Artificial Intelligence Threat Reporting & Incidence report System

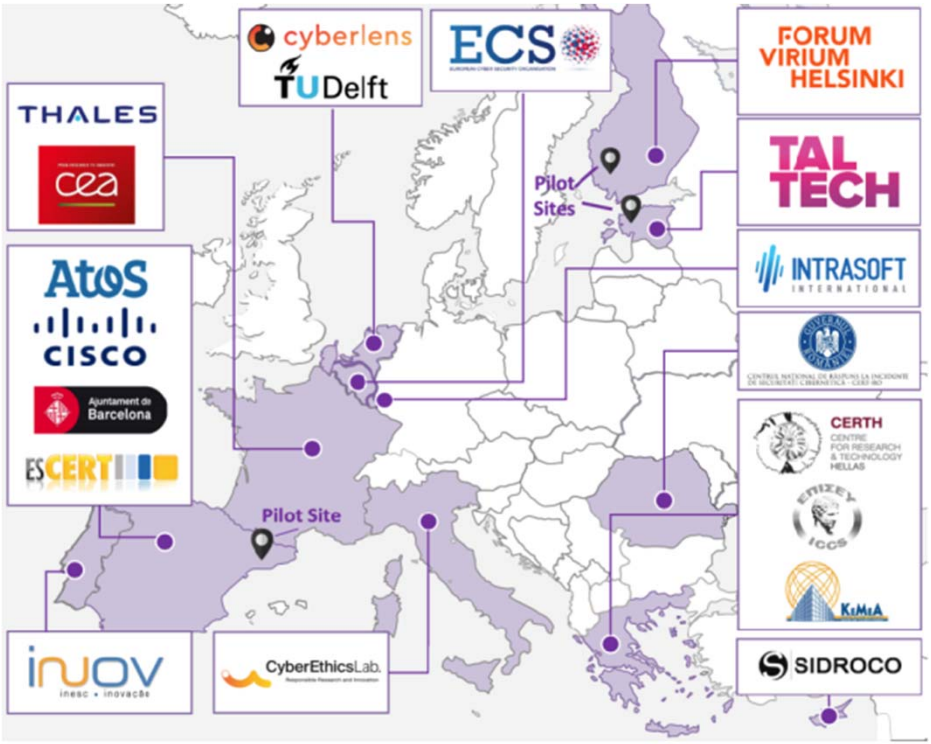
IRIS Project Presentation

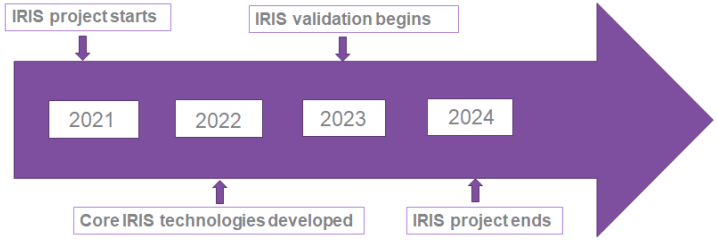
Mobile World Congress 2022

Gustavo González(ATOS)
Rodrigo Diaz (ATOS)
Xavier Azemar (Cisco)
Mariano Lamarca (IMI)
René Serral (UPC)

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

Project at a Glance





Call Identifier: 2020-SU-DS-2020

Topic: SU-DS02-2020 Intelligent security and privacy management

EC Funding: 4 918 790.00

Duration: 36 months (Sept 2021-Aug 2024)

Consortium: 19 partners

Coordinator: INOV - Instituto de Engenharia de Sistemas e Computadores, Inovacão, (INOV), Portugal

Learn More: www. iris-h2020.eu

Join us: @iris-h2020

IRIS H2020 Project

Consortium

- **6 Public organizations**
- **3 SMEs**
- **4 Large ICT industries**
- **6 Research institutions & Universities**

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

IRIS Motivation

As existing and emerging **smart cities** continue to **expand their IoT and AI-enabled platforms**, **novel and complex dimensions to the threat intelligence landscape are introduced**. These, are linked with identifying, responding and sharing data related to attack vectors, based on emerging IoT and AI technologies, whose architecture and behaviour are **not currently well understood** by security practitioners, such as CERTs and CSIRTs.

This lack of experience as well as of tools, for detecting and reporting IoT & AI attack vectors is further aggravated by potentially greater safety risks caused by such attacks.

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

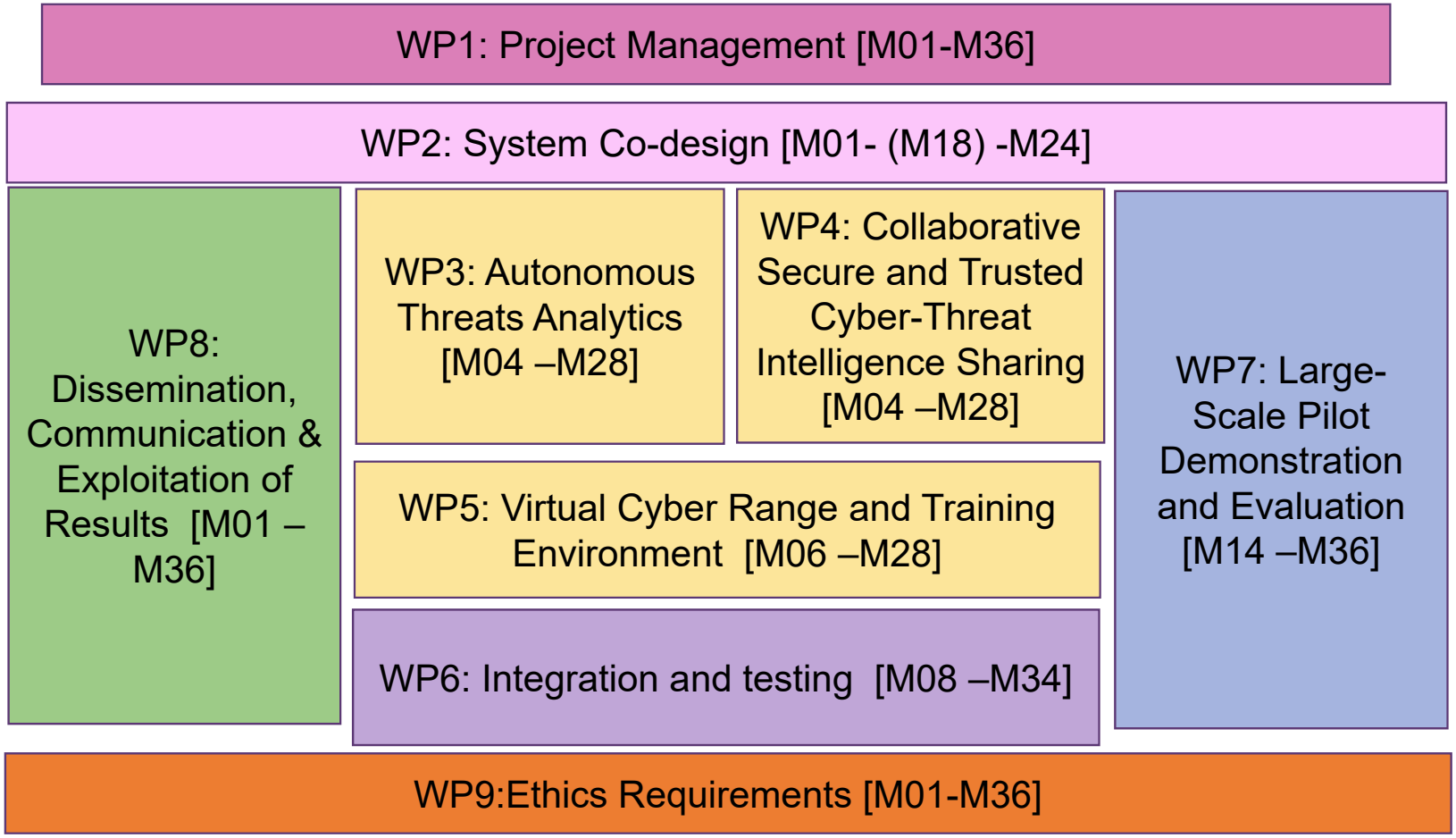
IRIS Vision

The **H2020 IRIS project** aims to deliver a framework that will support European CERT and CSIRT networks **detecting, sharing, responding and recovering from cybersecurity threats and vulnerabilities of IoT and AI-driven ICT systems,** in order to **minimize the impact of cybersecurity and privacy risks.**

The IRIS platform will be made available, **free of charge**, to the European national CERT and CSIRTs, by the end of the project.

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

IRIS Work Packages



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

IRIS Methodology

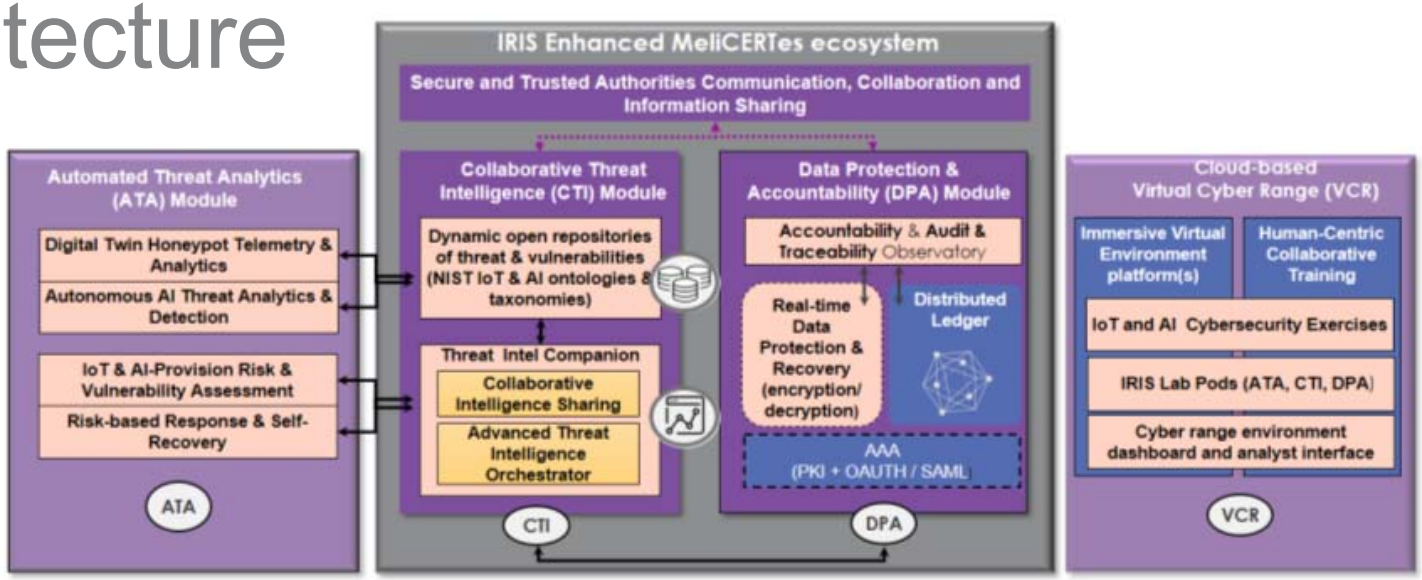
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

- To **identify** the user, technical and business requirements and **design** the architecture of an AI threat reporting and incident response system
- To **analyze** the relevant ethics principles and legal framework on privacy concerns
- To **develop** a collaborative platform for ICT stakeholders and European CERTs/CSIRTs for the successful operation of IoT and AI-enabled ICT systems
- To **demonstrate** and **validate** the integrated IRIS platform across three realistic pilot demonstrators in three smart cities
- To **ensure** wide communication and scientific dissemination of the IRIS results, efficient exploitation and contribution to relevant standardization bodies

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

IRIS Architecture



- **Collaborative Threat Intelligence (CTI)** that introduces Analytics Orchestration for supervising coordination between incident response and recovery;
  - an **Open Threat Intelligence** interface for disseminating taxonomies of IoT and AI threats;
  - intuitive **Threat Intelligence Companion** that serves as a key human-in-the-loop interface for collaborative incident response and threat intelligence sharing between CERTs/CSIRTs.
- **Automated Threat Analytics (ATA)** that extends existing intrusion detection tools with a novel threat detection engine for identifying specific IoT and AI attack vectors and includes digital twin honeypots for collecting attack telemetry against end-user systems reliant on these technologies.
- **Virtual Cyber Range** for collaborative CERT/CSIRT training exercises based on real-world environment platforms, providing representative adversarial IoT & AI threat intelligence scenarios.

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

IRIS

Artificial Intelligence Threat Reporting & Incidence report System

Tallinn Pilot Use Case

FinEst Centre
for Smart Cities

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

AI Enabled Infrastructure - Transportation

- Autonomous Vehicle Shuttles for Public Transportation
- Vehicle-to-Everything (V2X) Communication
- Teleoperation/Remote Control Operations Center
- Autonomous Vehicle Telemetry and Smart City Data fused into Urban Operating Platform (UoP)

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

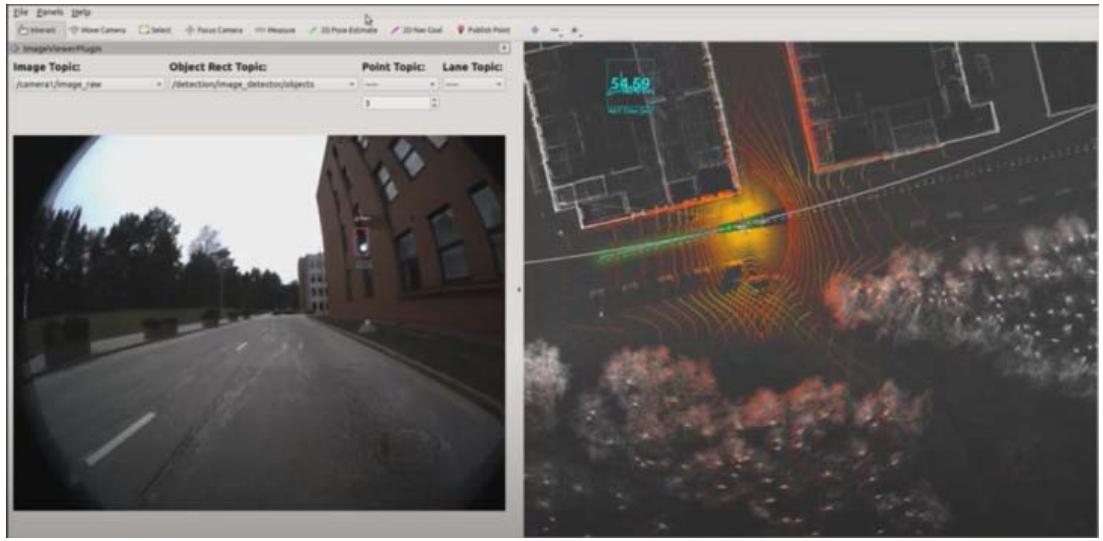
Scenario 1: Telematics and Smart City Data Exchange & Security

- The Autonomous Vehicle (AV) Shuttle fleet will navigate around the smart campus environment
- Urban Operating Platform (UoP) gathers AV Shuttle telemetry
- UoP stores
  - ✓ Location of the vehicles
  - ✓ Navigation
  - ✓ Odometry
  - ✓ …

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

Scenario 2: Trustworthiness of Machine Vision Telemetry

- The Autonomous Vehicle (AV) approaches a traffic-light controlled intersection or roadway
- The machine vision of the AV focusses on the traffic light
- The AV object-detection module detects the traffic light color
- Depending on the traffic light the AV will pass-through or stop



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

Cybersecurity importance

- The safety and security of passenger of Autonomous Vehicles
- Reputation and credibility of autonomous driving

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

Cybersecurity Challenges

- Ensuring availability of data and the operations of autonomous vehicle and supporting infrastructure.
- Lack of investigation of cyber defence mechanisms that facilitate autonomous detection and risk-based response for privacy breaches.

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

Tallinn Pilot Cyber Threat Scenarios

- Availability of telemetric data from the AV to the Urban Operating Platform (UoP)
- False information being fed to disrupt the ML/AI used for autonomous driving

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

Tallinn Pilot – IRIS Platform Validation

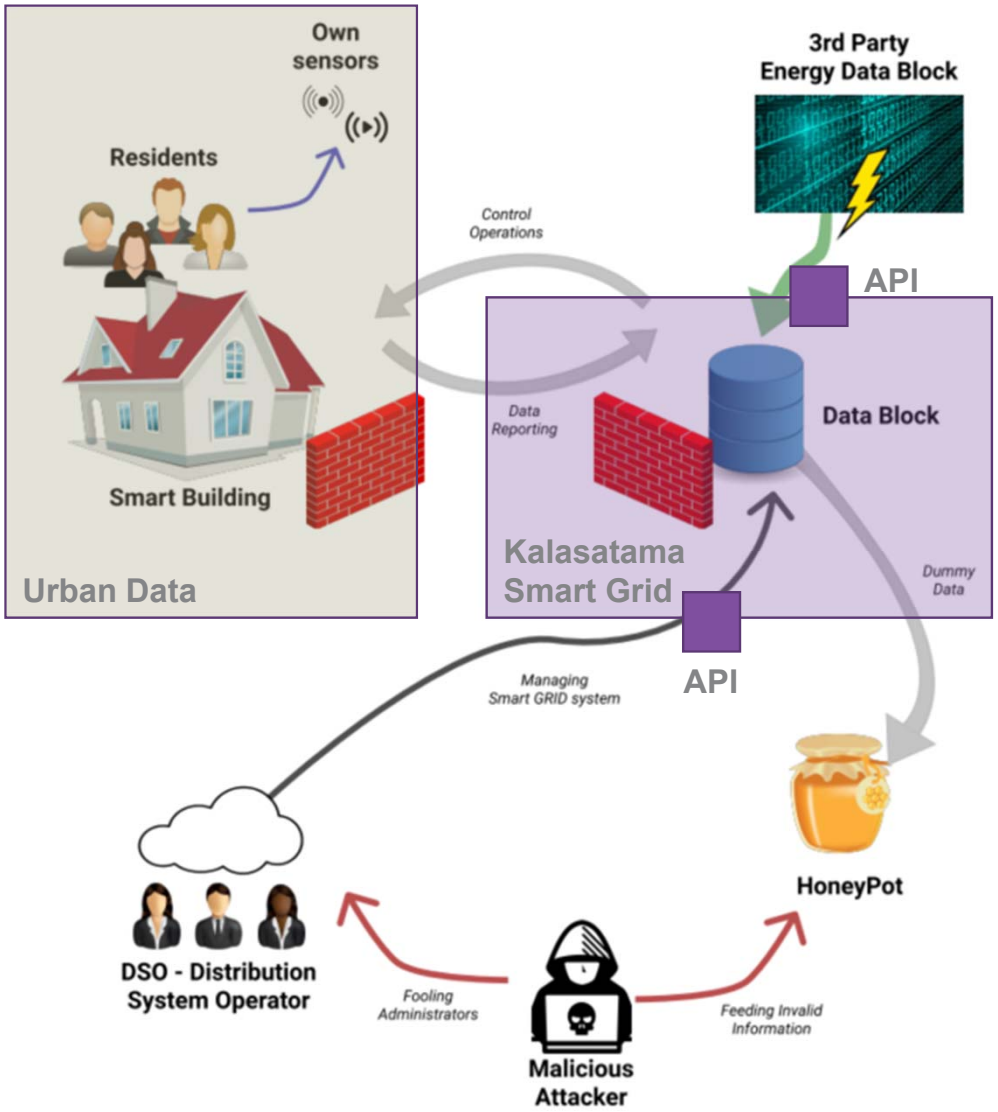
- Identification
- Self-Healing
- Information Sharing
- Enable Cyber Incident Response from CERTS/CSIRTS

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

Artificial Intelligence Threat Reporting & Incidence report System

Helsinki Pilot Use-Case

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



Components

- **Kalasatama smart grid** - enabling real time smart metering, electric vehicles network and new storage solutions for electricity.
- **Kalasatama smart grid APIs** (Environmental data to manage energy resources.)
- Kalasatama smart district **Digital Twin**.
- Provision of **load control functions** that the distribution system operator (DSO) can use in situations where the production has reached its peak.
- **Urban Data Platform**, a smart city data platform. *Modular IOT platform. Real-time data on urban environments.*
- **Smart grid APIs** from the city of Tallinn.

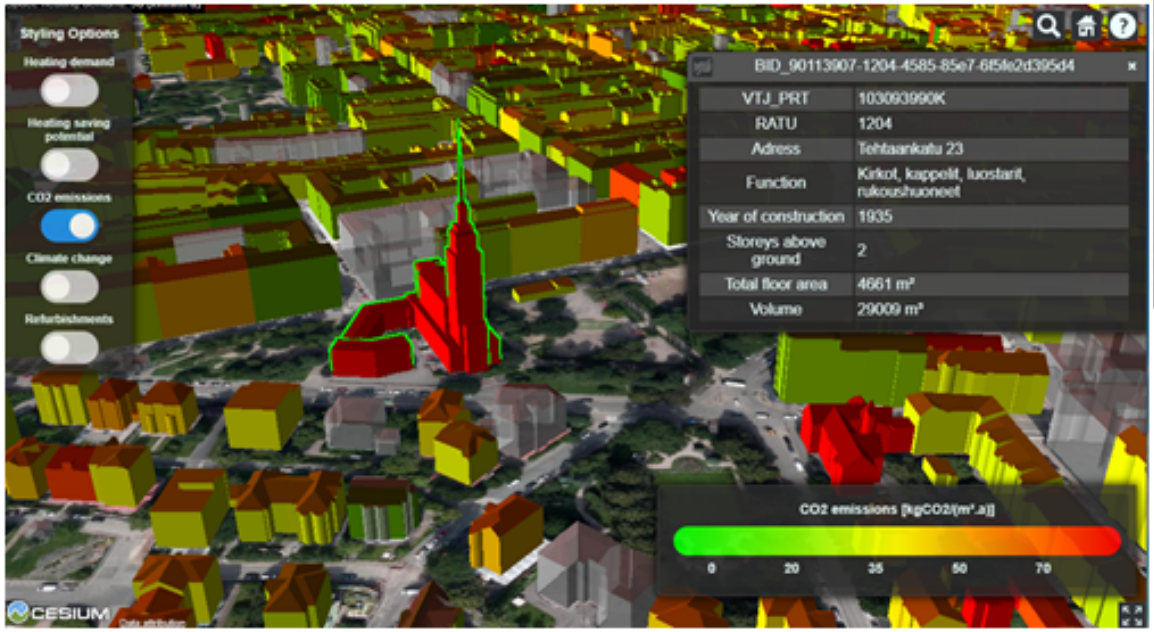
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

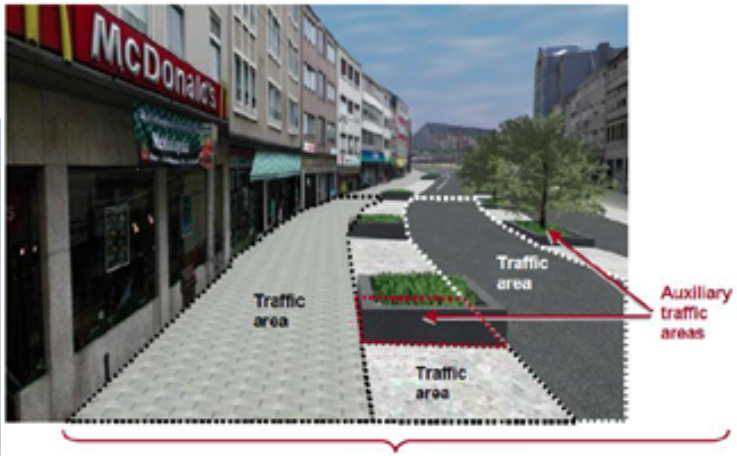
Smart Kalasatama Data Examples

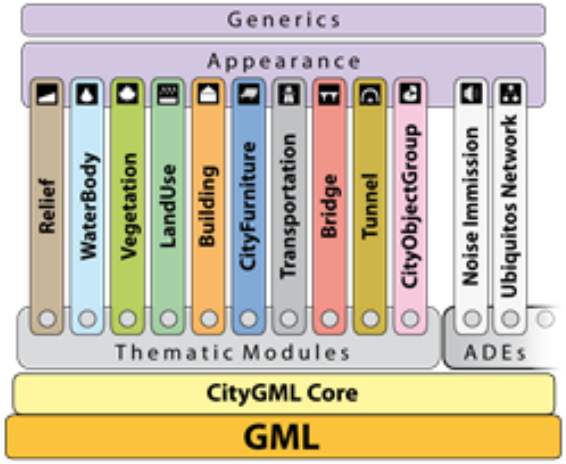
- Solar Energy Potential
  - ✓Amount of solar radiation in buildings
- Heating Demand Prediction
  - ✓Heating energy demand prediction until 2050
- Geoenergy Potential
  - ✓150m / 300m / 1000m deep well potentials, groundwater areas, ...
- Energy Data of Buildings
  - ✓Municipal registre information (e.g., heating method of buildings, usage, ...)
  - ✓Repairs and alterations
  - ✓Protected buildings
  - ✓Calculated energy consumption of buildings by age group

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

Digital Twin





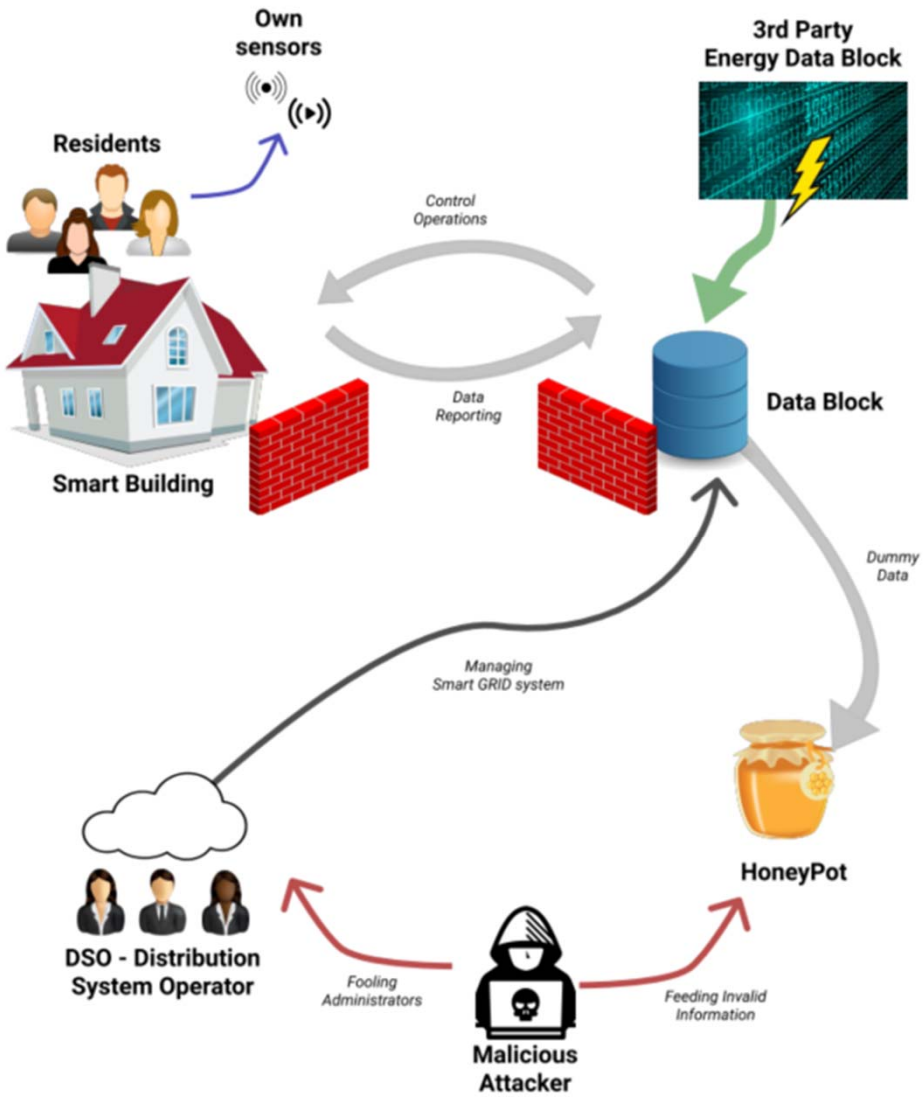


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Cybersecurity Challenge

- Effective incident response and threat intelligence collaboration for critical cross-border smart grid threats
- Customer facing components securing
  - ✓Against threats to control functions defined for the demand control
- API securing
  - ✓Smart Grid API from Kalasatama
  - ✓Smart grid APIs from the city of Tallinn.

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



Stakeholders to consider

- **DSO (Distribution system operator)**
  - Reporting of the energy demand, controlling the building load
  - Attack scenario to modify data in the load system
- **Building Residents**
  - Data wallets of personal data as a React application
  - Users with own sensors
- **CERTs/CSIRTs**
  - Feedback on handling and forecasting security incidents, complex attacks and propagated vulnerabilities in IoT and AI-driven ICT systems.

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

Helsinki – IRIS Platform Validation

- Detect the malicious information through its AI security mechanisms
- Attack impact mitigation
- Produce and publish systematic threat intelligence
  - ✓ Consumed by IRIS CTI for improving threat datasets
  - ✓ Offer this information to the different CERTS
- Notify automatically stakeholders about ongoing attacks

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

Artificial Intelligence Threat Reporting & Incidence report System

IRIS Barcelona Use Case

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

ABOUT BARCELONA TESTBED

Our Urban Model. Superblocks & Smart Services

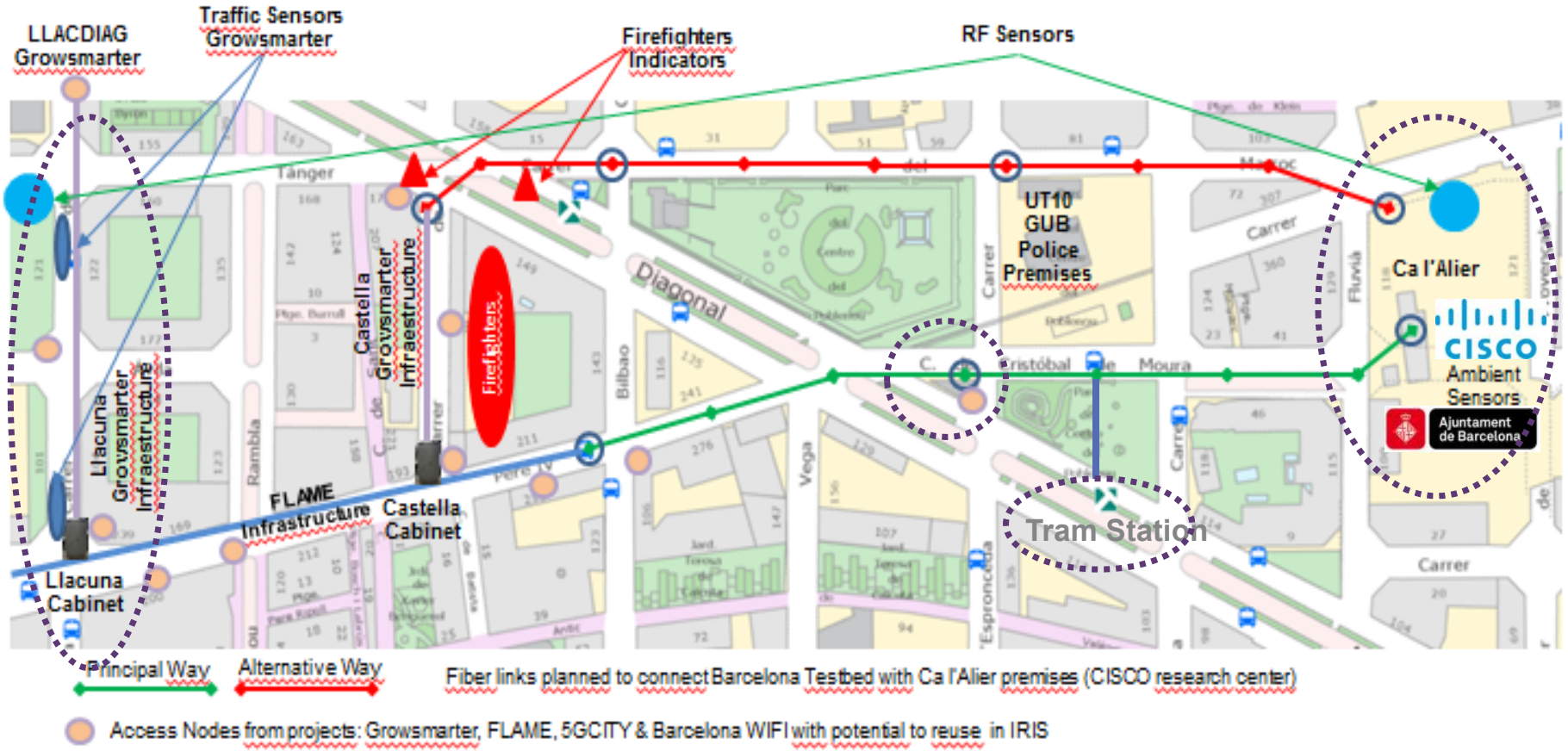
The superblocks are defined theoretically as an "area of urban organization, from which a series of structured transformation strategies towards a new urban model, where mobility and reorganization of public space represent the first step". Challenge is concentrate 95% services inside superblock, as a direct consequence Inside the superblocks the traffic and the environmental pollution (noise and gas) are reduced.

Each Superblock is based on a combination of City user services (US). Each US is composed by elements (Basic City Services). These Basic Services Will Be standardized worldwide thinking in superblock units.

IRIS will establish a model for security integration in ICT public space infrastructure over Superblock Urbanistic Model

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

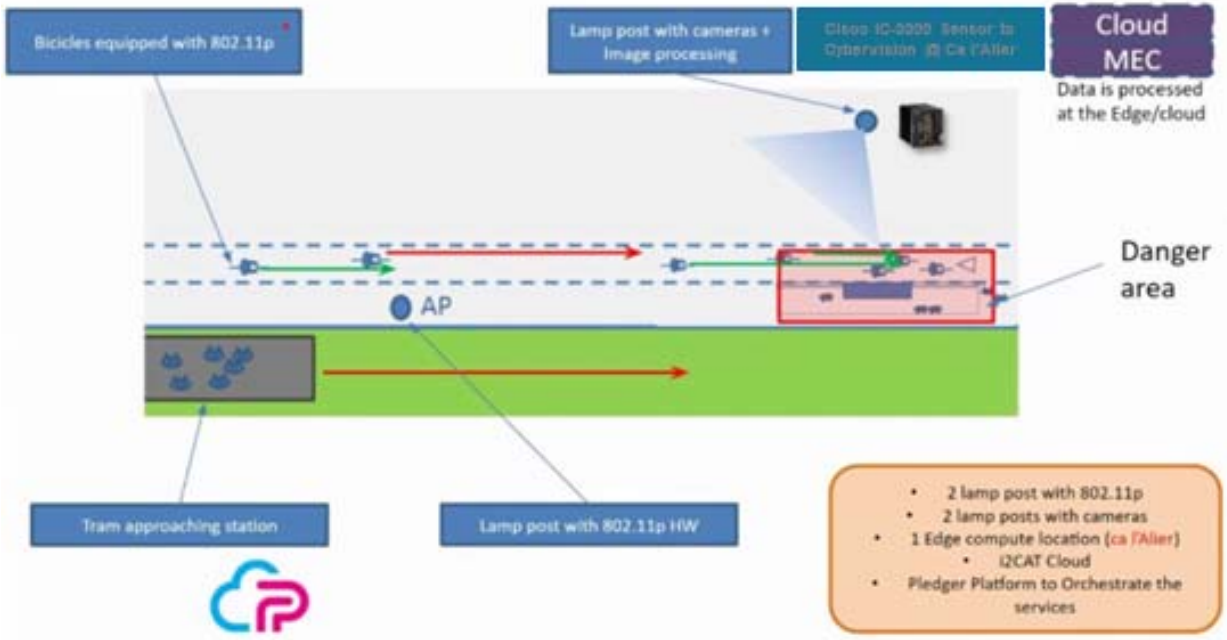
Integration of IRIS initiative in 5GBarcelona Testbed



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

Smart Cities Service: Vulnerable Road Users (VRUs) Protection

- VRUs (Bicicles/E-Scooters + pedestrians) are exposed to dangerous situations, when people exiting the tram at a station cross the bicycle lane to get to the pedestrian lane.
- With 802.11p to detect bicycles and image processing to detect the tram, possible risky situations are detected and notifications are sent out to warn the different actors.



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

Cybersecurity Challenges

- Ensuring availability of IoT and IA infrastructure for the safety of tram users.

- Lack of experience as well as of tools, for detecting and reporting IoT & AI attack vectors.

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

AI & IoT Infrastructure

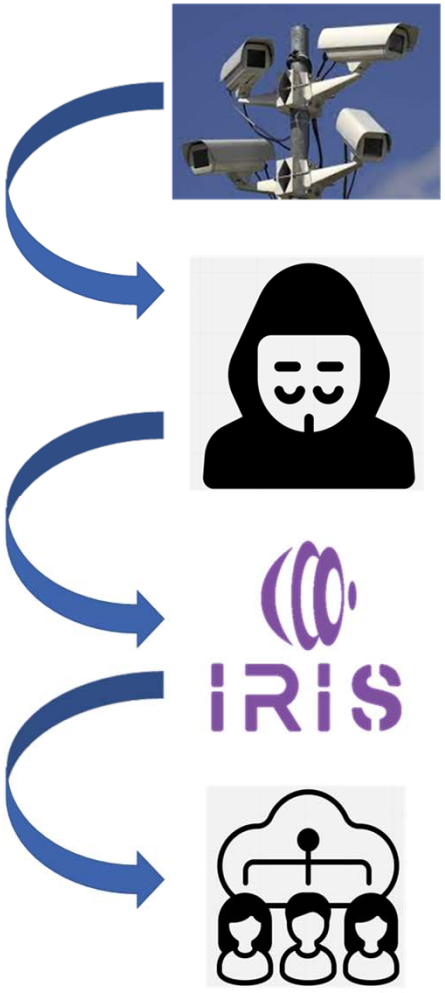
Leveraging Infrastructure of Horizon 2020 Project Pledger

IoT & AI attack vectors

- 801.11p Wireless devices
- Networking equipment routers and switches
- Edge computing
- Cameras
- AI computer vision

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

Cyber Threat Scenarios



On-Street cameras generate information about the intersection status. This information is used by Tramway operators to control (allow/disallow) the Tramway. This information is shared through an API.

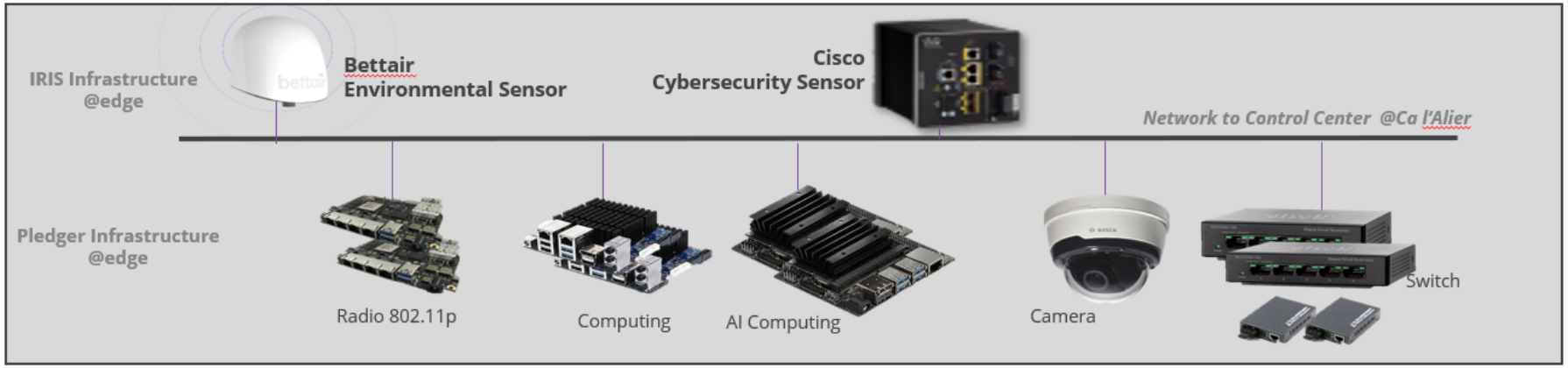
Threat Actor Injects fake data by targeting the different hardware appliances in the scenario with the goal of either denying the service, thus forcefully stopping the Tramway, or faking the presence of a possible pedestrian or bicycle approaching the intersection.

IRIS ATA module is able identify actionable and accurate cyber threats against the availability of the supporting infrastructure.
Also, IRIS will assist CERT investigation and incident response through the **CTI module**, Sharing the information about the attacks and security breaches.

CERT and Tramway operators are notified by IRIS Platform.

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

AI & IoT Infrastructure + cybersecurity and environmental sensors



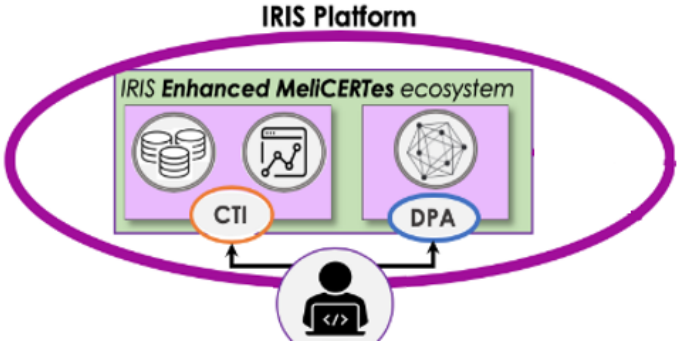
Cybersecurity Sensor and Control Center (CyberVision) → **Automated Threat Analytics (ATA)** → **Cyber-Threat Intelligence (CTI)** → **CERT**

Cybersecurity Sensor uses DPI technology to extract meaningful information (data & metadata) for the network devices using 100% passive sensor. Information is sent to **CyberVision Control Center** and reported to **IRIS Automated Threat Analytics (ATA)** module that extends existing intrusion detection tools to identify specific IoT and AI attack vectors, then shared through **IRIS Collaborative Secure and Trusted Cyber-Threat Intelligence (CTI)**

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

Connecting to IRIS Autonomous Threat Analytics (ATA) and Cyber-Threat Intelligence Sharing (CTI)

- Syslog UDP, TCP, TLS - RFC3164
- REST API
  i.e /api/3.0/dashboard/events/severities

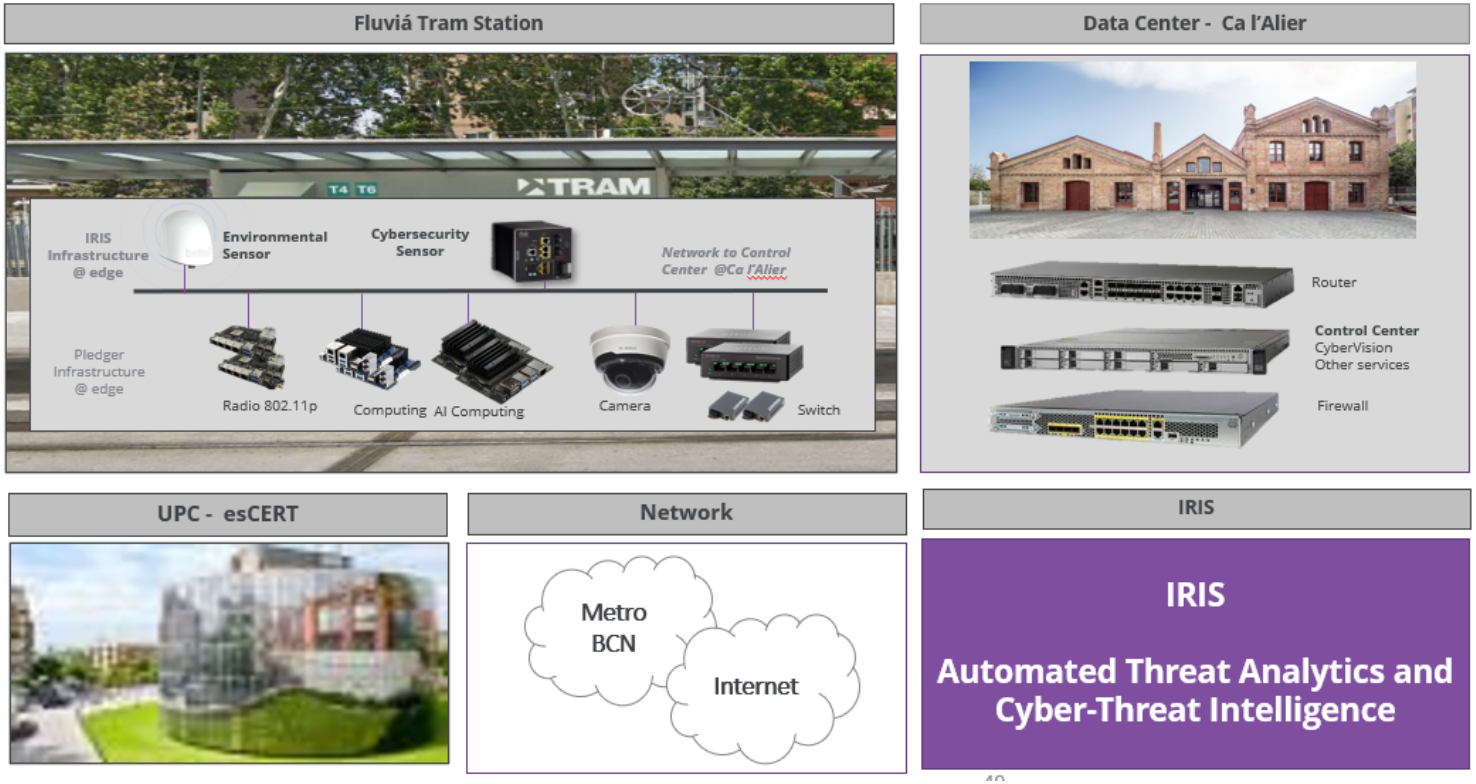



```
events: [
  {id: "63886854-d029-5742-9085-3d66a338fc29", severity: "HIGH", category: "Cisco Cyber Vision Operations",…},
  {
    id: "9be38302-eea8-51d6-973b-e79763ce8f7e",
    severity: "HIGH",
    category: "Inventory Events",
    date: 1645236068000,
    shortMessage: "New component detected"
  },
  {id: "22641a93-cdb9-573a-9ea6-297f01d3fa89", severity: "HIGH", category: "Inventory Events",…},
```


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

Barcelona Pilot – IRIS Platform Validation

- Identification of attacks
- Information sharing to IRIS platform of incidents
- Enable Cyber Incident Response from CERTS



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

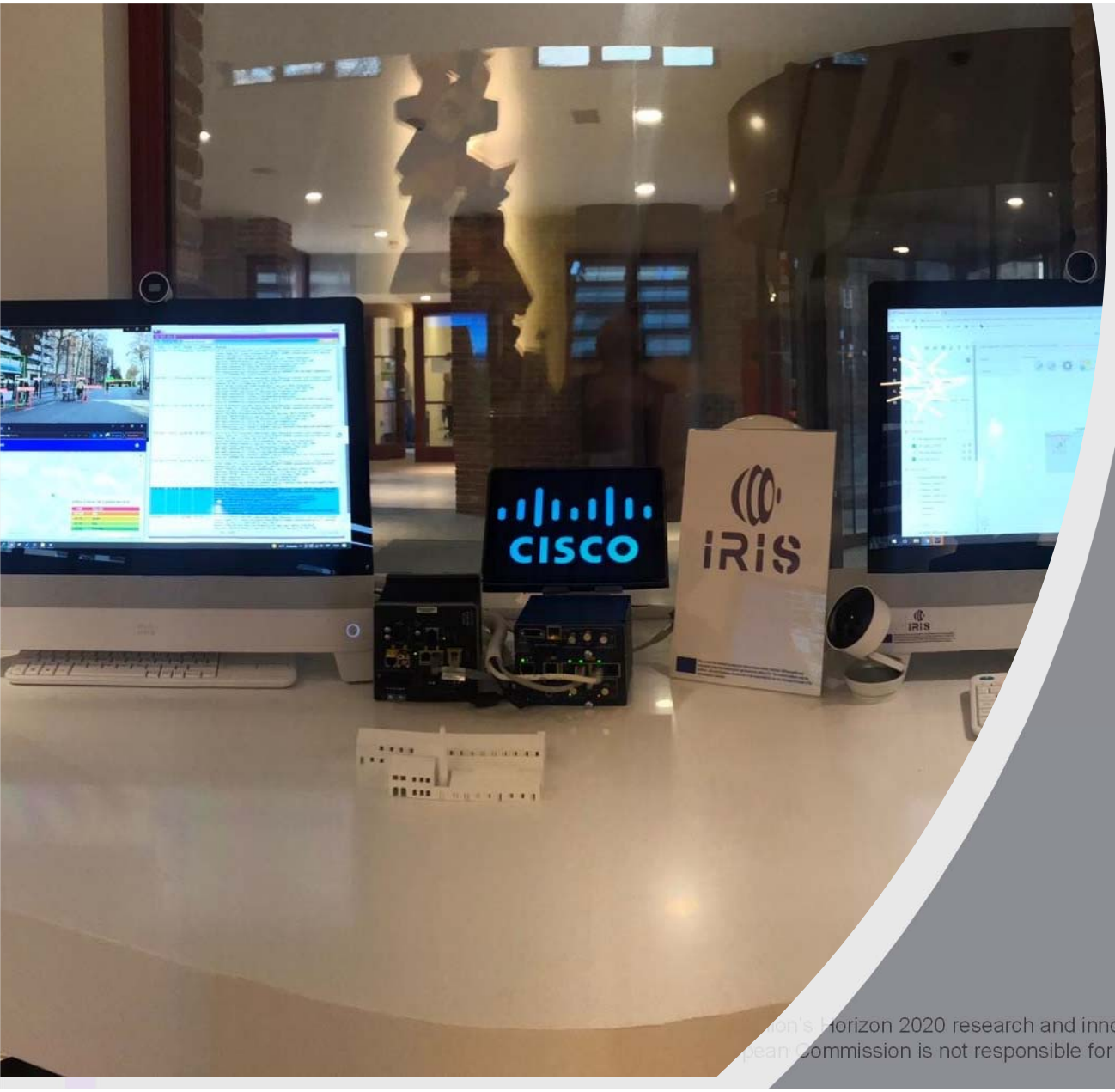
Thank you for your attention !
Any questions ?

iris-h2020.eu

IRIS H2020 Project

iris_h2020

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



Demo

on's Horizon 2020 research and innovation programme under grant agreement no 101021727.
pean Commission is not responsible for any use that may be made of the information it contains.

Fluvià Tram Station

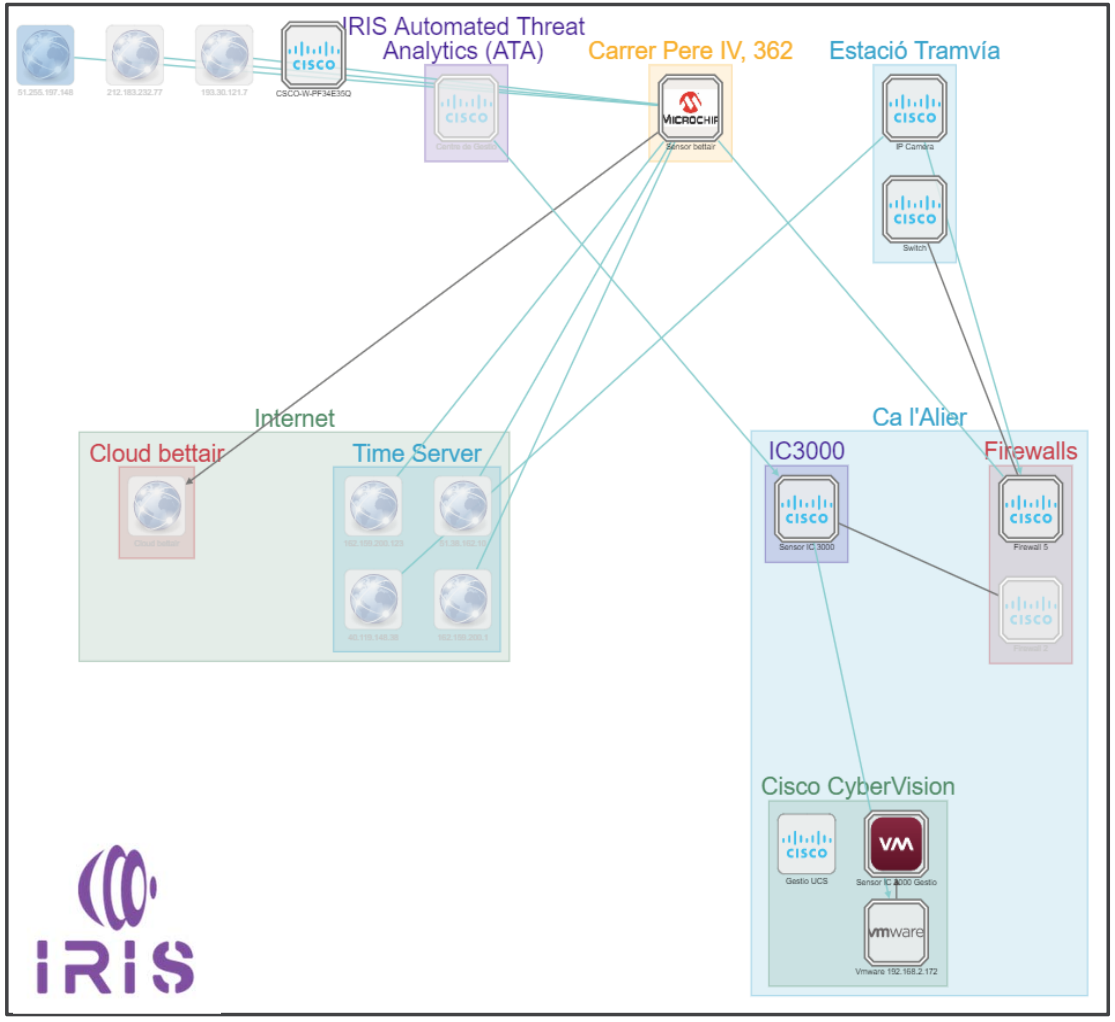
Sensor @ Ca l'Alier

Cisco Innovation Center

Last Connection:01:02:01 19/02/2022 (UTC)

Serial Number	210826014	State	active
Model	MK2.5	Location	41.409967, 2.203482
ID	BET00210073	Battery Level	100%
FW	1.6.0	Last Data	16:30:00 19/02/2022

Network Map



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