Artificial Intelligence Threat Reporting & Incidence report system

IRIS Project Presentation

Rodrigo Díaz (ATOS), Xavier Azemar (Cisco), Andrew Roberts (Taltech), Mariano Lamarca (IMI), René Serral (UPC)

SmartCity World Congress Expo 2021

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

Consortium

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

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

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.

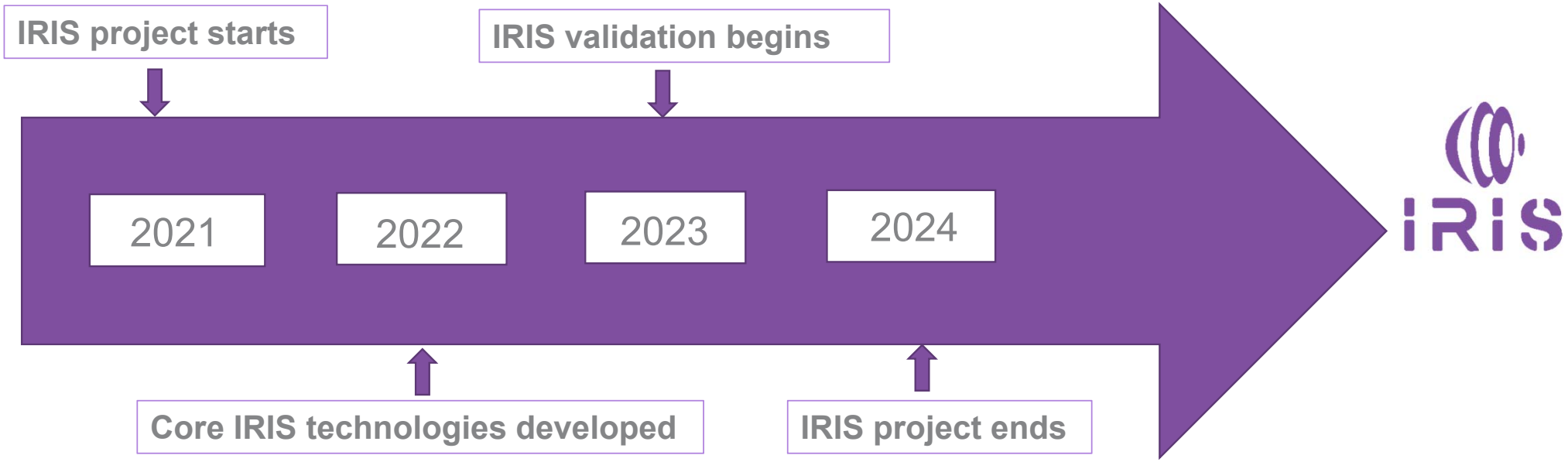
IRIS Vision

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.

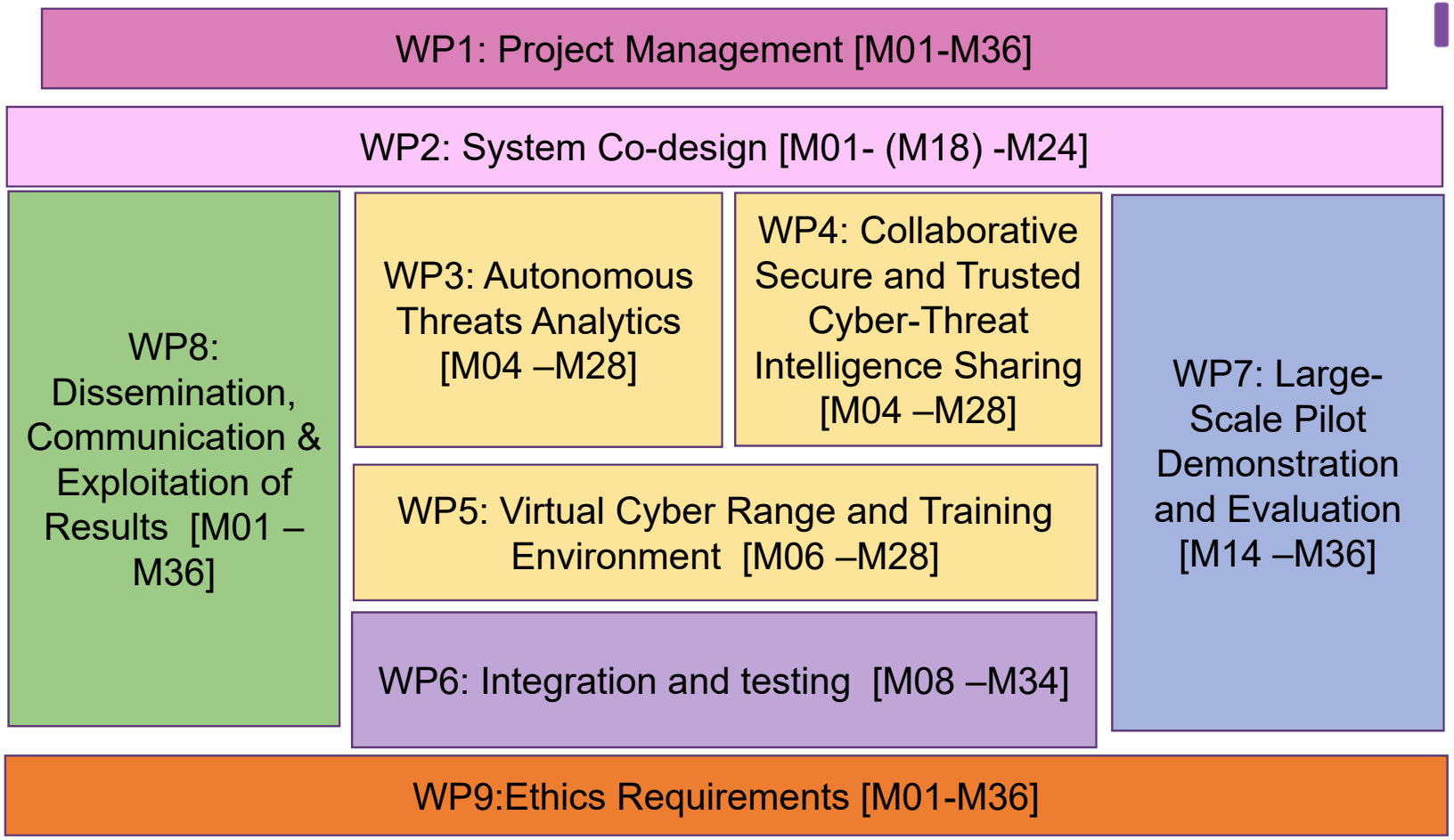
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Time Plan



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 support the operations of CERTs/CSIRTs towards minimizing the impact caused by cybersecurity and privacy risks in IoT platforms and AI-provisions
- To **analyse** the relevant ethics principles and legal framework on privacy concerns, as well as to understand relevant stakeholders' behaviour to identify the main legal, ethics and social enablers for the IRIS solution
- To **develop** a collaborative threat intelligence and information sharing toolkit that allows ICT stakeholders and European CERTs/CSIRTs to create and seamlessly share context-rich information about cyber threats targeting IoT and AI-driven ICT systems

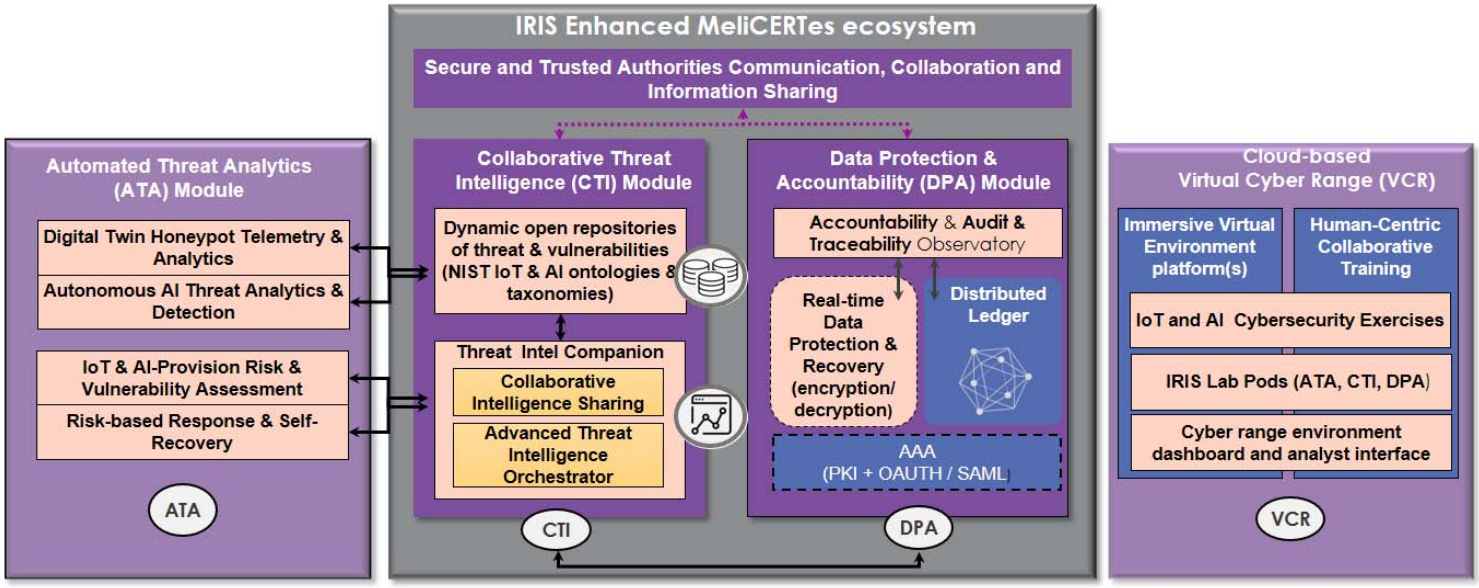
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Objectives

- To **design and implement**:
  - an automated threat analytics framework capable of detecting and responding to cyber threats targeting IoT and AI-driven ICT systems, while exhibiting advanced recovery capabilities
  - a virtual cyber range platform for training cybersecurity professionals to fight against adversarial AI and machine learning attack
  - a data protection and accountability module to establish trust and enable the protection of data necessary 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 to the research, academic, and CERT/CSIRT community, efficient exploitation and business planning of the IRIS concepts and solutions to the market, and contribution of specific project results to relevant standardisation 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.

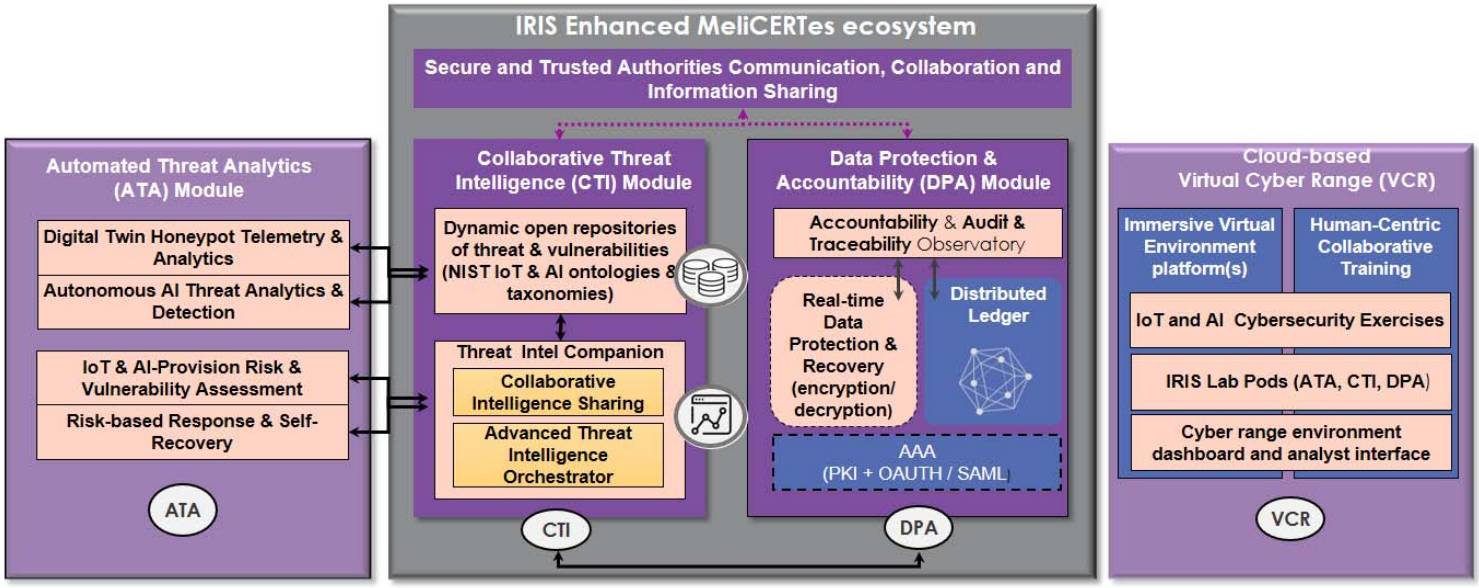
IRIS Architecture



- **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;
- an 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 at both the municipal and national level.

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



- **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 (VCR)** for collaborative CERT/CSIRT training exercises based on real-world environment platforms, providing representative adversarial IoT & AI threat intelligence scenarios and hands-on training.

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

Barcelona Pilot Use Case

Xaver Azemar, Mariano Lamarca

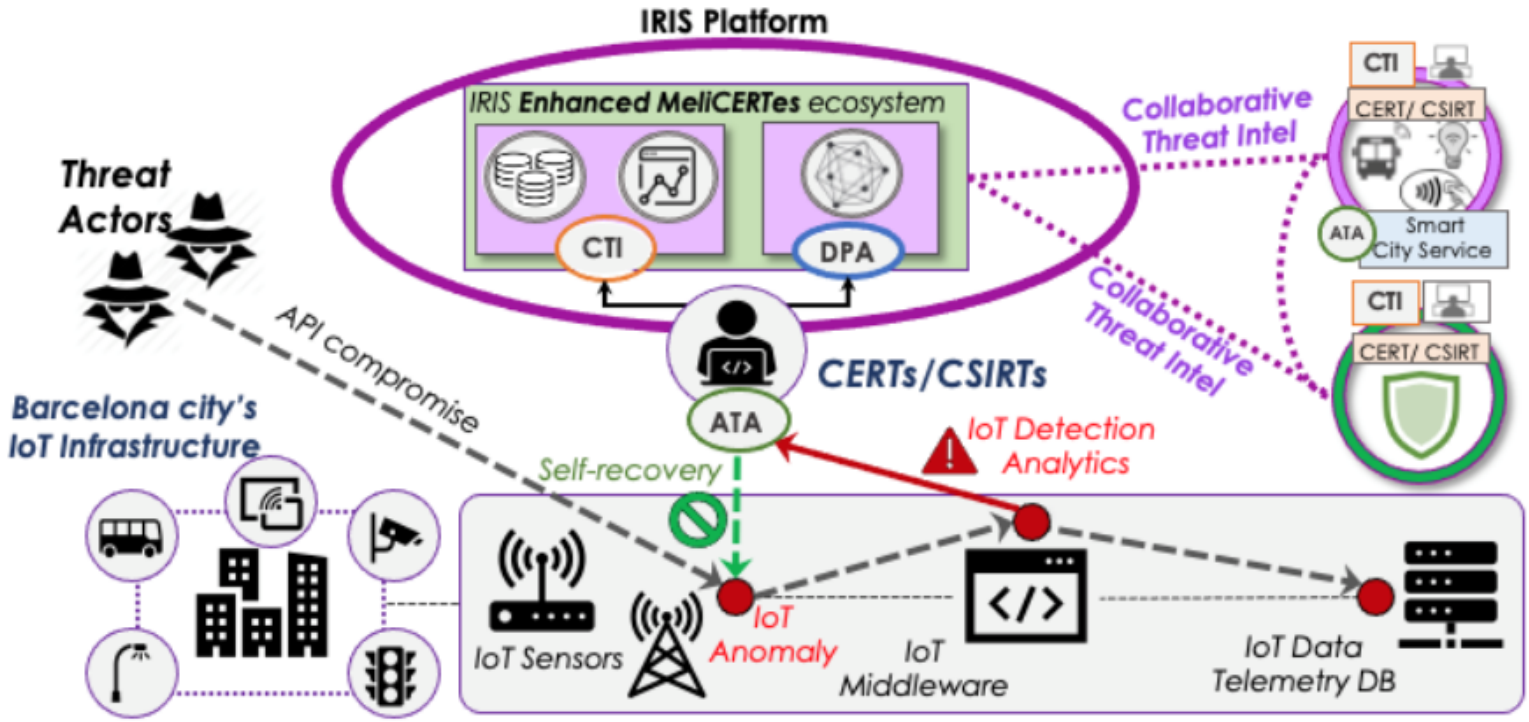
CISCO

Ajuntament de Barcelona

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 Pilots: **Pilot Use Case 1**

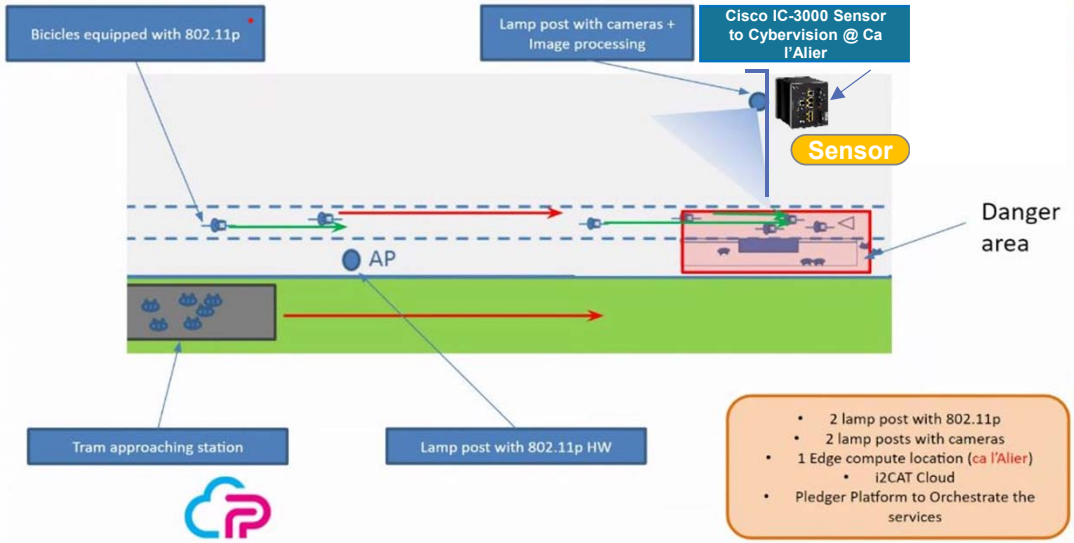
Securing the smart city's IoT and control systems against confidentiality and integrity breaches (Barcelona, Spain)

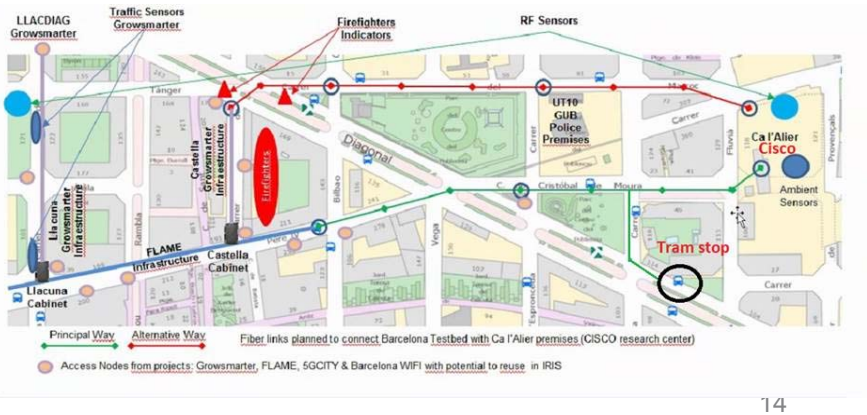


This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 101021727.
This material reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

IRIS Pilots: **Pilot Use Case 1- Barcelona**

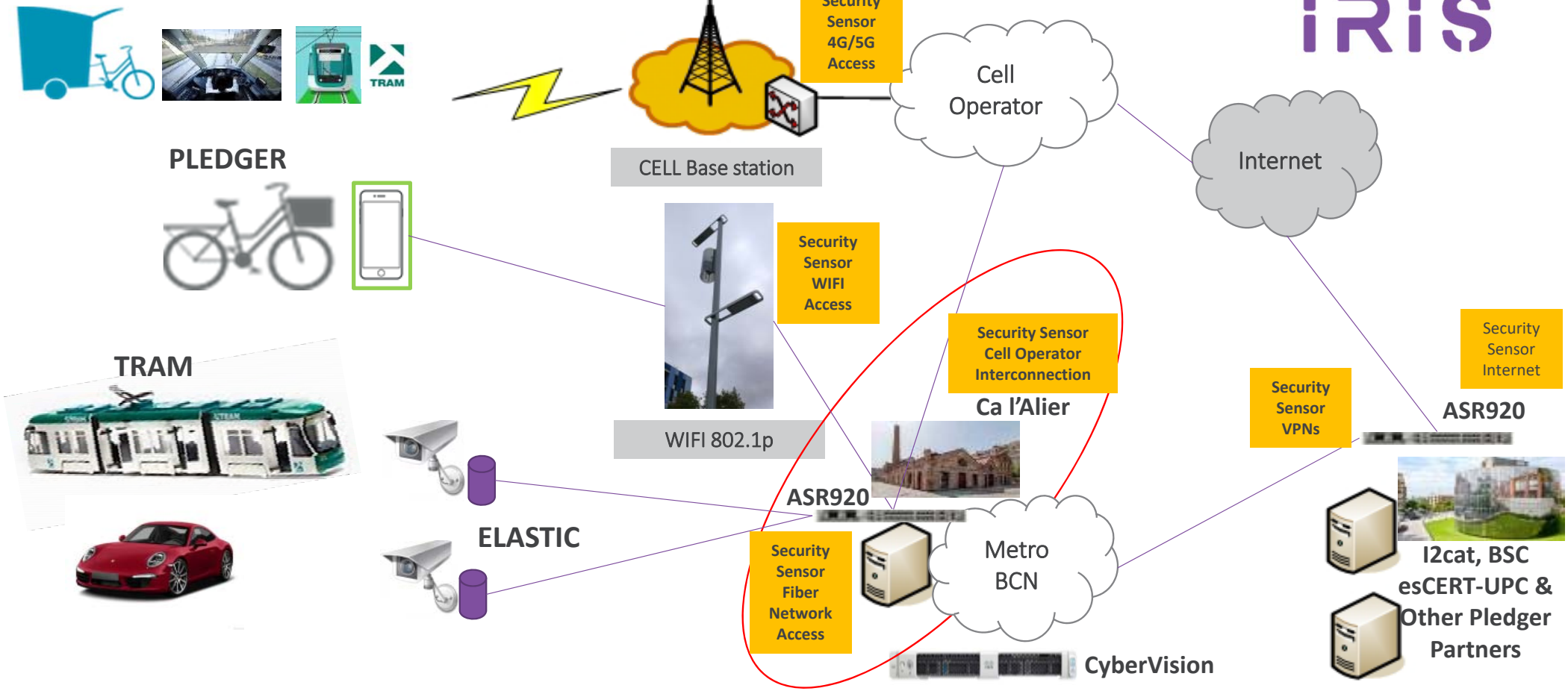
- VRUs (Bicicles/E-Scooters + pedestrians) are exposed to dangerous situations, when people exiting the tram at a station cross the bicycle lane to get to the pedestrian lane.
- With 802.11p to detect bicycles and image processing to detect the tram, possible risky situations are detected and notifications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

5.- IRIS Integration Ex.: PLEDGER+Tram+ELASTIC



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 Pilots: **Pilot Use Case 1-** Cisco Cyber Vision

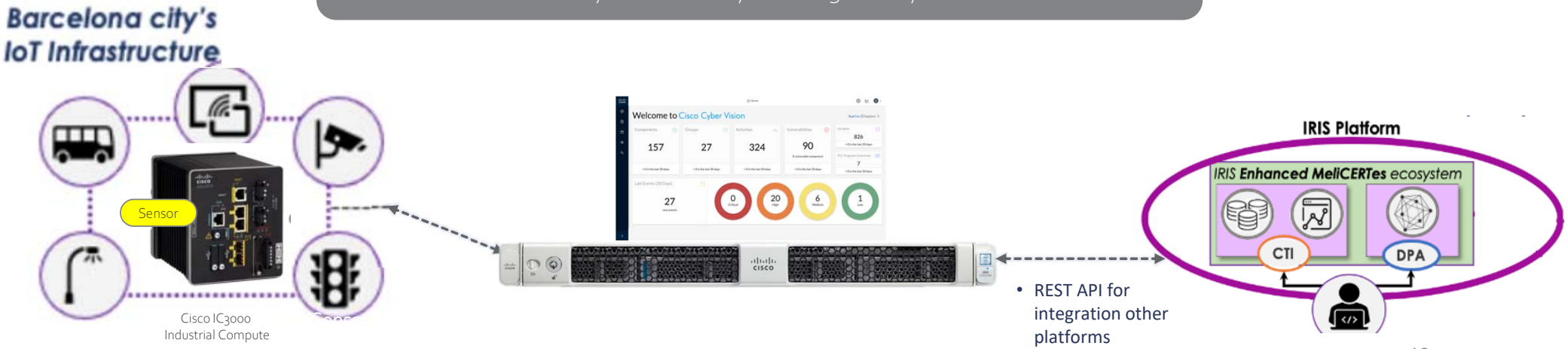
Asset inventory & security platform for IoT

ICS Visibility
Asset Inventory
Communication Patterns
Device Vulnerability

Operational Insights
Identify configuration changes
Record control system events
relevant to the integrity of the system

Threat Detection
Behavioral Anomaly Detection
Signature based IDS
Real-time alerting

Protect your control systems against cyber risks



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 Pilots: **Pilot Use Case 1-** Cisco CyberVision

Key capabilities

VISBILITY

- Asset inventory
- Identify relationships between assets
- Generate inventory reports

Benefits
Store all data collected within the CyberVision center database, export or link to other systems (CMDB).

OPERATIONAL INSIGHTS

- History of events & asset modifications
- Highlight changes to asset configurations
- View key events on the control system
- Generate Controller reports

Benefits
Provide situational awareness and empower OT staff to reduce attack surface.

ANOMALY DETECTION

- Automated baselines for asset behaviors
- User created baselines
- Alerts on deviations

Benefits
Identify malicious behaviors.

VULNERABILITY

- Threat Intelligence database
- Identify asset vulnerabilities
- Generate vulnerability reports

Benefits
Provide situational awareness and empower OT staff to reduce attack surface.

INTRUSION DETECTION

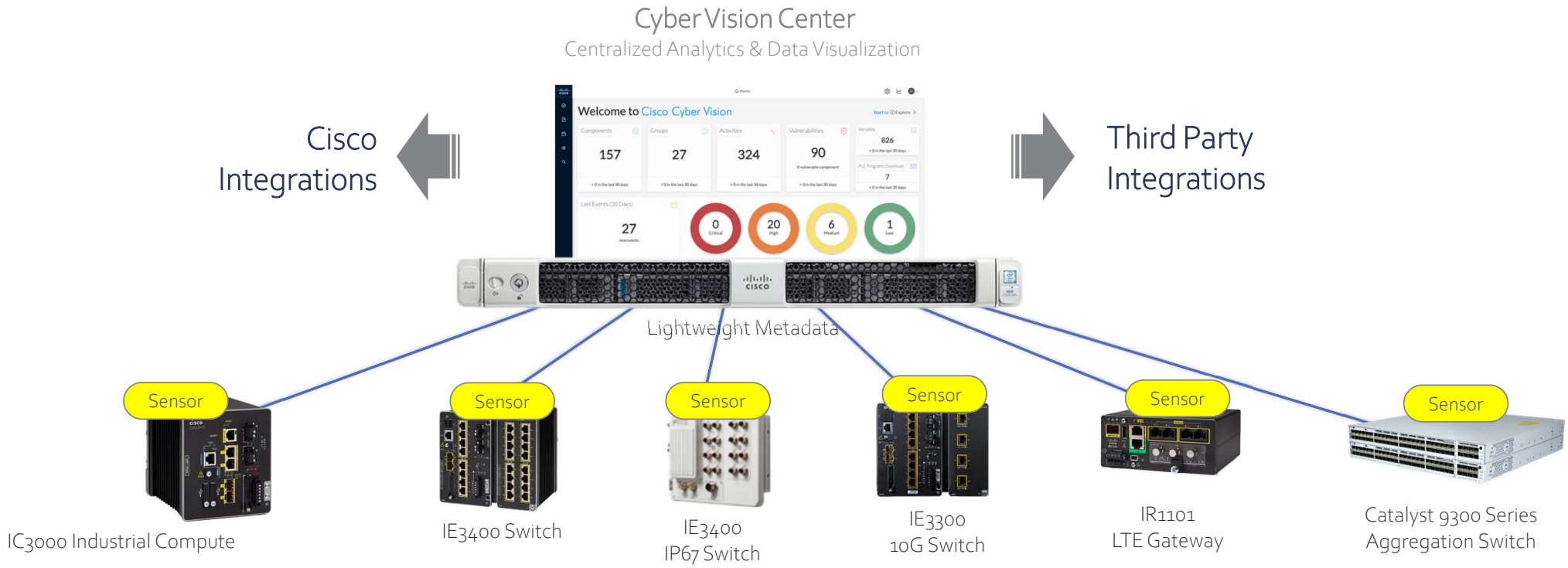
- Snort based Intrusion Detection
- Signatures curated for industrial networks

Benefits
- ❑ Enable and streamline incident response.
- ❑ Accelerate remediation & recovery.

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 Pilots: **Pilot Use Case 1- Barcelona**

Security you can easily deploy at scale



Hardware-Sensor

DPI via SPAN to support brownfield

Network-Sensors

Deep Packet Inspection built into network-elements eliminating the need for SPAN

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

Andrew Roberts – FinEst Smart City Center of Excellence

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

Cybersecurity is predominant for the safety and security of passenger of Autonomous Vehicles and the 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.

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.

AI Enabled Infrastructure - Transportation

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

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

This project
1021727.
This materi
ntains.

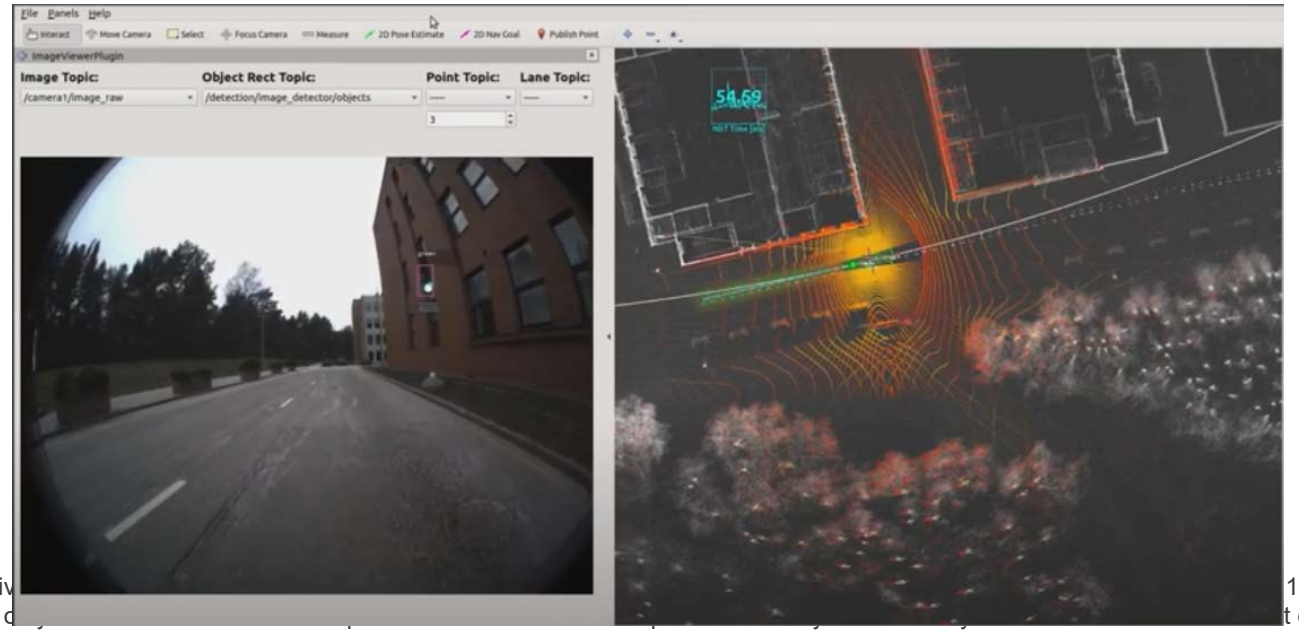
Use-Case Scenario 1: Telematics and Smart City Data Exchange & Security

The Autonomous Vehicle (AV) Shuttle fleet will navigate around the smart campus environment. The AV Shuttle telemetry is communicated to the Remote Operations Center and the AV logging database which is connected to the Urban Operating Platform (UoP). The UoP receives information on the location of the vehicles, navigation, odometry and other sensor data.

This project has received funding from er grant agreement no 101021727.
This material reflects only the authors ade of the information it contains.

Use-Case 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 and the AV object-detection module detects the traffic light color and makes a driving decision to pass-through or stop.



This project has receiv 101021727.
This material reflects c t 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.

IRIS

Artificial Intelligence Threat Reporting & Incidence report system

Helsinki Pilot Use-Case

Nikita Akmaikin (Forum Virium Helsinki)

Updated 11 November 2021

FORUM VIRIUM HELSINKI

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.

Cross-Border Smart Grids – Helsinki Pilot

- **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.)**. API should follow the IEC 61987 standard on Common Information Model and its communication should be secured with a VPN.
- 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 based on Apache Kafka, Apache Spark, Microsoft Azure, Building automation system demo and training kits for API development. *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.

Urban Data Platform Use-case examples

Use Case 1: Environmental noise monitoring

Use Case 2: Smart Home Sensor Using LoRaWAN network

Use Case 3: Solar Panel Monitoring

Use Case 4: Smart Street Lighting

Use Case 5: People Counters

Use Case 6: Electrical Vehicle Charging Monitoring

Use Case 7: Maintenance Vehicle Telemetry

Use Case 8: Building Automation System

Use Case 9: Dynamic Attributes in 3D City Model

Use Case 10: Natural Language Processing in Helpdesk

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

- The amount of solar radiation in buildings on a monthly and annual basis

Heating Demand Prediction

- Heating energy demand prediction and building renovation estimates for almost the entire Helsinki building stock from 2020 to 2050

Geoenergy Potential

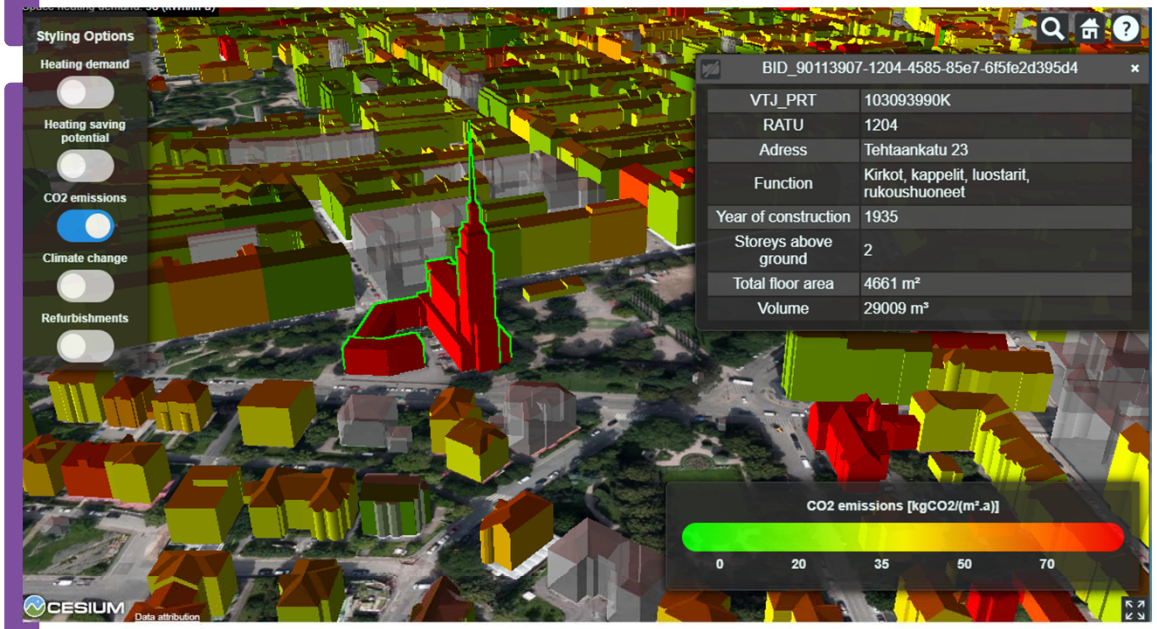
- 150-m / 300-m / 1000-m deep well potentials, groundwater areas, bedrock (rock types and thermal conductivity, specific heat capacity, density parameters for geoenergy calculations) and soil data to support geoenergy well design work

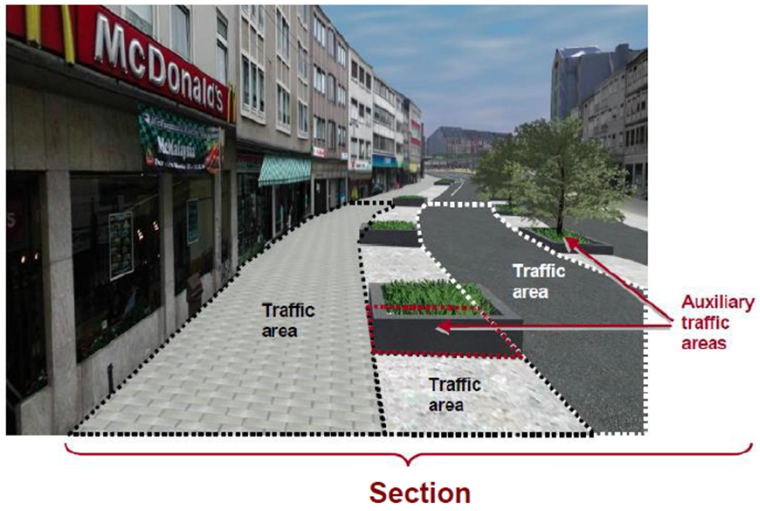
Energy Data of Buildings

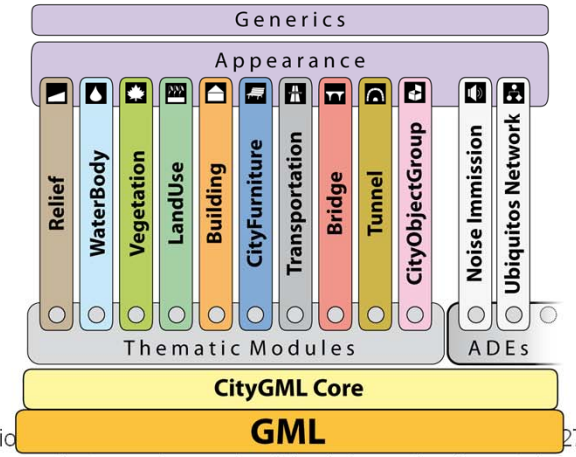
- Municipal register information (e.g. heating method of buildings, usage, volume, building material)
- Repairs and alterations
- Protected buildings (protection markings)
- Calculated energy consumption of buildings by age group (heat consumption, user electricity, building electricity)
- Potentials and costs for improving the energy efficiency of a typical 1970s-80s building in the Merihaka district
- Energy performance certificates and proposed improvement measures
- Measured consumption data of HEKA buildings for 2015 and 2016 (district heating, building electricity, water consumption)

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 innovatio 27.
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

- Focus on protecting the customer facing components of the smart grid against threats to control functions defined for the demand control. The pilot will use two smart grid APIs, the Smart Grid API from Kalasatama, and the 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.

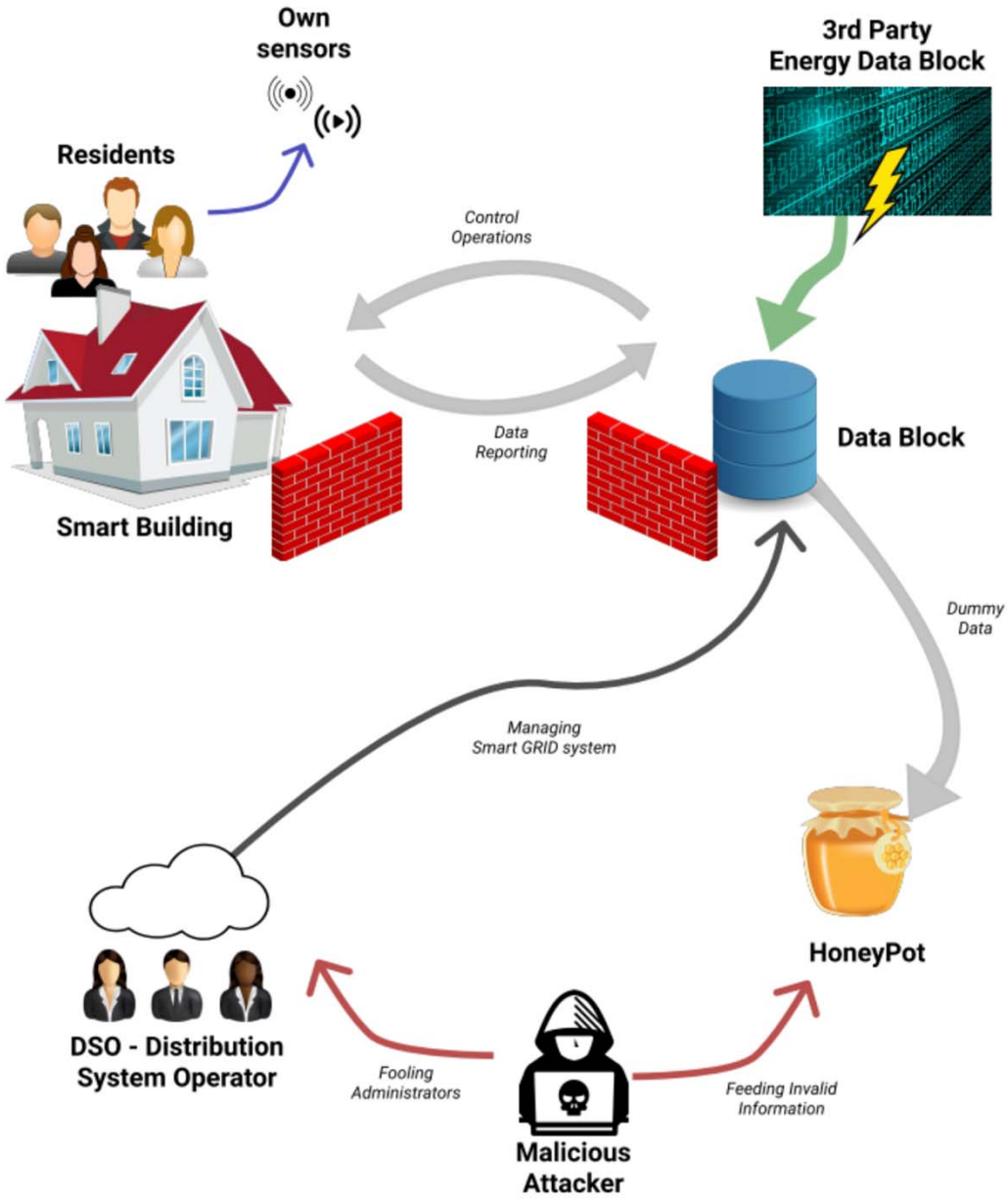
Use-Case Scenario: Kalasatama Smart District

- 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 decreases load.

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.

PUC3 design



Stakeholders to consider

- **DSO (Distribution system operator)** – Acting as a party who directly reports the energy demand, controlling the building load. Attacking scenario is supposed to malform the data in the load system, therefore confusing the DSOs and the system behind the load control.
- **Building Residents -** Having data wallets of personal data as a React application, allowing users to map own sensors in the system. Might be an interested party in terms of security of personal data.
- **CERTs/CSIRTs –** Feedback on handling and forecasting
- security incidents, complex attacks and propagated vulnerabilities in IoT and AI-driven ICT systems.

ation programme under grant agreement no 101021727.
y use that may be made of the information it contains.

Helsinki – IRIS Platform Validation

- Detect the malicious information through its AI security mechanisms and mitigate the impact of the attack.
- Produce systematic threat intelligence that will be able to be consumed by IRIS CTI for improving threat data sets, as well as notifying stakeholders automatically of attacks that are occurring in near real-time.

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

Questionnaire Form

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.

Questionnaires

- **Part 1:** Use Case Survey for Stakeholders
- **Part 2:** User Requirements Survey

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-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.