRIS better help your organization? 42
7 IRIS Features Covered by Use Cases 43
8 Conclusions 45
References 46

List of Figures

Figure 1. IRIS platform architecture as deployed at PUC1 IoT infrastructure 12
Figure 2. IRIS interaction with PLEDGER project 13
Figure 3. Outdoor scenario description 13
Figure 4. Scenario assets location 16
Figure 5. IRIS platform positioning 16
Figure 6. PUC3 Scenario Flow (Assets assigned with the number are described in “Technical assets” section) 28
Figure 7. Distribution of number of employees for stakeholder companies 35
Figure 8. PUC1 - Opinion regarding use-case 36
Figure 9. PUC1 - Aspects to improve regarding the use-case 36
Figure 10. PUC1 - Will the scenario be beneficial for the city? 37
Figure 11. PUC2 - Opinion regarding use-case 38
Figure 12. PUC2 - Aspects to improve regarding the use-case 38
Figure 13. PUC2 - Other city infrastructure involvement 39

Figure 14. PUC2 - Will the scenario be beneficial for the city 39
Figure 15. PUC3 - Opinion regarding use-case 40
Figure 16. PUC3 - Aspects to improve regarding the use-case 41
Figure 17. PUC3 - Other city infrastructure involvement 41
Figure 18. PUC3 - Will the scenario be beneficial for the city 42

List of Abbreviations and Acronyms

Abbreviation/ Acronym	Meaning
AI	Artificial Intelligence
ATA	Automated Threat Analytics
CA	Consortium Agreement
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DoA	Description of Action
EC	European Commission
ICT	Information and Communications Technology
IoT	Internet of Things
PUC	Pilot use case
WP	Work Package

Executive Summary

Cybersecurity is an important topic in any digital area as has been proven with the large amount of attacks based on ransomware, denial of service, data exfiltration and others. It becomes even more important in infrastructures found in our Smart Cities and other infrastructures with IoT and smart devices. IRIS aims at designing a treat detection and mitigation system for such environments.

In this document we provide the description of the different pilots involving three different cities, together with the high-level definition of the security challenges and risks involved in having such infrastructures open to the public.

To complement this description, we designed a questionnaire for stakeholders contacted in public events, as well as directly by the consortium partners. This questionnaire has the ultimate goal of validating that IRIS will be a suitable platform to provide the required security in such scenarios.

1 INTRODUCTION

Due to the largely complex deployments of smart city infrastructure and AI-enabled platforms, it becomes clear that such environments may be subject to a large amount of possible attacks. This environment introduces new levels of complexity to threat intelligence, especially in identification, threat response and data sharing of the different attack vectors in such IoT and AI environments.

IRIS aims at the integration and demonstration of a single platform addressed to CERTs/CSIRTs for assessing, detecting, responding and sharing information regarding such threats and vulnerabilities of IoT and AI-driven systems.

IRIS aims to help European CERTs/CSIRTs minimize the impact of cybersecurity and privacy risks as well as threats introduced by cyber-physical vulnerabilities in IoT platforms and adversarial attacks on AI-provisions and their learning/decision-making algorithms.

The IRIS platform will be demonstrated and validated in highly realistic environments by engaging three stakeholders and end users (in Helsinki, Tallinn and Barcelona) along with the involvement of national CERTs/CSIRTs, as well as cybersecurity authorities.

The project duration extends from September 2021 to August 2024.

1.1 Deliverable purpose

This deliverable is an outcome of *"Task 2.1: Use cases and application scenarios definition"* with a twofold goal; on the one hand, this deliverable provides a formal definition of the different scenarios, pilots and use-cases that will be used to validate the IRIS platform; and on the other hand, the deliverable also provides the feedback gathered from the stakeholders, to support the definition of the particular attacks that need to be issued for the validation of the different use cases.

To clearly define and continually update the scenarios' definitions, a template was developed containing the required information. The outcome of this data gathering will allow during the project to have a clear idea of the particular environment of each scenario, along with the critical security aspects to consider.

We also map the pilot use cases with IRIS features to highlight the completeness and focus of the solution's demonstration and evaluation strategy.

The specification of the scenarios, use cases, and related security requirements is an agile process, to be conducted along iterative, incremental, and adaptive cycles, according to software development best practice [4]. The up-to-date artifacts are made available in the official IRIS repository.

2 SCENARIO DEFINITION

The project proposal provided a general description of the environment for IRIS validation in the form of three Pilots. The pilots were centered on already existing infrastructure in three different cities, PUC1 on Barcelona, PUC2 on Tallinn, and PUC3 on Helsinki.

- The Barcelona Scenario is centered on monitoring an AI computer vision system at the edge and an IoT infrastructure deployed at the Tramway.
- The Tallinn Scenario is centered on the hardening of a smart autonomous vehicle infrastructure available in the University campus.
- The Helsinki Scenario is focused on smart grid and cross-border smart grid security threats.

The goal within IRIS for these pilots will be the analysis of the security concerns and potential vulnerabilities of the scenarios and underlying smart city services and infrastructures. Despite of this, instead of focusing the effort on each pilot separately, we propose a generic scenario definition form, to be used along the project to support the definition of the scenarios and their potential vulnerabilities.

2.1 Generic scenario specification template

In order to enable uniform data gathering of the different scenarios, we prepared a generic scenario specification template that includes the following data description dimensions:

Scenario overview: general description of the pilot.

Covered stakeholders' needs: to further understand the scenario, it is important to understand the obtained benefits of the different actors, in particular the needs that are covered by deploying the scenario.

Involved actors: list of actors in the whole scenario. An actor is an active asset of the scenario. For completeness the actors involve: infrastructure, software, hardware and human actors. It is necessary to specify the **Type** of actor (Human, Software, Hardware, …), its **Role** within the scenario and a short **Description**.

Technical assets: list of passive assets relevant for the scenario. This, jointly with the Involved actors, will allow to determine the attack surface of the scenario. It comprises the following information: **Type**, i.e., Hardware, Software, Sensors, Code, Network, Database, Other, **Attack Surface**, with information regarding how this asset may be exploited. Finally, **Description** of the asset.

Data in transit or in use: to understand the sensitivity of the whole scenario, it is necessary to determine which important data will be stored or transmitted in the workflow of the scenario. The particular information required is: **Type** of information, its **Importance** and a **Description**.

Risk of the scenario: informs about the potential risk of a security breach in such a scenario, especially considering the potential impact over its users. Such risk may be Low, Medium, High, Critical. Together with a description of the risk.

IRIS platform involvement: to better understand how IRIS may help and assist the scenario this part will determine the **Type** of involvement: Identification, Validation, Detection, Prevention, Response, or Other, the **Description** of the involvement, and when applicable which **Partner's tool** will be used to assist in hardening the security of the scenario.

IRIS platform benefits: continuing with the assessment of IRIS involvement and benefit for the scenario, this part will gather information regarding the **Added Value** and a **Description** of that value.

User Story: as the last important aspect to gather is the whole description of the user story, how the scenario works and which is the interaction among all the actors.

3 PILOT USE CASE 1: TRAMWAY MONITORING

Title: Securing the smart city's IoT and control systems against confidentiality & integrity breaches.

City: Barcelona.

3.1 Scenario overview

As described in the IRIS workplan, in the context of PUC1, the IRIS Platform will be deployed in the Barcelona City Council's IoT testbed network, as depicted in the following architecture diagram:

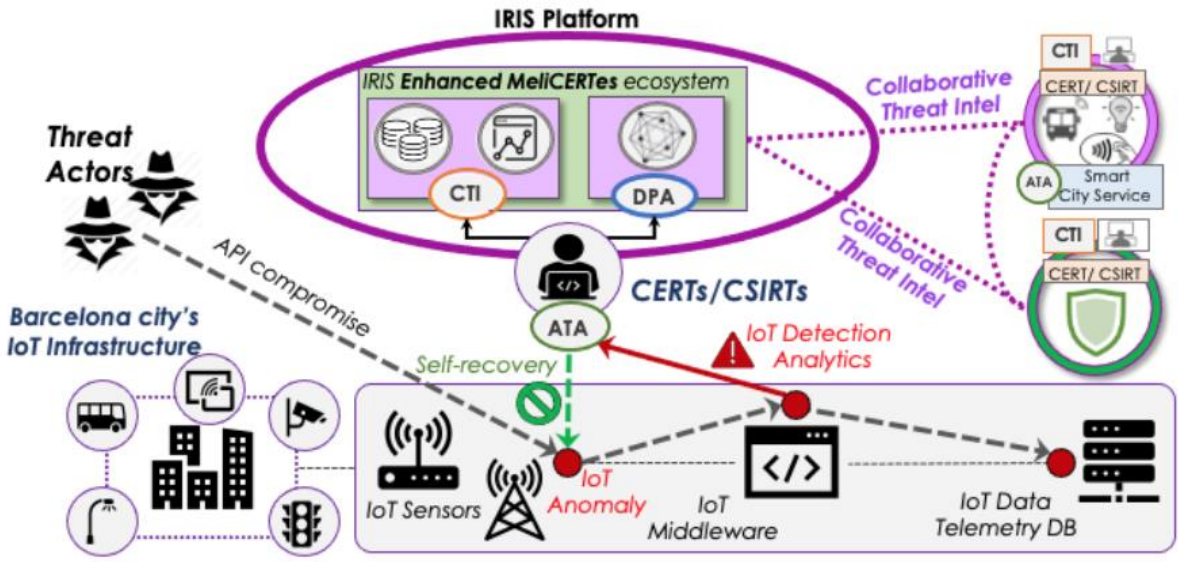


Figure 1. IRIS platform architecture as deployed at PUC1 IoT infrastructure

This PUC1 customized IRIS platform will allow us to achieve most of the pilot's objectives, which are:

- (a) Detecting threats on IoT devices and their integration with telemetry systems,
- (b) Efficient reporting the impact and the purpose of availability, confidentiality, integrity and privacy breaches on smart city's IoT and control systems,
- (c) Handling the different effects of the threats and vulnerabilities in state-of-the-art multi-connected IoT infrastructure.

More specifically, the pilot will monitor an IoT infrastructure deployed at an intersection nearby the Tramway station in Diagonal street by leveraging the work done in the Pledger project, also Horizon 2020 funded.

As a consequence, the city provides improved safety for vulnerable road users.

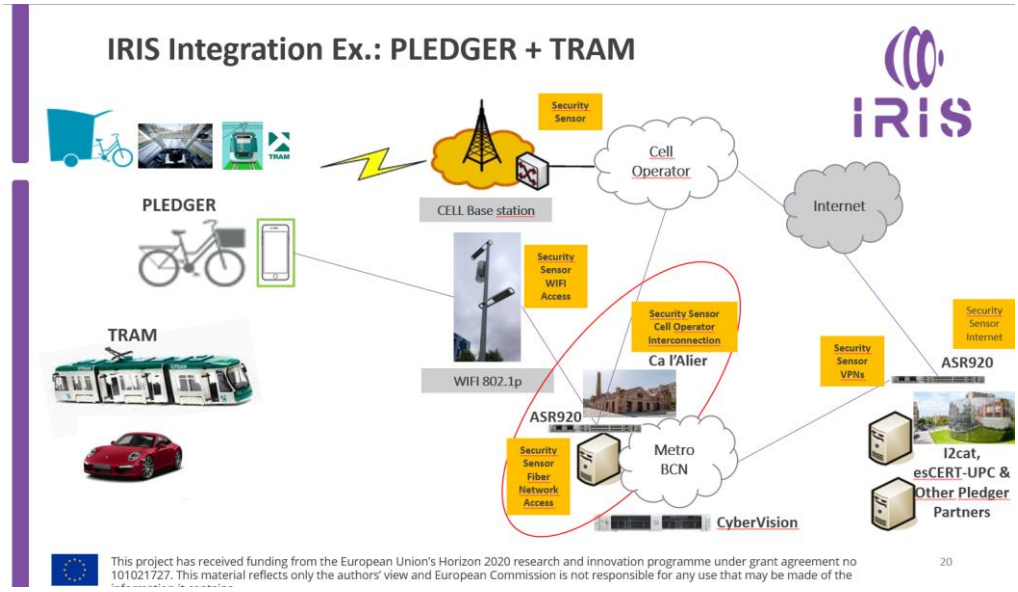


Figure 2. IRIS interaction with PLEDGER project

Pledger project consists of a 802.11p wireless system which recognizes the presence of trams and bicycles, thus flagging risk situations and avoiding potential accidents between bicycles and pedestrians getting off the train, when such situation is detected an alarm is fired to inform the tram driver to stop the vehicle. In addition to that, within the IRIS project we will simulate the addition of video surveillance cameras on the street to assist in the detection.

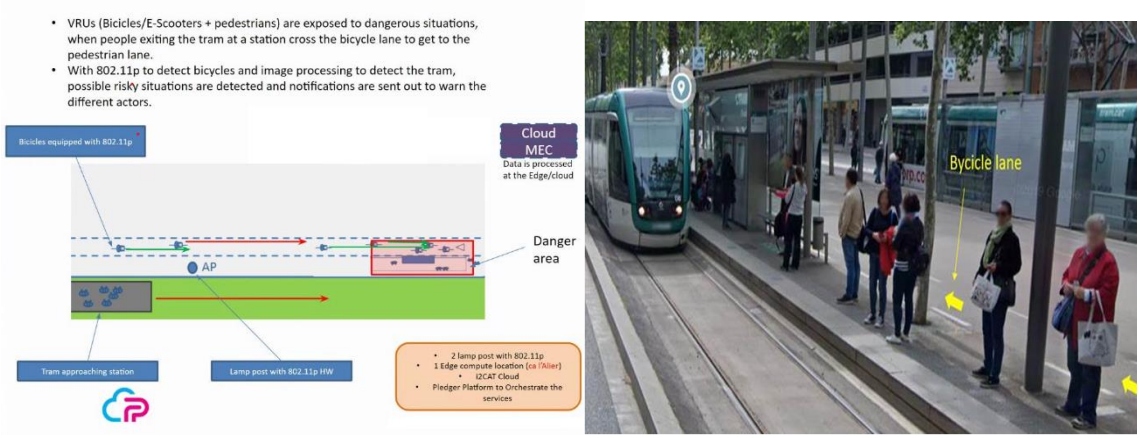


Figure 3. Outdoor scenario description

This infrastructure is deemed critical for the pedestrians and other persons crossing the streets, a potential attacker may disrupt the service and put lives at stake. For this reason, malicious attacks of the city infrastructure like this one is becoming a major concern. Moreover, giving if an unauthorized access to the video-cameras happened, the scenario would incur on severe confidentiality issues, since the attacker could exfiltrate images of the pedestrians on the area or images of the security agents on their post within the data center may be leaked.

Adding IRIS into this infrastructure has a twofold impact, on the one hand it will allow the city to ensure continuity and resilience of the service. Thus, ultimately guaranteeing safety of vulnerable road users.

3.2 Covered stakeholders' needs

This PUC will provide a better user experience to Barcelona City, as the system will provide a safer environment where Tramways, pedestrians and bikes may coexist with less safety issues and accidents, that could result also from man-made cyber-attacks.

From the IRIS platform perspective, securing such infrastructure will provide a safer Tramway experience while guaranteeing confidentiality, as a potential cyber-attack to this infrastructure may cause delays or even breaking disruption of the scheduled tramways frequency, as well as potential life endangered incidents, considering the cyber-physical system interdependencies and hence the cascading effects of such cyber-attacks to the physical world.

3.3 Involved actors

The main active actors in this scenario will be:

- Human and non-technical actors:
  - Tramways
  - Pedestrians
  - Bike users
- Entities:
  - Transport Operators
  - CERTs

3.4 Technical Assets

The list of actively used assets by the testbed relevant to IRIS are the following:

PLEDGER Assets	**Urban Assets**	**IRIS Assets**
Router	Dark Fiber	Server
Server	Cabinets	Firewalls
IoT devices – Odroid	Pole	Switches
IoT devices – RSU		Camera

		Ambient Sensors Cybersecurity Sensor

3.5 Data in transit or in use

The infrastructure will have two different types of data: data in motion and data at rest.

- **Data in Motion**
  - Information about the location of the different tramways
  - Information about the position of the different pedestrians and bicycles
- **Data at Rest**
  - Historical data about tramway locations and frequency
  - Historical pedestrian and bicycle information
  - Camera video feed stored in the camera itself

3.6 Risk of the scenario

Security challenges of the scenario:

- Attacks in the network infrastructure of tramway station
- Providing access to malicious actors to the video feed of the different cameras
- Malicious actor accessing the data harvested by the sensors
- Disruption: by sending fake signals to the system to mimic the presence of a pedestrian or bike on the Tramway tracks, thus forcing the Tramway to stop.

3.7 IRIS platform involvement

The IRIS project will improve the Barcelona City Council's IoT testbed network to enhance its security.

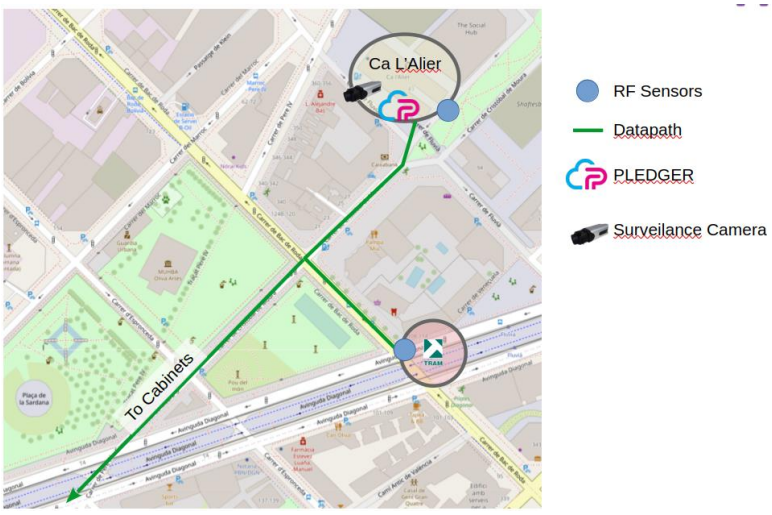


Figure 4. Scenario asset's location

As illustrated in Figure 4, the project requires the extension of the fibers of the testbed network of the City Council from the station in Diagonal Avenue to Ca l'Alier (Fluvià street) where the data-center of the Barcelona City Council and the Cisco Innovation Center is located.

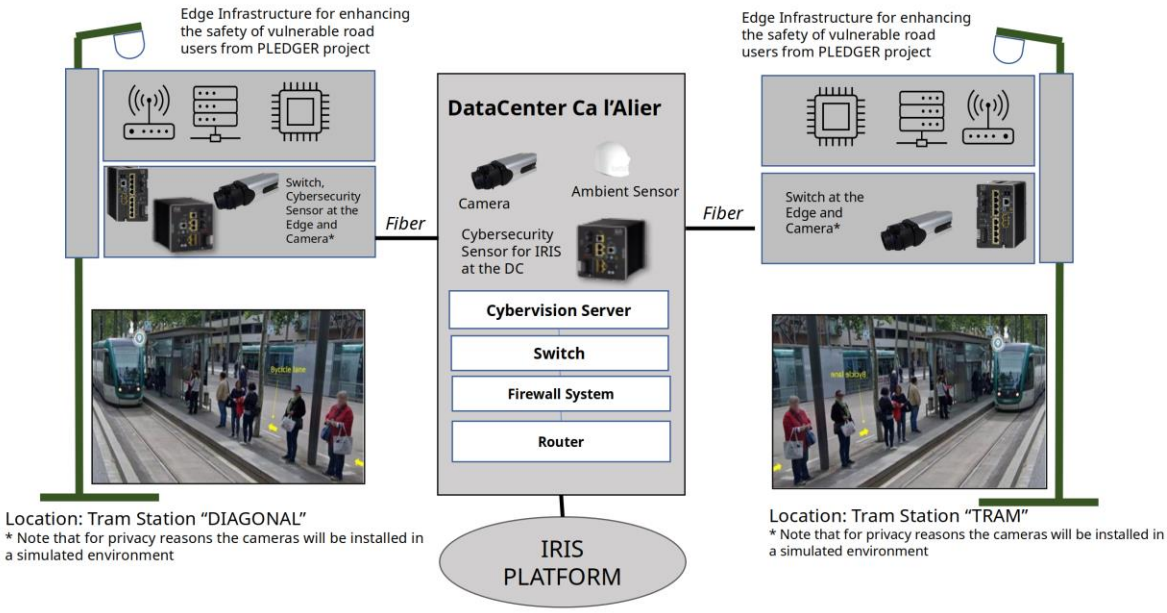


Figure 5. IRIS platform positioning

To complement the scenario, the scenario has the Cyber Vision monitoring infrastructure, in charge of the 2-tier architecture having Cyber Vision sensors collecting all traffic generated in the tram station and a Cyber Vision Center located at Ca l'Alier for centralized analytics, data visualization and population of the data to third-party access (IRIS).

All data traffic will be analyzed by Cyber Vision sensors who only send lightweight metadata to the Cyber Vision Center for further analytics. The Cyber Vision API will expose the same data as the ones used by the Cisco Cyber Vision webapp through a REST API, to allow the creation of third-party clients, scripts and automation.

3.8 IRIS platform benefits

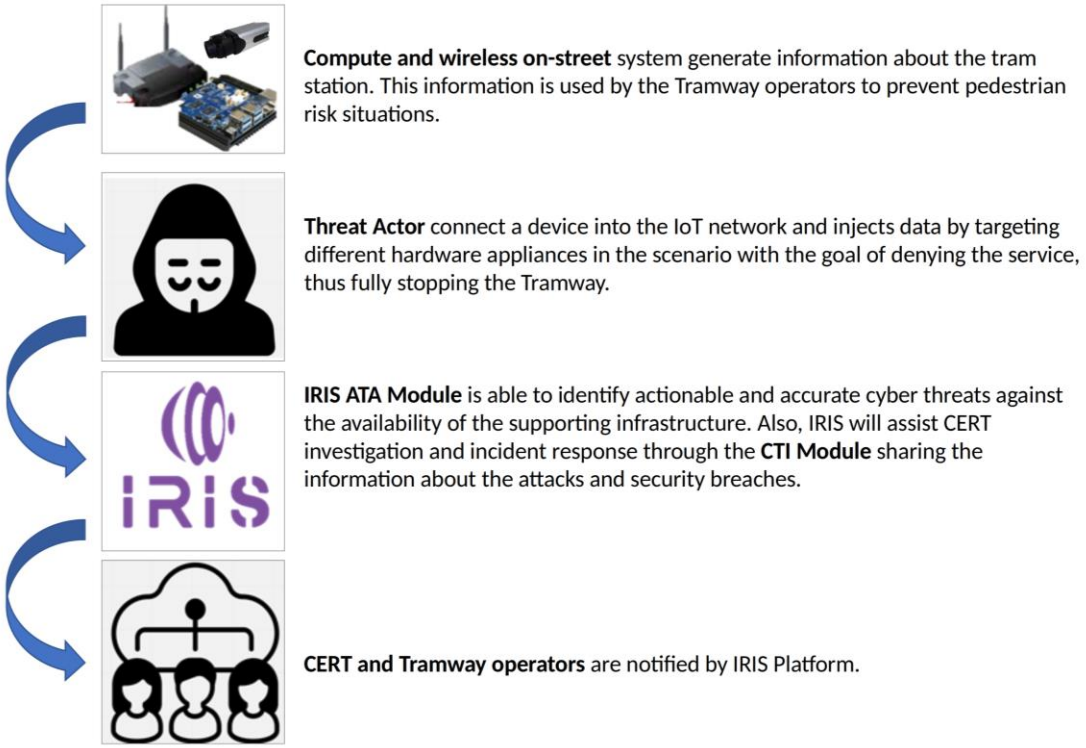
The benefits expected of IRIS are the following:

- IRIS can minimize and mitigate the impact of cyber-attacks. This will be accomplished by threat identification, threat recovery and with the shared knowledge base acquired from other related platforms.

- Thanks to the IRIS platform, the Tramway operators will be able to effectively identify when an attack in the tramway network infrastructure is occurring, effectively denying the service of the tramway.
- Tramway operators will be able to self-heal from such attacks.
- With the shared knowledge base, IRIS will effectively inform, and thus, improve the security of other similar systems vulnerable to the same type of attacks.
- The scenario confidentiality will be preserved. IRIS will provide the necessary protection to guarantee that any malicious actor with the purpose of acquiring information from the IoT infrastructure will be banned from the network and forbidden access to the data.
- Thanks to IRIS, the camera feeds, besides guaranteed confidentiality, they will obtain also integrity guarantees, along with the necessary privacy for the users of the tramway and the surrounding pedestrians.

3.9 User story 1: Enhancing safety of vulnerable road users

The goal of this use case is to detect and act upon vulnerabilities into the Tramway enhanced perception system. IRIS is expected to complement the PLEDGER project by providing a very secure and reliable smart city infrastructure. Particularly, IRIS will guarantee availability.



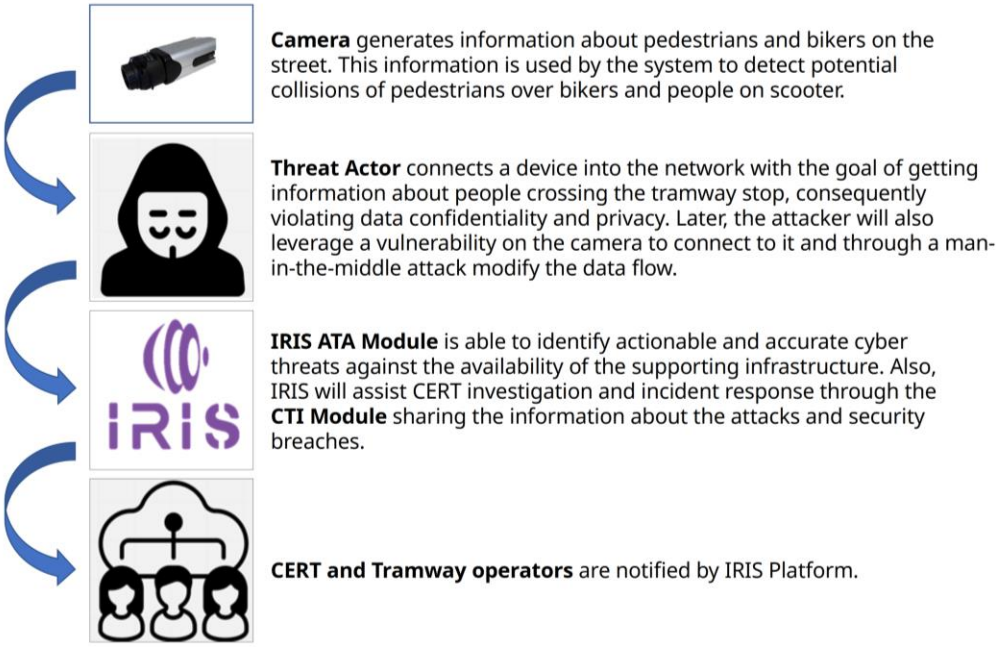
The main goal is to reduce the number of accidents, especially with Vulnerable Road Users (VRUs). In particular, the scenario will be deployed and secured by IRIS on intersections where the drivers' visibility may be obstructed, thus missing the presence of a pedestrian or a bicycle approaching.

Then, the pilot will simulate the presence of attacks into the network infrastructure in the tramway station with the goal of effectively denying the service of the tramway.

In summary, this user story will cover ATA and CTI modules, by analyzing and mitigating possible attacks and by sharing and reporting the threat intelligence to the different CERTs/CSIRTs.

3.10 User story 2: Protecting the confidentiality, integrity and privacy of the video feed system

The goal of this use case is guarantee confidentiality, integrity and privacy of the pedestrians passing by the tramway, either using bikes, scooters or stepping down from the train. These guarantees will be provided by IRIS, where it is expected to prevent the attacker to access the video surveillance system.



This scenario represents an advancement of User Story 1 within this pilot. Here, the malicious attacker has a dual objective. First, the attacker aims to gain unauthorized access to the video feed in order to engage in surveillance of individuals, and second the attacker wants to send a modified video to the server. To this end, the attacker attempts to establish a connection with the video camera, which compromises both the confidentiality of the

data and people's privacy. Subsequently, the attacker through ARP spoofing wants to alter the video feed to suit their own malicious intentions[1].

In this scenario IRIS, through its monitoring capabilities within the ATA and CTI modules, will detect such misbehavior and then, the IRIS orchestrator will enforce the necessary rules in the network to effectively forbid the access to the malicious actor to the video feed, consequently guaranteeing the confidentiality and integrity of the IoT network. It is worth noticing that the rest of IoT devices will be protected in the same manner. Finally, all this information will be shared through MISP to the different CERTs and CSIRTs.

[1] It is important to notice that due to regulatory issues the actual tests will be performed on an indoor scenario, simulating the presence of pedestrians and the attack.

4 PILOT USE CASE 2: AUTONOMOUS TRANSPORTATION SYSTEM

Title: Securing AI-enabled infrastructure of autonomous transport systems in a smart city

City: Tallinn

Autonomous transportation systems offer a new and innovative approach to intelligent transportation in the smart city. However, autonomy leaves a city exposed to highly-impactful cyberattacks via the attack surface created by a dense interconnected ecosystem of autonomous vehicles and surrounding infrastructure. The city of Tallinn established a pilot trial of autonomous vehicle shuttles (AV shuttle) for public transportation. These AV shuttles operate without a human driver and are monitored by a centralised remote operation center. To enable this, the AV shuttle exchanges telemetry that includes information critical for safe navigation. Telemetry from the AV shuttle is published via API to a "Urban Platform"; an abstract collection of services and microservices. Within the infrastructure, an AI/ML module which consumes the telemetry data via KAFKA data streams is provided by separate microservices that can also utilize 3rd party on-demand platforms.

As the protection of the AI-enabled infrastructure of autonomous transport systems is of vital importance, the aim of the PUC2 IRIS pilot are the following:

- to assess IRIS's utility of disseminating actionable and accurate AI threats against availability to the safe operation of the AV Shuttle.
- to validate the capabilities of IRIS's cybersecurity training platform as a learning tool for collaborative response to emergency incidents on autonomous transport.
- to demonstrate how the IRIS platform can facilitate autonomous detection and risk-based response for privacy breaches.
- to evaluate IRIS's virtual cyber range for establishing mature CERT/CSIRT communities equipped with processes and experience for AI provision threat detection and incident response.

4.1 Scenario overview

In the scenario, explored in this pilot, this autonomous transportation system is the target of an orchestrated attack. The malicious actors aim to disrupt the traffic flow of the city to gain notoriety and exposure. In a first attack, the attackers aim to disrupt the telemetric data of the autonomous vehicles by targeting their API connectivity to the Universal Platform, by injecting false information (e.g., location data, bus cyber and physical sensor data)

causing the Universal Platform to display false information. The false information on Universal Platforms results in diminishing the trust of the public towards the innovative city services and its AI technologies in general. Second, the malicious actors aim to vandalize and physically disrupt the autonomous buses by feeding false information about physical traffic signs and lights (ML evasion attack). The principle behind this attack is to carefully craft the data that is commonly collected from the vehicle's sensors to deceive its AI navigation modules, to evade its model concept, and to invoke erroneous decisions. As a result, several of the city's autonomous buses will exhibit erratic behavior or will be totally immobilized in central locations. In the case of the ML-evasion attack on the autonomous bus, a vulnerable ATA Digital Twin honeypot will be deployed to the system which mimics the data footprint and functionality including its AI components. The high-interaction Digital Twin will facilitate the collection of ML attack telemetry and demonstrate IRIS's ability to supply threat analytics for advanced IoT and AI attacks that can be used by systems to self-recover in real-time.

This scenario will demonstrate the potentially catastrophic consequences of a coordinated attack to the infrastructure of a modern, AI-controlled public transportation system; and how IRIS can minimize impact by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms. By using the IRIS platform, system operators can effectively identify when specially crafted data, designed to confuse AI-based decision making, (e.g., spoofed/fuzzed) is received from onboard vehicle sensor, or injected directly to APIs using directly monitored data on target systems or via its unique Digital twin honeypots. Operators can then leverage IRIS to self-recover from such malformed data injection. IRIS's CTI provision will provide collaborative parties to discover and share attack signatures to respond to IoT and AI-targeted attack vectors. Moreover, IRIS will provide CSIRTs/CERTs with the tools capable of identifying where an attack has breached, and exposed, large-scale private data. Such privacy data breach identification equips incident response with key information to operate at speed for protecting citizens from vulnerable IoT and AI systems.

4.2 Covered stakeholders' needs

We have identified three possible stakeholders. The first one is the Smart City Transport Provider, for whom this scenario will provide safe and secure operation of the autonomous transportation, as well as receiving notifications of any cyber threats to the autonomous transportation systems and traffic infrastructure.

The second stakeholders are CERTs, which will get notified of privacy and data breaches to the autonomous transportation ecosystem.

Lastly, this scenario will provide confidence in the safe transportation of autonomous vehicles to Smart City Passengers.

4.3 Involved actors

There are several actors in play is this scenario. The CERT will act as an actor responsible for the protection of smart city services and citizen data. It coordinates incident response and notifies stakeholders of cyber threats to smart city services and privacy of citizen data.

The Smart City Transport Provider Administrates and monitors the smart city transport environment. They coordinate with CERT.

The malicious threat actor, the human or system/software performing an attack, has the capability to inject false data by targeting the API connectivity of the autonomous vehicle telematics systems and the Universal Platform and inject false information about physical traffic signs and lights to evade AI/ML model and invoke erroneous vehicle responses.

There is also the Autonomous Transportation System / Digital Twin, which encompasses the autonomous self-driving vehicle shuttles and supporting traffic infrastructure. It generates telemetry which is used for logging and publishing to APIs. The Digital Twin honeypot is used for AI/ML model testing.

Finally, the Universal Platform software. Telemetry data generated by the autonomous transportation system is published to an API into the Urban Platform. The Urban Platform is an abstract collection of services and microservices which consume telemetry data via KAFKA data streams.

4.4 Technical assets

The list of actively used assets by the testbed relevant to IRIS are the following:

1. **Type:** Software - Autonomous Vehicle Middleware Platform
   Generic Threats:
   - Fuzzing – non-sanitized, malicious data input
   - Spoofing of Master and Nodes in middleware platform
   - Threats which compromise open connections such as debug and developer ports.

   Description: The Middleware platform is based on the Robotic Operating System (ROS). The ROS system is an open-source suite of software libraries and tools used for autonomous vehicle and robotics software development.
2. **Type:** Sofware - Autonomous Vehicle Control System
   Generic Threats:
   - Fuzzing – non-sanitized, malicious data input
   - Robust physical invariants and ML/AI evasion threats

   Description: AutoWare is an open-source software project that provides self-driving modules, including localization, detection, prediction, planning and control.
3. **Type:** Software - Teleoperation Software Module

Generic Threats:

- Supply Chain compromise
- Software Fuzzing and Network Protocol Fuzzing
- Spoofing of software module and interception of teleoperation data

Description: The teleoperation software module is provided by a commercial, proprietary vendor. It is a ROS module which is designed to enable a remote-control center to monitor and take driving actions of the operational autonomous vehicle.

4. **Type:** Hardware - Autonomous Vehicle Cyber-Physical and Embedded Devices
   Generic Threats:
   - Sensors can be fuzzed, injected with false or manipulated data.
   - Ghost images and robust physical invariants can manipulate sensory perception.

   Description: Cyber-physical sensors on the autonomous vehicle include LiDAR, Camera, GNSS, ECUs (Electronic Control Units), CAN (Controller Area Network) OBUs (On-Board Units). These sensors are used for environmental perception and serialization, localization, and mapping.
5. **Type:** System - Autonomous Vehicle Logging System
   Description: This system consists of a server that collects the autonomous vehicle telemetry, in the form of a ROSBag.
   Generic Threats:
   - False/Malicious data injection or deletion of data
   - DDoS attacks which impact availability of data
6. **Type:** Software – Urban Platform
   Description: Urban Platform; an abstract collection of services and microservices. Within the infrastructure, an AI/ML module which consumes the telemetry data via KAFKA data streams is provided by separate microservices that can also utilize 3rd party on-demand platforms.
   Generic Threats:
   - False data injection
   - Excessive Data Exposure attacks

4.5 Data in transit or in use

There are two types of data in this scenario. The first one is Autonomous Vehicle Telemetry Data. Telemetry Data of the autonomous vehicle contains a broad range of data from odometry to AutoWare (Control Software) messages. This data is published in a ROSBag. An API will connect the vehicle telemetry to the Urban Platform. It is critical in nature.

The second type of data is AI/ML Training Data. It consists of data used by the Autonomous Vehicle Control System to train the AI/ML model for navigation in the smart city traffic environment. It is also critical.

4.6 Risk of the scenario

Considering all this, the repercussions of a successful attack are highly critical. The manipulation or false injection of the telemetry data and data used for ML model, which determines decision making for the Autonomous transportation will have a severe impact on the safety of the vehicle and passengers within the vehicle and in the driving environment.

4.7 IRIS platform involvement

IRIS can assist the scenario considering the following aspects:

Type: Identification
Description: The IRIS Platform will be able to identify actionable and accurate cyber threats against the availability of the autonomous transportation system and supporting infrastructure.

Partner's tool to use (optional): ATA Module

Type: Detection
Description: Assist CERT investigation and incident response, IRIS will enable autonomous detection and risk-based response for privacy breaches.

Partner's tool to use (optional): ATA Module, Enhanced MeliCERTes platform

Type: Detection
Description: Validate capabilities of IRIS's cybersecurity training platform as a learning tool for collaborative response to emergency incidents on autonomous transport.

Partner's tool to use (optional): VCR

4.8 IRIS platform benefits

The benefits expected of IRIS are the following:

- IRIS can **minimize impact of cyber threats** by identifying the threat, self-recovering from it and sharing the corresponding intelligence with other related system operators and platforms.
- By using the IRIS platform, system operators can effectively **identify when specially crafted data, designed to confuse AI-based decision making**, (e.g., spoofed/fuzzed) is received from onboard vehicle sensor, or injected directly to APIs using directly monitored data on targets systems or via it's unique Digital twin honeypots.
- Operators can then leverage IRIS to **self-recover from such malformed data injection**.
- IRIS platform can facilitate autonomous detection and risk-based response.

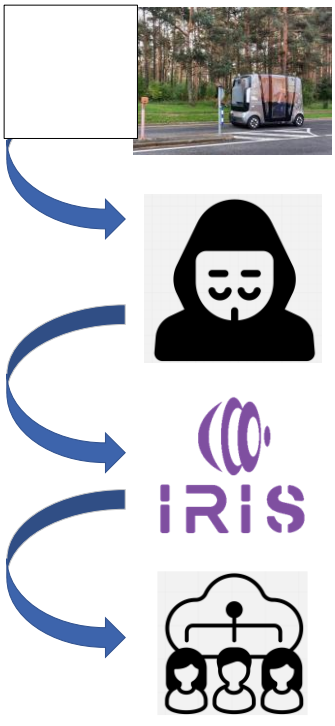
- IRIS's CTI provision will provide collaborative parties to **discover and share attack signatures** to respond to IoT and AI-targeted attack vectors.
- IRIS will provide CSIRTs/CERTs with the tools capable of identifying where an attack has breached, and exposed, large-scale private data.
- The IRIS platform has the capability to be used as a cybersecurity training platform and a learning tool for CSIRTs/CERTs.
- The IRIS platforms virtual cyber range can be used to establish mature CSIRT/CERT communities.

4.9 User story

This Tallinn Pilot-Use-Case scenario can be considered one predominant scenario divided into two distinct user stories, focused on two diverse cyber threats. The scenario focusses on an orchestrated attack against the AI enabled autonomous transportation infrastructure of the city of Tallinn.

4.9.1 User story 1

In this user story, the AV shuttle is navigating the smart city environment.



Autonomous Transportation System/Digital Twin generates telemetry which is used for teleoperation/remote control support and monitoring of journey in traffic environment. Telemetry is published to Urban Platform via API

Threat Actor Injects false data by targeting the API connectivity of the autonomous vehicle telematics systems and the Universal Platform.

IRIS ATA module is able identify actionable and accurate cyber threats against the availability of the autonomous transportation system and supporting infrastructure. Also, IRIS will assist CERT investigation and incident response, IRIS will enable autonomous detection and risk-based response for privacy breaches.

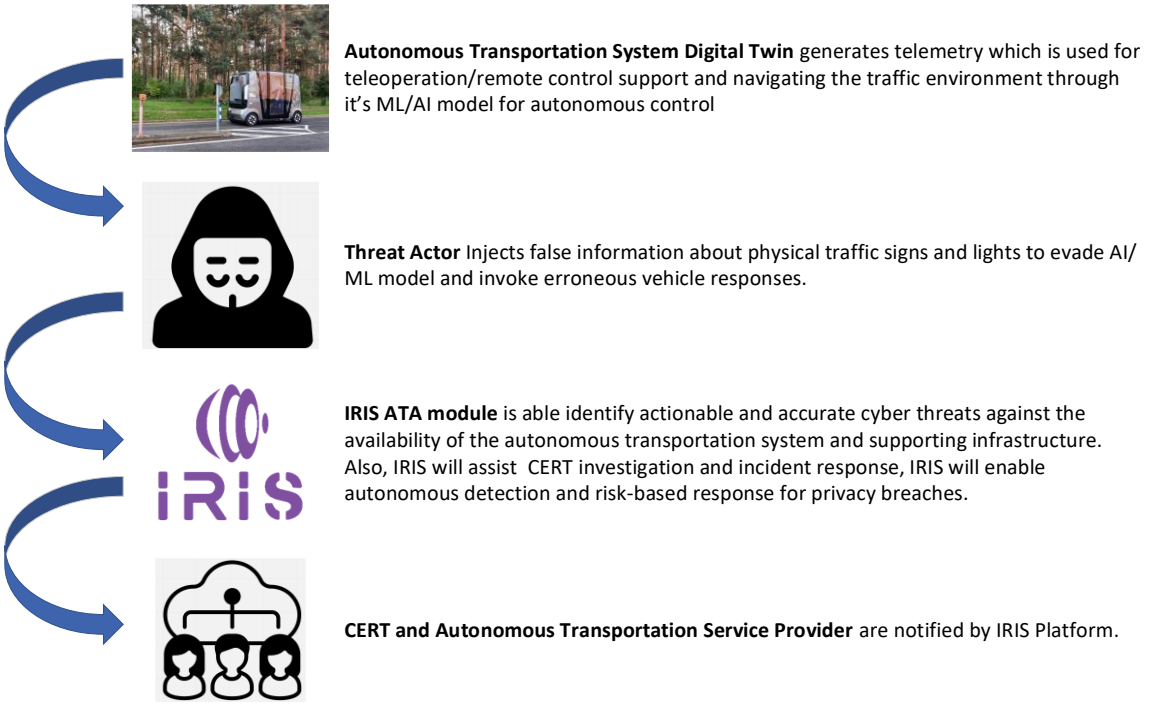
CERT and Autonomous Transportation Service Provider are notified by IRIS Platform.

During this journey, the AV shuttles collect passengers for transit to their final destination. During the operation, the AV shuttles are generating telemetry of the diverse sensors and cyber-physical devices which are processed by the Urban Platform and the Teleoperation/Remote Control. Cyber threat actors are motivated to disrupt the traffic flow

of the traffic environment to gain notoriety and exposure. The attackers disrupt the telemetric data of the AV Shuttle by targeting their API connectivity to the Universal Platform, by injecting false information (e.g., location data, bus cyber and physical sensor data) causing the Universal Platform to display false information. The false information on Universal Platforms results in diminishing the trust of the public towards the innovative city services and its AI technologies in general. The IRIS platform will identify the attack and enable the transportation service provider and CERT to perform incident response

4.9.2 User story 2

The story follows on from User Story 1. In User Story 2, the malicious cyber threat actors aim to vandalize and physically disrupt the AV Shuttles by feeding false information about physical traffic signs and lights (ML evasion attack).



The attackers carefully craft the data that is commonly collected from the vehicle's sensors to deceive its AI navigation modules, evade its model concept, to invoke erroneous decisions. As a result, several of the AV Shuttles will exhibit erratic behavior or will be totally immobilized in central locations. In the case of the ML-evasion attack on the AV Shuttles, a vulnerable ATA Digital Twin honeypot will be deployed to the system which mimics the data footprint and functionality including its AI components. The high-interaction Digital Twin will facilitate the collection of ML attack telemetry and demonstrate IRIS's ability to supply threat analytics for advanced IoT and AI attacks that can be used by systems to self-recover in real-time

5 PILOT USE CASE 3: SMARTGRID SYSTEM

Title: Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats

City: Helsinki

The energy market and its electric utilities can be affected by cyberattacks through the whole value chain, including threat impacts on the generation of electricity, transmission, distribution, and network. Integration of IoT/AI-powered ICT systems into the energy sector introduces benefits in managing electric utilities, but also introduces new vulnerabilities. And since the threat landscape is continuously increasing, it is required to better protect such systems and its elements.

The city of Helsinki has an established Smart Kalasatama eco-district, that meets most demanding standards in terms of energy efficiency as a sustainable city. Various intelligent energy systems work on Kalasatama's smart grid and its co-products. To support PUC3 Forum Virium Helsinki will use a technical infrastructure of one of the Smart Kalasatama buildings, consisting of various hardware and software components.

As it can be seen in Figure 8, PUC3 infrastructure is built up from various blocks. It includes a residential building block, consisting of energy meters, switches, KNX/IP modules connecting every apartment with the energy system. Another block is a server block, containing an Urban data platform (UoP) for data operations, visualizations, CIM operations etc. UoP will additionally be used to collect the data from the energy players and then mask it for further simulation of attacks.

Next, a data block, which represents the existing energy suppliers' data, including both Helsinki and Tallinn energy infrastructures. Lastly, an actor block showing PUC3 involved actors: Threat actor, DSO, and building residents.

The aim of PUC3 is following:

- To assess the ability of the IRIS platform to detect malicious information through its AI security mechanisms and mitigate the impact of the attack.
- Validate VCR's (Virtual Cyber Range) efficiency in educating CSIRTs/CERTs on the incident response for emerging and complex attacks on smart control systems.

Evaluate if IRIS will be able to monitor the interfaces of the smart grids and their automated decision-making processes.

5.1 Scenario overview

In the demonstration scenario the APIs and the public interface of the smart grids and their automated processes will be stress tested. During the demonstration, the public interfaces will consume environmental data to manage energy resources. The stress testing scenario will feed malformed data to the public interfaces and APIs to provoke

incorrect decisions from the automated systems of the smart grid, and the operators who rely on the system to report accurate energy demand for increasing and decreasing load. The IRIS platform will be able to detect the malicious information through its AI security mechanisms and mitigate the impact of the attack. Furthermore, IRIS will produce systematic threat intelligence that will be able to be consumed by the IRIS CTI module for improving threat data sets, as well as notifying stakeholders automatically of attacks that are occurring in near real-time. This demonstration will be emulated as a cross-border crisis management exercise on the Virtual Cyber Range (VCR), with Digital Twins of the target smart grid systems, as well as Digital Twin honeypots which will be introduced as a key capability of the IRIS ATA for deceptive threat analytics and detection of threats against dynamic IoT and AI systems. A VCR extension to the smart grid system will be introduced that enhances the ruled-based AI system of the existing system with a machine learning model capable of providing accurate and autonomous forecasting on energy use which directly decrease or increase in load provided to different buildings in the smart city. The VCR will educate CSIRTs/CERTs on incident response for emerging and complex attacks on intelligent ML-based AI extensions to a smart control system, which aim to disrupt the systems energy distribution with significant physical impact (e.g., blackout of affected buildings).

The overall technical scenario may be observed in the following figure.

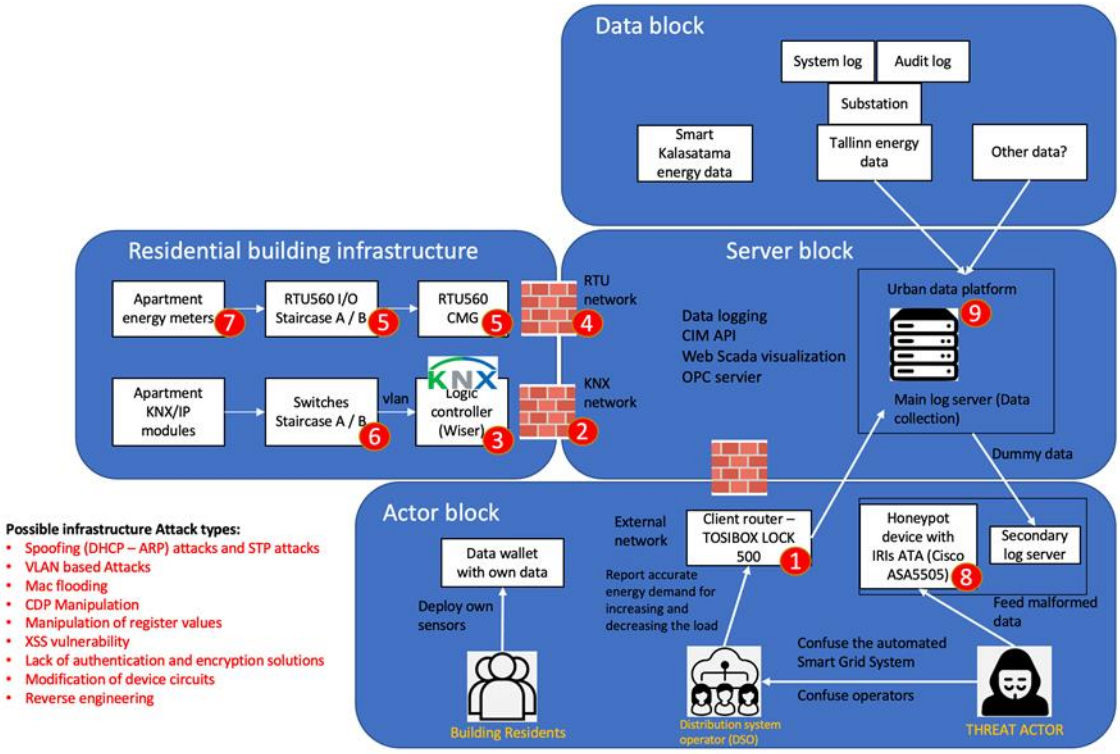


Figure 6. PUC3 Scenario Flow (Assets assigned with the number are described in "Technical assets" section)

5.2 Covered stakeholders' needs

This scenario aims to cover a few stakeholder's need. We have identified two types of stakeholders, **Distributed System Operators (DSO)** and **Building Residents**, meaning, the people living in the buildings. For DSO, it will help run load control functions safely by ensuring correct load decisions from the automated system and its operator. It will also help notify of possible intrusions into the system. In regards to the building residents, it will generate confidence of the safety of building data.

5.3 Involved actors

There are several actors in play in this scenario. In this case, stakeholders also act as actor for the scenario (DSO and building residents). A DSO directly reports the energy demand, controlling the building load. The Attack scenario is supposed to malform the data in the load system, therefore confusing the DSOs and the system behind the load control. Building residents might be an interested party in terms of security of personal data (especially in the data wallet) and may be directly affected in the event of an attack.

There is also a human and/or system or software threat actor, who can manipulate the localized information that smart buildings elicit from their environment to initiate cascading attacks to the smart grid. Finally, another software actor, the data wallet, stores personal data as a React application, allowing users to map their own sensors in the system.

5.4 Technical assets

The list of actively used assets by the testbed relevant to IRIS are the following:

1. **Type:** Hardware (External router – TOSIBOX LOCK500)
   Attack Surface:
   - Email spoofing.
   - Website and/or URL spoofing.
   - Caller ID spoofing.
   - Text message spoofing.
   - Man-in-the-middle attacks.
   - Extension spoofing.
   - IP spoofing.

   Description: Remote access and networking device that serves as an endpoint for secure remote connections. Devices connected to the Lock are securely accessed over the Internet and most LAN and WAN networks through an encrypted VPN connection.
2. **Type:** Networks (KNX network)
   Attack Surface:
   - Lack of authentication and encryption solutions in the protocol.

Description: KNX is a uniform, manufacturer-independent communication protocol for intelligently networking state-of-the-art home and building system technologies.

3. **Type:** Hardware (Logic controller – KNX wiser)
   Attack Surface: Manipulation of register values
   Description: KNX Wiser is used to visualize and control a complete Home Automation Solution in KNX and Modbus networks. Also used as:
   - Gateway to translate and enable communication between different products.
   - As an aggregator to stock, analyze, and send the data
   - As an event controller that sends email in case of issues
   - WEB SCADA visualization for PC and touch-devices
   - Cross-standard gateway between KNX and Modbus RTU/TCP
   - BACnet Server
4. **Type:** Networks (RTU network)
   Attack Surface: To be analyzed
   Description: A remote terminal unit (RTU) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.
5. **Type:** Hardware (RTU560 IO, RTU560 CMG)
   Attack Surface: To be Analyzed
   Description: RTU560 represents high-end network interfacing - offering maximum flexibility with the highest number of supported protocols for sub and host communications. Designed to handle the highly complex systems in grid automation and control interfacing. RTU560 connects to all kinds of IEDs, parallel I/Os, serial connected and communication via IEC 68150. All this real time data can then be transmitted to the central SCADA systems for critical actions.
6. **Type:** Hardware (Switches – Cisco)
   Attack Surface:
   - physical access to the switch
   - Spoofing (DHCP / ARP) attacks and STP attacks
   - VLAN Based Attacks
   - Mac flooding
   - CDP Manipulation

   Description: Switches are used to connect multiple devices on the same network within a building or campus.
7. **Type:** Sensors (Energy meters)
   Attack Surface:
   - hardware and firmware reverse engineering
   - modification of the control unit circuit board with one encompassing parasitic electronic components which would enable the attacker to remotely control the smart meter
   - physical access to the smart meter

8. **Type:** Hardware (Honeypot – Cisco ASA 5505)
   Attack Surface:
   - XSS vulnerability
   - physical access to the device

   Description: The Cisco ASA 5505 delivers high-performance firewall, SSL and IPsec VPN, and rich networking services in a modular, "plug-and-play" appliance.
9. **Type:** Software (UoP - Kafka instance)
   Attack Surface: To be analyzed
   Description: Used to set up Tallinn energy endpoint and the Smart Kalasatama one, ensuring the project reaches the cross-border perspective. There should also be a resource to make the meter data a dummy data to therefore get attacked by the threat actors.
10. **Type:** Hardware/Software/Sensors/Code/Networks/Databases/Other
    Attack Surface: To be analyzed

5.5 Data in transit or in use

The main type of data in transit in this scenario is energy data, which represents energy generator, distribution and consumption. It consists of an API that connects buildings to smart grid and electrical energy markets. The API should follow the IEC 61987 standard on Common Information Model and its communication should be secured with a Virtual Private Network.

5.6 Risk of the scenario

Since the stress testing scenario will feed malformed data to the public interfaces and APIs to provoke *incorrect decisions from the automated systems* of the smart grid, and the operators who rely on the system to report *accurate energy demand* for increasing and decreasing load, we are considering the scenario to be of the highest risk (critical).

5.7 IRIS platform involvement and benefits

There are three main ways in which the IRIS platform will be involved in this scenario. The IRIS platform will be able to detect the malicious information through its AI security mechanisms and mitigate the impact of the attack. It will integrate the ATA module in order to do so.

Also, by using Digital Twin honeypots which will be introduced as a key capability of the IRIS ATA for deceptive threat analytics and detection of threats against dynamic IoT and AI systems.

IRIS CTI will improve threat data sets, as well as notify stakeholders automatically of attacks that are occurring in near real-time.

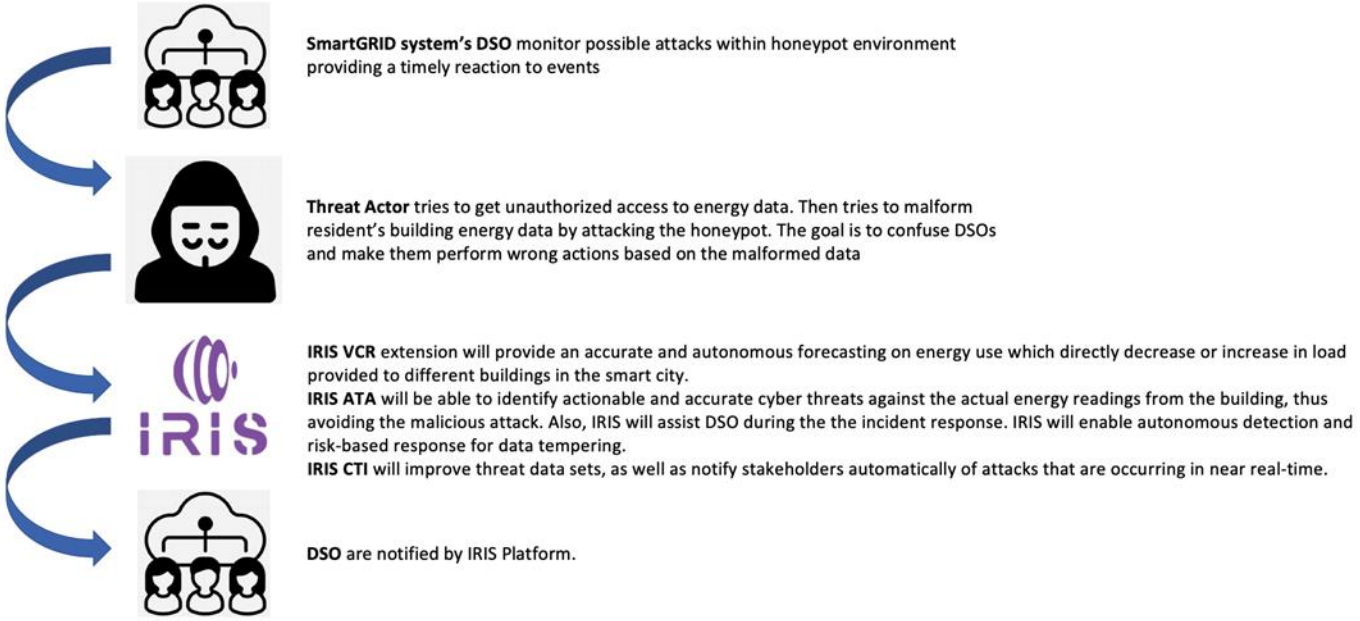
Lastly, there will be a cross-border exercise. The demonstration will be emulated as a cross-border crisis management exercise on the Virtual Cyber Range (VCR), with Digital Twins of the target smart grid systems. The VCR will educate CSIRTs/CERTs on incident response for emerging and complex attacks on intelligent ML-based AI extensions to a smart control system.

5.8 User story

This pilot use case is divided into three different user stories, focusing on three types of threat actors.

5.8.1 User story 1

The first threat actor is targeting the energy APIs by attacking the honeypot and malforming the energy data to confuse the DSO.



5.8.2 User story 2

The second threat actor is focused on targeting the system logs to clear threat actor's malicious activities and make DSO unaware of threat actor's intrusion.

This user story builds up on top of the previous one, in this case the final goal is to hide the logging system to avoid detection.

Threat actor tries to get an authorized access to the system/audit logs of the energy company by attacking the honeypot. The goal is to delete malicious activities of the threat actor from the system to therefore make DSO unaware of the intrusion.

SmartGRID system's DSO monitor possible attacks within honeypot environment providing a timely reaction to events

IRIS VCR extension will provide an accurate and autonomous forecasting on energy use which directly decrease or increase in load provided to different buildings in the smart city.
IRIS ATA will be able to identify actionable and accurate cyber threats against the actual energy readings from the building, thus avoiding the malicious attack. Also, IRIS will assist DSO during the the incident response. IRIS will enable autonomous detection and risk-based response for data tempering.
IRIS CTI will improve threat data sets, as well as notify stakeholders automatically of attacks that are occurring in near real-time.

DSO are notified by IRIS Platform.

5.8.3 User story 3

The third threat actor aims at malforming the energy meter data to therefore make wrong energy readings visible at the DSO system level.

Threat actor tries to get an authorized access to the energy meter logs of the residential building/appartments by attacking the honeypot. The task is to malform the energy meter data to therefore make wrong energy readings visible at the DSO system level. The goal is to be able to cut the final billing of the specific resident or group of residents.

SmartGRID system's DSO monitor possible attacks within honeypot environment providing a timely reaction to events

IRIS VCR extension will provide an accurate and autonomous forecasting on energy use which directly decrease or increase in load provided to different buildings in the smart city.
IRIS ATA will be able to identify actionable and accurate cyber threats against the actual energy readings from the building, thus avoiding the malicious attack. Also, IRIS will assist DSO during the the incident response. IRIS will enable autonomous detection and risk-based response for data tempering.
IRIS CTI will improve threat data sets, as well as notify stakeholders automatically of attacks that are occurring in near real-time.

DSO are notified by IRIS Platform.

6 STAKEHOLDERS FEEDBACK

To support continual improvement of the pilots´ scenario definitions and related use cases, a questionnaire was developed to help elicit stakeholders' feedback. The feedback assesses the usefulness and relevance of the different scenarios.

6.1 Stakeholders questionnaire

The goal of the questionnaire was to gather feedback from the stakeholders about the usefulness of the scenarios in the context of the IRIS project. This form was created and shared during the project dissemination activity in the SmartCity World Congress Expo in Barcelona from November 16th to November 18th, but also circulated among other stakeholders who could not join in the event due to the Covid-19 pandemic.

The questionnaire is composed by a set of questions divided into three different blocks:

- Introductory questions to set the contextual background of the stakeholder.
- Per PUC questions to assess the usefulness of the PUC related to IRIS.
- Closing questions to see potential collaborations and future steps with the stakeholder.

All the questions in the questionnaire were designed with two purposes: simplicity to answer and validation that IRIS is the proper platform to harden the security of the system and to assess its vulnerability.

6.1.1 Introductory questions

1. Company Name
2. Number of employees:
    a. Less than 10
    b. From 10 to 25
    c. From 25 to 100
    d. From 100 to 1000
    e. More than 1000

6.1.2 PUC particular questions

1. Which is your opinion concerning this use-case?
    a. It is very interesting, there are plenty of security concerns in such a scenario
    b. I do believe it is interesting but there are no security concerns
    c. I don't see the practical applicability of IRIS in such a scenario
    d. Other
2. Do you think the scenario is vulnerable to other type of attacks?
3. Which aspects of the use case would you improve? (Multichoice)
    a. Consider more attack vectors
    b. Provide more technical detail to be able to better assess the use-case
    c. Consider physical security

   d. Other
4. Would you involve another city infrastructure to the use case? (Short answer)
5. Do you think this scenario, once deployed, will be beneficial for the city?
   a. Yes, and there are no critical security risks
   b. Yes, but IRIS is critical to guarantee security
   c. Yes, but IRIS is not sufficient to guarantee security on such infrastructure
   d. Not at all
   e. Other
6. Provide a possible alternative use case for this Pilot

6.1.3 Final remarks

1. How could IRIS better help your organization?
2. Additional comments or suggestions

6.2 Questionnaire results

After showing the different questions, this section summarizes the current results, obtained after sharing the form with the different stakeholders.

6.2.1 Introductory questions

Due to privacy concerns we do not disclose in the questionnaire results the companies of the stakeholders. Nevertheless, with the obtained results we observe an interesting diversity in terms of company sizes:

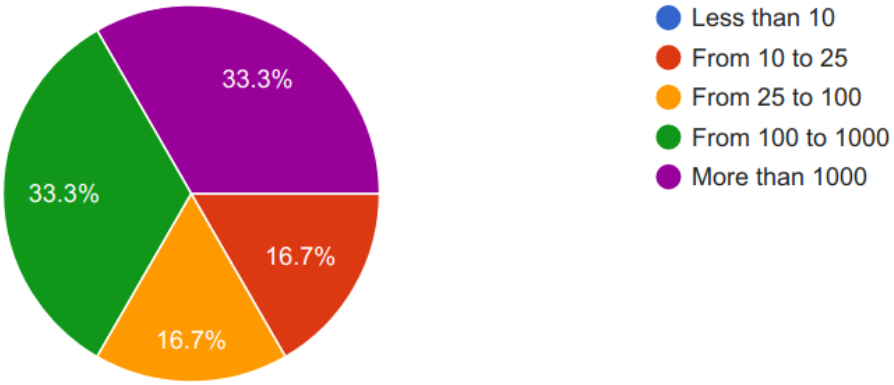


Figure 7. Distribution of number of employees for stakeholder companies

6.2.2 PUC 1 Questions

For the Barcelona scenario, we obtained the following results.

6.2.2.1 Question: Opinion regarding the use-case

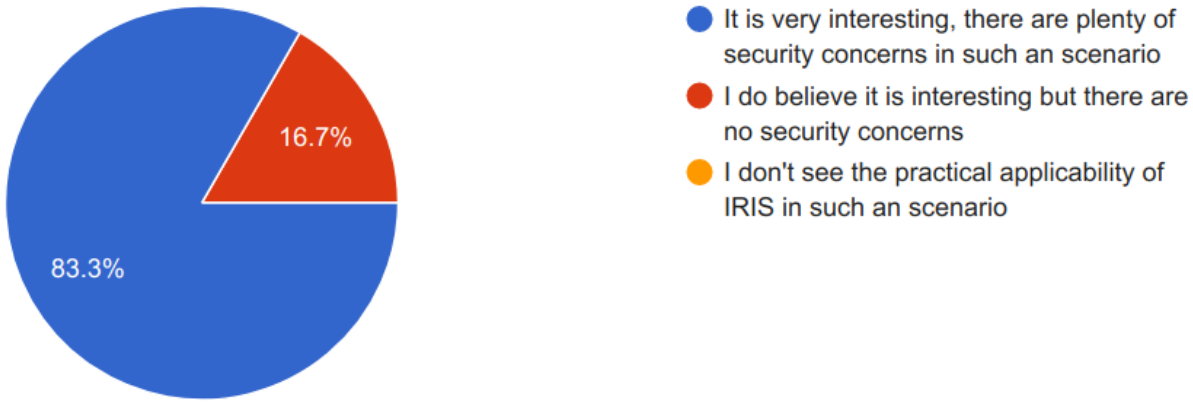


Figure 8. PUC1 - Opinion regarding use-case

The feedback related with the use-case is that it is a very interesting and challenging scenario, where security is paramount and needs to be closely monitored.

6.2.2.2 Question: Do you think the scenario is vulnerable to other type of attacks?

This open question led to concerns regarding DoS and DDoS or accessibility issues.

6.2.2.3 Question: Which aspects of the use case would you improve?

As it can be observed in the figure, the project needs to provide more technical information to stakeholders to better understand the scenario.

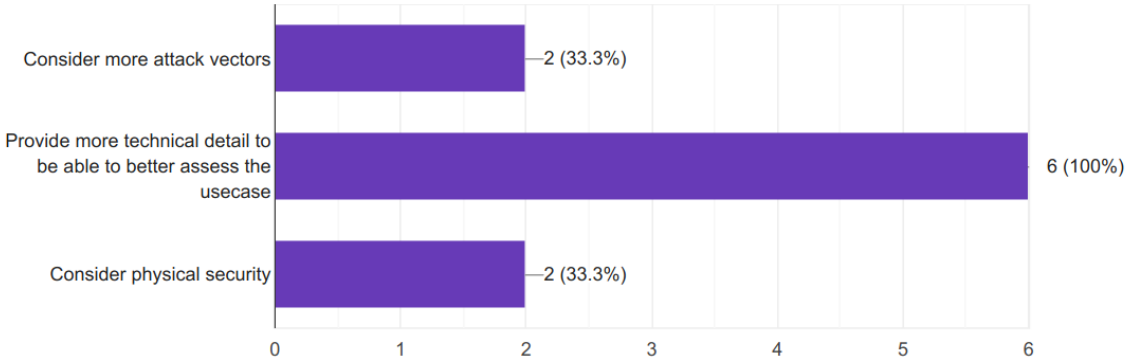


Figure 9. PUC1 - Aspects to improve regarding the use-case

To overcome this, we use this Deliverable as extra information regarding the PUC in particular. Another interesting issue is that a non-negligible amount of answers believe that having more attack vectors and physical security is important as well. We plan to tackle these issues in D2.2 onwards.

6.2.2.4 Question: Would you involve another city infrastructure to the use case?

The proposal in this case is to add Traffic Light system and other Public Transport infrastructure.

6.2.2.5 Question: Do you think this scenario, once deployed, will be beneficial for the city

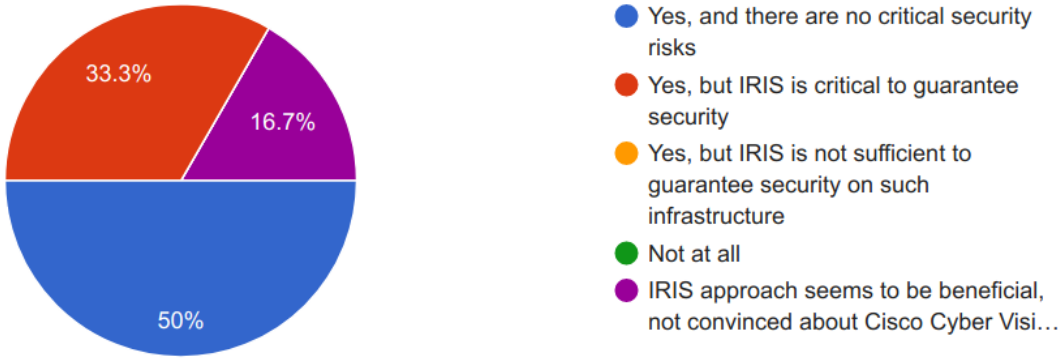


Figure 10. PUC1 - Will the scenario be beneficial for the city?

Most answers lead to believe that there will not be critical security issues. But a non-negligible number do believe IRIS approach is useful.

6.2.2.6 Question: Provide a possible alternative use case for this Pilot

No feedback was received for this question.

6.2.3 PUC 2 Questions

For the Tallinn scenario, we obtained the following results.

6.2.3.1 Question: Opinion regarding the use-case

In this case all stakeholders concurred stating that besides having a very interesting use-case, there are plenty of security issues with the scenario, as it covers autonomous vehicles, which in practice may signify issues with pedestrians, commuters and other actors within the use-case.

Figure 11. PUC2 - Opinion regarding use-case

6.2.3.2 Question: Do you think the scenario is vulnerable to other type of attacks?

In this case, the main feedback was the fact that such sensible infrastructure may be the target of plenty of attacks, from malicious actors to unsatisfied students, who want to disrupt the service.

Another relevant point was the concern raised by the possibility of attacks on integrity and availability of Control Operations Centre.

6.2.3.3 Question: Which aspects of the use case would you improve?

Consistently with PUC1, one of the main concerns to improve is the communication of the particular use-case technical information, as we show in the following figure.

However, as an important point is the consideration of other attack vectors, this highlights the fact that in this technology the use-cases affect directly to users of the platform, who are really concerned about safety during their trips using the service.

Surprisingly, in this case the consideration of physical security does not seem to be of great concern to the potential stakeholders.

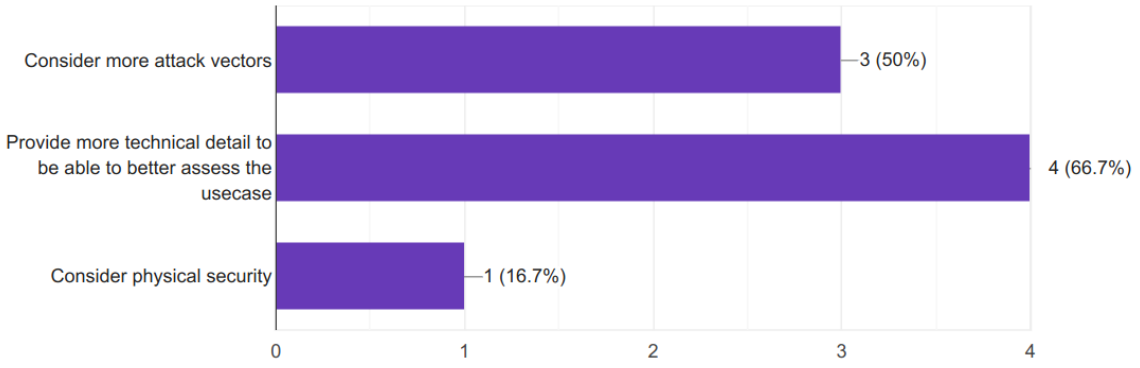


Figure 12. PUC2 - Aspects to improve regarding the use-case

6.2.3.4 Question: Would you involve another city infrastructure to the use case?

Most stakeholders do not think it is necessary to have another infrastructure from the city involved in the use-case. Despite of this, there is a part of the interviewees who believe that it would be interesting to involve other infrastructure such as:

- Traffic counting system
- City Public Transport
- Real-time traffic information systems, …

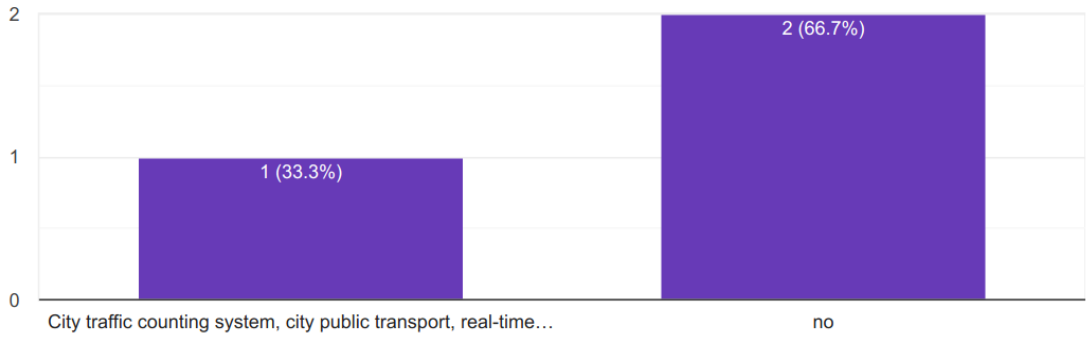


Figure 13. PUC2 - Other city infrastructure involvement

6.2.3.5 Question: Do you think this scenario, once deployed, will be beneficial for the city

Clearly, the answer to this question follows the logic that such infrastructure is very sensible to its users, as a misbehavior of the system may cause human injuries and a perception of potential insecurity, given how disruptive the use-case may be.

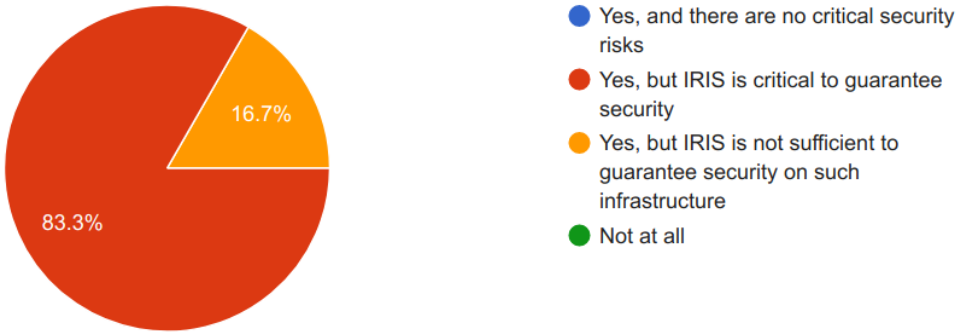


Figure 14. PUC2 - Will the scenario be beneficial for the city

6.2.3.6 Question: Provide a possible alternative use case for this Pilot

The main feedback in this case was in the direction that such infrastructure has plenty of collateral requirements which certainly make this use-case part of a bigger development. Such as:

- Ticketing system
- Fleet management
- Real-time tracking
- Timetables
- Vehicle battery management

Should be considered as well.

6.2.4 PUC 3 Questions

For the Helsinki scenario, we obtained the following results.

6.2.4.1 Question: Opinion regarding the use-case

Consistently with the rest of the use-cases, we can assess that the scenario is mainly regarded as an interesting infrastructure with enough security issues that justify the presence of IRIS to secure the environment.

Figure 15. PUC3 - Opinion regarding use-case

6.2.4.2 Question: Do you think the scenario is vulnerable to other types of attacks?

Most answers in this section assess that as a matter of fact they do believe the scenario is vulnerable to other types of attacks, but without specifying which. Despite of this, some answers hint the analysis to go into areas such as supply chain attack of malicious own sensors.

6.2.4.3 Question: Which aspects of the use case would you improve?

As it can be observed in the figure, we have to provide a better understanding of the technical details to allow the stakeholders to provide a more specific contribution to the use-case. As we discussed before, we will use this deliverable as a mechanism to perform this task.

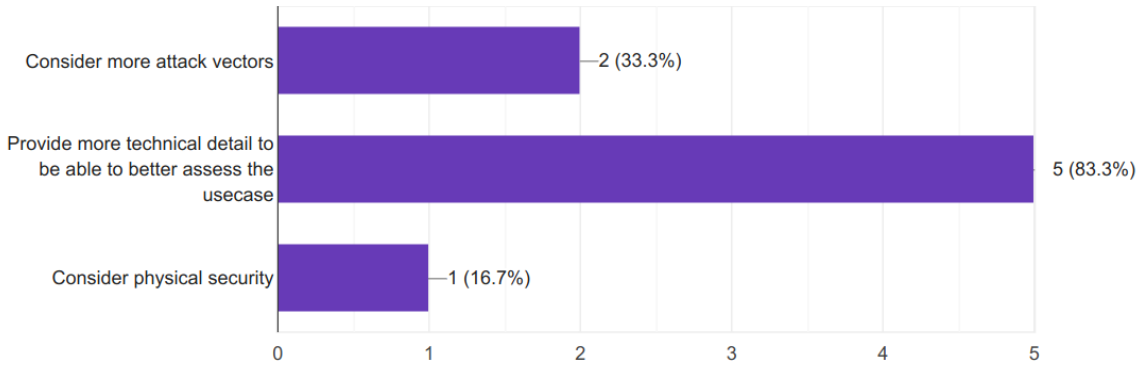


Figure 16. PUC3 - Aspects to improve regarding the use-case

6.2.4.4 Question: Would you involve another city infrastructure to the use case?

Most feedback in this case deemed unnecessary to involve other infrastructures to the use-case, as it may be enough as it is. Even in this case, there are some stakeholders who, consistently enough, believe that they need more information to be able to answer the question.

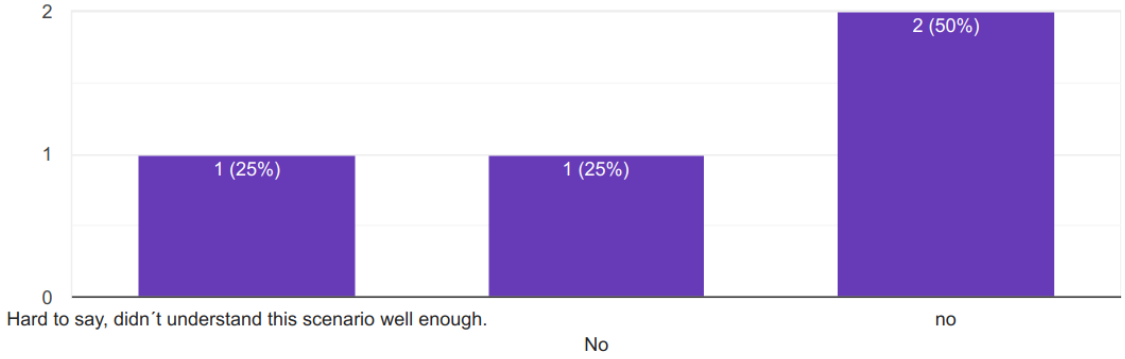


Figure 17. PUC3 - Other city infrastructure involvement

6.2.4.5 Question: Do you think this scenario, once deployed, will be beneficial for the city

Most of the stakeholders believe that IRIS will provide a better security and a better experience to the end-users. Opposed to that there are some of the stakeholders who think that in this case there are neither benefits nor security concerns in such local infrastructure.

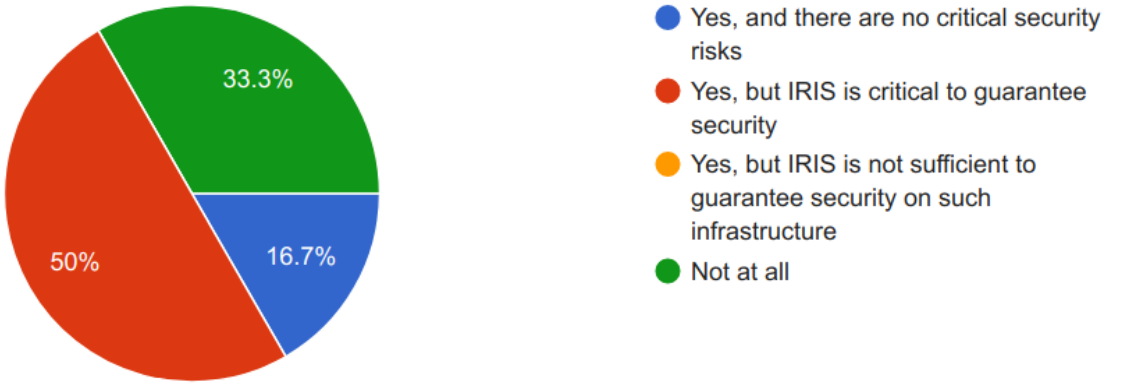


Figure 18. PUC3 - Will the scenario be beneficial for the city

6.2.4.6 Question: Provide a possible alternative use case for this Pilot

With this answer we understood that we should provide better understanding of this pilot to make it more self-explanatory for the stakeholders, as no feedback was received to do so.

6.2.5 Final remarks

6.2.5.1 Question: How could IRIS better help your organization?

Some stakeholders answered asking for more information, while others think IRIS would be beneficial to them in OT security of warehouses and other infrastructure. Others believe that IRIS would allow them to be more prepared to possible future attacks.

7 IRIS FEATURES COVERED BY USE CASES

As we have seen, the three pilots provide three diverse environments where to validate different features present on the IRIS solution. In this section, we enumerate the most relevant aspects of the IRIS platform and which Pilot provides the best environment to test and validate them. It is important to notice that we consider detection features but also mitigation which completes the aspects covered by the IRIS platform.

The following table summarizes the IRIS features mapped to the different pilots. As we can see, the table is composed by four columns, the first one with the feature and the other three with the pilots which allow the system to test the particular feature.

IRIS Features	PUC1	PUC2	PUC3
Incident management regarding cyberthreats to confidentiality	x		
Incident management regarding cyberthreats to availability	x	x	
Incident management regarding cyberthreats to integrity		x	x
Automated system processing orchestration workflows	x	x	x
Configuration of response policies and semi-automated (human in the loop) response workflows	x		
IoT & AI-Provision Risk & Vulnerability Assessment	x	x	
Autonomous AI threat analytics and detection engine	x	x	
Risk-based Response & Self-Recovery	x	x	x
Digital Twin Honeypot Telemetry & Analytics		x	x
Collaborative Threat Intelligence Sharing and Storage	x	x	x
Advanced threat intelligence and analytics orchestrator	x	x	x
DLT-based accountability, auditing and traceability		x	x
Advanced real-time data protection and recovery		x	x
Training and cybersecurity exercises (for technical staff)			x
Customized SIEM dashboards and information visualization	x	x	x
Role-based access management with governance and information sharing policies	x	x	x
Stakeholder community's online collaboration and communication	x	x	x

The table shows how IRIS' pilots provide a suitable demonstration and evaluation environment, with an adequate balance between completeness and focus, where all IRIS features may be demonstrated, evaluated, and thus validated.

8 CONCLUSIONS

In this deliverable we have provided detailed descriptions of the three different project use cases which we will use as demonstrators and platform validators for the IRIS platform. The pilots are deployed into three European smart cities, namely, Barcelona, Tallinn, and Helsinki.

In PUC1, focused in Barcelona, the aim is to provide a Tramway and bicycle alerting system based on smart cameras (Cyber vision) which detect potentially dangerous situations for bicycles and pedestrians passing nearby the Tramway. IRIS will assess and detect the vulnerabilities for such a system.

Regarding PUC2, it will be centered in the analysis of the security of the autonomous transportation system. In particular, IRIS will provide the means to analyze and study the security of the system for orchestrated attacks.

Finally, in PUC3, the focus will be on the Smart Grid system. Specifically, on the stress test of the automated processes and the cross-border threat analysis. Where IRIS will provide security hardening for the public API and detection of malformed data potentially introduced by a malicious actor.

In this deliverable we have defined all the use cases, identified the different actors, the risks of the platform, and IRIS benefits and role for each PUC. These definitions will be used as a starting point for continual development and testing during the project.

To complement the definitions, the scenarios and use cases were validated by external stakeholders, using a questionnaire to assess their usefulness and relevance.

REFERENCES

[1] H2020 - Paving the Way for Next-Generation Edge Computing (PLEDGER) - http://www.pledger-project.eu/

[2] H2020 – A Software Architecture for Extreme-Scale Big Data Analytics in Fog Computing Ecosystems (ELASTIC) - https://elastic-project.eu/

[3] Nai-Fovino, I., Neisse, R., Hernandez-Ramos, J.L., et. al., *"A Proposal for a European Cybersecurity Taxonomy"*, JCR Technical Reports – European commission, 2019

[4] Software Extension to the PMBOK Guide Fifth Edition, PMI – Project Management Institute, 2013