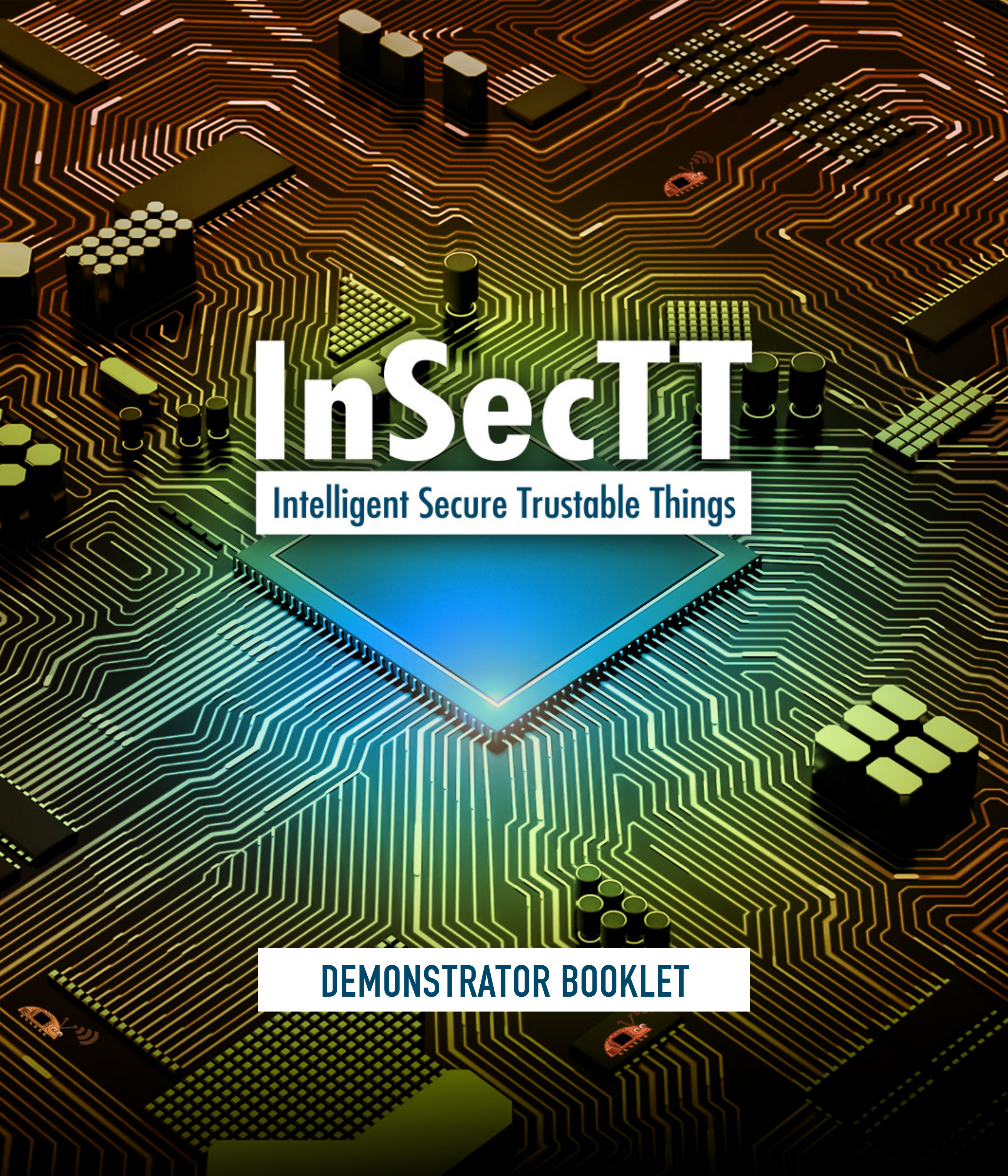


InSecTT

Intelligent Secure Trustable Things

DEMONSTRATOR BOOKLET

Use Case 5.1

Platoon Communication System supported by Single Base Station

This demonstrator targets scenario that consists of single platoon and one base station. Each vehicle as well as the BS are assumed to have multiple antenna transceiver. Different physical and medium access control layer assumptions are used to model both the channel, the MIMO tool used, and the organization of the information transmitted between the entities of the platoon. The BS is assumed to be used to either assist or even replace V2V links. The channel modelling is as accurate as possible to reflect the main aspects of the physical environment.

In Tunnel Propagation Wireless Communications and testing

This demonstration site is derived from the previous demonstrator with single platoon and one base station. The objective is to test the reliability of communications inside highly multipath reflective scenario under different situations. The tests will also be conducted mainly in simulator with realistic propagation models.

The main difference between this demonstrator and the previous one is the limited conditions where the UE does not have proper line of sight and the properties of the tunnels that usually are semi-circular.

Platoon Resource Management System Level

This demonstration involves system level simulation in Manhattan grid network with multiples cars and/or platoons interacting with each other on the streets of the scenario. Realistic propagation models using BSs located at strategic positions in the grid will be used. Basic platoon operations will be considered such as platoon movement on given itinerary, platoon gap and speed change.

Dependable wireless communication system simulator

This demonstrator shows an ASIL-B prepared wireless communication system based on the 802.11p communication standard.

Platoon Communication System supported by Single Base Station.

Under this demonstrator an emergency braking scenario is examined, where the platoon transmits at high-priority braking signals to all formation elements. This scenario is composed by two main testbeds, one based on software, and another based on hardware robotic testbed.

This demonstrator consists of the following elements:

- Connected Cars Digital Twin Platform which allows to realize emulated V2X communication in the artificially generated vehicle traffic (using real vehicle trace analysis or 3D physics simulators) and feeds through CCSP.
- Physical communication protocols.
- AI mechanisms to detect interference.
- Wireless resource management mechanisms.
- RAN simulator implementing some features of physical layer and allowing the creation of slices for cell capacity.
- OSS platform (ONAP) to manage and automate the network, following O-RAN standards and implementing closed loop for monitoring and optimization of the RAN. Integrated with RAN simulator, which exposes the metrics allows ONAP to collect the data and on Non-RT RIC perform the analysis. Provides policies for network optimization. Additionally, brings the MANO functionalities allowing the deployment of VNFs/CNFs near the end users to reduce latency.
- Validation Framework.
- robotic testbed which consists of emulated vehicles with multiple sensors and communication interfaces to replicate and test platooning behavior. These cars can be used to test aspects of the transmission and channel modelling in more real setup. Metrics about performance as well as modelling of the platoon can be collected. Further it supports AI algorithms for sensor and RF data to be implemented using the on-board micro controllers and microprocessors. The wireless communication chipset based on 802.11p from NXP-NL is also integrated within the robotic testbed to provide secure V2X communication link for experimentation

In Tunnel Propagation Wireless Communications and testing

- Connected Cars Digital Twin Platform which allows to realize emulated V2X communication in the artificially generated vehicle traffic (using real vehicle trace analysis or 3D physics simulators) and feeds through CCSP.
- Physical communication protocols.
- AI mechanisms to detect interference.
- Wireless resource management mechanisms.
- RAN simulator implementing some features of physical layer and allowing the creation of slices.
- OSS platform to manage and automate the network.
- Validation framework.

Platoon Resource Management System Level

This demonstrator derives from the previous ones, it considers multiple cell site and platoon network in urban or dense environments. The objective of this scenario is to evaluate the performance of the V2V and V2X infrastructure in the presence of inter platoon and inter cell interference. This demonstrator consists of the following elements:

- The Manhattan simulator is virtual testbed that emulates realistic urban and suburban cellular vehicular scenario with system level simulation tools. The Manhattan demonstrator is particularly focused on the validation and verification of advanced physical layer tools for 5G/enabled vehicular communications such as 3D-beamforming, massive MIMO, coordinated relaying and NOMA. Each of its components have been designed to be interoperable to be integrated with other simulation platforms.
- Physical communication protocols.
- AI mechanisms to detect interference.
- Wireless resource management mechanisms.

- RAN simulator implementing some features of physical layer, and MAC layer, handling aspects such as the mobility of vehicles. One important feature if the cell capacity handling by creating different network slices.
- OSS platform (ONAP) to manage and automate the network, following O-RAN standards and implementing closed loop for monitoring and optimization of the RAN. Integrated with RAN simulator, which exposes the metrics allows ONAP to collect the data and on Non-RT RIC perform the analysis. Provides policies for network optimization.
- Validation framework.
- Dependable wireless communication system simulator

Figure 1, below, presents an overview of the key components of the demonstrator and their dependencies.

The submodules of the demonstrator are:

- Platoon communication submodule containing an ASIL-B prepared 802.11p transceiver. The relevant software components that are deployed on this module are:
  - EnsembleApp and exampleETSI: Together these components handle the communication of the messages of the EU multi-brand truck platooning protocol called “Ensemble”.
  - Safety Monitor: This component detects and reports safety faults, incorporates fail silent behavior and provides an API to trigger fault recovery.

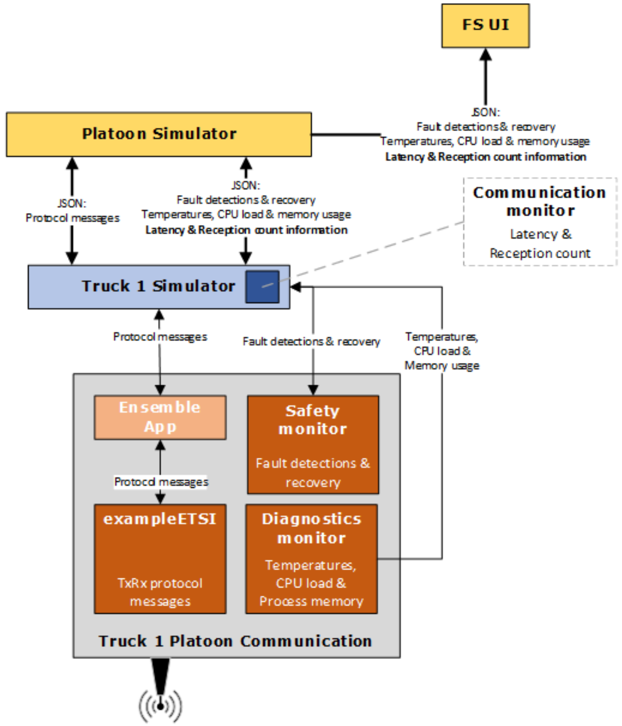

FS UI
JSON:
Fault detections & recovery
Temperatures, CPU load & memory usage
Latency & Reception count information
Platoon Simulator
JSON:
Protocol messages
JSON:
Fault detections & recovery
Temperatures, CPU load & memory usage
Latency & Reception count information
Communication monitor
Latency & Reception count
Truck 1 Simulator
Protocol messages
Fault detections & recovery
Temperatures, CPU load & Memory usage
Ensemble App
Safety monitor
Fault detections & recovery
Protocol messages
exampleETSI
TxRx protocol messages
Diagnostics monitor
Temperatures, CPU load & Process memory
Truck 1 Platoon Communication

Figure 1: NXP Platooning Simulation System

  - Diagnostics Monitor: This component monitors properties in the hardware and the software of the platoon communication module while the communication is active (for example: CPU load and memory load).

- Platoon Simulator submodule is responsible for the execution of the platooning behavior in the system simulator.

- FS UI submodule, the user interface to control the execution of the system simulator and to show detected faults and values of the monitored diagnostics properties.

- Truck Simulator submodule facilitates the integration of multiple Platoon Communication submodules into the Platoon Simulator, by providing the required network topology and by providing protocol translations between the Platoon Simulator format and the Platoon Communication format.

- The safe system principle of operation, executed by the ASIL-B prepared 802.11p transceiver, combined with the safety monitor, diagnostics monitor and the simulator components, is shows in Figure 2.

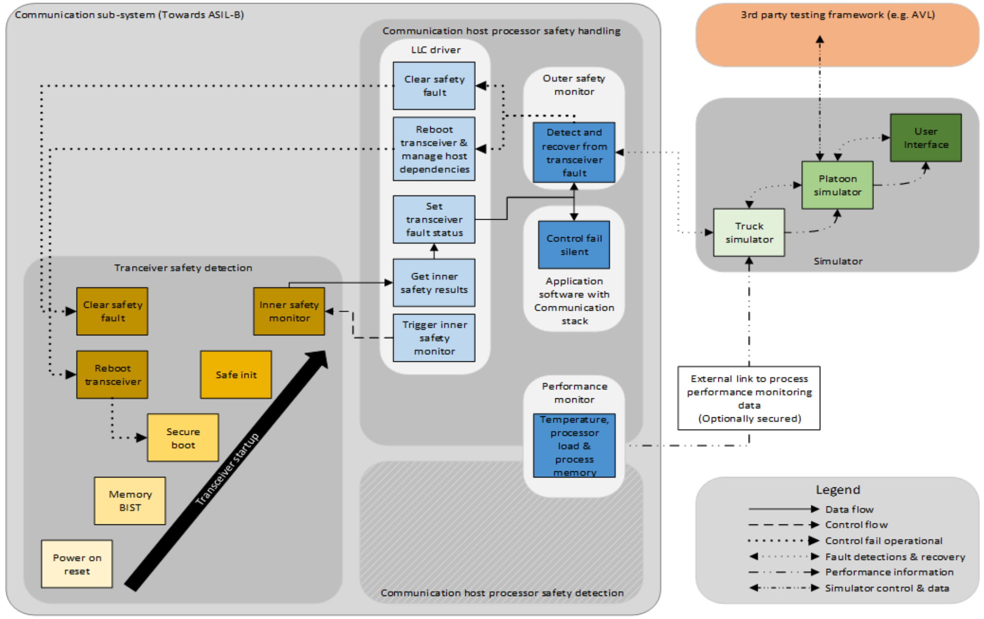

Communication sub-system (Towards ASIL-B)
Communication host processor safety handling
LLC driver
Clear safety fault
Reboot transceiver & manage host dependencies
Set transceiver fault status
Get inner safety results
Trigger inner safety monitor
Outer safety monitor
Detect and recover from transceiver fault
Control fail silent
Application software with Communication stack
Performance monitor
Temperature, processor load & process memory
Communication host processor safety detection
Tranceiver safety detection
Clear safety fault
Inner safety monitor
Reboot transceiver
Safe init
Secure boot
Memory BIST
Power on reset
Transceiver startup
3rd party testing framework (e.g. AVL)
User Interface
Platoon simulator
Truck simulator
Simulator
External link to process performance monitoring data (Optionally secured)
Legend
Data flow
Control flow
Control fail operational
Fault detections & recovery
Performance information
Simulator control & data

Figure 2: Safe System principle of operation

Platoon Communication System supported by Single Base Station.

This demonstrator addresses the question of whether to use V2V, V2I or mixture of both types of link for reliable platoon communication. The objective is to ensure industrial grade connectivity and reliability level that enables business models and end user trust.

In Tunnel Propagation Wireless Communications and testing

This demonstrator attempts to test wireless communication in difficult environment and use multiple tools to counteract all the potential impairments and keep connectivity to the same levels as in other environments.

Platoon Resource Management System Level

This demonstrator addresses the issue of controlling or partially controlling network of platoons and the vehicles of the platoon in order to meet all the requirements from different stakeholders at the urban and suburban level.

Dependable wireless communication system simulator

Wireless communication systems can be an ultra-fast sensor for automated operations in vehicle. Examples are: CAEB, CACC and Platooning. Depending on the Operation Domains, ASIL-B requirements could emerge in Safety Analysis. The EU multi-brand platooning project called “Ensemble” has demonstrated these emerging requirements. This demonstrator shows towards ASIL-B 802.11p transceiver, combined with safety and diagnostics monitoring and integrated into system simulator.

Exploitation plans

- CAP

  - The system simulation framework developed is based on O-RAN standards, featuring closed-loop control system for the RAN, where we can monitor and optimize the network targeting scenarios such as the future of transportation. It implements Non-RT-RIC rAPP and it will serve as validation framework to accelerate the development and testing of new RAN control applications.

  - The results and the developed framework will provide solid starting point for usage in follow-up and future research projects.

Use Case 5.2

Interference characterization demonstrator

This demonstrator has dual component. Real life measurements and an emulated aircraft for positioning of nodes (virtual location). In this demonstrator, channel model is adjusted to the measurements across different positions of the aircraft. The channel model is very detailed with the metallic objects of the aircraft and for internal networks it considered details such as seats and even absorption models for passengers. The effects of leakage of signals through the windows of the aircraft have also been integrated to evaluate interference between

One of the most challenging aspects of the technology WAICs to be highly reliable and trustable is the relatively small area of deployment and the complexity/density of all critical subsystems of an operational aircraft. This can be worsened by the highly unpredictable propagation channels and the extreme environmental conditions that can be found at different moments of flight mission: take-off, taxi, landing, etc. Perhaps the most important issue on board an aircraft is the potential interference towards the WAICs network or the interference from the WAICs system to other on-board equipment. This scenario is focused on the modelling, measurement, detection and rejection/compensation of several sources of non-intentional or intentional (Jamming) interference on board the aircraft considering different positions of the interfering nodes or different strategies of the jamming attackers. Artificial intelligence tools will be designed to improve all the detection and compensation mechanisms and thus boost the reliability of WAICs systems under different aircraft conditions.

Verification and validation demonstration of WAICs

As wireless communication starts playing an important role in avionic intra-communication, reliable testing environment becomes necessity. Main objective of this scenario is to provide framework for verification and validation of Wireless Avionics Intra-Communication. The location is mainly virtual, but we make use of series of measurements and parameters of the physical world that must be collected in the real settings: an operational aircraft. The purpose of this demonstrator is to emulate complete wireless avionics network used for particular application such as the sensing of environmental parameters such as angle of attack, flow, speed, turbulence flow formation, pressure, temperature, etc.

Battery-less sensors and communication demonstration

The demonstrator also consists of two main components. Our partner TUDelft has produced realistic battery-less components to be implemented for several applications on board commercial aircraft. The characteristics of these nodes are imported into the developed WAICs simulator and system level evaluation is performed of the performance of these real hardware nodes. The location is also dual, our partner TUDelft has results of the nodes operating on board realistic aircraft, but we have also virtual implementation using the characteristics of the nodes and the applications intended by TUDelft.

Channel model

An advanced channel model for wireless avionics has been developed that is accurate to the propagation prediction of wireless avionics network. It is so detailed it can include the effects of seats, passengers, and windows of an aircraft. It is also flexible to include different profiles of aircraft, and different shapes of wings on the external side of the airplanes.

System level simulator

System level simulation is the name given to set of verification and validation methodologies for new cellular technologies in representative large-scale environments comprising multiple transmitters and receivers. In conventional cellular technologies this means including multiple cells in the simulation loop to calculate the effects of interference, near-far channel differences, as well as frequency reuse patterns or radio resource management. system level simulation unusually needs set of experts to agree and validate the models and the interfaces between the different modules and granularity levels of simulator.

AI-components

AI components have been designed to improve multiple aspects of the wireless transmission processes, including beam-forming, channel prediction, signal reception, and interference rejection.

Reconfigurable antennas and MIMO

The use of multiple antennas is crucial to improve reliability in wireless avionics networks. The use of reconfigurable antennas provides flexibility, lower cost and good reliability improvement.

Battery-less devices

The use of devices that can reuse environmental or mechanical energy to be powered off aims to create revolution in avionics, where energy consumption must be minimized. The use of these devices paves the way for cleaner flights, optimized wireless avionics performance and lower fuel consumption of the industry.

What business need/problem does the demonstrator address?

The aeronautics industry will experience revolution in the years to come. The use of advanced wireless networks on board promises to open multiple opportunities as well as riks in the industry. The advantages using AI to protect multiple systems and to make wireless transmission more efficient and safe.

Exploitation plans

Wireless avionics will be commercial in the near future. Battery-less devices will proliferate in the market as well. The results here will be exploited in standardization as part of the current liaison between InSecTT and ISO/JTC1 SC41 WG5.

Use Case 5.3

Demonstrator: Emergency Vehicle Approaching under Jamming Conditions is located at VeNIT Lab, Marmara University Dragos Campus. The scenario is tested within the Connected Cars Digital Twin Platform (CCDTP) along with simulators and integration of third party models.

Demonstrator: Emergency Vehicle Approaching under Jamming Conditions

The purpose of this demonstrator is to showcase cyber-attacks, specifically in the physical layer, particularly jamming, on large scale. To accomplish this, we utilize the Connected Cars Digital Twin Platform (CCDTP), PhyWise tool, and Connected Cars Service Platform (CCSP). These components allow us to virtually test and demonstrate various V2X (vehicle-to-everything) communication scenarios by simulating movement, physical conditions (like channel effects and 3D physics), and communication between different agents.

The setup of the demonstrator has the capability to illustrate the impact of cyber-attack on V2X communication for multitude of vehicles equipped with on-board units (OBUs) and roadside units (RSUs) in the environment. Taking high-level view, the demonstrator consists of three components, which are described below.

Connected Cars Digital Twin Platform (CCDTP):

This platform generates the virtual demonstration environment, including vehicle traffic, OBUs, RSUs, their protocol stacks, and applications. It facilitates V2X communication among the Cooperative Intelligent Transportation Systems (C-ITS) entities.

CCDTP simulates the wireless channel effects on V2X communication by leveraging built-in tools or external channel simulators/emulators (such as PhyWise in this case).

PhyWise:

PhyWise calculates the impact of the wireless channel on V2X communication, specifically considering the signal-to-noise ratio, based on the positions of the receivers and transmitters.

This component operates during the preparation stage, as it is supplied with the scenario map and the potential coordinates on the map where receivers or transmitters can be located.

Connected Cars Service Platform (CCSP):

CCSP stores the logs and metrics collected while executing scenarios in CCDTP. These data can be analyzed and visualized in real-time or after the scenario execution.

The collected data can be utilized by third-party components, either in real-time or post-execution.

Additionally, CCSP acts as service intermediary between CCDTP and the PhyWise tool, facilitating the transfer of scenario configurations like maps and possible receiver and transmitter locations.

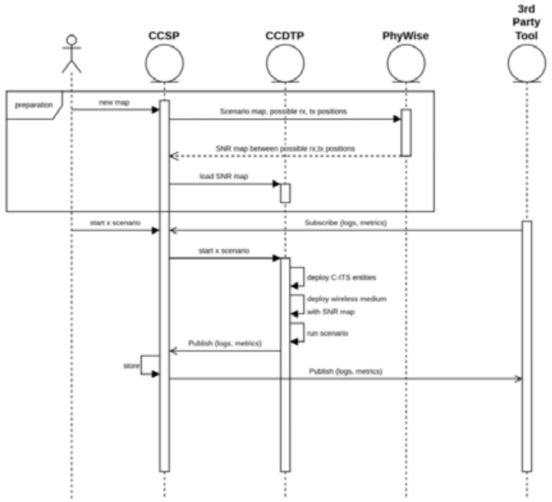


Figure 3: Sequence diagram: the interaction between the components of the Demonstrator

Demonstrator: Testbed for Embedded Wireless Devices

This demonstrator consists of testbed for automatic testing of embedded wireless devices. The testbed is intended to enhance the development process and verify the correct operation of the wireless embedded devices. Thus, it consists of elements to interact with the device under test (DUT), of elements which modify the environments of the DUT, of elements which verify certain test parameters, and of elements which orchestrate the testing procedure and verify the overall test results. The architecture is shown in Figure 4.

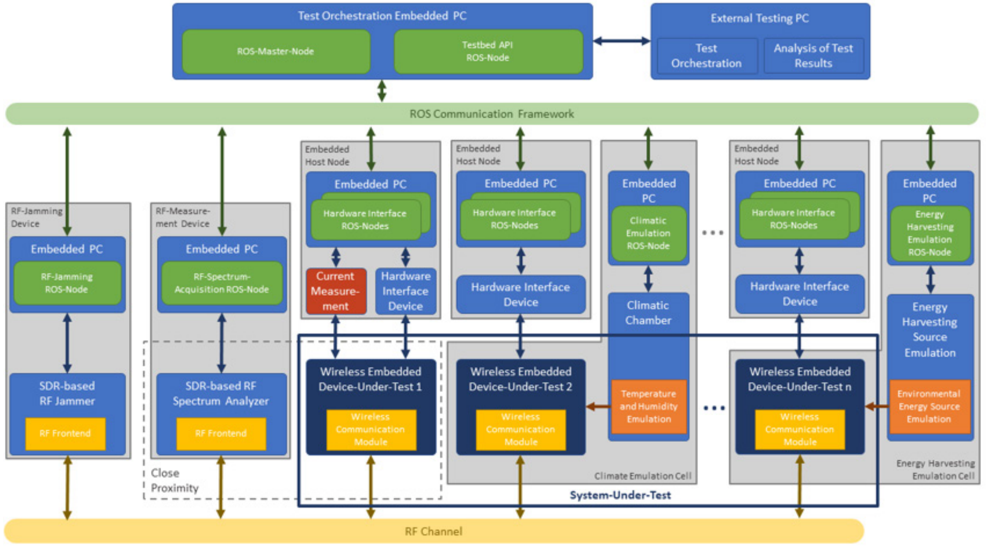
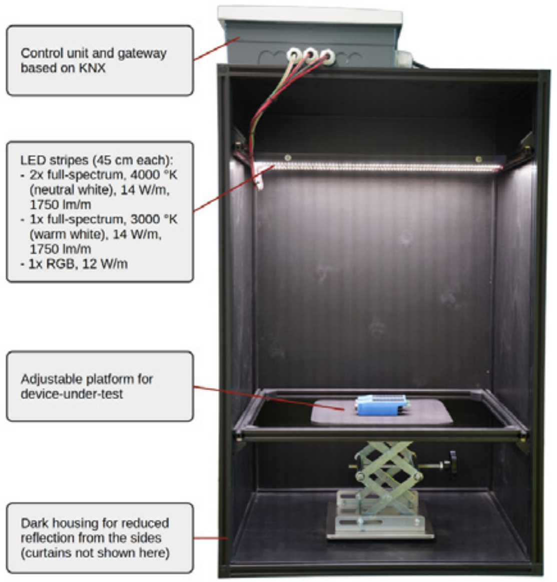

Test Orchestration Embedded PC
ROS-Master-Node
Testbed API ROS-Node
External Testing PC
Test Orchestration
Analysis of Test Results
ROS Communication Framework
RF-Jamming Device
Embedded PC
RF-Jamming ROS-Node
SDR-based RF Jammer
RF Frontend
RF-Measurement Device
Embedded PC
RF-Spectrum-Acquisition ROS-Node
SDR-based RF Spectrum Analyzer
RF Frontend
Close Proximity
Embedded Host Node
Embedded PC
Hardware Interface ROS-Nodes
Current Measurement
Hardware Interface Device
Wireless Embedded Device-Under-Test 1
Wireless Communication Module
Embedded Host Node
Embedded PC
Hardware Interface ROS-Nodes
Hardware Interface Device
Wireless Embedded Device-Under-Test 2
Wireless Communication Module
Embedded PC
Climatic Emulation ROS-Node
Climatic Chamber
Temperature and Humidity Emulation
Climate Emulation Cell
Embedded Host Node
Embedded PC
Hardware Interface ROS-Nodes
Hardware Interface Device
Wireless Embedded Device-Under-Test n
Wireless Communication Module
Embedded PC
Energy Harvesting Emulation ROS-Node
Energy Harvesting Source Emulation
Environmental Energy Source Emulation
Energy Harvesting Emulation Cell
System-Under-Test
RF Channel

Figure 4: Structure of the testbed, showing hardware elements (blue blocks), functional groups of hardware elements (grey blocks), ROS-based computation.

The testbed integrates different components from LCM, GUT, SAL, and JKU. The main components are listed below:

- Testbed API Node: This element is used for central orchestration and controls every other entity of the testbed. It is accessible via web service using the OpenAPI specification. It is used to execute test procedures and retrieving the test results by calling the API function.
- Embedded Host Node (EHN): Each EHN is connected to one DUT, for example wireless sensor node. The EHN is used to program the DUT with test-specific firmware version, to reset the DUT, and log status output via serial interface. Each EHN may also integrate power analyzer which measures the power consumption of the DUT during the testing procedure.
- RF Jamming Device (RFJD): The software-defined-radio-based RFJD is used to generate different types of RF signals (for example sine, white or Gaussian noise etc.) on specified frequencies during certain periods of the test, emulating attacks or interference from various other RF technologies. Also, the temporal occurrence can be specified. This enables emulation of short term or permanent interference as well as complex interference patterns.


Control unit and gateway based on KNX
LED stripes (45 cm each):
- 2x full-spectrum, 4000 °K (neutral white), 14 W/m, 1750 lm/m
- 1x full-spectrum, 3000 °K (warm white), 14 W/m, 1750 lm/m
- 1x RGB, 12 W/m
Adjustable platform for device-under-test
Dark housing for reduced reflection from the sides (curtains not shown here)

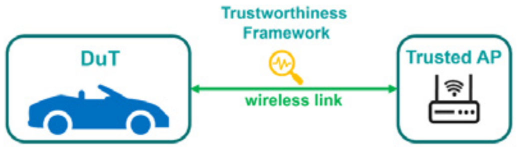
- RF Measurement Device (RFMD): The RFMD (also software-defined-radio-based) is placed in close proximity to one DUT to measure the interference signal strength. The measurement results are used to verify the interference at the DUT.

- Energy Harvesting Emulation Cell (EHCell): To emulate certain photovoltaic energy harvesting profiles, the EHCell consists of an opaque shielded box and controllable illumination inside to enclose fully assembled DUT containing solar cell. Figure 4 shows the constructed EHCell.

Figure 5: Energy harvesting emulation cell for testing of photovoltaic-basedenergy harvesting enhanced DUT.

Demonstrator: Wireless Trustworthiness Attack Detection

This demonstrator aims to evaluate the trustworthiness of wireless link in different wireless attack scenarios. We're interested in identifying any abnormal behaviors that deviate from the normal and intended operation of the system. It is important to note that in this context trustworthiness extends beyond just security considerations. We also want to evaluate the reliability of the link. Essentially, we're asking ourselves: How much trust do we have in the wireless communication system to transmit the data according to our predefined requirements in secure way?



To demonstrate these concepts of trustworthiness, we combine two outcomes of the project. First, the conducted extensive research on various cyber-attacks targeting wireless communication systems. Second, the acquired knowledge on evaluating trust and reliability in wireless sensor networks.

As specific use case for this concept, we have chosen the detection of Wi-Fi IEEE 802.11 connection hijacking in scenarios with high security and reliability requirements, such as factory automation or wireless vehicle updates. To accomplish this, we will employ an adaptation of the "Evil Twin Attack" in Wi-Fi and combine it with detection methods based on continuous observation of wireless link trustworthiness parameters.

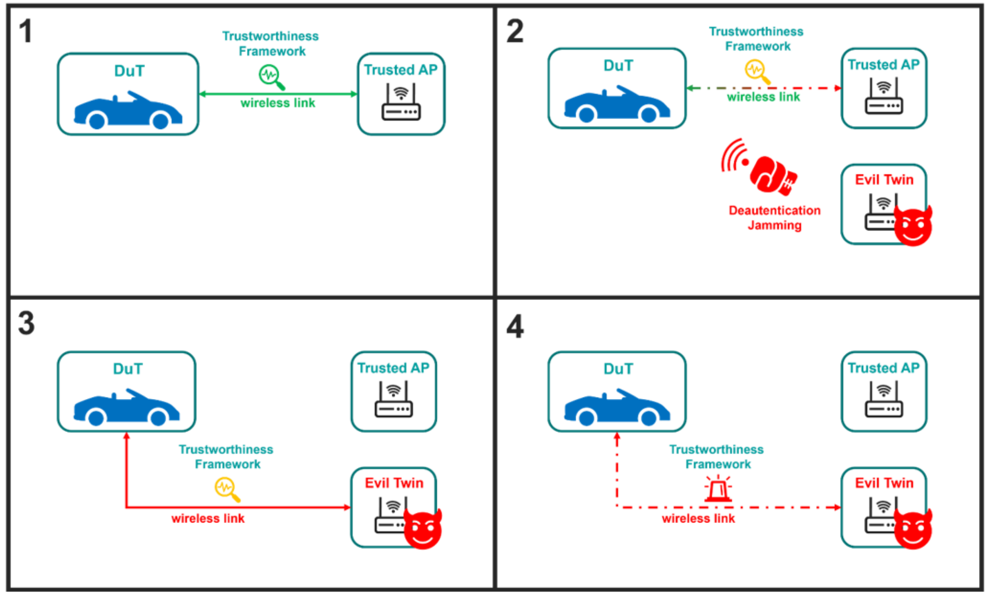


Figure 6: Wireless link trustworthiness parameters

Demonstration will contain following steps:

1. The device-under-test (DuT) will establish wireless connection with the trusted access point (AP). and carry out various tasks such as sensor value updates, file downloads, or control commands. The Trustworthiness Framework will collect lower layer measurements of the wireless link. These trustworthiness parameters are application specific and can for example include RSSI values, packet error rates, time difference of packet arrival, or data rate. For this trusted connection the trustworthiness parameters are collected, evaluated, and the results stored.

2. The malicious device known as the Evil Twin will initiate an attack on our DuT (e.g., deauthentication attack), forcing the DuT to disconnect from the trusted AP. At this stage, the Trustworthiness Framework will already identify certain security issues with the connection and place the DuT in an untrusted state. However, it is important to note that deauthentication itself may not necessarily indicate security issue, requiring further evaluations.

3. The Evil Twin will impersonate the trusted AP, tricking the DuT into connecting to the malicious device and for example enabling man-in-the-middle attack. This vulnerability is well-known issue with IEEE 802.11, resulting from ensuring seamless user-friendly roaming between different APs. From the DuT perspective the connection looks completely the same, if only higher network layers are considered. However, this represents significant security and reliability issue since the malicious device gains control over the data flow to the DuT.

4. The Trustworthiness Framework continues to evaluate the trustworthiness parameter of the new connection. Even though higher layer evaluations of the communication protocol may not reveal any differences compared to before, physical layer and link layer parameters can reveal significant variations. The RSSI value is one simple example where two different APs on two different locations might show huge difference in value. However, significant differences might also be found by observing timing related parameters due to different paths in the network. By comparing the statistics of the trustworthiness parameter before and after the detected change, we can evaluate the trustworthiness level of the link and for example terminate the connection completely if needed. In case of simple reconnection to the trusted AP, this step will show similarities, allowing the DuT to resume secure operations.

The Evil Twin attack is only one explicit example for the trustworthiness evaluation and other attack scenarios like jamming and physical obstruction of the DuT can be covered in parallel with this approach.

Demonstrator: Emergency Vehicle Approaching under Jamming Conditions

The main objective of the emergency vehicle approaching demonstrator is to establish methodology and metrics for analyzing the effects of jamming and other potential cyber-attacks in safety-critical scenarios by using the Connected Cars Digital Twin Platform (CCDTP) and Connected Cars Service Platform (CCSP). By leveraging CCDTP, we can virtually replicate real-world scenarios, including the movement of passenger vehicles and electric vehicles (EVs). By examining the maneuvers of passenger vehicles and electric vehicles (EVs), we can measure latency and assess the safety risks associated with these maneuvers. This enables us to conduct an impact analysis of jamming attacks in this particular scenario. The novelty and value of this demonstrator lie in its integration of CCDTP and CCSP, which go beyond the state of the art. CCDTP allows us to simulate and analyze the impact of cyber-attacks on V2X communication, offering comprehensive understanding of the vulnerabilities in the system. CCSP, on the other hand, stores and utilizes the data collected during scenario execution, enabling real-time analysis and visualization of logs and metrics. This combination of CCDTP and CCSP provides unique and powerful capability to assess the impact of cyber-attacks and evaluate the effectiveness of mitigation mechanisms in realistic virtual environment.

This demonstrator provides valuable tool with the ability to manage risks associated with cyber-attacks in safety-critical systems. Organizations and individuals can leverage the CCDTP and CCSP to gain insights into the vulnerabilities of V2X communication, make informed decisions regarding risk management, and test novel mitigation mechanisms and test custom-made scenarios of their own. The integrated nature of this solution showcases its innovation and advances the field of cybersecurity by enabling more comprehensive analysis of cyber-attack impacts on safety-critical scenarios and explore novel mitigation mechanisms, ultimately contributing to enhanced security and safety in these domains.

Demonstrator: Testbed for Embedded Wireless Devices

The main objective of the testbed is to automate the testing procedures of distributed embedded devices which are communicating wirelessly via radio-frequency channel. The testbed is intended to enhance the development process and verify the correct operation of the wireless embedded devices.

The communication architecture of the testbed is based on the so-called robot operating system (ROS) in version 1. The communication between the different testbed devices is realized via the ROS communication framework. ROS uses different underlying network protocols for communication. It abstracts the communication and operates as middleware between the distributed testbed devices. Due to this architecture, the testbed is very flexible and modular, and can be adapted to various testing scenarios for specific embedded devices and systems.

Furthermore, the openAPI-based specification of the testbed's API enables both, automated machine-based testing as well as manual interaction with the testbed which is often necessary during the development process of the embedded devices.

The implemented testbed components together with the modular architecture of the testbed and its flexible API enables the testing of operational aspects, security aspects, aspects of robust communication, power consumption aspects, energy harvesting aspects, and environmental condition aspects.

Demonstrator: Wireless Trustworthiness Attack Detection

With more and more wireless devices, trustworthiness of wireless link becomes essential. Especially in industrial communication or scenarios involving human interaction (e.g., vehicular communication, automated factories), constant observation of the wireless link is necessary to ensure predefined behavior. The overall goal is to assess the trustworthiness of the wireless link and detect issues during specific attack scenarios. While trustworthiness is usually defined at higher network layers, involving topics such as cryptography, secret key exchange, and security exploits of overlaying applications, comprehensive concept of trust and reliability requires evaluation from lower network layer perspective, specifically focusing on the wireless link itself.

In industrial settings the use of wireless communication is still avoided in lot of use-cases. lower-level view on trustworthiness can have huge security and safety impact in these settings, extending the applications for wireless communication.

Demonstrator: Testbed for Embedded Wireless Devices

The intended usage of the testbed is to enhance the development process of embedded wireless devices. Thus, the testbed will be exploited in future industry as well as research projects which integrates the development of such devices. This will enhance the competitiveness of LCM, GUT, SAL, and JKU.

Use Case 5.4

Use Case (UC5.4) entitled 'Intelligent wireless systems for smart port cross-domain applications'. This Use Case focuses on the implementation of IoT solutions in the maritime industry to address real business and industry needs. The results of this work are presented through various demonstrators in different locations, each of which showcases specific applications of IoT technology.

Potential benefits for the maritime sector:

- Safety: Improved communication and security measures increase the safety of autonomous operations.
- Efficiency: Network simulations and digital twins optimise port operations, increasing efficiency and reducing downtime.
- Security: Enhanced authentication, monitoring and detection improve overall security.
- Maintenance: Predictive maintenance reduces costs and increases equipment reliability.
- Situational awareness: Systems improve understanding of the maritime environment and support decision making.

Demonstrators at the GUT Campus:

Real-time measurement and monitoring of V2X communication quality for safe and efficient operation of autonomous robotic vehicles

The sub-scenario of real-time measurement and monitoring of V2X communication quality for autonomous robotic vehicles was merged with the previously documented sub-scenario of network quality situation awareness. GUT, KAI and VEMCO collaborated to create demonstrator at the GUT campus that demonstrates the autonomous movement of robot while monitoring V2X communication in real time.

This demonstrator introduces an innovative approach to monitoring V2X communication and improving communication quality awareness on mobile platforms. KAI developed real-time wireless communication monitoring system with measurement agent installed on the V2X transceiver. This agent relays communication quality information to listener service on the robot controller.

The robot responds to deteriorating signal quality by moving backwards and sending notification to the VEMCO PSIM application.

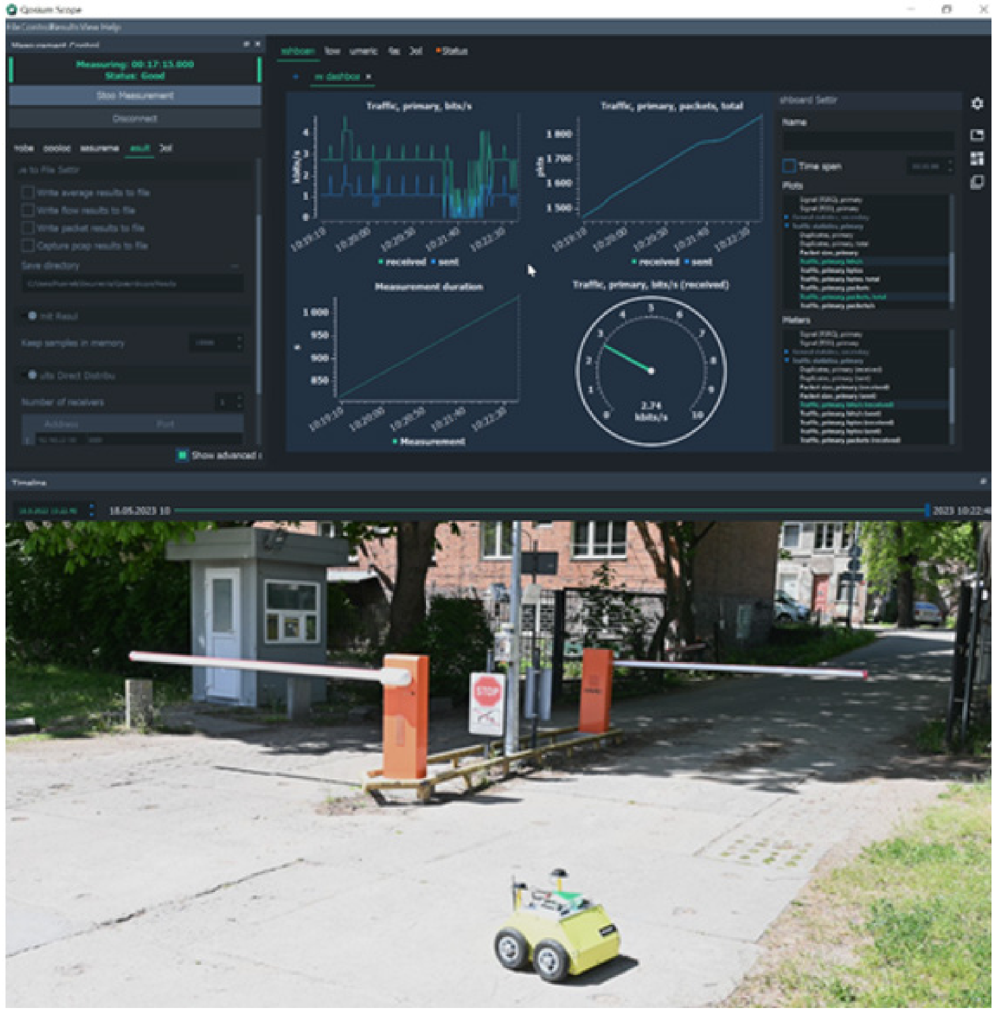


Figure 7: Autonomous robot / Quosium Scope application

In addition, the measurement results are sent to KAI's results solution, which triggers an alarm in the PSIM system when network quality degradation is observed. The alarm is based on continuous monitoring of Quality of Service (QoS) values, and an alarm is generated when these fall below pre-defined thresholds.

VEMCO extended the integration capabilities to handle additional network quality statistics included in the alarm messages. The value of this demonstrator lies in improving the self-awareness of mobile platforms and informing PSIM operators of detected problems, enabling timely action or enhancements for future mobile platform operations.

Localisation and secure communication for mobile platforms, including tracking with varying accuracy.

Simulation of dense wireless networks for smart port applications.

GUT, JKU and LCM conducted measurement campaign to evaluate GNSS-less positioning algorithms using UWB (Ultra-Wideband) and BLE (Bluetooth Low Energy) technologies. They implemented these algorithms on mobile platform provided by GUT, which was equipped with dedicated sensors for position estimation. The platform also included high-precision RTK-based positioning system for outdoor use. In addition, wireless sensor nodes for UWB time-of-arrival localisation (LCM), UWB time-of-flight localisation (JKU) and BLE beacons for signal arrival direction estimation (GUT) were installed on the autonomous mobile platform.

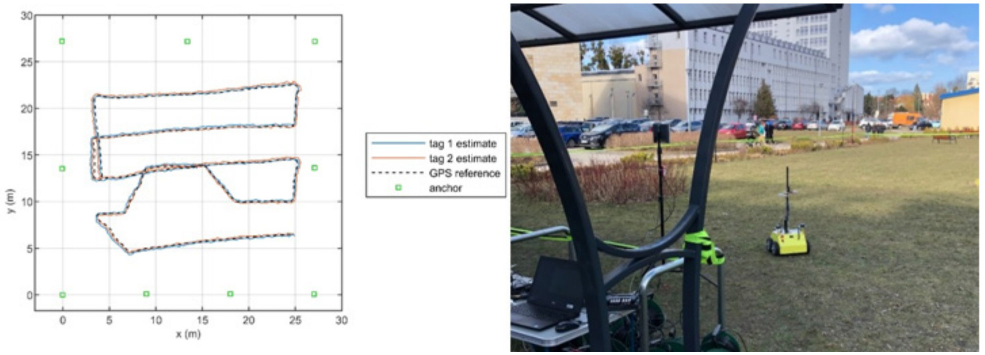


Figure 8: Joint demonstration and measurement campaign of GUT, LCM and JKU localization systems at GUT campus

By using different localisation systems, the project aimed to enable localisation and tracking with varying degrees of accuracy depending on the specific application requirements and available infrastructure. The results of these systems were visualised on map and compared to the accurate RTK data that served as the reference or ground truth. All three location systems demonstrated the ability to locate tags both indoors and outdoors. The project also included the ability to send notifications to the VEMCO PSIM platform when the robot entered pre-defined zones, increasing situational awareness and safety.

Authentication and authorisation of autonomous units.

During the InSecTT demonstration at the GUT campus, CISC was challenged to develop hardware device that would enable GUT's autonomous robot to securely access infrastructure wirelessly, using proximity wireless protocols such as BLE and UWB. They developed cloud-based device management platform to monitor and manage user identities across multiple services, including mobility, public transport and smart cities.

This service platform was integrated with GUT's cloud services to incorporate location information and monitor the autonomous robot. Secure elements and wireless protocols were implemented to ensure user trust. mobile application provided user-friendly interface for accessing nearby services through the hardware device. Identity and privacy tokens were securely updated and stored on the hardware device for user or robot access.

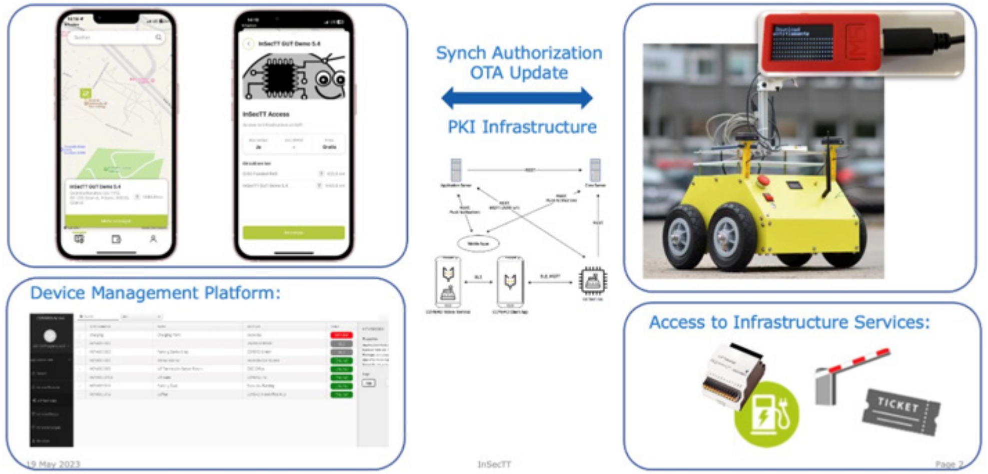


Figure 9: System architecture for wireless secure access for the autonomous robot to infrastructure

GUT installed the hardware device at one of the entrances to the GUT campus, allowing autonomous robots to enter. The opening of the entrance barrier depended on the authorisation system provided by CISC, which allowed access to the autonomous platform. Notifications of barrier openings were also sent to VEMCO's PSIM platform for further monitoring and control.

Digital twin for connected cars

The main objective of this scenario is to use the MarUn toolsets to improve the development and testing of V2X (Vehicle-to-Everything) applications. This includes conducting large-scale demonstrations of V2X applications through the Connected Cars Digital Twin Platform (CCDTP) and developing monitoring applications for V2X communications.

Within the CCDTP, each V2X application is emulated and able to communicate with each other, fostering cooperative awareness and delivering real Intelligent Transportation System (ITS) services as seen in real-world scenarios. The CCDTP will serve as testbed to verify and validate the functionality and proper integration of modules developed by other project partners. In the context of the Smart Port, such system can be used to validate V2X communication between vehicles and port infrastructure elements, e.g. to exchange information about traffic or collisions on internal port roads, especially when it comes to planning and dynamically changing infrastructure.

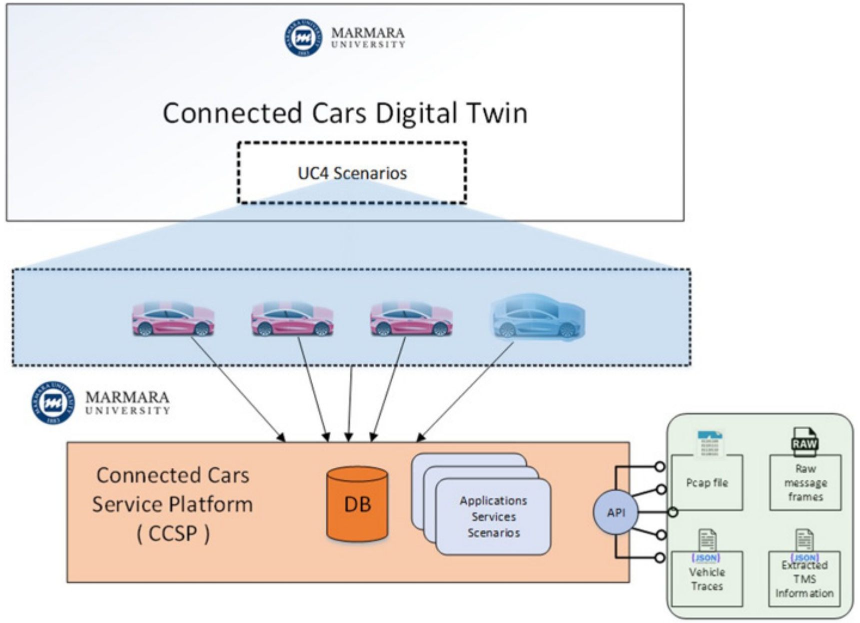

MARMARA UNIVERSITY
Connected Cars Digital Twin
UC4 Scenarios
MARMARA UNIVERSITY
Connected Cars Service Platform (CCSP)
DB
Applications Services Scenarios
API
Pcap file
RAW
Raw message frames
JSON
Vehicle Traces
JSON
Extracted TMS Information

Figure 10: System High Level Architecture

In addition, the platform uses real or realistically generated vehicle traces to execute scenarios and interfaces with third-party components through the Connected Cars Service Platform (CCSP), enabling message transmission, storage and visualisation.

Asset tracking at the campus

GUT has developed calibration-free localisation system using BLE tags and ESPAR antennas, which can be easily extended in range by adding more gateways, each consisting of an ESPAR antenna and transceiver. This system has been deployed in GUT campus corridor to track assets equipped with BLE tags. GUT and VEMCO collaborated on demonstrator that alerts VEMCO's PSIM platform when monitored assets leave designated zone.

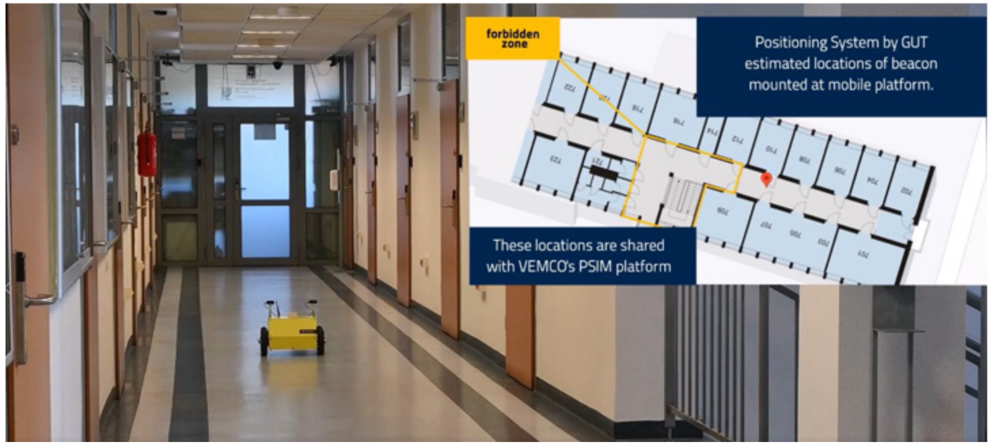

forbidden zone
Positioning System by GUT estimated locations of beacon mounted at mobile platform.
These locations are shared with VEMCO's PSIM platform

Figure 11: Asset tracking at GUT campus corridor

The PSIM operator can then decide whether to notify security personnel via mobile application. This low-cost system offers novel approach to asset tracking, particularly for indoor environments, making it suitable for tracking valuable or critical equipment such as fire extinguishers.

Location awareness to detect unauthorised presence in the area

The Localisation Awareness - Unauthorised Presence in Area demonstrator is integrated into two sub-scenarios: "Asset tracking at the campus" and "Localisation and/or Secure Communication for Mobile Platforms". Both of these demonstrated systems have the capability to send presence notifications to VEMCO's PSIM platform. This functionality enhances security measures by alerting the PSIM platform to any unauthorised presence within defined area.

Image-based surveillance

The image-based surveillance demonstrator is collaboration between WAPICE and VEMCO systems. It was originally intended to be recorded at the GUT campus, but was moved to the WAPICE campus due to difficulties in setting up the video stream. This demonstrator is associated with another demonstrator called "Machine Vision-based Object Detection". It focuses on the use of machine vision technology to detect and monitor objects, demonstrating its capabilities in the context of surveillance and monitoring applications.

Monitoring of security seals

ISS RFID has developed intelligent IoT tags in the form of reusable security seals with both passive (UHF, NFC) and active (BLE) communication capabilities. These security seals consist of PCB with tamper-evident features and logging capabilities, mechanical locking mechanism monitored by the PCB, and protective housing for all components. The primary communication method is BLE.

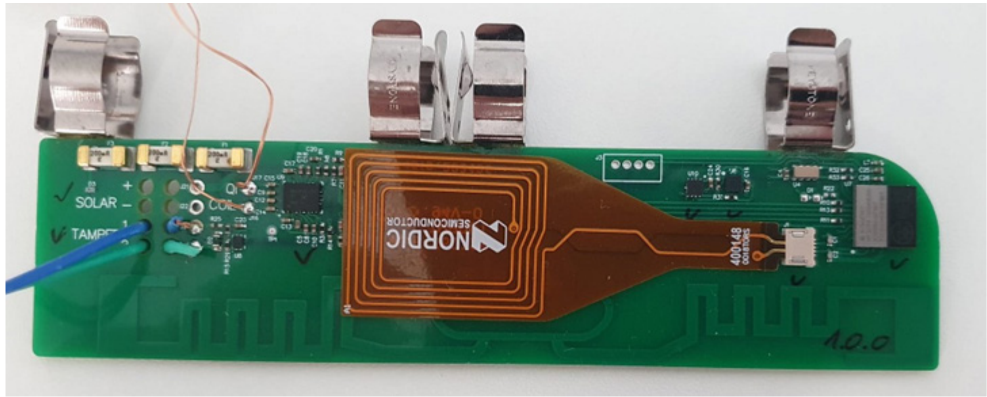


Figure 12: Reusable security seal

GUT integrated this solution into their MPS system and established connectivity to the VEMCO PSIM platform. demonstrator was set up at the GUT campus to demonstrate the use of ISS RFID's smart security seals in various applications. These seals can be applied to items such as safety equipment (e.g. fire extinguishers), personal safety equipment on ships or access points (e.g. gates).

In the scenario shown, the security seal is monitored by GUT's MPS location monitoring system. In the event of unauthorised access or tampering with the equipment or access point, the MPS system sends an alert to the PSIM platform. The PSIM platform then notifies operators to inspect and verify the affected area. In addition, the MPS system continuously tracks the location of the seal in real time, enabling secure monitoring of moving assets. This system enhances security and asset protection in various contexts within the maritime domain.

Demonstrator at the Port of Gdansk:

Vehicle localisation within port infrastructure

GUT has developed an advanced system for monitoring the location and operating parameters of vehicles in an industrial environment using wireless communication. This system has been tested at the Szczecińskie Quay in the Port of Gdansk and is designed to track heavy motor vehicles, such as Kalmar heavy forklifts, in real time.

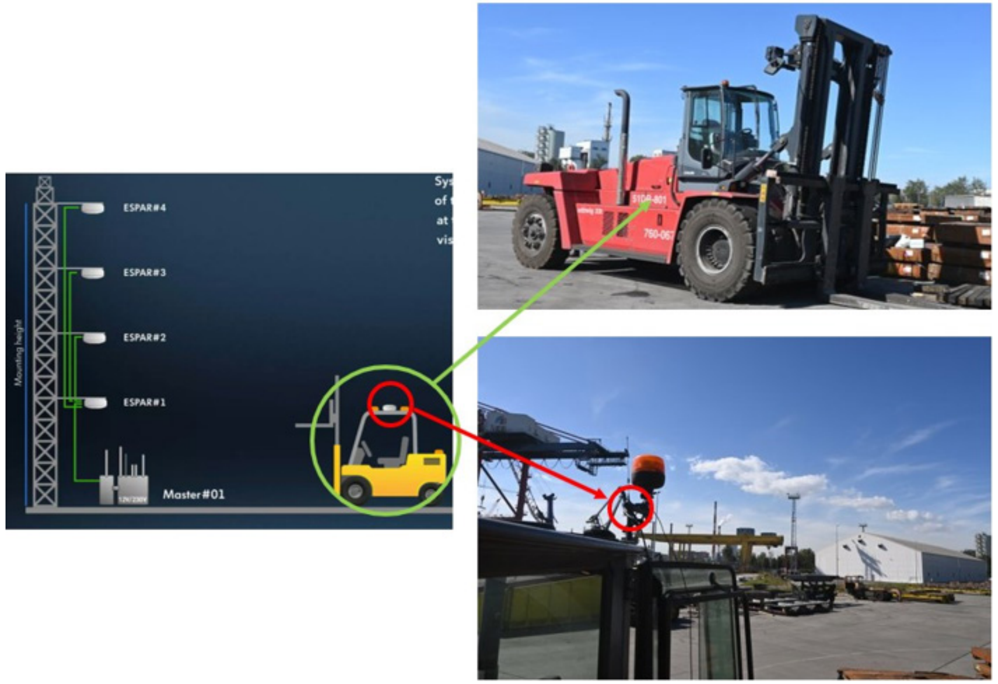
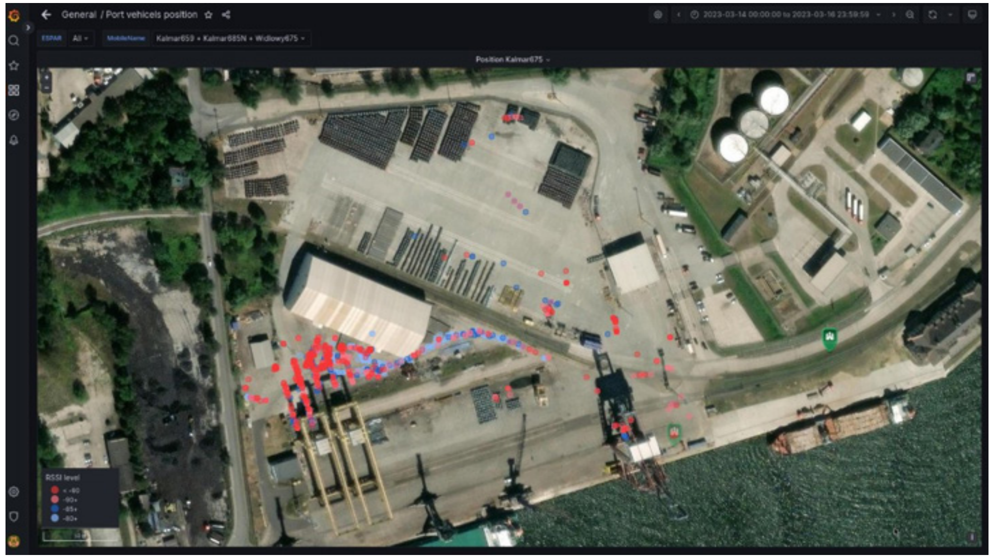


Figure 13: Localized module mounted on the port vehicle

The tracking system at the Port of Gdansk includes four gateways equipped with Bluetooth Low Energy (BLE) receivers and ESPAR antennas. These gateways receive BLE advertising packets from vehicle-mounted transmitters. The BLE transmitters, designed as beacons, transmit signals containing GPS coordinates, battery charge levels and engine status. Importantly, these beacons are passive devices that do not require active connections to other devices and have their own battery power systems, ensuring continuous monitoring even when vehicles are switched off.


General / Port vehicels position

2023-03-14 00:00:00 to 2023-03-16 23:59:59

ESPAR: All

MobileName: Kalmar659 + Kalmar685N + Widlowy675

Position Kalmar675

RSSI level

●	< -90
●	-90+
●	-85+
●	-80+

Figure 14: Port vehicle tracking with open source Grafana dashboard

GUT's system provides accurate vehicle location information and integrates data collection and visualisation mechanisms to create user-friendly interface. It provides essential information in straightforward and intuitive manner. The independent power supply system allows continuous monitoring even when the vehicle's power unit is switched off. In addition, the system can generate summaries of vehicle working times and analyse trajectories, which can lead to optimisation of vehicle use and improvements in operational efficiency. This innovative solution is beneficial for improving fleet management and operations in industrial environments.

Demonstrator on Tucana ship:

Data Analysis for Predictive Maintenance

GUT in collaboration with RTE and RISE has developed machine learning (ML)-based platform for anomaly detection in industrial IoT systems, specifically for predictive maintenance. They equipped the m/v Tucana motorboat in the port of Gdansk with eleven sensors and developed ML algorithms for anomaly detection and classification. The focus of the anomaly detection was on identifying predefined states for on-board systems. For practical purposes, they simplified the task to serve as proof of concept.

The project implemented end-to-end communication from the boat to the ML-based platform and on to the user interface managed by Vemco. Near real-time predictions in live system influenced the choice of algorithms, communication protocols and software design, with focus on reliability and error handling, especially in the ML components.

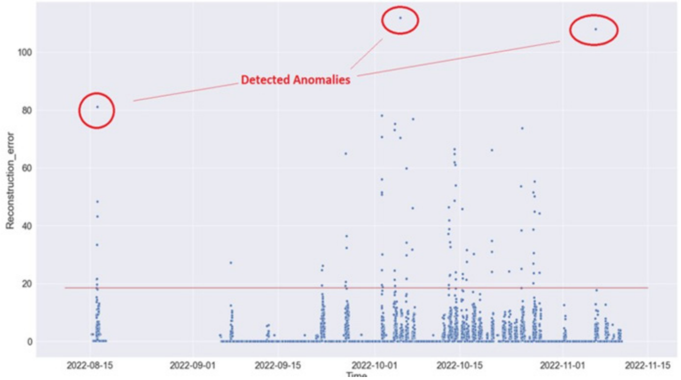


Figure 15: Output of the trained model on the validation data

In the first stage, sequential neural network was developed using the TensorFlow framework, and the model was saved in format suitable for deployment on various hardware devices.

In the second stage, neural network was trained in cloud environment and exported as TensorFlow Lite model, optimised for on-device machine learning with broad platform support. An exploratory approach was also taken using an unsupervised ML model (clustering).

RISE worked on ML-driven data analysis using sensor data from the autonomous boat Tucana. They developed data analysis pipeline for intelligent anomaly detection, including pre-processing, statistical analysis and autoencoder-based ML models. The autoencoder model effectively detected anomalies with high degree of accuracy.

The project highlighted the challenges of working with ML in embedded systems, considering limited resources, security, real-time requirements, throughput, cloud vs. edge computing, robustness and transparency. It emphasised that the effectiveness of an ML algorithm is closely linked to data exploration and interpretation.

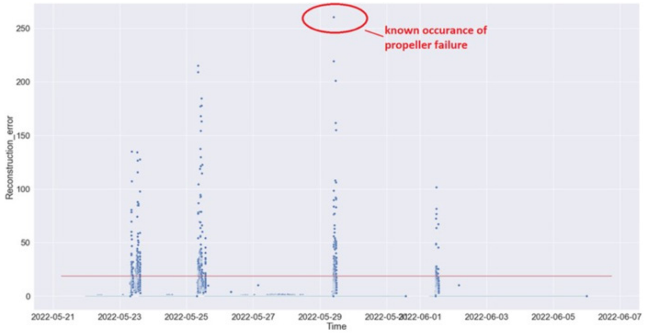


Figure 16: Effectiveness of the trained model on the test data containing the known defect. Detects the known defect in the test data set with high accuracy

key conclusion was that while ML can be powerful tool during development, it may not always need to be included in the final product. Suggestions for further development included combining cloud and edge computing based on network availability, and implementing dynamically retrained framework architecture for embedded AI.

Situational awareness system.

GUT has developed Situational Awareness System designed to enhance the captain's awareness of objects on the water surface and ultimately improve maritime safety. The primary configuration of the system includes flexible payload consisting of two LIDAR's, two RGB cameras and radar, all connected to central processing unit (main box). The main box processes real-time data from the ship and detects objects on the water surface.

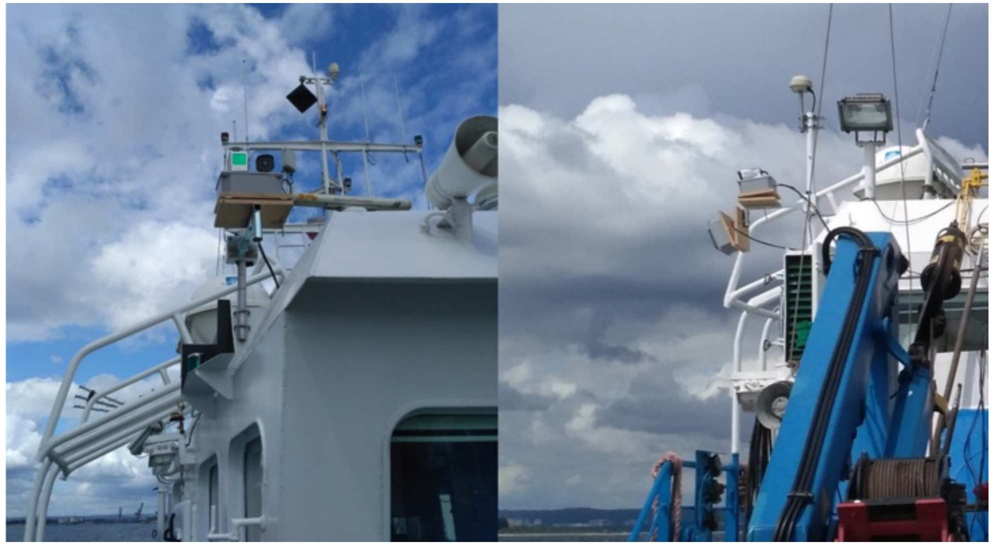


Figure 17: The Flexible Payload installed on m/v Tucana

For the final demonstrator, GUT installed this flexible payload on the m/v Tucana. Throughout the third year of the project, GUT conducted series of tests using variety of objects including buoys, lifebuoys and fishing net markers. The system demonstrated the ability to detect larger objects such as buoys at distances of up to 179 metres, with reliable detection at 126 metres. The detection range is dependent on the quality of the sensors, and the flexible payload is designed to be adaptable for different tasks, making the sensors easily interchangeable.

The system combines data from LIDAR, cameras and radar to provide comprehensive situational awareness. Even small objects such as lifebuoys, which are barely visible to the naked eye from few metres away, can be reliably detected by the system from distance of 47 metres. Importantly, the situational awareness system operates independently of lighting conditions, ensuring its effectiveness both day and night.

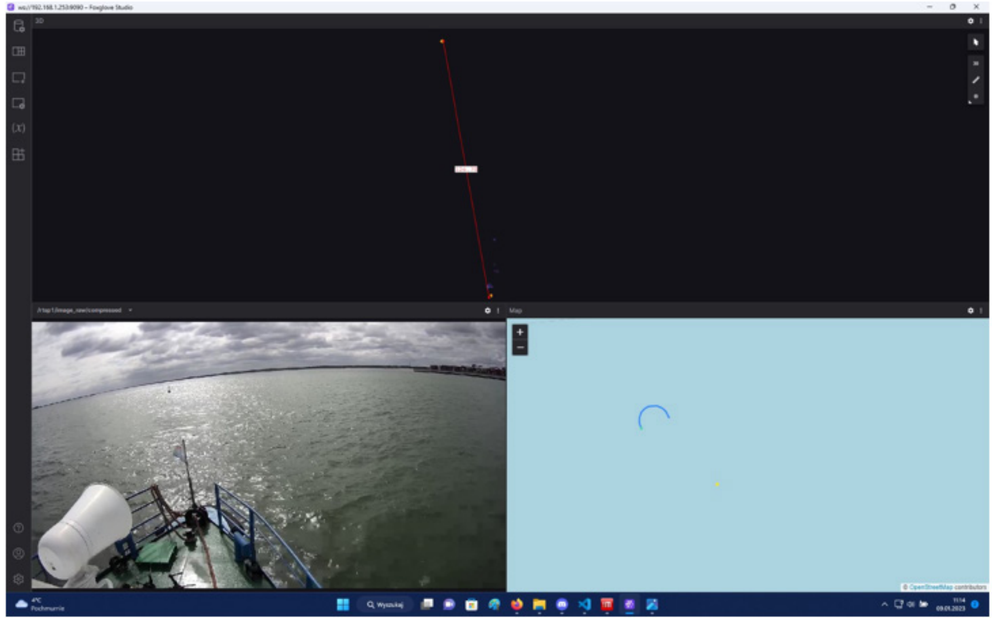


Figure 18: Example of detecting buoy at distance of 126 m

In summary, GUT's Situational Awareness System significantly enhances ship's captain's ability to detect and respond to objects on the water's surface, improving maritime safety and navigation in variety of conditions.

Demonstrator on ISS RFID test vessel (Baltic Sea):

(Semi)autonomous vessel operation – remote inventory management.

Demonstrator present capability of the system designed to monitor items on ships, with the aim of improving the safety of the crew and the level of security on board. It uses IoT tags in various forms, including passive RF tags, active tags and multi-use security seals based on passive (UHF, NFC) and active communication (BLE) technologies.

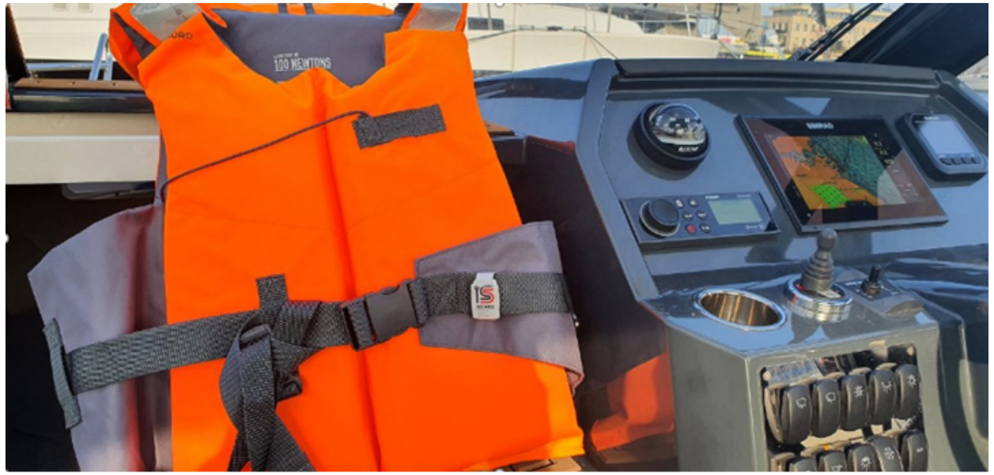


Figure 19: IoT tags attached to items on the vessel

The demonstrator shows IoT tags attached to items that need to be monitored, such as safety equipment like fire extinguishers and personal safety equipment on ships. These tags can be monitored in two main ways:

Through handheld devices and through dedicated platform: Users can use dedicated Android app or web-based asset management platform to monitor tagged equipment. The Android app enables semi-autonomous monitoring to check if the equipment is still on board and if it needs maintenance or inspection. The app checks the information against database accessible via REST API from the web platform.

Via the GUT MPS location monitoring system: Real-time monitoring of the availability and location of equipment on board the vessel is provided by the GUT MPS location monitoring system. This system continuously tracks the status of equipment and intelligent security seals can trigger alerts in the event of unauthorised access or tampering.

In addition, the system has the capability to monitor "man overboard" scenarios where equipment is suddenly in the water, ensuring rapid response in critical situations.

In summary, the system leverages IoT technology and intelligent security seals to enhance the security and safety of crew members and items on board vessels. It provides real-time monitoring, asset tracking and the ability to respond quickly to emergencies.

Demonstrator at the Port of Cetraro (Italy):

Port surveillance

The proposed system aims to monitor unauthorised access to port areas from the sea shore and will be tested independently in specific scenario, as it does not require integration with other systems. CINI-UNICAL and LDO-SDI have selected the Port of Cetraro in southern Italy (Calabria) as the ideal location for the demonstration, as it is primarily used for tourism and fishing, ensuring minimal disruption to normal port activities.

Figure 20: Panorama of Cetraro Harbour (Source: Porto di Cetraro-Marina Resort)

The architecture of the surveillance system is designed as an underwater access control system. It consists of network of acoustic and magnetic sensors strategically placed at choke points, approach routes or specific locations. These sensors are interconnected by wires for both power and data distribution. The system uses an MQTT architecture with sensors as publishers and junction boxes (JB) as brokers. The configuration can range from simple local control station wired to barriers for data collection and processing, to more integrated solution using Smart Communication Node (SCN) to connect the system to remote harbour control station. The SCN is Software Defined Network (SDN) consisting of an SDN Controller and Forwarding Devices (FDs) that manage and control communication within the barriers.

The SDN Controller includes Reliability Module to automatically select wireless interfaces based on network conditions, and Security Module with an AI-based Intrusion Detection System (IDS) to detect and mitigate cyber-attacks. The IDS uses an innovative Deep Learning (DL) model to detect zero-day attacks.

The proposed architecture is integrated with the VEMCO platform for event notification and tracking generated by magnetic and acoustic sensors and SDN controller modules. This integration enhances event management capabilities, enabling real-time detection and response to potential security threats. The architecture can leverage VEMCO's capabilities to store sensor detections, generate alerts and provide historical context for events.

To conduct realistic testing, barrier prototypes will be deployed outside the harbour at depths of 5 to 10 metres. These tests will involve remotely operated vehicles carrying magnetic targets along pre-defined or operator-controlled routes, and divers passing near/over the nodes to simulate intrusions. Depending on the availability of prototypes, the two barriers may be tested together or separately.

Demonstrator at Venit Lab (Marmara University Campus):

Network quality monitoring

Marmara University's demonstrator emphasises the use of artificial intelligence (AI), anomaly detection and network performance monitoring within the IoT network. The focus is on the development of an application that collects critical quality of service (QoS) parameters from IoT devices.

This application serves as data collection tool, collecting information related to link quality, network performance, delay measurements and device-specific details. The collected parameters are continuously monitored and analysed at central control centre to identify anomalies, connectivity issues and service availability problems. By using AI to analyse and track changes in the measurements, the system can detect connectivity issues and performance variations between devices, acting as indicators for anomaly detection and ensuring service availability.

The algorithms developed for this purpose focus on analysing the collected data to assess the reliability and availability of wireless links and services. Data is cached on the IoT devices and then transmitted to the monitoring platform. The control centre operates monitoring platform with RESTful interfaces and MQTT broker that provides APIs for the application.

In summary, this demonstrator covers various aspects of end-to-end data communication, analysis and management within the IoT network. It enables multiple applications and algorithms to run concurrently and demonstrates the integration of Marmara University's monitoring platform with VEMCO's PSIM platform to improve overall network performance and reliability.

Demonstrator at Pavotek Campus (Teknopark Istanbul):

Network anomaly detection

Pavotek has developed an intrusion prevention system that uses machine learning to detect targeted attacks. This system is designed to analyse network traffic in real time, as well as network captures such as pcap files and network streams generated by Zeek/Bro. Its primary purpose is to process and analyse input data and alert the user to any suspicious behaviour detected.

The system uses Convolutional Neural Network (CNN) based model to detect malicious traffic using machine learning techniques. It runs detection modules and stores all reports, alerts and characteristics in Redis database. The system generates output, including logs, which are stored in designated folder (output/directory) containing alert.json, alerts.log and error.log files.

In the context of smart ports, the use of such intrusion prevention systems, which use machine learning to identify malicious activity in network traffic on port infrastructure, can significantly improve the overall security of IoT network operations. This proactive approach helps protect network assets and data from targeted attacks, contributing to safer and more secure maritime domain.

Demonstrator at UCC Campus (University College Cork):

Analysis of crane vibration sensor data.

UCC (University College Cork) has used machine learning (ML) and data mining (DM) algorithms to analyse vibration in ship-to-shore crane drive trains. Vibration sensors placed on key drivetrain components collect and log data, typically at half-hourly intervals, capturing various vibration metrics. To facilitate analysis, an automated workflow was developed to consolidate vibration data from multiple cranes into standardised dataset suitable for ML and DM algorithms. This dataset contains approximately 7.6 million records, each representing sensor reading with associated metadata indicating the source crane and the location of the sensor on the driveline.

Notably, this dataset lacks labels for typical predictive maintenance tasks such as predicting remaining useful life. Instead, UCC used ML and DM techniques to sift through the data and identify patterns and anomalies that might be of interest to those responsible for maintaining or operating the crane.

To present the results, the demonstrator uses the Grafana platform to visualise the vibration sensor data and present the results of the ML and DM algorithms. The drive train data is stored in PostgreSQL database and Grafana instance is connected to this database. The database can be queried to provide input to an analysis pipeline, and the results are written back to the database. Grafana dashboards are then used to demonstrate some of the patterns discovered and example use cases, providing valuable insights for the maintenance and operation of the crane.

Video feed verification.

Video camera orientation and position estimation is achieved through combination of machine learning techniques and traditional computer vision algorithms. The aim is to determine the orientation and position of single networked camera without the need for stereo configuration in the scene. To ensure the authenticity and liveliness of the camera, method is used that compares the estimated trajectory of the camera with the crane’s motion management logs.

The approach uses machine learning and computer vision algorithms to estimate the trajectory and position of the camera. Camera calibration is performed using OpenCV. This technique is illustrated in the figure below, which shows an example of trajectory estimation using consumer-grade Logitech webcam.

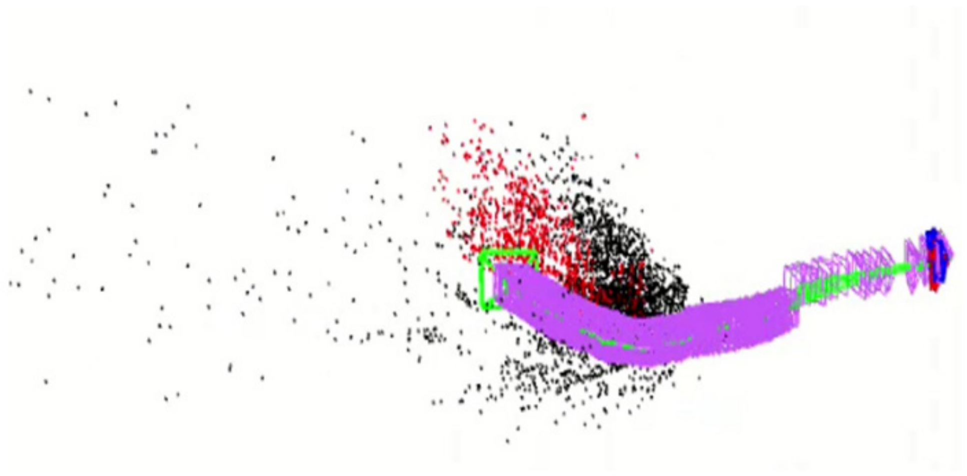


Figure 21: Trajectory and sparse point cloud

Demonstrator at LCC Client Container Terminal:

Live streaming of crane operational data

LCC (Client Container Terminal) has developed an architecture for live streaming of crane operational data from the crane PLC (and crane SCADA system) to cloud server for analysis and client reporting. This proof-of-concept demonstration was conducted at the Port of Cork and shows the basic functionality of the platform using sample operational metrics and graphics. The architecture is optimised for storage, communications, security and edge/cloud computing, providing an efficient and flexible configuration. The platform enables the integration of predictive monitoring models for crane drives using algorithms developed by UCC. These algorithms use the equivalent of 36 years of operational data from nine container cranes in Europe, combined with application expertise from LCC.

The condition monitoring aspect of the demonstrator focuses on models for hoist rope deflection and degradation, which enable the estimation of remaining useful life. These models, developed by LCC and UCC, have the potential to support the mandatory periodic inspection of ropes in accordance with ISO 4309 standards. Graphical representations are used to communicate the use and degradation of ropes. While the scenario meets the requirements for predictive maintenance, especially in the case of estimating the remaining service life of ropes, it is demonstrated as support system due to industry-specific standards such as ISO 4309.

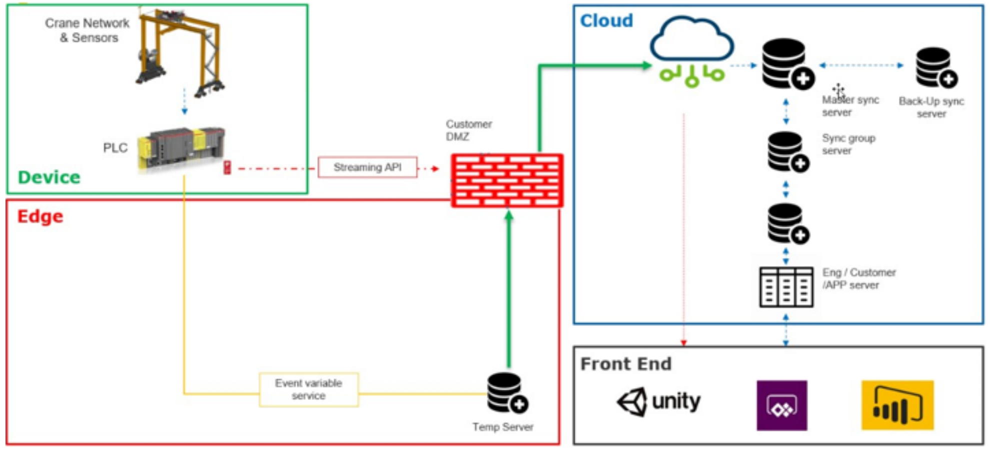


Figure 22: Container Crane IoT platform included in demonstrator and enabler for deployment of condition monitoring and prediction models

In addition, LCC has supported InSecTT partner UCC in the development of predictive maintenance algorithms and video feed verification algorithms. This support involves the acquisition of significant amounts of data from sensor-equipped cranes, including both vibration and video data, to improve crane monitoring and maintenance processes.

Demonstrator at WAPICE Lab:

Machine vision based object detection.

Wapice has developed machine vision system integrated with an IoT platform that enables the rapid creation of large-scale, production-ready IoT applications. In the context of smart ports, this platform is designed to create applications and dashboards for gathering information from various sources, including sensors and camera systems.

The core idea is to use the growing number of surveillance cameras in port areas and industrial zones to understand logistics. These cameras are often under-utilised, and Wapice's solution focuses on computer vision-based monitoring. It tracks the position of assets, vehicles or people within defined critical areas using video streams from existing or purpose-built cameras.

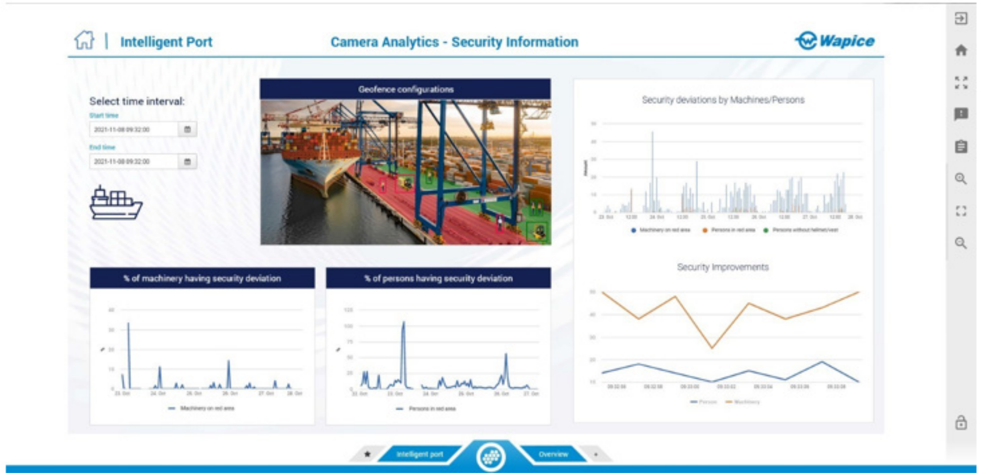

Intelligent Port
Camera Analytics - Security Information
Wapice
Select time interval:
Start time
End time
Geofence configurations
Security deviations by Machines/Persons
Security improvements
% of machinery having security deviation
% of persons having security deviation
Intelligent port
Overview

Figure 23: Dashboard schema visualizing port asset statistics and events

The system processes video streams from cameras, tracking and analysing areas of interest, such as entry and exit points. The processed information is sent to back-end server, where cloud applications can be developed using Wapice's IoT and AI back-end tools. This provides insight into areas for improvement, asset location and optimisation of logistics, such as evacuation procedures.

The configuration tool allows users to define critical areas within the camera's view, and this data is sent to the edge node, which is responsible for analysing the video stream. The system obfuscates sensitive GDPR data at the edge node, sending only non-sensitive information to the cloud.

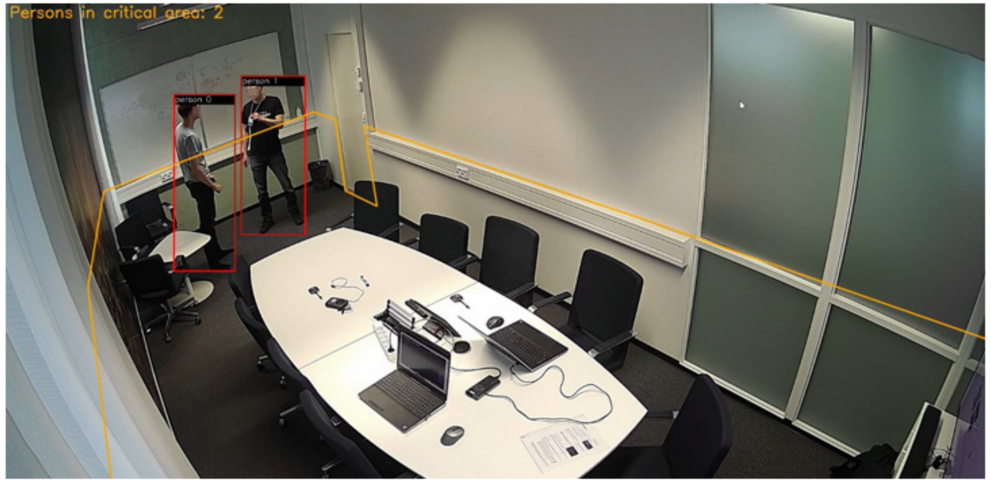


Figure 24: Critical area and detections

In practical demonstration, the system was deployed at Wapice's premises, demonstrating the detection of unauthorised individuals entering meeting room and triggering an alarm. Integration with Vemco's PSIM platform was also demonstrated, enabling event processing and visualisation.

The technology has wide range of applications in the port domain, including the detection of vehicles and individuals entering restricted areas. It ensures GDPR compliance by processing sensitive data locally, and only sending anonymised information to the cloud.

Use Case 5.5

Various demonstrators have been built for this use-case:

- Improved workflow solution for medical professionals doing rounds in hospital with many patient encounters by PRE in Eindhoven.
- Asset management solution for bed location tracking, role-based assignment, and status management by PRE in Eindhoven.
- Web based solution for the creation and training of explainable AI models by NXP-NL in Eindhoven.
- Contactless vital signs acquisition and quantification solution by VTT in Oulu.
- ECG acquisition and transmission solution for low data rate transmission from patient to cloud by TUD in Delft
- ECG anomaly detection web services and solution for cardiologists by JSI in Ljubljana.
- Heart disease qualification webservice by NXP-NL in Eindhoven
- Length of stay prediction service for hospitalized patients by NXP-NL in Eindhoven
- Automatic network slicing solution for hospital networks to achieve QoS guarantees for devices and applications by UTwente in Enschede.

Demonstrator Key Components

The following components for the demonstrators have been developed and integrated in the use-case demonstrators:

- patient health status and logistics dashboard application demonstrating the typical workflow for medical staff member who is doing round at the hospital to see all patients that are under his/her care by PRE in Eindhoven. It runs on portable tablet or laptop that the medical staff member can carry with him/her. To facilitate secure logon of the medical professional and to enable instant access to the data of any nearby patient, unique NFC cards are used for identification and data access. This demonstrator integrates all the TBBs that provide insights to patient's health and patient related hospital logistics, such as described below and shown in Figure 1.

- Image and radar-based vital signs prediction services by VTT, demonstrating two scenarios for single stationary patient:
    - Near real-time vital signs measurement using camera and radar.
    - AI-enriched vital signs for video data.

Based on patient ID as an input, as well as other parameters such as time period and types of observations, vital sign observations are returned in FHIR compliant format.

- ECG AI analytics and anomaly detection services and solution based on 12 lead ECG signals by JSI. These run as cloud-based services that processes ECG signals uploaded by medical professional and which return the detection results.
- wearable IoT device by TU Delft, that enables smart monitoring of body temperature and ECG of person 24x7. The wearable sensor is attached via waterproof surgical adhesive onto the chest of the person and will be connected via Bluetooth LE (BLE) to mobile phone in the vicinity.
- dynamical systems model for synthesizing PQRST ECG cycles by TU Delft, running on the wearable IoT device. Model parameters are updated per ECG cycle in real-time, after which the compressed set of meta parameters are transmitted instead of raw signals, thereby reducing transmission load, storage requirements.
- Webservice by TU Delft that enables retrieval of both compressed and raw ECG signals as collected and transmitted by the wearable IoT ECG sensor of TU Delft. Based on patient ID, type of ECG and time period, the service returns graphical representation of the data.
- XGBoost machine learning model ML engine by NXP-NL, predicting the length of stay of patient in hospital based on admission parameters (e.g., blood pressure, earlier admission, diabetic condition, etc). It runs as web service inside Docker container returning the explainability graph and predicted length of stay based on patient ID as input.
- TCN machine learning model ML engine by NXP-NL, calculating the probability of various heart diseases based on ECG signals with duration of 10 seconds, 5000 sample values. It runs as web service inside Docker container returning the probability distribution along with classification data for given patient ID.

- The eIQ toolkit of NXP to train explainable AI models for deployment in NXP chips. It is toolkit developed by NXP, currently based on imaging. Sensor data explainability will be added later, based on year 2 and 3 InSecTT research.
- AI based Wi-Fi network manager that performs automatic network slicing based on QoS requirements of network devices and applications by UTwente. It also integrates simulation of real-time sensor network with patients' cameras in hospital.

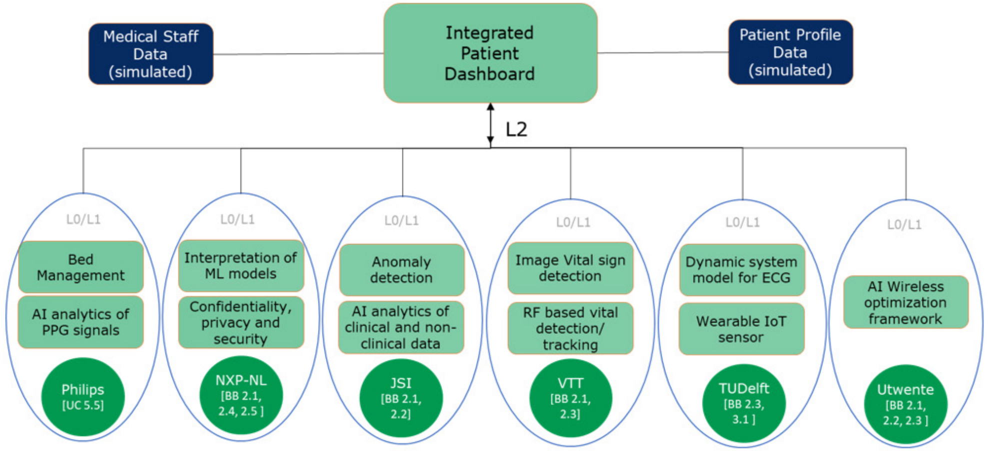
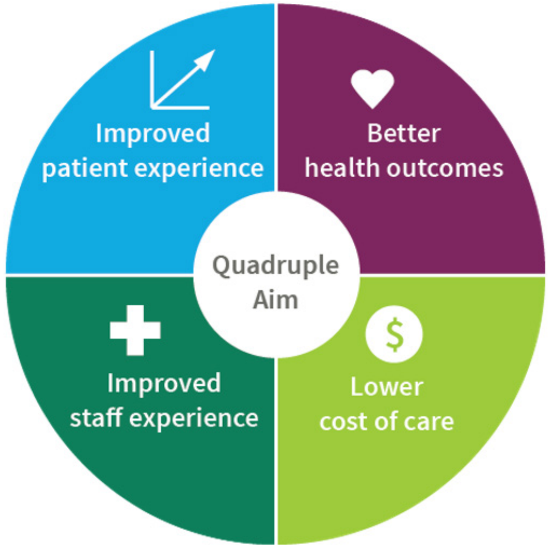

Medical Staff Data (simulated)
Integrated Patient Dashboard
Patient Profile Data (simulated)
L2
L0/L1
Bed Management
AI analytics of PPG signals
Philips [UC 5.5]
L0/L1
Interpretation of ML models
Confidentiality, privacy and security
NXP-NL [BB 2.1, 2.4, 2.5]
L0/L1
Anomaly detection
AI analytics of clinical and non-clinical data
JSI [BB 2.1, 2.2]
L0/L1
Image Vital sign detection
RF based vital detection/ tracking
VTT [BB 2.1, 2.3]
L0/L1
Dynamic system model for ECG
Wearable IoT sensor
TUDelft [BB 2.3, 3.1]
L0/L1
AI Wireless optimization framework
Utwente [BB 2.1, 2.2, 2.3]

Figure 25: High level architecture of Use Case 5.5.

The objective of the demonstrator is to show better workflow and care pathways for credible healthcare scenario in the hospital environment, in order to improve the Quadruple Aim of Healthcare (Figure 1).

Figure 26:. Quadruple Aim of Healthcare



In particular, the demonstrator shows how IoT and AI help to improve care and outcomes for patients, improve the wellbeing of patients and staff and improve the operational efficiency to reduce the overall costs.

IoT devices are used for tracking and state management of assets in the hospital, continuous ECG acquisition and transmission, as well as for the unique identification of patients and hospital personnel, including their role and associated permissions to enable effortless access to patient data.

AI is used for the prediction of patient health trends, detection of health issues and the provision of first diagnosis. Furthermore, AI is also used for the reliable and real-time transmission of critical health information, for extreme data compression without loss of information, for remote measurement of vital signs and for the prediction of patient's discharge date.

Seamless interoperability between remote siloed hospital information systems is demonstrated by the exchange of vital sign data from remote vital sign measurement system to the patient dashboard according to the FHIR healthcare data standard, which further improves the overall operational efficiency.

Note that in the USA, yearly costs of hospital readmissions have risen up to $26 Bn, employee turnover & burnout to $83 Bn and delayed discharge to $56 Bn, demonstrating strong business demand for improving the quadruple aim of healthcare.

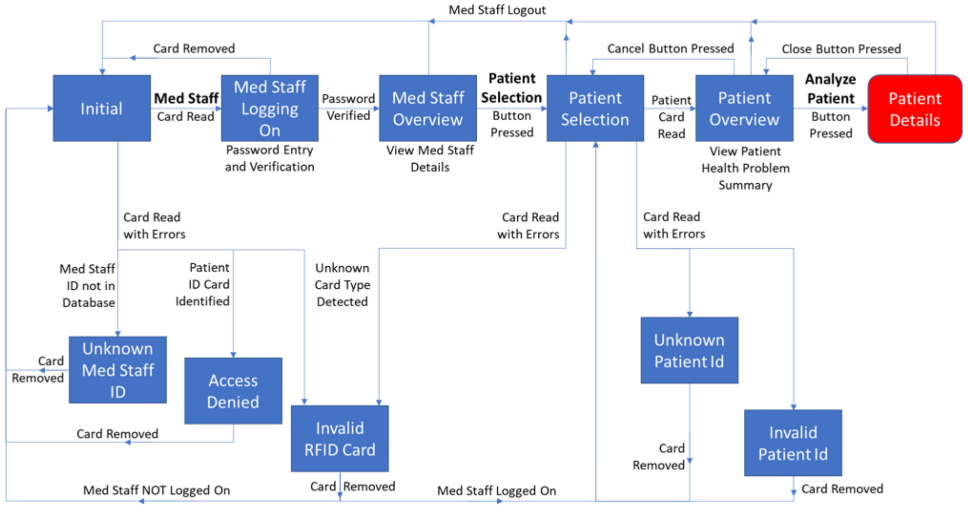
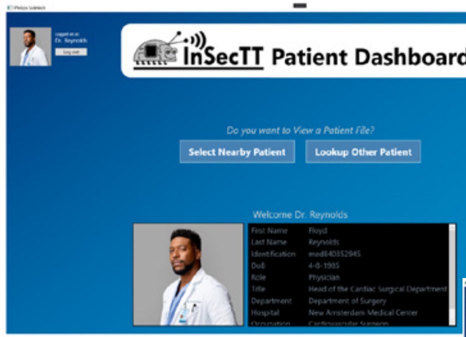


Figure 27: States and transitions for consultation workflow in the InSecTT patient dashboard.



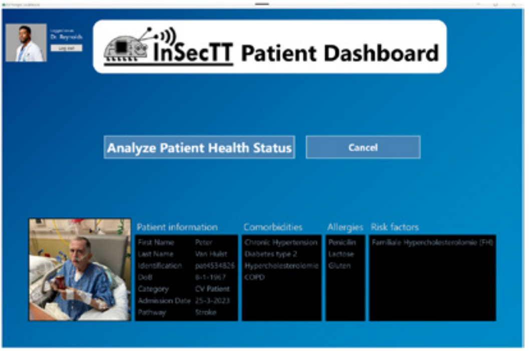
Do you want to View a Patient File?

Welcome Dr. Reynolds

First Name	Floyd
Last Name	Reynolds
Identification	med840352945
DoB	4-8-1985
Role	Physician
Title	Head of the Cardiac Surgical Department
Department	Department of Surgery
Hospital	New Amsterdam Medical Center
Occupation	Cardiovascular Surgeon

Figure 28: Patient selection after login of medical professional with his NFC ID card. Profile information is shown of the medical professional, who can logout at any time.

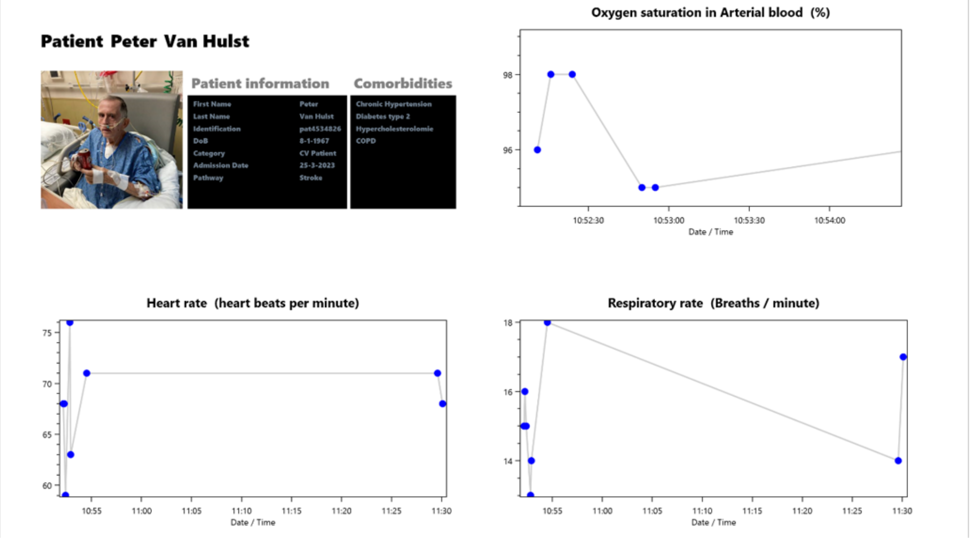
Figure 29: Important information shown after selection of nearby patient.



Patient information

First Name	Peter
Last Name	Van Hulst
Identification	pat4534826
DoB	8-1-1967
Category	CV Patient
Admission Date	25-3-2023
Pathway	Stroke

Comorbidities	Allergies	Risk factors
Chronic Hypertension	Penicilin	Familiale Hypercholesterolomie (FH)
Diabetes type 2	Lactose	
Hypercholesterolomie	Gluten	
COPD		



Patient Peter Van Hulst

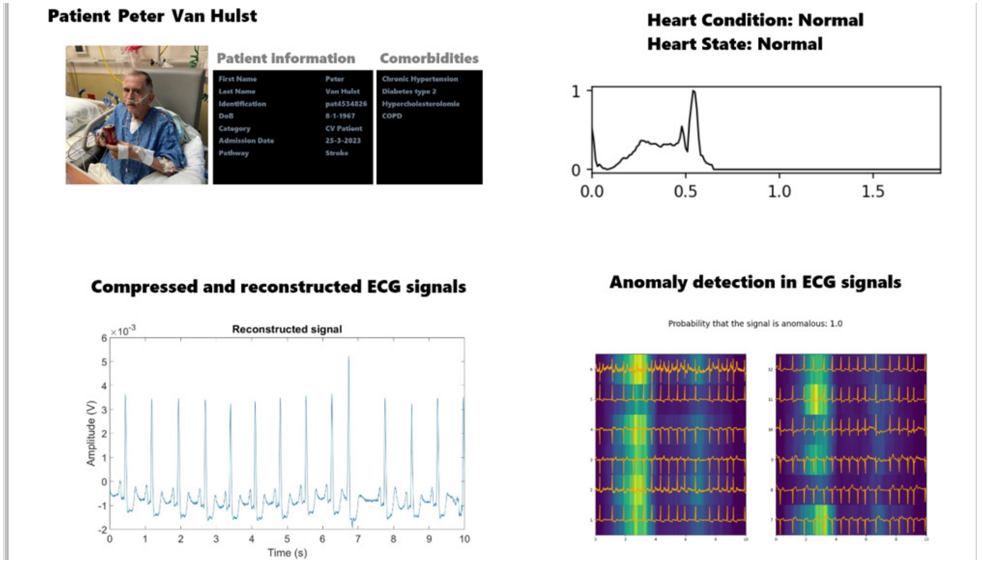
Patient information

First Name	Peter
Last Name	Van Hulst
Identification	pat4534826
DoB	8-1-1967
Category	CV Patient
Admission Date	25-3-2023
Pathway	Stroke

Comorbidities

Chronic Hypertension
Diabetes type 2
Hypercholesterolomie
COPD

Figure 30: Vital signs measurements tab, after completion of patient's health status analysis. Information retrieved in FHIR format from remote VTT services.



Patient Peter Van Hulst

Patient information

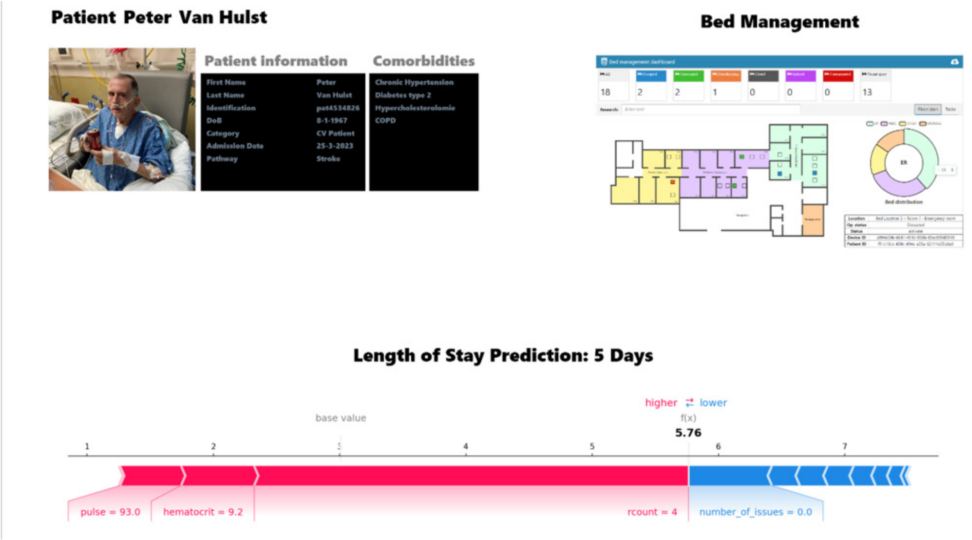
First Name	Peter
Last Name	Van Hulst
Identification	pat4534826
DoB	8-1-1967
Category	CV Patient
Admission Date	25-3-2023
Pathway	Stroke

Comorbidities

Chronic Hypertension
Diabetes type 2
Hypercholesterolomie
COPD

Heart Condition: Normal
Heart State: Normal

Figure 31: Heart status tab, after completion of patient's health status analysis. Information retrieved from remote TU and JSI services as well as service from local Docker container by NXP-NL.



Patient Peter Van Hulst

Patient information

First Name	Peter
Last Name	Van Hulst
Identification	pat4534826
DoB	8-1-1967
Category	CV Patient
Admission Date	25-3-2023
Pathway	Stroke

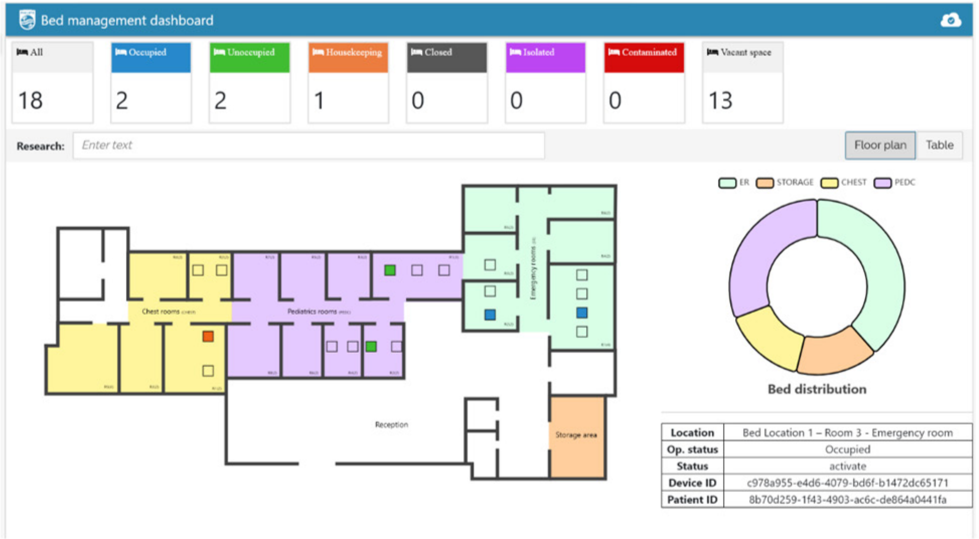
Comorbidities

Chronic Hypertension
Diabetes type 2
Hypercholesterolomie
COPD

Bed Management

Length of Stay Prediction: 5 Days

Figure 32: Patient logistics information displayed after retrieval from remote bed management service by PRE and service hosted in local Docker container by NXP-NL.



Bed management dashboard

All	Occupied	Unoccupied	Housekeeping	Closed	Isolated	Contaminated	Vacant space
18	2	2	1	0	0	0	13

Research: Enter text

Location	Bed Location 1 – Room 3 - Emergency room
Op. status	Occupied
Status	activate
Device ID	c978a955-e4d6-4079-bd6f-b1472dc65171
Patient ID	8b70d259-1f43-4903-ac6c-de864a0441fa

Figure 33: Bed management application showing location and status of beds in hospital.

Exploitation plans

- **PRE**

  - Using results from InSecTT to build and provide FHIR service for vital sign data in the Philips HealthSuite platform.

  - Using AI developed in InSecTT in clinical decision support solutions.

- **NXP-NL**

  - eIQ tooling for NXP MCU's and IoT devices. The eIQ tool is data curator for AI development whereby the InSecTT research results are added as separate extensions. Currently the AX module is available. The "image explainability through heatmaps" is pending product management approval. The eIQ tool and documentation can be downloaded after registration at the NXP website.

- In 2023, NXP-NL has added parts of the research to its eIQ service: eIQ® ML Software Development Environment | NXP Semiconductors.

- **JSI**

  - The developed cloud-based service for anomaly detection has been made available for evaluation to medical doctors. This service has the potential to enrich the public healthcare service by allowing for quick and accurate anomaly detection, ultimately leading to improved patient outcomes.

  - cloud service has been made available for the health community: It enables upload and processing of ECG data by registered users. After processing it returns the result in terms of explainable anomalies.

  - The results and wcloud service will provide solid starting point for usage in follow-up and future research projects.

- **VTT**

  - VTT has dedicated salesperson for medical domain customers. The results will be included to the sales deck and results will be presented to the relevant stakeholders with hospital and technology development community.

  - VTT will actively promote the results and provide them as background technology for new national and international research projects.

  - Results will be promoted in various forthcoming seminars and workshops. Currently VTT has participated into many events and is planning to participate more during the following months.

- **TUDelft**

  - TUDelft has prototype of the ECG hardware. The plan is to take it to TRL 6 where the functionality is demonstrated in real environment.

  - Try the full end-2-end solution in real hospital environment.

  - Try the full end-2-end solution in remote patient monitoring scenarios.

- **UTwente**

  - Applying the developed technology to hospital infrastructures that consist of large variety of devices, including time critical applications.

Use Case 5.6

Various demonstrators have been built for this use-case:

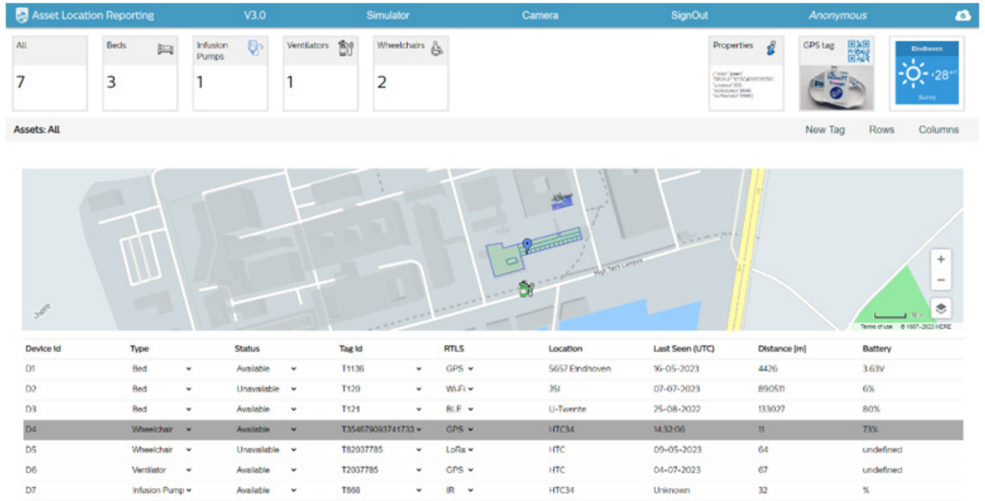
- "Emergency Logistics Services" (ELSE) for Mass Casualty Incident (MCI) handling by PRE in Eindhoven.
- Outdoor (and indoor) asset localization for healthcare equipment by PRE in Eindhoven.
- Asset localization for healthcare equipment using MPS solution by GUT in Gdansk.
- Indoor navigation solution using QR tags by JSI in Ljubljana.
- simulation framework for UWB by NXP-AU in Gratkorn.
- PIR/Thermopile location awareness solution by TU in Delft.
- Multimodal Indoor Positioning solution by U-Twente in Enschede.
- Situational awareness solution using camera's by Wapice in Vaasa.

The following components for the demonstrators have been developed and integrated in the use-case demonstrators.

- dashboard for MCI providing an overview of the incident, containing an incident information view, map view, casualty list-view and (selected) casualty data view. working prototype with basic functionality using the Google maps API is available.
- dashboard for asset localization providing an overview of asset locations, containing map view, casualty list-view and provisions to link an asset to location tag. working prototype with basic functionality using the "Here" maps API is available.
- geoJSON server with HTTPS REST API for storing and retrieving location reports and local floorplans. The server provides secure authentication and optional tag configuration. It runs on the Philips Health Suite Digital Platform (HSDP) and is used by various partners for integration purposes.
- Logistics tags for showing triage or asset status and reporting its location in geoJSON format. prototype for outdoor (GPS) localization is available using cellular IoT communication with the server. Another prototype using MPS has been developed by GUT.
- smartphone navigation App with triage support using printed QR code-based location tags, has been prototyped by JSI.
- PIR/Thermopile sensor with smart detection for indoor location awareness (with optional LoRA support) has been prototyped by TU Delft.
- Multi-directional Bluetooth Antenna for multimodal indoor positioning system has been prototyped by Twente.
- An explainable AI solution to build map for the multimodal indoor navigation system has been developed and evaluated by NXP-NL.
- simulation framework for UWB is (internally) available for NXP-AU.
- situational awareness dashboard for handling evacuations in crowded areas using video data analytics has been demonstrated by WAPICE.

"On average, nurses spend 20 minutes per shift searching for equipment. Over the cause of year, this translates to $500.000 in waste time for the typical hospital." Also "Healthcare is slowly moving out of hospitals & into homes" that requires additional awareness of locations (and status) of patients and medical equipment. For this reason, asset localization solutions for healthcare are already available on the market.

In the scope of this use case solutions have been investigated to improve and extend these typical indoor solutions with outdoor localization/communication, new indoor localization technologies including the use of MPS and AI/ML, navigation and triage in emergency situations using passive (QR) tags, improved UWB performance and situational awareness in case of emergencies using existing camera infrastructure in crowded areas. Specifically, the use of digitized triage solutions in emergency situations may save time and thus lives by providing remote dashboard overview in chaotic situations.



Device Id	Type	Status	Tag Id	RTLS	Location	Last Seen (UTC)	Distance [m]	Battery
D1	Bed	Available	T1136	GPS	5657 Eindhoven	16-05-2023	4426	3.63V
D2	Bed	Unavailable	T120	Wi-Fi	JSI	07-07-2023	890511	6%
D3	Bed	Available	T121	BLE	U-Twente	25-08-2022	133027	80%
D4	Wheelchair	Available	T354679093741733	GPS	HTC34	14:32:06	11	73%
D5	Wheelchair	Unavailable	T82037785	LoRa	HTC	09-05-2023	64	undefined
D6	Ventilator	Available	T2037785	GPS	HTC	04-07-2023	67	undefined
D7	Infusion Pump	Available	T868	IR	HTC34	Unknown	32	%

Figure 34: Asset localization Dashboard (PRE)

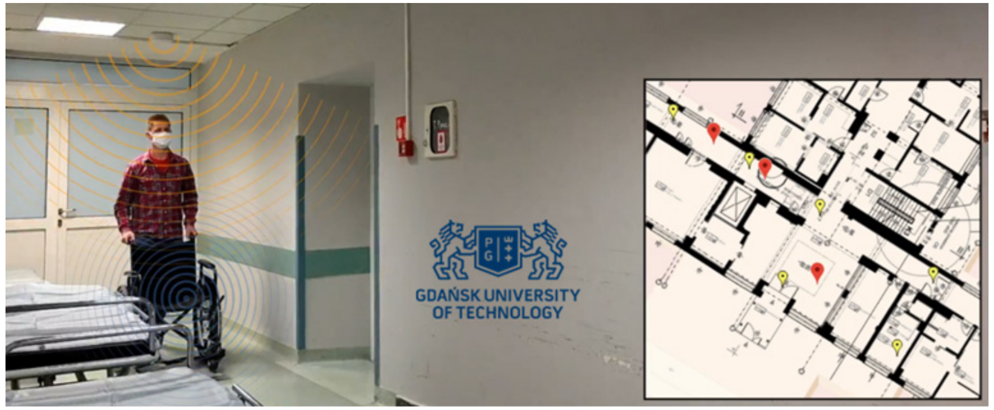


Figure 35: MPS based asset localization in Gdansk hospital (GUT)

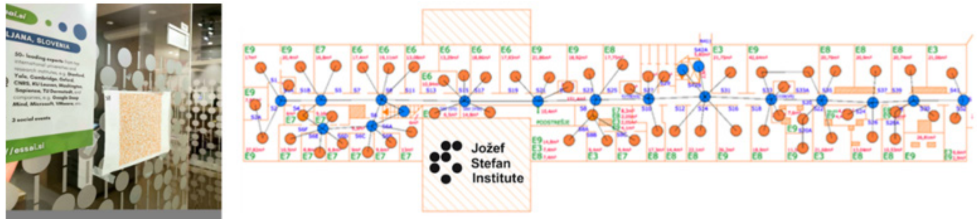


Figure 36: QR tags based indoor navigation (JSI)

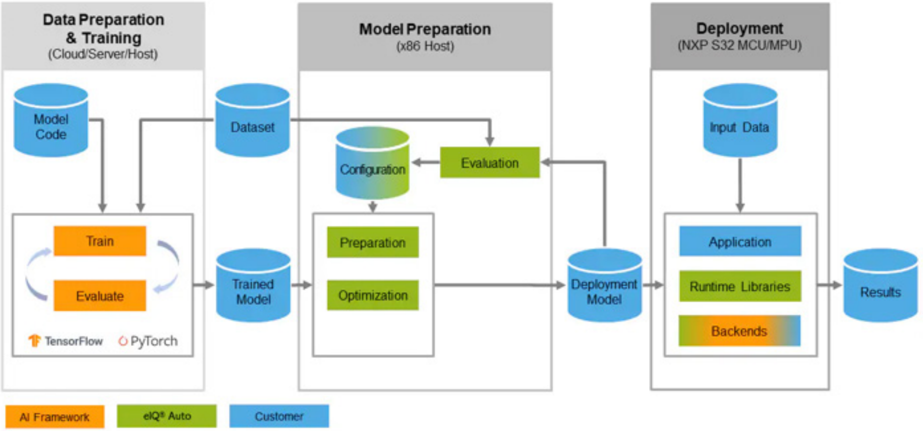


Figure 37: eIQ Auto Development Flow Diagram (NXP)

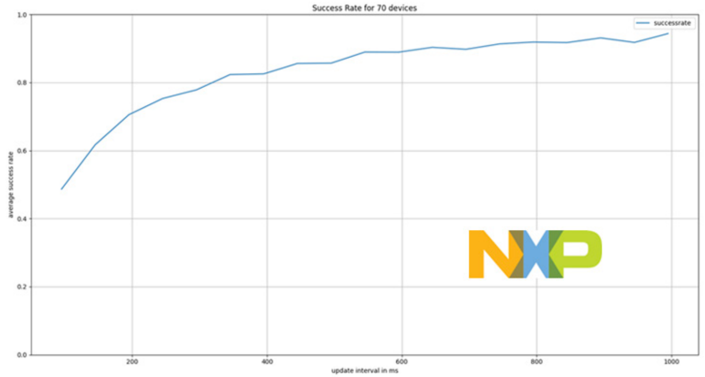


Figure 38: UWB performance simulation with multiple devices (NXP)

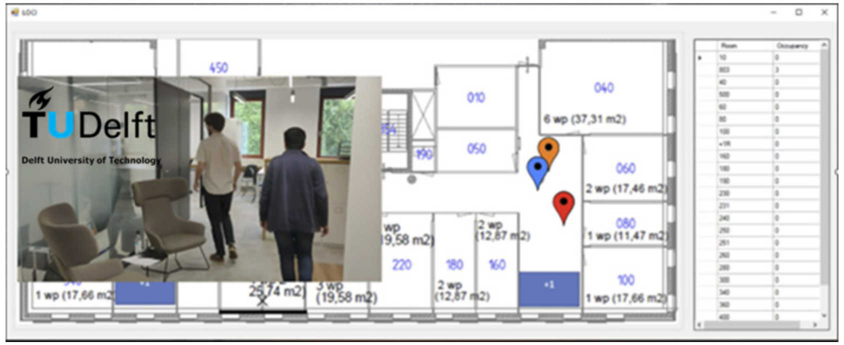
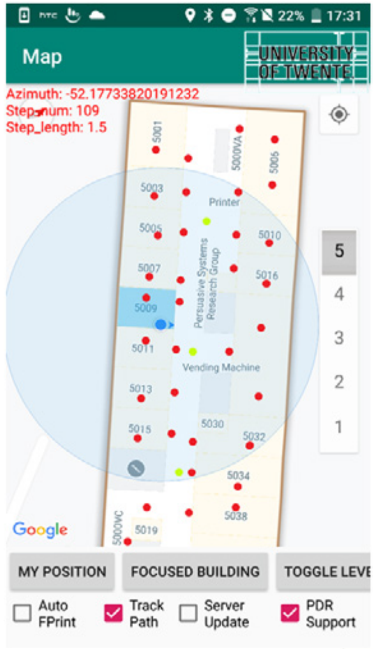


Figure 39: Location awareness using PIR/Thermopile (TU Delft)

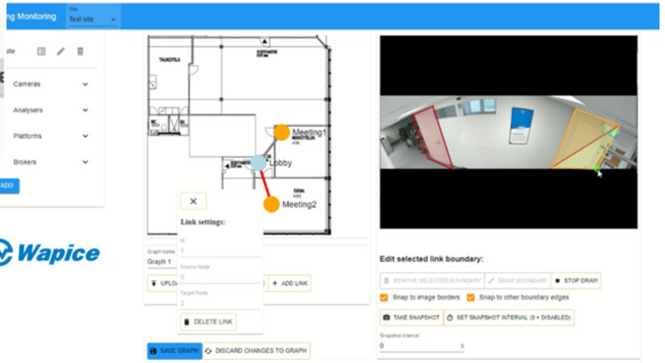


Azimuth: -52.17733820191232
Step_num: 109
Step_length: 1.5

☐ Auto FPrint ☑ Track Path ☐ Server Update ☑ PDR Support

Figure 40: Multimodal Indoor Positioning App with AI (U-Twente)

Figure 41: Situational awareness using camera's (Wapice



Exploitation plans

- The outdoor asset localization subsystem is considered as an extension of the Performance-Flow asset management solution.
- trial installation of the MPS solution for asset localization has been setup in hospital in Gdansk.
- Indoor navigation using QR tags is being discussed with healthcare providers in Slovenia.
- UWB protocol simulation is used by NXP to improve/optimize performance of existing UWB solutions.
- Explainable AI method(s) as investigated by NXP has been added to their eIQ toolkit.
- Situational awareness using PIR development has resulted in 2 scientific publications.
- Multimodal Indoor Positioning (including the Multi-directional Bluetooth Antenna) development has resulted in 2 scientific publications and has been used as platform for explainable AI methods.
- Situational awareness using cameras has been demonstrated using the IoT Ticket platform and can be considered as an extension to smart city solution.

Use Case 5.7

Rail- road traffic management system integration demonstrator

This demonstrator was carried out at INDRA premises in Madrid (Spain), deploying full lab environment as complete test case test bench.

The demonstrator was focused on testing the complete IR2SAM system, including integration road traffic management system (HORUS) and TMS with real data collected. This is the main demonstrator related with UC 5.7 and make use of all the data and results gathered in the rest of demonstrators detailed below.

Onboard Train Integrity (OTI) TRL6-7 demonstrator. Including OTI-for integrity and OTI-L for train length.

The Demonstrator took place in the United Kingdom (UK) at Grand Central Railway (GCR), located in Loughborough, England. Deploying dual train integrity, train positioning and train length systems with and without the AI modules developed in the project.

The demonstrator was focused on testing the IA modules developed for train integrity, positioning and safe train length calculation and generation of data set to be used in IR2SAM tests.

FR8Rail IV WP7 focused on the integration in the area of telematics and electrification.

This demonstrator has been carried out in Sweden deploying WSAN in freight train in commercial operation, running 400 km day weekly, from Nassjo Kombiterminal to Gotemburg harbor.

The demonstrator was focused on testing the IA modules developed for train integrity, positioning and safe train length calculation and generation of data set to be used in IR2SAM tests.

ACS Demonstrator

This demonstrator was carried out at INDRA premises, focused on the validation and monitoring algorithms and automated selection of available radio channel (4G/5G and wifi) based on AI algorithms developed in the project.

Rail-road traffic management system integration demonstrator

- Road management cloud system: Exchange the road traffic situation with IR2SAM-CL.
- TMS cloud: Exchange the trains timetable with IR2SAM-CL.
- IR2SAM-CL system: It receives inputs about the status of the rail domain: train table deviation from the TMS, train priorities based on the status of the shared areas from IR2SAM-OT, and road traffic information (traffic congestion estimations). With this information the module refines the vehicle priorities and sends proposals back to the OT counterpart. The main goal of this repurposing of priorities is to adapt rail/road objectives to the real traffic scenario. The generated priority is only proposal since the IR2SAM-OT always has the final decision on the effective priority vehicle must have.
- IR2SAM-OT: It is the main decisor in vehicle priority based on critical areas obstacle detection data. It receives train priority proposals from the CL counterpart and decides whether proposals can be executed or not.
- IR2SAM-OB: It is the OnBoard unit that sends train integrity , positioning and safe train length to IR2SAM –OT and execute the decisions of IR2SAM-OT based on exchange data.

Onboard Train Integrity (OTI) TRL6-7 demonstrator. Including OTI-for integrity and OTI-L for train length.

- WSAN: wifi based sensor network deployed along the train in each of wagons with data gathering coordinators.
- WSAN: UWB based proximity sensor network deployed along the train.
- WSAN: GNSS based positioning sensor network deployed along the train.
- WOBU: wireless OnBoard Unit providing wireless connectivity to the WSN.
- On track LIDAR based intelligent object detector.
- ML Measurements Correction Module and GNSS Modules Selector: This module collects all the measurements from the Positioning WSAN and corrects the noisy measurements using ML model. This ML model also integrates all the inputs from the On-Board Systems (entity that copes with the already equipped rail systems), and the digital map. Moreover, the module is in charge of selecting the GNSS source based on the metadata provided by each of them.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit, to the Train/Vehicle Positioning Agent Decisor, to check if the positioning measurements' accuracy is feasible for each service.

- Train/Vehicle Position Agent Decisor: This module takes all the inputs related with the position corrected measurement, On Board System metrics, and the rail services KPIs to generate the position measurement with quality tag.

- Train Integrity and Train Length Decisor: It is the Train Integrity and Train Length Decisor performed by the WTI using the weights generated with the ML model. The decision is validated with the KPIs of each service that requires the Train Integrity indicator and the real length of the train.

- ML Measurements Correction Module and Sensors Weights Evaluation: This module collects all the measurements from the Train Integrity Sensor filters and corrects the noisy measurements using ML model. This module assigns the weights for each of the sensors values that will be used for train integrity calculation.

- ML Measurements Correction Module and Proximity Modules Selector: This module collects all the measurements from the Proximity WSAN and correct the noisy measurements using ML model. This module also decides, based on the metadata reported, the proximity subsystem to be used.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit, to the Train/Vehicle Proximity Agent Decisor, to check if the proximity measurements accuracy is feasible for each service.

- Train/Vehicle Proximity Agent Decisor: This module takes all the inputs related with the proximity corrected measurement and the KPIs inputs to generate the position measurement.

- ML Measurements Correction Module and Sensors Weights Evaluation: This module collects all the measurements from the UWB modules and correct the noisy measurements using ML model. This module predicts the Train Integrity weights based on the composition where the sensors are equipped and the train mission.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit, to the ML Module, to check if the Train Integrity measurements accuracy is feasible for each service.

- ML Measurements Correction Module and Object Selector: This module collects all the measurements from the Cameras and the LIDAR Object Detection and correct the noisy measurements using ML model. This module predicts the Object attributes.

- Object Decisor: This module collects the models results and compares these measurements with the rail services KPIs.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit, to the DL module, to check if the objects detected measurements accuracy is feasible for each service.

- Priority Decisor: This module decides the speed to command the train based on the priority decided with the object detected information.

- CMW: AMQP based communication middleware.

- 4G communication gateway.

- On board (local) JRU (DDBB), dashboard and data analytics tools.

- Cloud based infrastructure with data base, dashboard and data analytics tools.

FR8Rail IV WP7 focused on integration in the area of telematics and electrification.

- WSAN: wifi based sensor network deployed along the train in each of wagons with data gathering coordinators.

- WSAN: GNSS based positioning sensor network deployed along the train.

- WOBU network: wireless OnBoard Units network providing wireless connectivity to the multiple WSNs.

- ML Measurements Correction Module and GNSS Modules Selector: This module collects all the measurements from the Positioning WSAN and corrects the noisy measurements using ML model. This ML model also integrates all the inputs from the On-Board Systems (entity that copes with the already equipped rail systems), and the digital map. Moreover, the module is in charge of selecting the GNSS source based on the metadata provided by each of them.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit, to the Train/Vehicle Positioning Agent Decisor, to check if the positioning measurements' accuracy is feasible for each service.

- Train/Vehicle Position Agent Decisor: This module takes all the inputs related with the position corrected measurement, On Board System metrics, and the rail services KPIs to generate the position measurement with quality tag.

- Train Integrity and Train Length Decisor: It is the Train Integrity and Train Length Decisor performed by the WTI using the weights generated with the ML model. The decision is validated with the KPIs of each service that requires the Train Integrity indicator and the real length of the train.

- CMW: AMQP based communication middleware.

- 4G communication gateway.

- On board (local) JRU (DDBB), dashboard and data analytics tools.

- Cloud based infrastructure with data base, dashboard and data analytics tools.

ACS Demonstrator

- Private V2V and V2I/I2V Communication Systems ML Online Models evaluations: These modules collect the data and metadata related with the Private Managed Communication Systems to evaluate, over predefined channel, the communication systems that fit better for the V2V and V2I/I2V interfaces independently of each other.

- Public Communication Systems ML Online Models evaluation: This module collects the data related with the Public Managed Communication Systems to evaluate, over predefined channel, the communication systems that fit better for the Rail environment to the Internet services.

- Private V2V and V2I/I2V System and Channel Agent Decisors: These modules collect the data form the ML model and the KPIs to select the communication system to deal with the V2V and V2I/I2V interfaces. This decisor also selects the adequate channel to be used.

- Public System and Channel Agent Decisor: This module collects the data form the ML model and the KPIs to select the communication system to deal with the Rail environment to the Internet interface. This Decisor also selects the adequate channel to be used.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit to the Agents checks the Communication systems selection accuracy is feasible for each service.

What business need/problem does the demonstrator address?

The aim of this UC is using Artificial Intelligence (AI), making use of the system that priory among the rail and other different urban stakeholders to enhance the control of the urban traffic. The use of wireless technologies with AI developments will be used to support V2X secure communications to develop smart rail services based on Metropolitan Area Networks (MANET).

Nowadays, the railways infrastructure coexists with other domains in urban environments where traffic events may occur. This UC aims to spread these developments to build, along with AI, smart management system for urban traffic control. This improvement on the urban traffic management will reduce the number of injures and human losses, by increasing safety and security in the railway lines due to the direct communication between the railway and other domains.

The urban traffic management system has to make the decisions taking into account the information provided by all the different domains, considering the amount of rail traffic within the smart cities. Increasing the intelligent in the decision maker, the traffic jams in urban areas will be manage in more effective way, making use of Artificial Intelligence mechanisms to develop the trustable decisor. The innovation potential of this solution is based on:

- Increasing the communication between all involved actors in the specific critical area for considering as much data as possible before assigning priorities to specific actor in an intelligent way.

- Enhancing the management of cross-domain areas making use of Edge-based AI mechanisms.

- Managing multimodal jams.

- Improving the efficiency on the rail and automotive domain, by increasing the efficiency in the decisions.

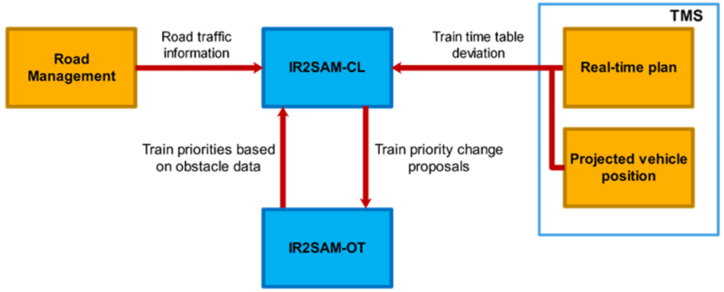

Road Management
Road traffic information
IR2SAM-CL
Train time table deviation
TMS
Real-time plan
Projected vehicle position
Train priorities based on obstacle data
Train priority change proposals
IR2SAM-OT

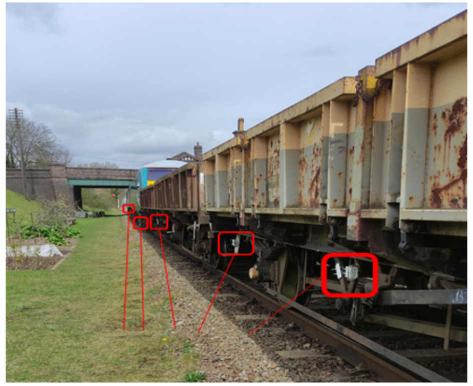
Figure 42: IR2SAM System Synoptic

indra

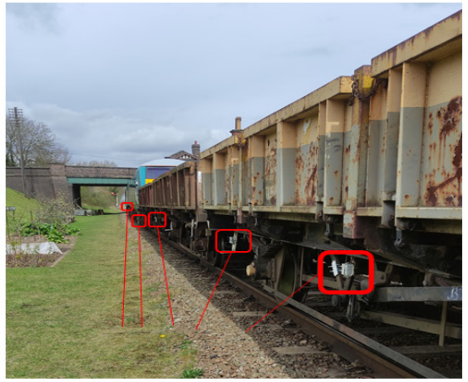
indra

82306

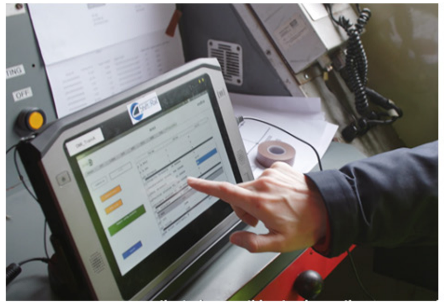
indra



indra



indra



indra
indra

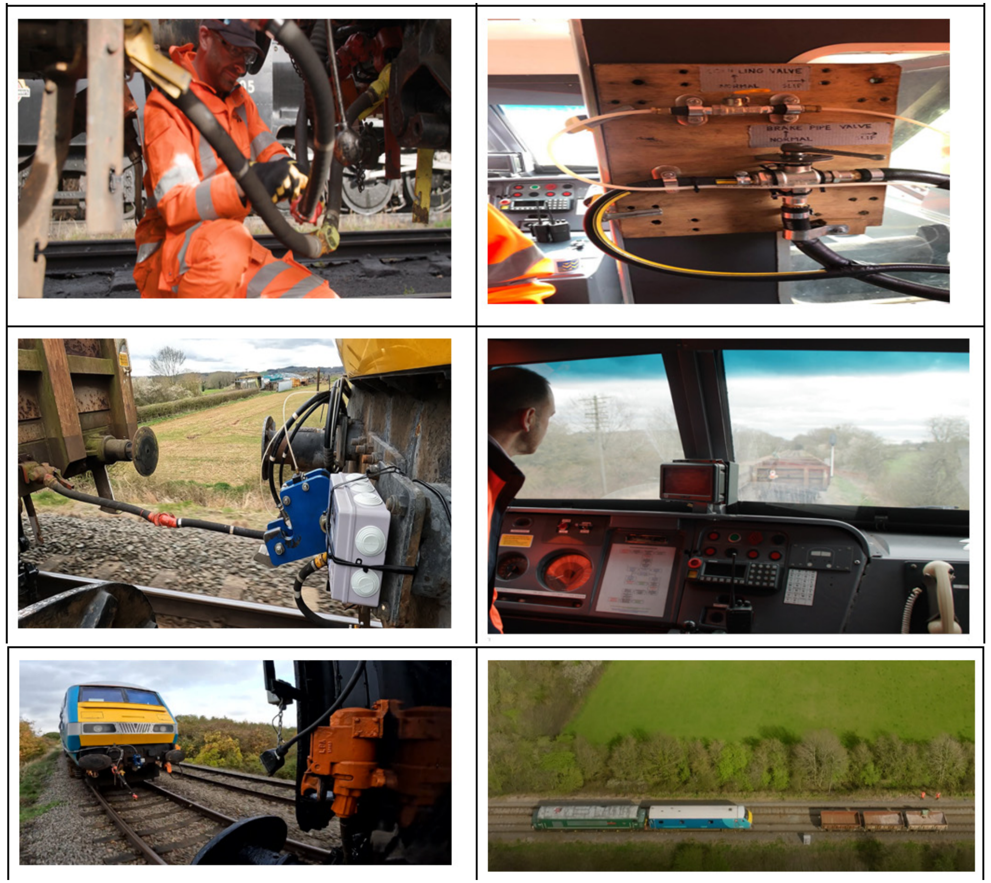


Figure 43: Onboard Train Integrity (OTI) TRL6-7 demonstrator site deployment

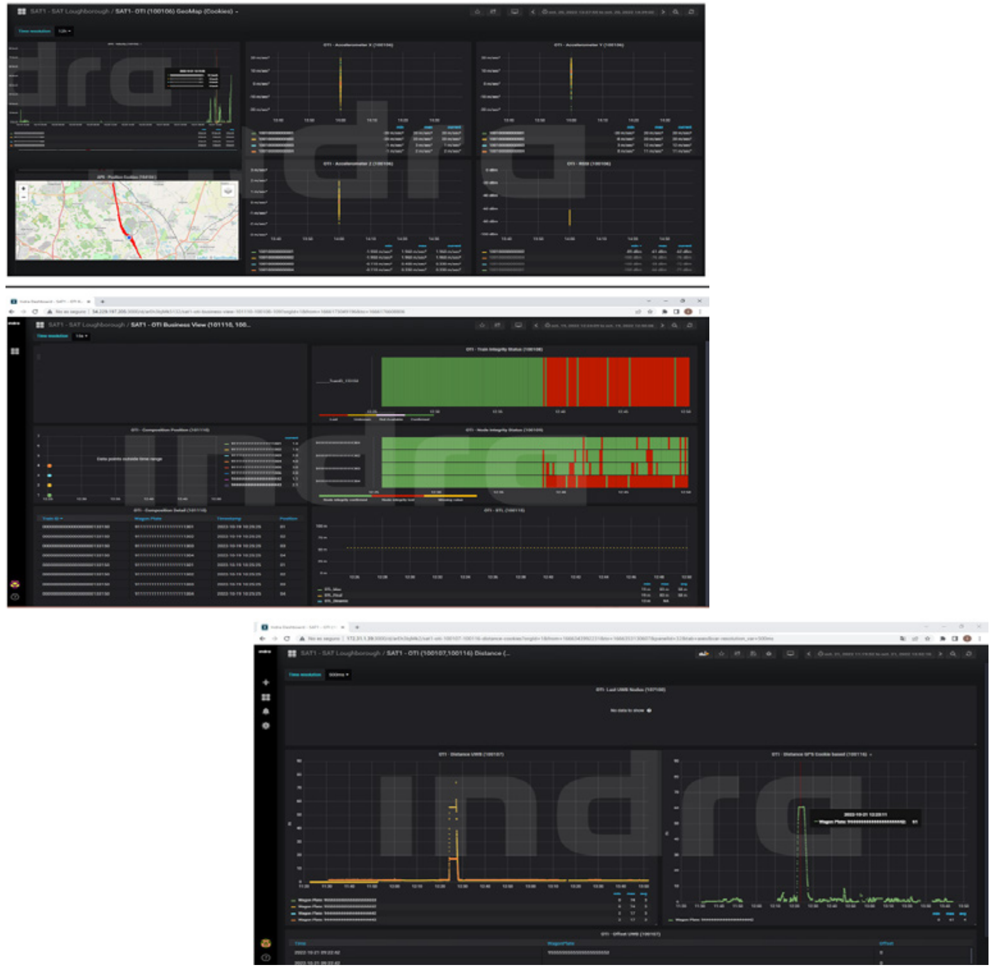


Figure 44: Onboard Train Integrity (OTI) TRL6-7 demonstrator site deployment

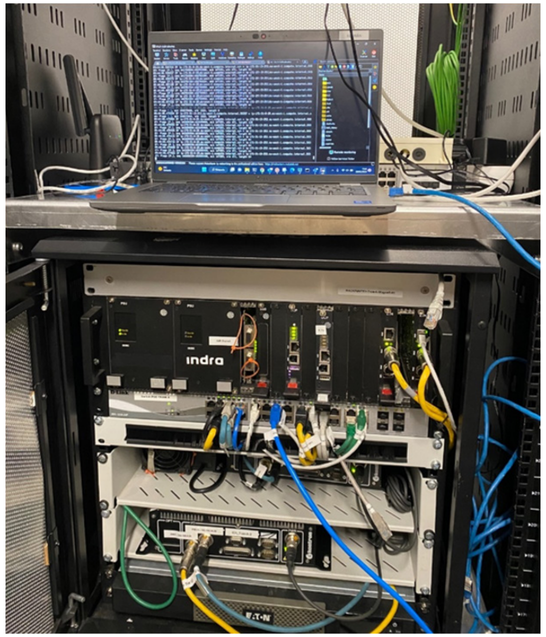


Figure 45: ACS Implementation in INDRA

Exploitation plans

INDRA intends to use the results achieved in INSECTT to improve already existing products and solutions, and develop new ones, delivering enhanced IOT and AI based solutions to the railway market.

Use Case 5.8

STCC/SAMC Demonstrator

This demonstrator was carried out at INDRA premises focused on simulation of virtual coupled trainsets operation optimization. This is UC 5.8 main demonstrator and makes use of all the data and results gathered in the rest of demonstrators detailed below.

Onboard Train Integrity (OTI) TRL6-7 demonstrator. Including OTI-for integrity and OTI-L for train length.

The Demonstrator took place in the United Kingdom (UK) at Grand Central Railway (GCR), located in Loughborough, England. Deploying dual train integrity, train positioning and train length systems with and without the AI modules developed in the project.

The demonstrator was focused on testing the IA modules developed for train integrity, positioning and safe train length calculation and generation of data set to be used in STCC/SAMC tests.

FR8Rail IV WP7 focused on the integration in the area of telematics and electrification.

This demonstrator has been carried out in Sweden deploying WSAN in freight train in commercial operation, running 400 km day weekly, from Nassjo Kombiterminal to Gotemburg harbor.

The demonstrator was focused on testing the IA modules developed for train integrity, positioning and safe train length calculation and generation of data set to be used in STCC/SAMC tests.

ACS Demonstrator for STCC

This demonstrator was carried out at INDRA premises, focused on the virtual coupling train use case.

STCC/SAMC Demonstrator

- SRAS-OT: The Smart Rail Automation System on Track (SRAS-OT) is module that decides best course of action based on the rail exploitation plan versus the real state of the vehicles to apply actions over them. It interfaces with TMS and the OB modules to accomplish the mentioned objective.

- The on-track module is centralized system that interfaces with TMS and the OB modules in order to calculate the best course of action in light of the planning versus the real state of the vehicles it obtains before updating the commands and sending them to the various vehicles in the system.

- SRAS-OB: This entity makes use of the information provided by its SRAS-OT counterpart in order to generate movement directives for the driver. Additionally, if the system loses connection with the SRAS-OT it must able to make its own movement decisions autonomously using positioning data from the APS module. It also sends continuous.

- STCC-OB: The on-board STCC module's role is to gather information about the position and speed of the vehicle as well as its relative surrounding vehicles in order to perform coupling and uncoupling manoeuvres by producing instantaneous speed, acceleration and objective distance between trains to compose movement directive. This output is sent either to the ATP or the TCMS entities. STCC also may receive feedback from TCMS about the vehicle's effective speed and acceleration.

- SAMC-OB: The Smart Adaptation Movement Control (SAMC) is subsystem to control and readjust the movement directives to the train. The role of this module is twofold.

  - On the one hand, it must compensate for the real vehicle's behaviour using historic data real speed and acceleration and the desired outputs from STCC/SRAS. In essence acting as feedback control loop system for the train's movement.

  - On the other hand it must perform speed and acceleration smoothing by tweaking the instantaneous values it receives from the main STCC-OB/SRAS-OB module using both historic (past) and planned (probable future) data from the full platoon of vehicles.

- Adaptable Communication System (ACS): It is the entity in charge of providing communication with the rest of the system, isolating the selection of the communication path from the elements that require it. This system will switch dynamically between different communication links in order to fulfil different KPIs defined, based on the service to be tackled.

- Autonomous Positioning System (APS): This entity fulfils critical role in delivering the system's location, acceleration, current speed, and current track direction with configurable degrees of precision and making use of different WSANs. This entity serves positioning report that is used by the InSecTT systems.

- Positioning Wireless Sensor-Actuator Network (WSAN): It is set of sensors and actuators for positioning based on the SCOTT solution. It provides to the APS data about the on-board speed, acceleration and triangulated position on the Global Position System (GPS).

- Integrity WSAN: This entity provides the SCOTT defined Wireless Train Integrity (WTI) with information about the status of the train wagons in certain composition in order to generate the integrity report.

- Orchestartor to inject all the data collected from other demonstrators in order to test the AI modules with real data.

ACS Demonstrator

- Private V2V and V2I/I2V Communication Systems ML Online Models evaluations: These modules collect the data and metadata related with the Private Managed Communication Systems to evaluate, over predefined channel, the communication systems that fit better for the V2V and V2I/I2V interfaces independently of each other.

- Public Communication Systems ML Online Models evaluation: This module collects the data related with the Public Managed Communication Systems to evaluate, over predefined channel, the communication systems that fit better for the Rail environment to the Internet services.

- Private V2V and V2I/I2V System and Channel Agent Decisors: These modules collect the data form the ML model and the KPIs to select the communication system to deal with the V2V and V2I/I2V interfaces. This decisor also selects the adequate channel to be used.

- Public System and Channel Agent Decisor: This module collects the data form the ML model and the KPIs to select the communication system to deal with the Rail environment to the Internet interface. This Decisor also selects the adequate channel to be used.

- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit to the Agents checks the Communication systems selection accuracy is feasible for each service.

- Two (2) On board train control unit equipment with integrated ACS.

- Cloud server with ACS and services.

- 5G MEC server with ACS and services.

FR8Rail IV WP7 focused on the integration in the area of telematics and electrification.

- WSAN: wifi based sensor network deployed along the train in each of wagons with data gathering coordinators.
- WSAN: GNSS based positioning sensor network deployed along the train.
- WOBU network: wireless OnBoard Units network providing wireless connectivity to the multiple WSNs.
- ML Measurements Correction Module and GNSS Modules Selector: This module collects all the measurements from the Positioning WSAN and corrects the noisy measurements using ML model. This ML model also integrates all the inputs from the On Board Systems (entity that copes with the already equipped rail systems), and the digital map. Moreover, the module is in charge of selecting the GNSS source based on the metadata provided by each of them.
- Rail Services' KPIs Evaluation Module: This module is in charge of providing the KPIs defined by the rail services to permit, to the Train/Vehicle Positioning Agent Decisor, to check if the positioning measurements' accuracy is feasible for each service.
- Train/Vehicle Position Agent Decisor: This module takes all the inputs related with the position corrected measurement, On Board System metrics, and the rail services KPIs to generate the position measurement with quality tag.
- Train Integrity and Train Length Decisor: It is the Train Integrity and Train Length Decisor performed by the WTI using the weights generated with the ML model. The decision is validated with the KPIs of each service that requires the Train Integrity indicator and the real length of the train.
- CMW: AMQP based communication middleware.
- 4G communication gateway.
- On board (local) JRU (DDBB), dashboard and data analytics tools.
- Cloud based infrastructure with data base, dashboard and data analytics tools.

What business need/problem does the demonstrator address?

Nowadays, the majority of current systems that provides automation in the railway environment are limited to control some operation services such as door opening and closing. The ability to operate, due to the infrastructure deployment, is currently limited to the ability to enhance the mechanisms to ensure higher grade of automation.

This Use Case focus on the automation of different train operation processes making use of Artificial Intelligence. The analysis of current technologies concerning the smoothing of virtual coupling and enhancing of ATO, ATC and ATP systems and the different grades of automation is needed to previously define the grade of automation that the system has to reach.

The integration of existing technologies and new ones to enhance the automatic train operation to make the difference in the railway market. By improving functionalities such as speed control, timing control of the stops and decentralizing the decisions, it is possible to enhance the current state of the railway transportation, having an important impact in the railway market.

Moreover, the use of artificial intelligence mechanisms to improve the deployment of smoother virtual coupling maneuvers during the trip will help to make the speed changes processes more comfortable for the passengers and safer for the cargo.

The development of this use case has to accomplish the objective of solving or reducing the drawbacks and comfort for passengers and certain type of cargo operations in safe and secure way. This will directly impact over the railway traffic, giving new vision for the market concerning the possibility of reducing risks and improve the line capacity by making more efficient and comfortable the coupling and uncoupling maneuvers.

More specific improvements aimed by this use case upon the services defined in SCOTT [11], [12], [13], [14], [15], [16]), specifically, those concerned with different rolling stock that are required to communicate with each other for the delivery of the service. Once the safety level is guaranteed, it is vital to introduce system able to make the different railway vehicles to communicate in smooth manner to avoid incidents, for the benefit of both cargo agents and passengers:

- Improving the citizen comfort and accessibility to every kind of rolling stock transportation system.
- Enhancing the management of On-Board functionalities making use of Edge-based Artificial Intelligence mechanisms.
- Including Artificial Intelligence mechanisms to improve the current state of the system to delegate the control for specific areas in an intelligent way.
- Improving the flexibility of the current systems by connecting all to all by means of an automated and distributed system.

- Using wireless communication to make possible the connection between On-Board and On-Track stakeholders in distributed and collaborative environment.

- Providing improved coupling manoeuvres via AI by smoothing the speed change processes in order to enhance passengers comfort as well as transport companies trust in this type of virtual composition.

- Increasing capacity and punctuality of operating lines reducing time and enhancing the timetable management in an automatic way. It improves the passengers and end-users experience, making the services more trustable.

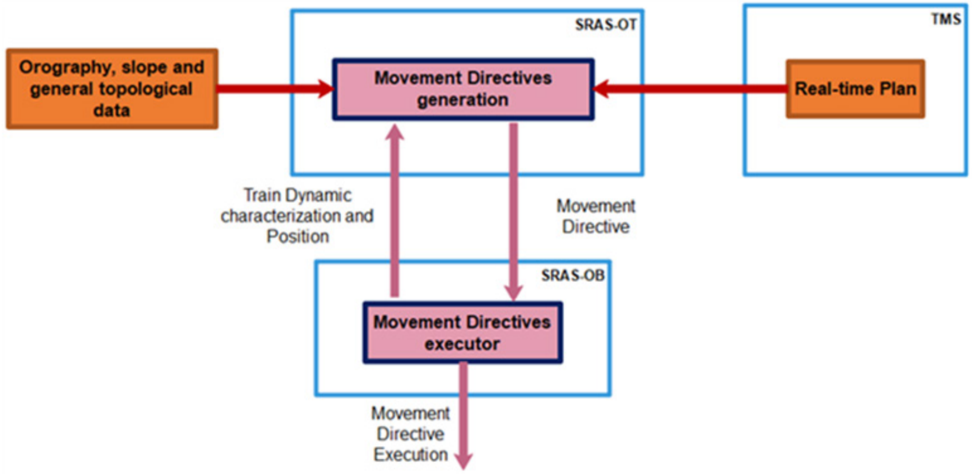

SRAS-OT
TMS
Orography, slope and general topological data
Movement Directives generation
Real-time Plan
Train Dynamic characterization and Position
Movement Directive
SRAS-OB
Movement Directives executor
Movement Directive Execution

Figure 46: UC 5.8 blocks diagram

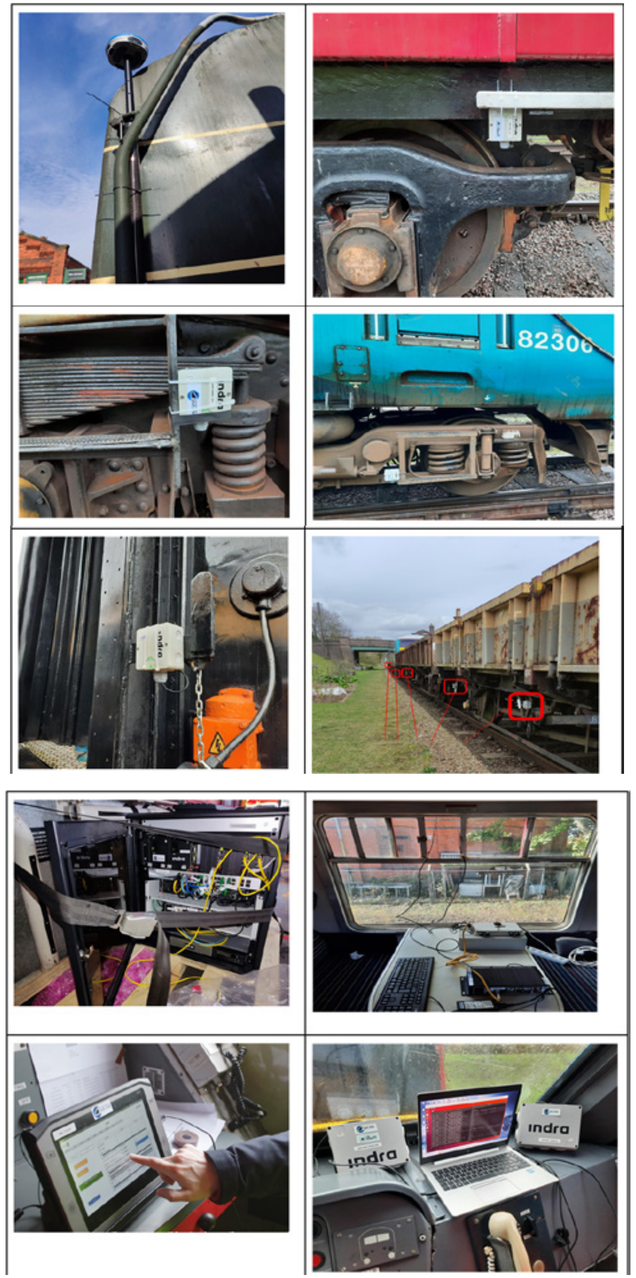


Figure 47: Onboard Train Integrity TRL 6-7 demonstrator site deployment

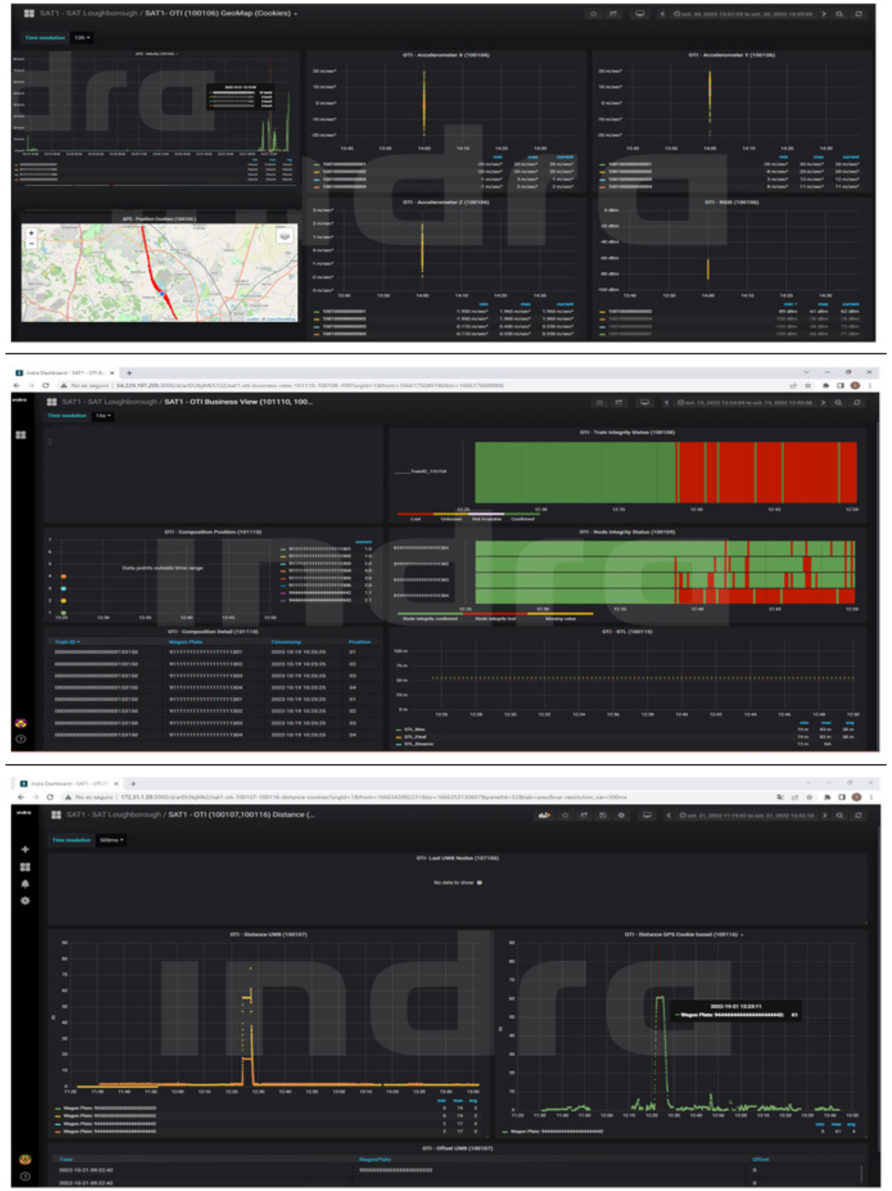

SAT1 - SAT Loughborough / SAT1- OTI (100106) GeoMap (Cookies)
Time resolution
OTI - Accelerometer X (100106)
OTI - Accelerometer Y (100106)
OTI - Accelerometer Z (100106)
OTI - RSSI (100106)
SAT1 - SAT Loughborough / SAT1 - OTI Business View (101110, 100...
OTI - Train Integrity Status (100106)
OTI - Composition Position (101110)
OTI - Node Integrity Status (100109)
OTI - Composition Detail (101110)
OTI - STL (100110)
SAT1 - SAT Loughborough / SAT1 - OTI (100107,100116) Distance (...
OTI - Last UWB Nodes (100106)
No data to show
OTI - Distance UWB (100107)
OTI - Distance GPS Cookie based (100116)
OTI - Offset UWB (100107)

Figure 48: Onboard Train Integrity (OTI) TRL6-7 demonstrator cloud dashboards

Exploitation plans

INDRA intends to use the results achieved in INSECTT to improve already existing products and solutions, and develop new ones, delivering enhanced IOT and AI based solutions to the railway market.

Use Case 5.9

VeNIT Lab Jamming Detection Demonstrator

MarUn built local demonstrator in VeNIT Lab with an OPCUA client and server application using Raspberry Pi in accordance with this use case to reflect the communication between an industrial robot and an edge device. Various jamming attacks were applied to the application using Software Defined Radio (SDR) to observe its behavior under jamming attacks.

Key components for the VeNIT Lab Jamming Detection Demonstrator is described below:

OPC-UA Server (Edge Device)

The OPC-UA Server is replica of the server that provides the axis information for the robot in manufacturing plant. It is receiving and transmitting data between the robot and the edge device.

OPC-UA Client – Robot

The robot is powered by servomotors and controlled by Raspberry Pi. It serves as representative of the robot in the real manufacturing plant. The OPC-UA Client allows the robot to connect with the OPC-UA Server, enabling data exchange and instructions from the server.

USRP 2932 SDR

The USRP 2932 Software Defined Radio (SDR) is device used to transmit different types of jamming signals. The USRP 2932 SDR helps simulate various jamming scenarios to study their effects and develop countermeasures.

LabVIEW Application / GNU Radio Application

LabVIEW and GNU Radio software applications are used to generate jamming attacks. These applications provide user-friendly interface to create different types of jamming signals such as constant, random, barrage (intense), or pulsed signal.

Jamming Detection Application

To combat jamming attacks, it's crucial to have way to detect them. The jamming detection application runs on both the edge device (OPC-UA Server) and the robot controller. It continuously monitors the network for signs of jamming such as sudden disruptions or abnormal behavior. This application helps identify when jamming attack occurs.

Robot Controller GUI

The Robot Controller GUI provides user interface that allows operators to observe the connectivity status and jamming attacks in real-time. It gives visual representation of the network's condition, allowing users to identify if the communication is affected by jamming. This real-time monitoring helps researchers and operators respond quickly to mitigate the impact of jamming attacks.

LEDs - Indication of Evaluation Results

LEDs serve as visual indicators of the evaluation results. In the context of the demonstrator, LEDs are used to show the status of jamming attacks on different Wi-Fi channels. They indicate whether the channels are affected by jamming or functioning normally.

The components of the demonstrator work together to simulate and study the effects of jamming attacks in lab environment. The OPC-UA Server and Robot establish communication, while the USRP 2932 SDR generates various jamming signals. The LabVIEW and GNU Radio Applications create different jamming attacks, and the Jamming Detection Application monitors for signs of interference. The Robot Controller GUI provides real-time overview, and the LEDs visually indicate the evaluation results. The setup enables understanding and developing strategies against jamming attacks in industrial settings.

The main objective of the demonstrator is to develop an advanced solution for detecting and mitigating jamming attacks in industrial environments. By simulating various jamming scenarios and collecting data, the demonstrator aims to enhance the security and reliability of industrial networks. By detecting anomalies and identifying jamming in real-time, the demonstrator helps prevent loss of connectivity, production delays, and potential product damage. It empowers operator or devices to respond to and mitigate the impact of jamming attacks, ensuring uninterrupted operations or safely failing the system. The demonstrator combines various components such as the OPC-UA Server, OPC-UA Client (Robot), USRP 2932 SDR, LabVIEW/GNU Radio Applications, Jamming Detection Application, Robot Controller GUI, and LEDs. This integrated system allows communication, generation of jamming attacks, real-time monitoring, and visualization of the network status. By collecting QoS parameters during normal and jamming scenarios, the demonstrator leverages machine learning algorithms to detect anomalies and identify jamming attacks. This goes beyond traditional rule-based approaches and enables the system to adapt and detect new and sophisticated jamming techniques.

Contact information

This deliverable is intended to be published as public document that will reach various stakeholders. Please provide main contact person in case of interaction with potential customers or interested parties.

For further information related to the VeNIT Lab Jamming Detection Demonstrator, please contact:

- Dr. Mujdat Soyturk, Marmara University, (mujdat.soyturk@marmara.edu.tr)
- Yavuz Selim Bostanci, VeNIT Lab, Marmara University (yavuz.bostanci@venit.org)

Exploitation plans

VeNIT Lab Jamming Detection Demonstrator

The developed detection and mitigation solutions for jamming attacks can be commercialized as standalone product or integrated into existing industrial security systems. They can enhance the security and resilience of industrial networks by incorporating jamming detection and mitigation capabilities into the fabric of the automation infrastructure. This can be done by collaborating with industrial automation vendors or offering integration services to end-users. Furthermore, the demonstrator can serve as foundation for further research and development for industrial cybersecurity. This may involve exploring advanced machine learning techniques for jamming detection, and refining the simulation of realistic jamming scenarios.

Use Case 5.10

The UC has implemented 2 demonstrators. The first demonstrator is located in Norway, within railway construction project that is being executed by ACCIONA. This project includes two tunnels built with conventional excavation methods. The UC components have been deployed inside the tunnel.

Figure 49: Demonstrator in Norway

The second demonstrator is located in Spain, within dam construction project also executed by ACCIONA, which includes utility tunnel that is being excavated with tunnel boring machine. The UC components have been deployed inside the tunnel and on the outdoor area in front of the tunnel portal.

Figure 50: Demonstrator in Spain

UC 5.10 targets the optimization of productivity and improvement of safety in the execution of construction projects through Artificial Intelligence of Things (AIoT).

To achieve this objective, the first step has been the implementation of Bluetooth-based tracking system for workers and construction machinery inside the tunnel of the demonstrator of Norway. These components allow presence detection and location of workers/machines in specific tunnel areas.

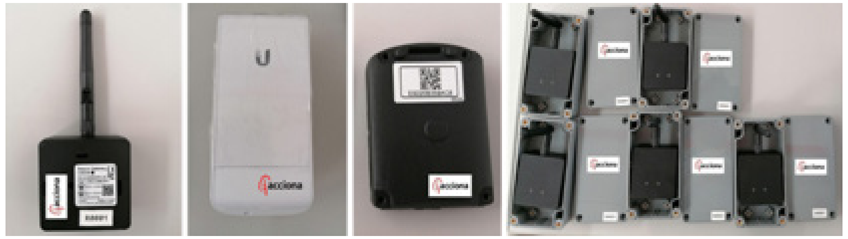


Figure 51: Tracking System Hardware

The tracking systems are complemented with distributed monitoring system installed in the tunnel that includes video cameras, gas detection stations, indoor air quality sensors, emergency actuators, and power analysers. Using the outputs from the tracking and distributed monitoring systems, additional components have been integrated for providing additional smart functionalities.

One important component is the activity tracker, which enables automated identification and measurement of construction tasks. For the case of the demonstrator of Norway, this component has been used for tracking the real progress and the resources used for the activities comprised within each tunnel excavation cycle with drill & blast method. Examples of these activities are drilling, blasting, grouting, etc.

The other main component is the safety manager, which provides different functionalities for detecting and managing different safety-related situations in the construction site, namely, detection of non-authorized persons and/or vehicles in specific areas, management of evacuation in case of emergency, and detection of high concentration of dangerous gases.

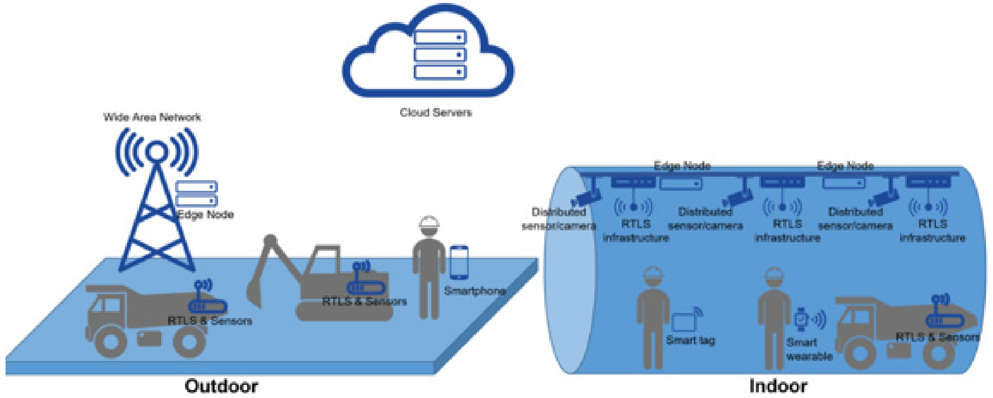


Figure 52: General UC Architecture

The demonstrator of Spain has been focused on the validation of an improved version of the tracking systems for workers and construction machinery, while at the same time it has allowed testing these systems in different scenario (tunnel built with tunnel boring machine instead of conventional tunnelling methods).

The functionalities from all the components of both demonstrators can be accessed through web-based Graphical User Interface.

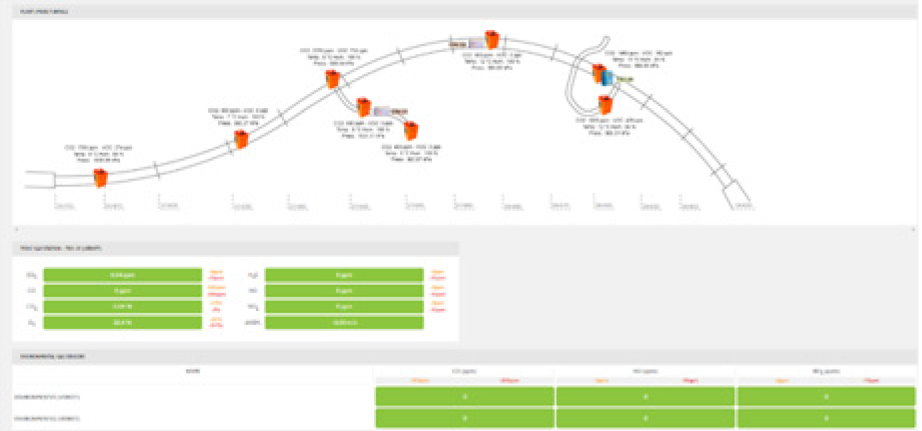


Figure 53: UC GUI

The construction sector has traditionally lagged behind other industrial domains in the adoption of innovative digital technologies. One of the reasons for the slower adoption is the challenging environment where these technologies shall be deployed. Each construction project is executed in specific location and for given period of time. The layout of the working site evolves in parallel with the progress of the project, and the construction environment typically presents harsh conditions for the deployment of ICT infrastructure and of electronic devices in general, as well as for wireless communications.

The UC demonstrators targets the application of digital technologies to track with higher precision the real progress of construction tasks, the use of resources (workers and machinery) to complete these tasks, and to improve safety at the construction site.

The main innovation of the UC lies in the integrated approach for providing these smart functionalities using as common base cost-effective tracking systems for workers and machinery and distributed monitoring system. Another particularity of the UC is the focus on the application in construction projects developing large civil infrastructures, as the digital innovations in the construction sector usually have building construction projects as their main target.

Exploitation plans

The UC exploitation plan is aligned with an internal strategy of ACCIONA for designing, integrating, and deploying digital platform to support the management of construction projects. The main target of the platform will be to facilitate the development and integration of smart applications for the construction sector with strong data usage component, thus supporting use cases oriented to reporting, data analytics, data visualization, etc.

The digital platform will provide support to any type of construction project/activity, e.g., construction of tunnels with conventional methods, construction of tunnels with tunnel boring machines, earthworks, maintenance of machinery, etc., and will be used both by the staff of the construction projects (main contractor and subcontractors), and by the central departments of the company.

As an example of future direct replication of the results of the project, there is currently plan for customizing and deploying some of the UC demonstrator components in new construction project that ACCIONA is executing in Poland. This project will build highway section that includes the construction of twin 2 km long tunnels, which will be excavated with tunnel boring machine. According to the plan, the following components will be evolved and replicated: worker and machinery tracking systems; distributed monitoring system inside the tunnel consisting of video cameras, gas detection sensors, and emergency actuators; and the safety management component.

Use Case 5.11

Asset Tracking Demonstrator

GUT and CISC have developed two systems in relation to the Assets Tracking Demonstrator, but each is designed to locate different classes of objects. However, both systems are interoperable through visualisation by GUT’s acquisition and visualisation system (MPS).

During Y3, GUT conducted extensive tests of localization system based on Bluetooth Low Energy (BLE) and dedicated ESPAR antennas at the Smart Infrastructure on the GUT campus. The test environment mimics the propagation conditions of the planned test in the Gdansk airport area. The propagation environment includes rapidly changing reflection conditions caused by the movement of cars. The aim of the tests is to validate GUT’s airport baggage trolley tracking method. To mimic the airport baggage, GUT used robot with metal housing containing BLE transmitter and RTK GPS, which provides an accurate reference for the localization estimation by GUT’s algorithms.

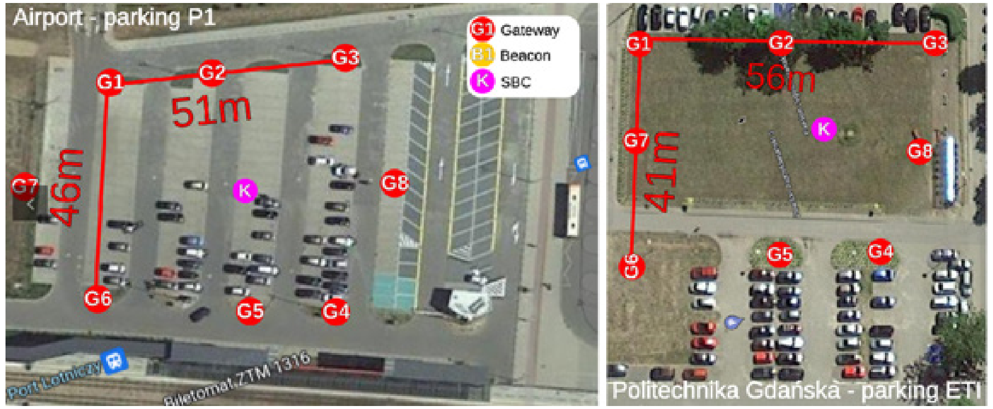


Figure 54: Asset Tracking Demonstrator

V2X communication

To incorporate Kaitotek’s network monitoring application and VIF’s V2x platform and show the most useful use of all components, GUT used its two components flexible payload and mobile testing platform. The demonstrator is based on two robots that exchange data with each other using V2X communication. The first robot is the mobile testing platform with V2X module, and the second robot is equipped with Flexible payload and V2X module. The second robot thanks to

Flexible payload is capable of performing critical infrastructure inspection, detecting objects on its road, and sending all perceptual data to the operator. The first robot can perform an autonomous mission along planned route but in this case, it is not equipped with any sensors. To increase the situational awareness of the first robot the GUT used the V2X communication provided by VIF. Thanks to cooperative perception messages (CPMs) the first robot is aware of all objects detected by the second robot and even without any sensors can avoid obstacles on its way. Additionally, the operator can continuously monitor the communication quality between the robots thanks to Kaitotek's application.

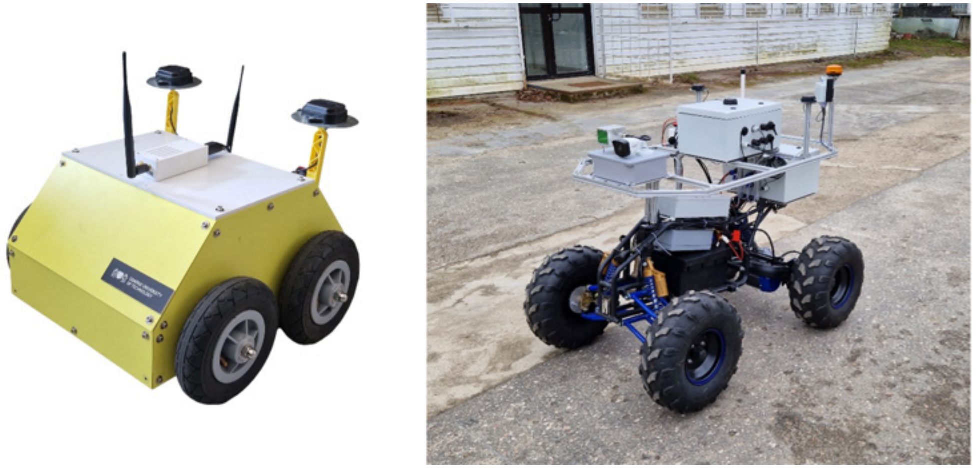


Figure 55: V2X communication

Marmara University Campus Smart Intersection Demonstrator

smart intersection testbed is provided by Marmara University in order to integrate and test the solutions developed by MarUn and other use case partners. The testbed is located in Dragos Campus, Istanbul. The infrastructure has data and electric connectivity and contains an RSU and an Edge Device which are used for development and testing of V2X applications.

Additionally, Marmara University has developed simulation environment with 1:1 scale for the roads. camera is mounted on the simulated testbed along with generated vehicle and pedestrian traffic for an object detection application to detects VRUs and vehicles and obtains 3D position information from them. This information is provided to the nearby entities via V2X communication. The simulation generates realistic driving scenarios and with that tool, dataset for 3D object detection with its provided object data including position, size and orientation is generated.

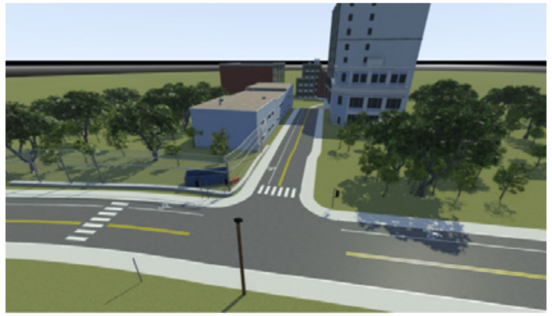


Figure 56: High-definition map of the campus within simulation

High-definition map of the campus within the simulation environment is constructed from scratch to determine the exact location of the objects in the intersection area. This map has enabled the precise positioning of objects within the intersection area and has been integrated into the environment.

Cameras are used to capture images and sensor data from the simulator, which is then used to create dataset of images and corresponding metadata. The generated dataset is used for training the monocular 3D object detection model for 3D localization. Marmara University uses the necessary infrastructure to conduct comprehensive test of the use case throughout the entire application.

Asset Tracking Demonstrator key components:

AI-Enhanced Direction of Arrival (DoA) estimation algorithms

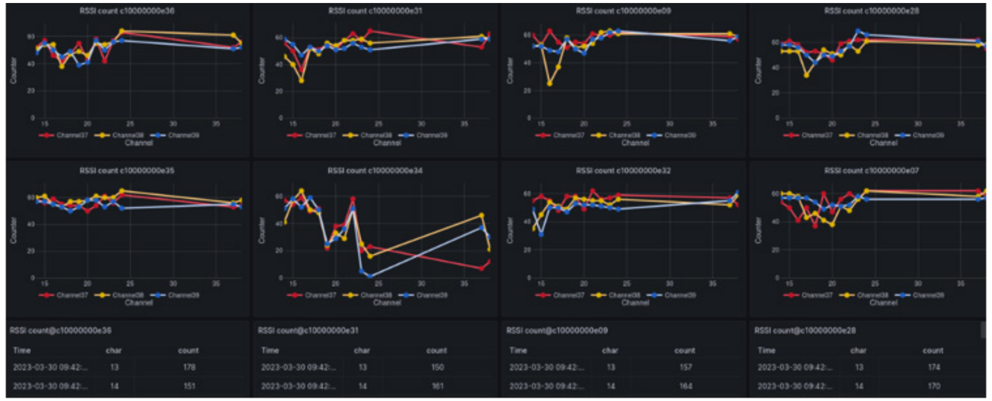
GUT has developed AI algorithms using ESPAR antennas for WSN localization. They collected real-world data for training DoA algorithms, highlighting the challenge of adapting DoA algorithms from controlled to real-world environments. They explored two AI approaches, one using anechoic chamber data and SVM regression, and the other using real data with MLP, achieving 30% error reduction compared to PPCC and reducing ESPAR antenna numbers while maintaining accuracy.

Objects localization

Localized tags are placed on selected items and configured to broadcast message frames, which are received by an ESPAR (reconfigurable) antenna connected to processing unit. Such message packets are passed to microservices for parsing and advanced computation. position calculation product is displayed on pre-defined map-based component that is scalable to the desired system facility.

Data acquisition and visualization system

Data collected during measurements and localisation process state is critical for further development of localisation algorithms. Self-sustaining gateway sends JSON-parsed message via MQTT message broker to Python-based application, which distributes message to desired end services.



RSSI count@c10000000e36

Time	char	count
2023-03-30 09:42:...	13	178
2023-03-30 09:42:...	14	151

RSSI count@c10000000e31

Time	char	count
2023-03-30 09:42:...	13	150
2023-03-30 09:42:...	14	161

RSSI count@c10000000e09

Time	char	count
2023-03-30 09:42:...	13	157
2023-03-30 09:42:...	14	164

RSSI count@c10000000e28

Time	char	count
2023-03-30 09:42:...	13	174
2023-03-30 09:42:...	14	170

Figure 57: Grafana Dashboard

V2X communication key components:

SW platform for V2X message exchange

In the demonstrator the vehicleCAPTAIN toolbox is used for V2X data exchange via 802.11p. The initial plan was to implement routing between 802.11p and upcoming V2X interfaces, i.e., 802.11bd and C-V2X (5G). However, the latter two are still not available for purchase, now, at the end of the project. The platform is ready for integration, but we cannot show the initial AI assisted switching of interfaces. However, we compensated by implementing V2N into the vehicleCAPTAIN toolbox. We also compensated by integrating AI assisted generation of CPMs into our ADDs.

- Objects localization
- Data acquisition and visualization system
- Flexible Payload

The Flexible payload in this use case is used as set of sensors enabling the inspection of critical infrastructure. The payload was mounted on mobile platform which allows for autonomous missions. The payload is equipped with pair of LIDAR and camera. In addition to raw data sent to the operator, the system additionally detects all objects observed on the road and sends it to both the operator and all devices with v2x modules.

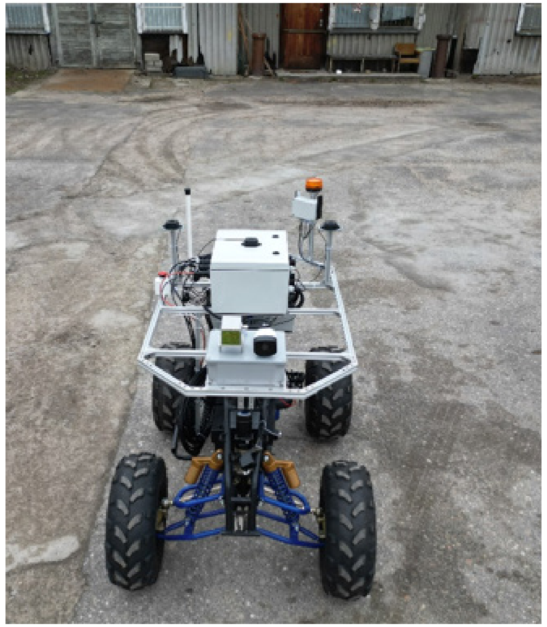


Figure 58: Flexible Payload

Mobile Testing Platform

In most outdoor RF test scenarios, there is need to execute repeatable measurements in multiply locations e.g. arranged on the grid. In order to meet this need, GUT created Mobile Testing Platform which is four-wheel-drive mobile robot capable of executing waypoint missions autonomously. The robot can localize itself with accuracy up to 1 centimetre using the RTK GNSS receiver.

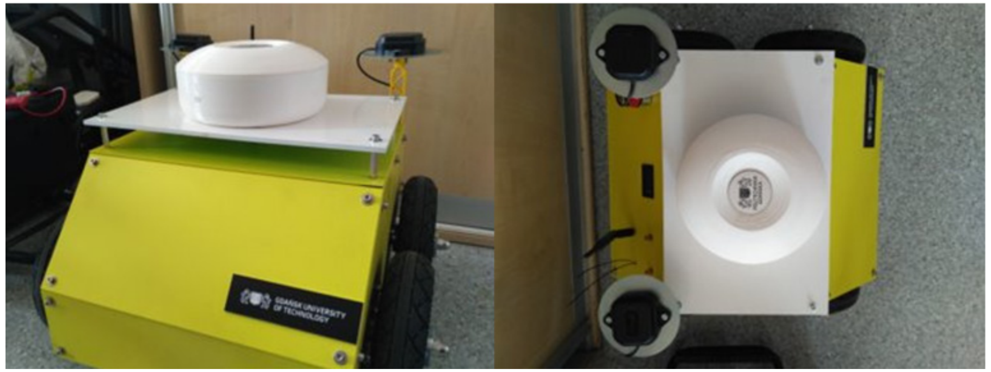


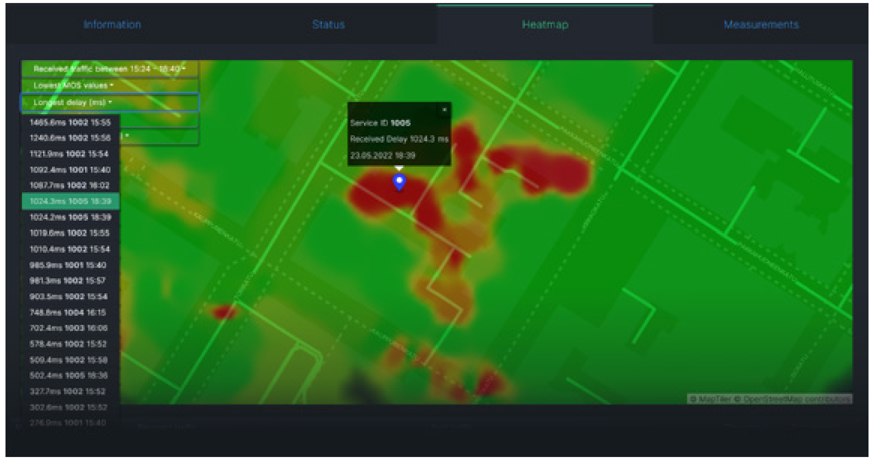
Figure 59: Mobile testing platform

Vehicle CAPTAIN Hardware

The vehicleCAPTAIN hardware is used as part of the V2X communication. Additionally, the vehicleCAPTAIN toolbox was integrated into the VIF ADDs to compensate for the lack of demonstrate ability of routing principles. To repeat the point, the 802.11bd and C-V2X (5G) technology is still not available for integration due to the hardware crisis in the last years; hence we implemented promised intelligent methods not in the routing core of the vehicleCAPTAIN toolbox, but in the generation of CPMs. Real-time monitoring and response.

Network quality situation awareness

The work has focused on measurement results solution, which receives measurement results from large number of measurements, pre-processes the results, stores them in database, and makes them available through web-based UI, REST API, and direct database connection. The main work has been on studying how the results data should be presented to provide the most value. heat map visualisation solution is improved for more intuitive usage, weekly and daily summary reports of the network quality are implemented, and an alarming solution is brought. The ongoing work item comprises studying more detailed graphs from the current and historical results data on network wide and user basis.



```
1465.6ms 1002 15:55
1240.6ms 1002 15:56
1121.9ms 1002 15:54
1092.4ms 1001 15:40
1087.7ms 1002 16:02
1024.3ms 1005 18:39
1024.2ms 1005 18:39
1019.6ms 1002 15:55
1010.4ms 1002 15:54
985.9ms 1001 15:40
981.3ms 1002 15:57
903.5ms 1002 15:54
748.8ms 1004 16:15
702.4ms 1003 16:06
578.4ms 1002 15:52
509.4ms 1002 15:58
502.4ms 1005 18:36
327.7ms 1002 15:52
302.6ms 1002 15:52
276.0ms 1001 15:40
```

Service ID 1005
Received Delay 1024.3 ms
23.05.2022 18:39

Figure 60: Heat map visualization pinpointing single results values

Real-time monitoring and response

KAI's passive network QoS/QoE measurement solution is used for real-time and continuous measurement and monitoring of the network quality for mission-critical applications. KAI has introduced many improvements and innovations in passive QoS/QoE measurement. The primary topics have been **(I)** Collection of radio interface statistics from different radio access technologies (4G, 5G, WLAN) and on different platforms (Linux, Windows, MacOS); **(II)** Delay estimation algorithm for measuring one-way delay despite lack or unreliability of clock sync between measurement points; **(III)** Improvements on the measurement controller and results analyser software, including, e.g., integration of the new measurement capabilities and capability to draw even worldwide scalable heat maps; **(IV)** Automated measurement control solution.

Marmara University Campus Smart Intersection Demonstrator key components:

Object Detection Application

The object detection application focuses on developing and implementing 3D object detection model for localizing objects within the intersection area. MarUn utilizes state-of-the-art 3D object detection model to identify and locate vehicles and vulnerable road users (VRUs) within the camera feed of vehicle-mounted camera. new method for generating 3D object dataset is investigated, and simulation environment is chosen for dataset generation. The created simulation environment resembles the campus infrastructure realistically. Surveillance cameras mounted within the simulation are used to collect realistic images of vehicles and vulnerable road users similar to real-life scenarios. The data from the simulation environment can be used to train the 3D object detection model. The optimized 3D object detection model enables real-time inference on an edge device (NVIDIA Jetson Nano). The detected 3D information is transmitted between the edge device and roadside unit (RSU) over the infrastructure in the CPM format. The RSU broadcasts this information to nearby vehicles, providing information about the detected objects' position, size, and orientation.

Model Framework

The model framework study addresses domain discrepancy problems in machine learning models. The aim is to connect feedback from edge devices with cloud service, which helps gather real-time samples and increase the number and diversity of the training dataset. The experiments reveal bias in the model and performance degradation in terms of accuracy.

The demonstration involves the development and implementation of 3D object detection model to enhance safety and security in the intersection area. It includes model adaptation, training, testing, and the generation of synthetic datasets within simulation environment. V2X communication allows vehicles to receive essential information about detected objects through RSUs, enhancing drivers' awareness of their surroundings.

What business need/problem does the demonstrator address?

Asset Tracking Demonstrator offers several capabilities that can address various business needs:

- Improved Asset Management: The AI-enhanced DoA estimation algorithms can help businesses track the precise location of assets within their facilities. This can be particularly valuable in industries like logistics, manufacturing, and healthcare where tracking assets is crucial for efficient operations.
- Inventory Optimization: By localizing tagged items, businesses can gain insights into the movement and utilization of their assets. This data can be used to optimize inventory levels, reduce excess stock, and streamline supply chain operations.
- Enhanced Security: Asset tracking can improve security by providing real-time monitoring of the location of valuable assets. If an asset deviates from its expected location, it could indicate theft or unauthorized movement, allowing for quick response and recovery.
- Operational Efficiency: Knowing the precise location of assets can lead to improved operational efficiency. For example, in manufacturing setting, it can help optimize the placement of equipment and reduce downtime.
- Resource Allocation: Businesses can use the data acquisition and visualization system to collect and analyse data on asset movement and usage patterns. This information can inform decisions about resource allocation, such as personnel deployment or equipment maintenance schedules.
- Compliance and Reporting: In industries with regulatory requirements, such as healthcare or food production, the demonstrator can help ensure compliance by providing detailed record of asset movements and conditions.
- Customer Experience: For businesses in retail or hospitality, knowing the location of assets can enhance the customer experience. For example, it can help locate items in store or track the movement of service personnel to improve response times.

- Cost Reduction: By reducing the need for manual tracking and improving asset utilization, businesses can potentially lower operational costs and increase overall profitability.
- Scalability: The system's scalability allows it to adapt to various facility sizes, making it suitable for businesses with different operational scales.
- In summary, the Asset Tracking Demonstrator can address wide range of business needs, from asset management and security to operational efficiency and cost reduction, making it versatile solution for various industries.

Asset Tracking Demonstrator offers several capabilities that can address various business needs:

- V2X Message Exchange Platform: The SW platform for V2X message exchange using 802.11p is essential for enabling vehicle-to-vehicle and vehicle-to-infrastructure communication. The demo can showcase the readiness of this platform for integration and highlight its potential for facilitating real-time data exchange in connected vehicle environments.
- Objects Localization: Demonstrating accurate objects localization capabilities is crucial for businesses involved in autonomous vehicles, smart transportation, and infrastructure monitoring. The demo can showcase how the system accurately identifies and tracks objects in its surroundings.
- Data Acquisition and Visualization: Businesses may require efficient data acquisition and visualization systems for various applications, such as traffic management, safety monitoring, or infrastructure inspection. The demo can illustrate how data is collected, processed, and presented to operators in useful and actionable format.
- Flexible Payload for Critical Infrastructure Inspection: Companies involved in critical infrastructure monitoring and inspection can benefit from flexible payload equipped with sensors like LIDAR and cameras. The demo can demonstrate how this payload enables autonomous missions and real-time data sharing with operators and other V2X-enabled devices.
- Mobile Testing Platform: For businesses engaged in RF (Radio Frequency) testing and coverage analysis, the Mobile Testing Platform offers way to perform repeatable measurements in different locations. The demo can show how this platform operates autonomously and provides precise location data using RTK GNSS technology.

- V2X Communication Hardware: The demo can highlight the hardware used for V2X communication, showcasing its compatibility and integration capabilities with existing systems. It can emphasize how this hardware supports communication in the absence of certain technologies like 802.11bd and C-V2X.

- Network Quality Situation Awareness: Companies relying on network quality for their operations, such as telecommunications or autonomous vehicle services, may need solutions to monitor and maintain network performance. The demo can illustrate how the system collects, processes, and presents network quality data in way that provides valuable insights and supports decision-making.

- Real-Time Monitoring and Response: Real-time monitoring of network quality and mission-critical applications is vital for businesses that require uninterrupted services. The demo can showcase how the system continuously measures and monitors network quality, enabling immediate responses to issues or anomalies.

- Passive QoS/QoE Measurement: Companies offering network services can benefit from passive quality of service (QoS) and quality of experience (QoE) measurement solutions. The demo can explain how these solutions collect data from various platforms and technologies, estimate delays accurately, and provide valuable insights for service optimization.

In summary, the demo addresses various business needs, including efficient V2X communication, precise object localization, data acquisition and visualization, critical infrastructure inspection, RF testing, network quality monitoring, and real-time response. These capabilities can be valuable for companies operating in the fields of transportation, telecommunications, infrastructure monitoring, and network services.

Marmara University Campus Smart Intersection Demonstrator

Smart intersection testbed provides controlled environment for the integration and testing of V2X solutions. By simulating realistic scenarios and generating dataset for 3D object detection, the testbed enables us to assess the effectiveness and performance of V2X applications in safe and reproducible manner. The innovation behind this solution lies in the integration of smart intersection testbed with simulation environment. By combining these elements, MarUn provides beyond-SotA platform for the development, testing, and evaluation of V2X applications especially for collective perception services and can test on-site with the real demonstrator constructed in the campus.

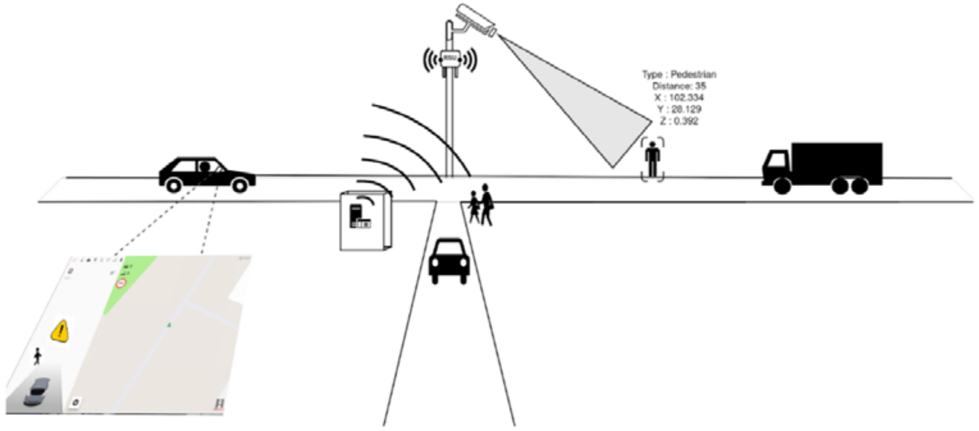


Figure 61: Smart Intersection demonstrator for object detection and V2X communication

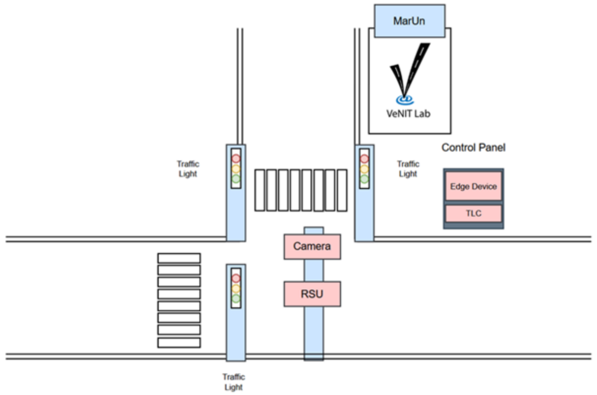


Figure 62: Demo Site Layout in Marmara University Campus

Asset Tracking Solution:

Market: Logistics, Manufacturing, Healthcare
Commercialization: Offer comprehensive asset tracking system powered by AI-enhanced DoA estimation algorithms. Target businesses looking to improve asset management, optimize inventory, enhance security, and boost operational efficiency. Provide scalable solutions for different facility sizes and compliance reporting.

V2X Communication Platform:

Market: Automotive, Transportation, Smart Cities
Commercialization: Provide robust V2X message exchange platform that supports 802.11p communication. Target vehicle manufacturers, infrastructure operators, and smart city initiatives seeking to enhance vehicle-to-vehicle and vehicle-to-infrastructure communication for safety and efficiency.

Objects Localization and Tracking:

Market: Autonomous Vehicles, Smart Transportation, Infrastructure Monitoring
Commercialization: Develop and market accurate objects localization and tracking technology. Serve businesses and industries that require precise location data for autonomous vehicles, traffic management, safety monitoring, and infrastructure inspection.

RF Testing and Coverage Analysis:

Market: Telecommunications, Wireless Network Operators
Commercialization: Offer the Mobile Testing Platform for RF testing and coverage analysis. Target telecommunications companies and network operators needing accurate and autonomous RF measurements in various locations. Emphasize the platform's ability to provide reliable data for network optimization.

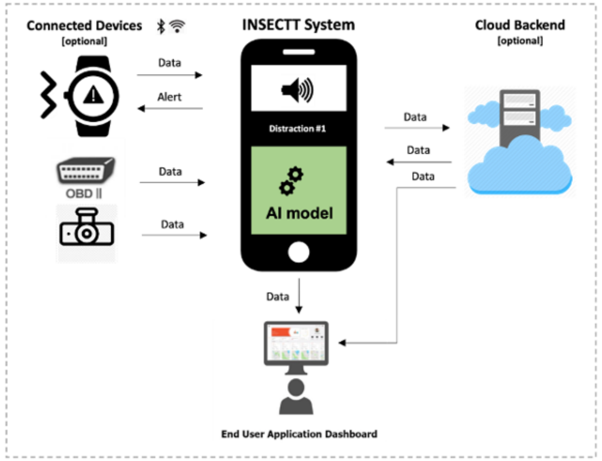
Network Quality Monitoring and QoS/QoE Measurement:

Market: Telecommunications, Autonomous Vehicles, Network Service Providers
Commercialization: Provide solutions for real-time network quality monitoring and passive QoS/QoE measurement. Target telecommunications companies, autonomous vehicle service providers, and network service providers. Emphasize the ability to ensure network performance, detect issues in real-time, and improve service quality.

These commercialization directions leverage the capabilities of the described components to address specific industry needs, including asset tracking, V2X communication, object localization, RF testing, and network quality monitoring. Each direction offers opportunities for businesses to provide innovative solutions in their respective markets. The object detection application and model framework has commercialization opportunities for potential stakeholders in the automotive industry, traffic management agencies, or smart city initiatives. Dissemination of findings by MarUn through academic publications, conferences, and workshops enhances the visibility and credibility of the solutions. Moreover, integration with existing traffic management systems and smart city infrastructure is aimed.

Use Case 5.12

The UC has produced four demonstrators, Smartphone application for driving distraction detection located at Virtual Vehicle (VIF) in Graz Austria, Smartwatch application for driving distraction detection located at Research Institutes of Sweden (RISE) in Stockholm Sweden, Camera-based system for activity and object detection located at TietoEvry in Stockholm Sweden and Dashboard Web application for driver distraction and trip data visualisation located at JIG Advanced Solutions (JIG) in Logroño Spain.



The following figure shows the InSecTT components developed and how they are combined to address the topic of driver distraction detection and driver alerting/educating.

Figure 63: End User Application Dashboard

The driver can be informed about distractions occurring while driving that involve smart devices usage (such as smartphone usage — e.g., calling, texting, picking up the phone, use of applications — as well as smartwatch usage). This type of information can be provided either synchronously (while using smartphone or while using the smartwatch from the smartphone/watch itself) through beeping sound, or asynchronously on computer — using the camera-based system for activity or object detection or via web application.

The approach is comprising of the following components:

I. Smartphone app for driving distraction detection,

II. smartwatch app for driving distraction detection,

III. AI backend where offline processing occurs of the data and AI modelling,

IV. camera-based system for activity and object detection,

V. driver distraction dashboard that supports web interface, cloud data storage, data analysis and data visualization. These are visualised in the figure below.

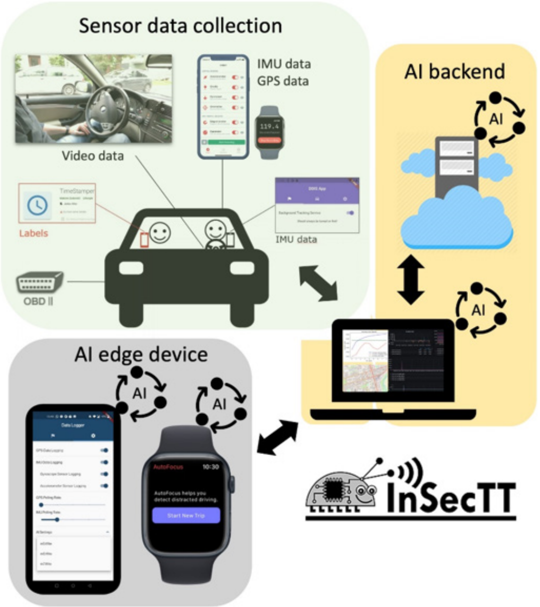


Figure 64: Data flow

The main objective of the demonstrator is to address the topic of driver behaviour monitoring, part of which is distraction detection and specifically distraction from the use of smart devices while driving. Distraction and particularly, distraction caused by the use of electronic devices, such as smartphones for texting or talking on the phone, is one of the leading causes of vehicle accidents. Even though there is an abundance and variety of methods and approaches, they are either approaching the topic with camera-based (camera-vision) systems or with the use of sensors. Our approach brings these two approaches together, bridging the gap as they intent to solve two interrelated challenges, one being the scarce datasets availability of driving distraction data (especially with significant proportions of labelled distractions) and second, accurate driving distraction detections with online (out in the field) testing.

Nowadays, with the increasing number of sensors available in vehicles, there is an abundance of data available to monitor driver behaviour, but it has only been available to vehicle manufacturers and to limited extent through proprietary solutions. Our approach has shifted the paradigm to the use of smartphones and other smart devices (such as wearables) to detect driving distractions and monitor distracted driving behaviour and provide driving habit recommendations or corrections in relation to distractions. Therefore, the driver is educated and trained to avoid taking risks associated to driving distractions that are associated to the use of smart devices.

Exploitation plans

Each involved partner has individual exploitation plans. In relation to the demonstrators and their components video is produced to summarise the achievements and highlights. Regarding exploitation, there's established visibility of the project promoted through dedicated webpage of the Swedish research institute Research Institute of Swedem (RISE) (i.e., https://www.ri.se/sv/vad-vi-gor/projekt/intelligent-secure-trustable-things). Moreover, an analysis of the project goals, objectives and achieved results will be presented to partners and collaborators of the institute during dissemination and exploitation events and forums, like the ones presented in the list below, welcoming past, present and future collaboration partners and where feedback can be collected from industry, and also the scientific and research community.

Use Case 5.13

The Network Anomaly Detection Demonstrator, is located at Westermo Research and Development, in Västerås, Sweden. See Figure 2.

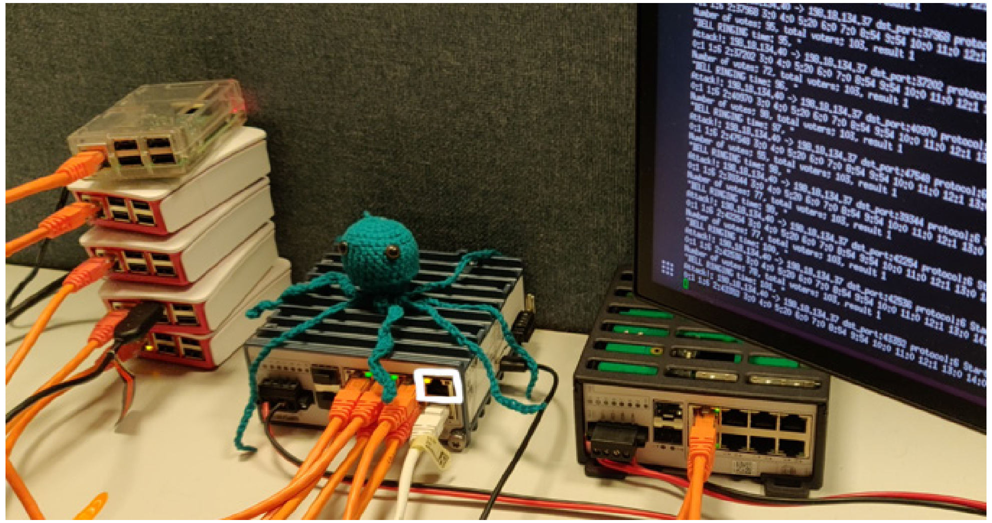


Figure 65: The network anomaly detection demonstrator has detected an anomaly. The router is blinking with an LED (highlighted with white square) and printing "BELL RINGING" on the screen.

Use Case 5.13 targets secure industrial communications systems (ICS), and has aimed at extending knowledge of AI/ML for anomaly detection in industrial communication systems by growing the possibilities for simulation and testing in virtual environment, by creating an attack toolbox that interacts with the simulation, by recording data for off-line development of AI tools, and finally by integrating all parts: running AI tools in physical Westermo router for anomaly detection, as well as development of distributed AI for anomaly detection. The use case implementation is divided into components, and the demonstrator illustrates component on resource constrained AI-powered anomaly detection in an edge device, as well as second component on anomaly models and assurance cases (the anomalies) incorporated in third component on digital twin simulating factory.

Other components developed in the use case are on: anomaly detection in network traffic by using machine learning; on distributed/federated learning where multiple AI's work individually and also coordinate anomaly detection; on distributed/federated AI for intrusion detection in industrial communication system; as well as virtual and hybrid environments for testing cybersecurity.

Strong cybersecurity in industrial communication systems is an important goal for the normal operation of factories, trains, power distribution, etc. This use case aims to investigate AI-powered intrusion detection systems in this domain. Both to explore it with centralized or federated approaches, as well as if these algorithms can run in resource constrained edge devices. In order to explore the topic, anomaly models and assurance cases need to be defined. With these we created two separate data sets to support development and experimentation. With virtual, hybrid and physical simulators we demonstrate how we achieved the goals.

While working on the use case, we have explored the state of the art, and to some extend reached beyond it, as shown in the publications from the use case. Two of these are data sets, two are software repositories, eight are student theses, and ten peer-reviewed/academic publications published, accepted, in submission or under finalization.

The main achievements were:

- During InSecTT, the Westermo operating system (WeOS) was extended with feature to run applications in container (for some products and some customers). From security perspective, the possibility to limit access to resources with containers is very desirable.
- RISE prototyped an IDS extension of security framework for ICS to detect sensor attacks using Digital Twin-based approach and open-source tools. RISE also developed ICSSIM, an open-source framework designed for creating customizable ICS testbeds that simulate various realistic network attack scenarios. In ICSSIM, virtual WeOS nodes were incorporated. To validate ML-based IDSs, RISE developed the ICSFlowGenerator tool, and introduced the 'ICS-Flow' dataset, which includes normal and anomalous network packets and flows obtained from realistic ICS testbed.
- MDH and Tieto developed an extension of the federated learning framework based on random forest for intrusion detection on existing datasets. MDH made an extension of the feature reduction framework based on autoencoders and multi-objective optimization algorithm tested on an existing dataset.

- In collaboration with all partners in the use case, Westermo drove the definition, collection and publication of data set from physical IDS where both attacks and human errors were conducted to trigger network events, and data was also recorded in several places in the network in order to support research on federated AI/ML tools.

- MDH are driving the application of AI methods and their federated learning version to the Westermo data set with the goal to finish experiments and submit for publication before end of the project if extended, or at least finish experiments otherwise.

Exploitation plans

From student or interested layman perspective, there are several important components from our use case that could aid in education, project courses, thesis projects and other experimentation:

- The factory simulator ICSSIM **[1]** and the related ICSFlowGenerator **[2]**, both developed by Alireza Dehlaghi-Ghadim, can be downloaded freely as open source, and used to simulate an industrial control system and used to conduct cybersecurity experiments.

- The Westermo network traffic data set **[3]** and the ICS-Flow dataset **[4]** could aid in developing intrusion or anomaly detection systems with centralized or federated AI/ML, or using other methods.

From Westermo's perspective, work on implementing an AI in an edge device is of course very interesting **[5]**. In the current plans, this could be extended with further AI methods, or possibly become standardized AI toolbox for other AI applications in addition to anomaly detection.

From more academic perspective, the use case has resulted in new knowledge on AI-powered centralized or federated/distributed network intrusion detection, as illustrated in the publications from InSecTT. Future research should build on these findings to generate even more interesting algorithms or tools.

Use Case 5.14

In Use Case 5.14, two demonstrators are developed, looking at different levels of collaborative manufacturing systems:

- Demonstrator: Ice Cream Factory, which is located at the Mälarldalen University laboratory in Västerås, Sweden.

- Demonstrator: HistoTrust, located at the CEA Leti, Laboratory of Security of Embedded Systems, Grenoble, France

Industrial control systems are undergoing transformation driven by business requirements as well as technical advances, aiming towards increased connectivity, flexibility and high level of modularity, that implies need to revise existing cybersecurity measures. In use case 5.14, we aim to investigate and increase the resilience and security of collaborative manufacturing systems, which is one of the emerging system types within the Industry 4.0 paradigm. Components within the area of anomaly detection, access control and system integrity are developed and show-cased in two different demonstrators:

- The Ice-Cream Factory that demonstrates anomaly detection/injection and dynamic authorization in manufacturing system build using the Modular Automation design strategy, with interconnected modules orchestrated using high-level recipe execution.

- The HistoTrust platform, focused on the module/device-level, demonstrates complete blockchain-based attestation process of embedded industrial application based on embedded IA. HistoTrust is generic platform suitable for any production line including the Ice-Cream Factory scenario.

Ice-cream Factory Key Functionalies and Components

The Ice-cream factory demonstrator is complete distributed control system designed according to the Modular Automation strategy, i.e., the physical environment is separated into set of individually controlled modules, e.g., mixer module, pasteurizer, etc. The synchronization between the modules is conducted by an orchestrator unit, executing high-level recipes. modular automation simulation engine has been developed to provide the functionality of separate controlled modules, which are physically interconnected. An architectural overview of the Ice-cream factory demonstrator is provided in Figure 1. The hardware used is COTS products, set-up is displayed in Figure 2.

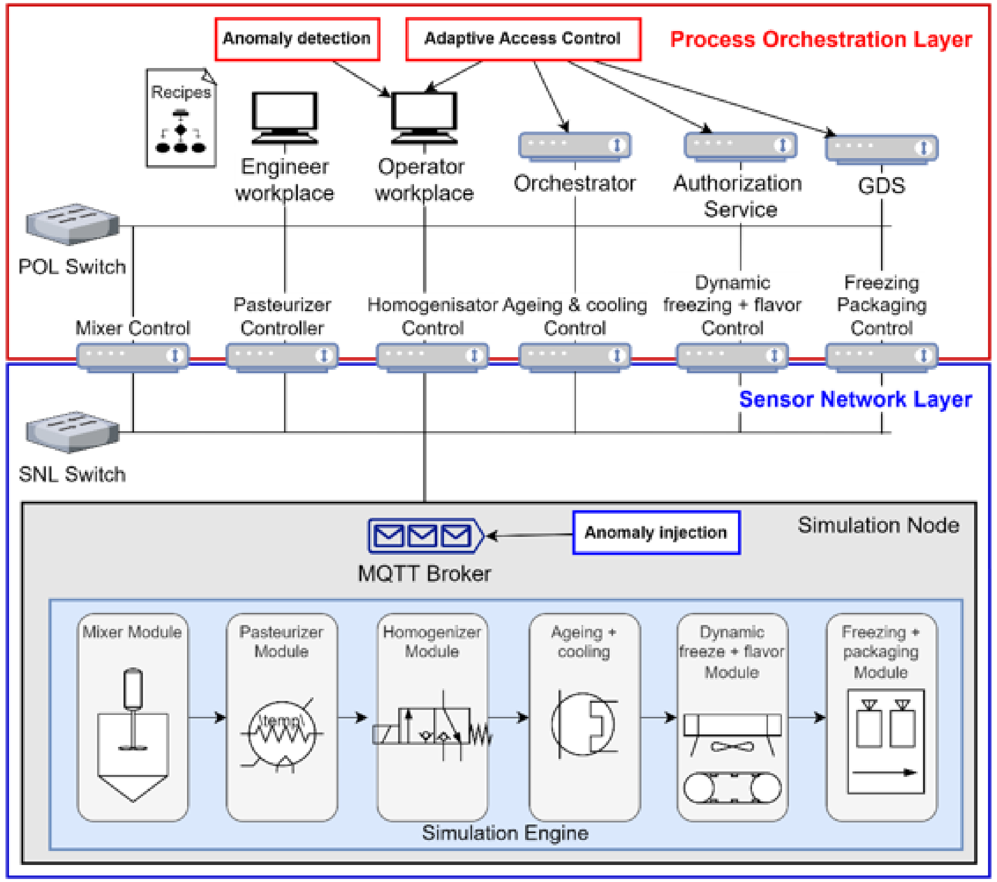


Figure 66: Demonstrator Ice-cream factory hardware set-up (I)

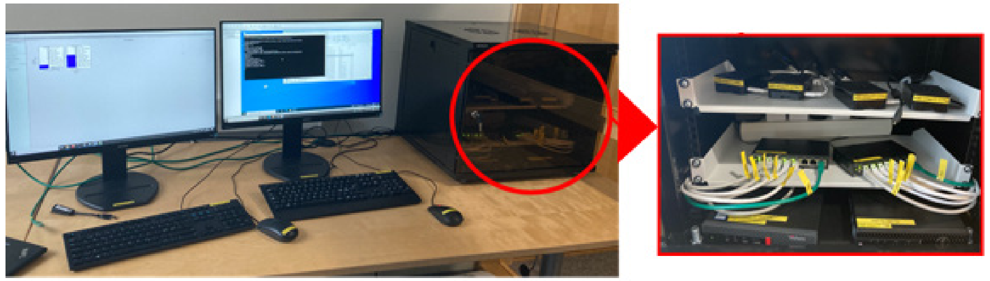


Figure 67: Demonstrator Ice-cream factory hardware set-up (II)

Methods for network as well as sensory data extraction from the demonstrator system has been developed, needed for the anomaly detection methods. The Ice-cream factory includes functionality that enables injection of sensor level anomalies, used to create publicly available dataset, named Modular Ice-cream Factory Dataset on Anomalies in Sensors (MIDAS).

Key Components:

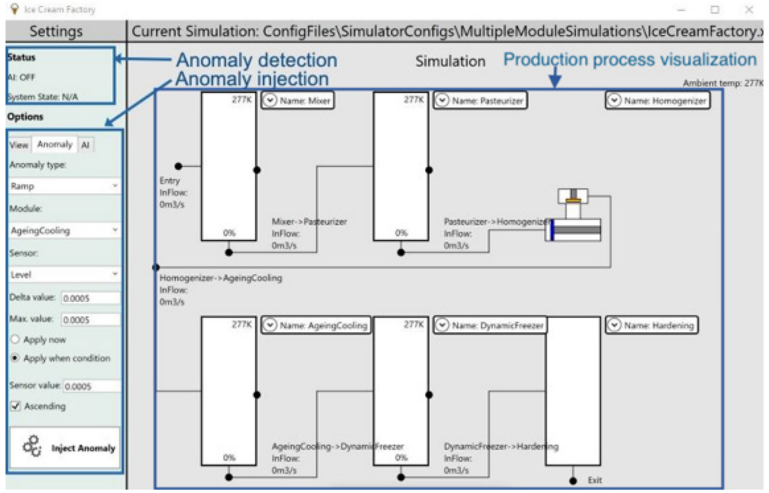
- C1. Enforcement architecture.
- C2. Dynamic Authorization.
- C3. Anomaly models & attack simulations.
- C4. Anomaly detection by ML algorithms.
- C5. Blockchain-based attestation device.
- C6. Authentication of the devices through smart contract and decentralized application (dApp).
- C7. Security of the history of the data produced by industrial applications embedded at the edge.
- C8. Distributed learning algorithms for edge.

Components C1 and C2 are both related to adaptive access control, i.e., the formulation and enforcement of rules which follow the dynamic behaviour of collaborative manufacturing system.

C1 is related to the access control enforcement architecture, specifically providing an architecture solution based on policy delegation with dynamic policy decisions being taken by central authorization service, and static policy decisions being handled locally by the resource server. C2 is related to policy rule formulations, with the aim of keeping the policy decisions synchronized with the currently running set of recipes, i.e., workflow-based policy decision framework.

As prerequisite for the access control mechanisms, Public Key Infrastructure (PKI) is implemented, using certificate push management based on the Global Discovery Server (GDS)-implementation from the OPC foundation .NET stack for OPC UA, and novel virtual provisioning mode needed to support the transition from self-signed to CA-signed certificates of OPC UA servers.

The components C3, C4 and C8 are related to the development of reliable Intrusion Detection System (IDS) that will be part of the demonstrator. For C3, that covers attacks simulations and anomaly injection, the work is done directly on the simulation engine, and the software is upgraded with the module for anomaly simulation. This module is used to generate an open dataset to evaluate different ML algorithms for anomaly detection and classification for components C4 and C8. Evaluation of the ML algorithms showed that Long Short-Term Memory (LSTM) had the best performance on the generated dataset and that algorithm was integrated in the demonstrator (C4). When it comes to the distributed learning algorithm for edge (C8), the integration of the developed federated learning framework based on random forest is currently ongoing and should be completed in the upcoming months. User interface that enables access to the integrated functionalities for anomaly injection (C3) and anomaly detection (C4) is shown Figure 43.


Ice Cream Factory

Current Simulation: ConfigFiles\SimulatorConfigs\MultipleModuleSimulations\IceCreamFactory.x

Status
AI: OFF
System State: N/A

Options
Anomaly type: Ramp
Module: AgeingCooling
Sensor: Level
Delta value: 0.0005
Max. value: 0.0005
○ Apply now
● Apply when condition
Sensor value: 0.0005
☑ Ascending

Ambient temp: 277K
Entry InFlow: 0m3/s
Mixer->Pasteurizer InFlow: 0m3/s
Pasteurizer->Homogenizer InFlow: 0m3/s
Homogenizer->AgeingCooling InFlow: 0m3/s
AgeingCooling->DynamicFreezer InFlow: 0m3/s
DynamicFreezer->Hardening InFlow: 0m3/s

Figure 68: User interface of the ice-cream factory demonstrator including: production process visualization, anomaly injection and anomaly detection

The demonstrator HistoTrust is composed of several devices – the high-end STM32MP157a-EV1 platform from STMicroelectronics – (see Figure 44) each embedding state-of-the-art deep neural network model for inference purpose. The architecture is based on both Cortex-and Cortex-M4 cores. For demonstration and evaluation purpose (i.e., benchmarking the embedded inference process in the Cortex M4 through the STM.CubeMX,AI library from STMicrolectronics), the neural network model used is classical convolutional neural network (CNN) performing an image classification task. However, HistoTrust is suitable for any other types of data (text, time series, ...) and machine learning models. These devices act as decentralized, asynchronous and independent automatons. Smart contracts are employed to orchestrate the transactions sent by each device and register the evidence – also called attestations – in the ledger of the Ethereum blockchain.

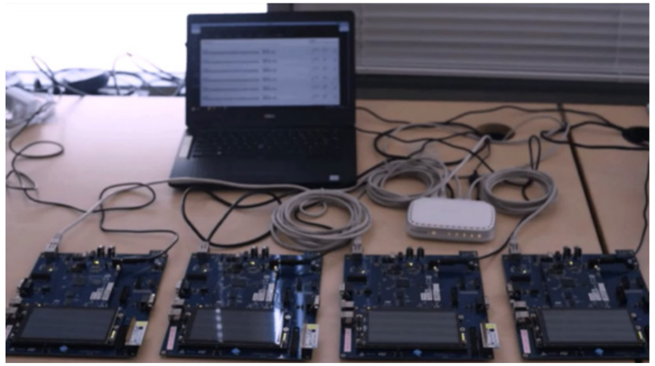


Figure 69: Demonstrator HistoTrust composed of decentralized electronic boards issuing attestations to an ethereum blockchain

HistoTrust enables the traceability of an embedded neural network activity through the registration of evidence in an Ethereum blockchain. This scheme allows to ensure the accountability by the legitimate legal entity of the operations performed in production line. The platform could be generalized to many other IoT domains where the traceability of the data and inference program are critical information.

Key Components. Components C5, C6 and C7 (cf. list above) are integrated to build the demonstrator HistoTrust, enabling the traceability of AI behaviour through an historic of attestations maintained by an Ethereum blockchain. The ordered attestations bring evidence that authenticate the issuing device – and thus the embedded AI – and protect the integrity of the AI inputs and inferences. This enables the reproducibility and the explainability of the AI behaviour. HistoTrust relies on software and hardware security features by combining cryptographic modules (elliptic curves), Ethereum ledger and smart contracts, ARM TrustZone and Trusted Platform Module (TPM, ST33 from STMicroelectronics) as illustrated in Figure 5 with the overall architecture.

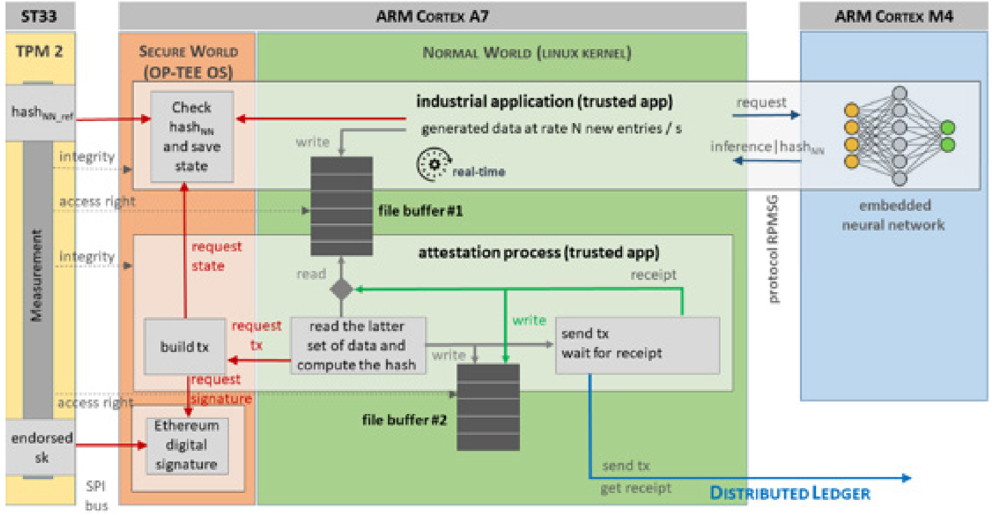


Figure 70: Overall architecture of the HistoTrust platform

The Ice-cream factory and HistoTrust demonstrators focus on complementary aspects which are highly relevant in future secure collaborative manufacturing scenarios. The Ice-cream factory focuses on system-wide functionality for fine grained access control and intrusion/anomaly detection, and the HistoTrust demonstrator focuses on device-level attestation and data authentication.

With respect to the state-of-art, the following major aspects characterize the novelty of the two demonstrators:

- The policy inference algorithm of C2 can provide access control policy decisions following active workflows, something currently not available in industrial system. The algorithm is specifically developed for modular automation, but may be adapted to other variants of formalized workflow descriptions.

- The technologies used for the enforcement architecture (C1) are fine-grained and dynamic enough to enforce the workflow-based mechanisms of C2. Available standardized components are used for the architecture, e.g., OPC UA for the communication stack and JWT for access tokens, making the suggested solution applicable in any domain utilizing these standards.

- The anomaly injection functionality can be used to simulate different scenarios for various production processes and generate more datasets. The MIDAS dataset is publicly available and it brings opportunities for different research areas within ML.

- To the best of our knowledge, HistoTrust is the first platform to fully demonstrated blockchain-based attestation process for an embedded AI with an architecture that leverages both software and hardware security features. The platform demonstrates an innovative way to perform full authentication process directly at the edge-level with advanced security primitives and an interesting trade-off with the system performance requirements. HistoTrust may be used in different IoT application domains where the traceability of the data and inference program are critical information.

- HistoTrust authentication process relies on complex and innovative mechanism that enables cryptographic attestations to be registered in Ethereum ledger through smart contracts. That includes the management of elliptic curves secret keys and the use of secure components (TPM, ARM TrustZone) with strong effort of optimization on the STM32MP1 platform to avoid any latency issues. This process is not data-dependant and may be used in different IoT application domains.

Contact information

For further information or enquires related to demonstrator Ice Cream Factory and HistoTrust, please contact:

- Björn Leander, ABB AB (bjorn.leander@se.abb.com)
- Christine Hennebert, CEA (christine.hennebert@cea.fr)
- Pierre-Alain Moëllic, CEA (pierre-alain.moellic@cea.fr)

The two demonstrators and their components will be exploited in different ways including:

- European patent application is filed for some of the results related to the access control enforcement architecture, as preparation for potential future exploitation. Several findings in the use case have had indirect impact on ABB internal R&D projects. ABB is participating in several standardization activities, e.g., IEC 62443, OPAS, etc., that could be of relevance in the context of this use case.

- The demonstrator Ice-cream Factory is installed at MDH and will be used for research and education purposes in the future. It was already used in the Distributed Software Development course as base for the project of developing the user interface for the simulator, as well as for several master and bachelor theses.

- The open dataset MIDAS is exploitable for ML research in manufacturing systems.

- The Federated Learning Framework for Network Attacks Detection and Classification Based on Random Forest, can be exploited and used in different areas.

- Based on preliminary study performed by RISE and MDH, which examined the temporal relations of attack consequences, we have obtained promising results for enhancing IDS effectiveness. RISE aims to build upon this technique as foundation, expanding its application to generate even more effective IDS.

- HistoTrust is the proof-of-concept that demonstrates that physical devices can act as autonomous and independent entities in decentralized context. Thanks to this use-case, CEA-LETI aims at generalizing histoTrust to other IoT domains (e.g., healthcare, transport) related to other industrial partners and collaborative research project opportunities at the national and European scale. Actions are in progress to standardize the smart contract developed as Verifiable Credentials for the community.

- CEA based the development and evaluation of HistoTrust on standards related to Security for Industrial Automation and Control Systems, more particularly IEC 62443-1-1 et 62443-3-2 (security risk assessment).

Use Case 5.15

The Demonstrator will consist of three videos. The first (Audio anomaly detection demonstrator) will be standalone demonstration of the audio anomaly detection component developed by CINI-UNIROMA3, which has not been integrated in the Modena test in M35 for logistic reasons. The second video (Modena test ride demonstrator) will show the results of the test ride in Modena, where the different component developed by the partners involved in the UC have been integrated by means of the IoT infrastructure based on Eclipse Kura and Kapua provided by ETH. The components integrated are: video anomaly detection by CINI-UNIMORE, air quality monitoring by ETH and CINI-UNIPR, people counting strips by ETH and the potholes detection module by LDO. The last video (Predictive maintenance demonstrator) is presentation of the results achieved by LDO for the creation of dataset for predictive maintenance, its analysis and proof-of-concept of recurrent neural network approach for the development of an AI-based prediction system for vehicle maintenance interventions.

Demonstrator Key Components

The Audio anomaly detection demonstrator consists of standalone demonstration of the audio anomaly detection component. The component developed by CINI-UNIROMA3 consists of 2 stage audio anomaly detection module which works with MEL spectrograms to (first stage) detect an anomalous audio event and (second stage) provides classification of the event. Originally conceived to perform the detection of the anomalous event on the edge and the classification on the enterprise side, the component has been fully integrated on an NVIDIA Jetson Xavier board to be deployed on the edge. Data collection campaigns conducted with the partner SETA allowed CINI-UNIROMA3 to improve the robustness of the system by constructing dataset comprising the mechanical background noise of an operative bus during ride. The component integrates an MQTT client; detections and classification of anomalous sounds are communicated to the MQTT broker and displayed by means of GUI prepared by the partner CINI-UNIROMA3.

Modena test ride demonstrator consists of the results of the test ride in Modena in M35, exhibited by means of dashboard collecting information gathered from the different monitoring subsystems integrated by means of Eclipse Kura / Kapua IoT framework. The component shown in the demonstrator are: CINI-UNIMORE's video anomaly detection system for the monitoring of anomalous behaviour inside the bus; ETH and CINI-UNIPR's air quality monitoring system to detect concentration of dangerous substances in the air, check CO2 levels along the ride etc.; ETH's people counters based on variations of the electromagnetic field; LDO's potholes detection system to detect the presence of potholes on the road-surface, in order to help the public transportation company to solicitate intervention of the municipality. It is worth to mention that the ride has been conducted through the streets of Modena and not in more controlled environment as originally stated (the MASA dynamic area).

The predictive maintenance demonstrator is presentation by LDO's researcher of the AIRC laboratory representing the workflow, the dataset construction and the results obtained regarding the development of an AI-based method for predictive approach to prevent mechanical failures during the rides.

At high level, the UC5.15 tackles the problem of public security and safety in restriction to the bus environment, and more precisely with busses serving urban area, such as Modena. The different services which have been designed, realized as prototypes and tested within the UC5.15 respond to this logic. Furthermore, the 5G (and beyond 6G) revolution is going to make available several scenarios thanks to low latency and high throughput data transmission, which will make the combined use of IoT and Artificial Intelligence prominent in the years to come. In this sense, the UC5.15 tried to explore some of these services, based on the end-user's SETA needs and knowledge of the difficulties and peculiarities of the operations in this market segment.

More in detail, the first two demonstrators are related to the safety of passengers during the bus ride. The services envisaged by the partners participating to the UC, and validated by end-user SETA, relies on the deployment on the edge of artificial intelligence based systems integrated via an IoT architecture designed and realized by the partner ETH, based on the Eclipse Kura / Kapua framework, an open source framework for IoT mainly developed by ETH in collaboration with RedHat. The monitoring systems tackles different problems: video anomaly detection (CINI-UNIMORE) and audio anomaly detection (CINI-UNIROMA3) are strictly related to human activities and anomalous behaviours which may occur inside the bus, from brawls, to robberies, to arguments which are relatively common in public transportation user experience. The systems are conceived as tools which may help security operators to respond timelier to such situations and by no means they constitute standalone automated monitoring systems. It should be noted that, such system could significantly improve safety without jeopardizing privacy, as the security personnel of the public transportation company is already allowed to retrieve information from the CCTV system present on-board, and the system only transmit alerts and metadata, minimizing transmission of personal data, which is stored in the edge device only when an anomaly is detected and may be retrieved offline. The environmental monitoring system (ETH) tackles the problem of air-quality monitoring within the bus environment. It is well known (and common citizen experience) that, especially in highly industrialized areas air quality becomes often an issue depending on weather conditions such as absence of wind, atmospheric pressure and absence of precipitations. The situation may be aggravated when people are stuck in traffic. The new prototypes provided by ETH (with CINI-UNIPR collaboration for the analytics), IoT ready and compact, are the first of new generation of sensors which will enlarge ETH's market on this line of products. The system allows for near real-time evaluation of air-quality conditions inside the coach, from particulate to dangerous gaseous substances, and thanks to IoT readiness they could be integrable in more sophisticated system which automatize some mitigation measures, from air conditioning to automatic window opening, or even restrict the access to new passengers on-board in cases where the previous mitigation measures are ineffective. Besides, users, drivers are certainly the stakeholders which are more interested in the air-quality inside the coach, and HSE departments as well as workers could greatly benefit from such system, allowing for better turn planning. The people counters (ETH) deploy variation in the electromagnetic field (VERIFICARE) to count the number of people crossing fence (for example, people mounting on board or demounting from the vehicle) which is completely privacy preserving. The ability to count people on-board is crucial to public transportation companies, both for planning rides along given route, but also for the purpose of aggregate estimate of payment evasion from the users, which may also allow for better scheduling of controllers teams among the different rides. Usually, this kind of statistics can be recovered from ticket machines, but the data which can be extracted is not entirely reliable due to human behaviour. The solution proposed by ETH is non-intrusive, privacy preserving technology which may help public transportation companies to improve their ability to retrieve information regarding bus rides. Finally, LDO's solution for potholes' detection respond to an explicit need of the end-use. Public transportation companies often work in close contact with municipalities for what concerns road surface status, indeed, besides dedicated lanes, the busses often take ordinary lanes and the capillarity of the service makes them the best candidate to represent the situation of the road surface along the city road network. The system designed and realized by LDO works in real time, processing video streams from frontal camera pointing to the road surface to detect potholes, provide size estimation thanks to dedicated calibration procedure keeping into account both the camera positioning and optical distortion, and sending alerts to the central system via MQTT protocol, together with BASE64 encoded reference image, whenever the detected potholes exceed certain threshold, thus allowing the public transportation company to have near real-time alert system and thus prompt intervention of the municipality, with benefits both for the mechanics of the vehicles moving along the route and of passengers as well.

The predictive maintenance demonstrator will give an account of the work conducted by LDO towards an AI-based system to predict the necessity of maintenance intervention. The business problem has obvious implications related to business continuity and cost optimization for public transportation companies as well as security of passenger on-board. Indeed, poor maintenance scheduling could lead to critical incidents (up to ignition of the coach itself) posing severe threat to the safety of passengers and of the drivers. Advantages in terms of cost optimization for condition based/predictive approach to maintenance rather than preventive (or worse corrective) maintenance approach has been studied econometrically and the advantage is significant. It should be noticed however that the green transition of public transportation vehicles will significantly change variables into play, as usually electric vehicles are less subject to mechanical stress due to vibration caused by the ignition system in gas and fuel vehicles.

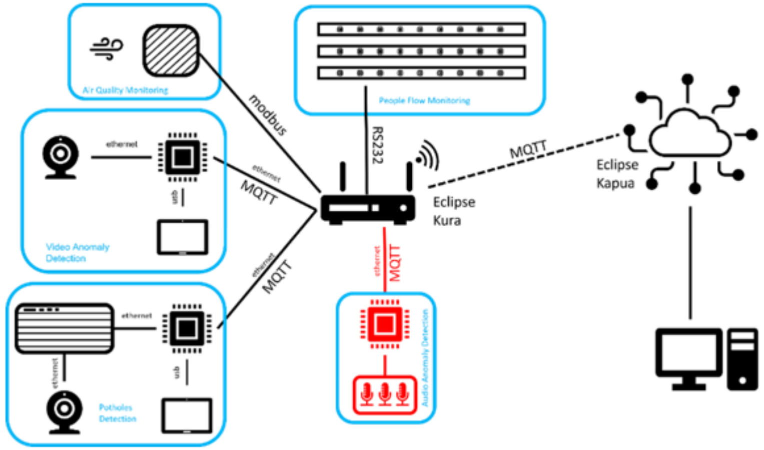


Figure 71: Synthetic integration scheme of UC5.15 demonstrator

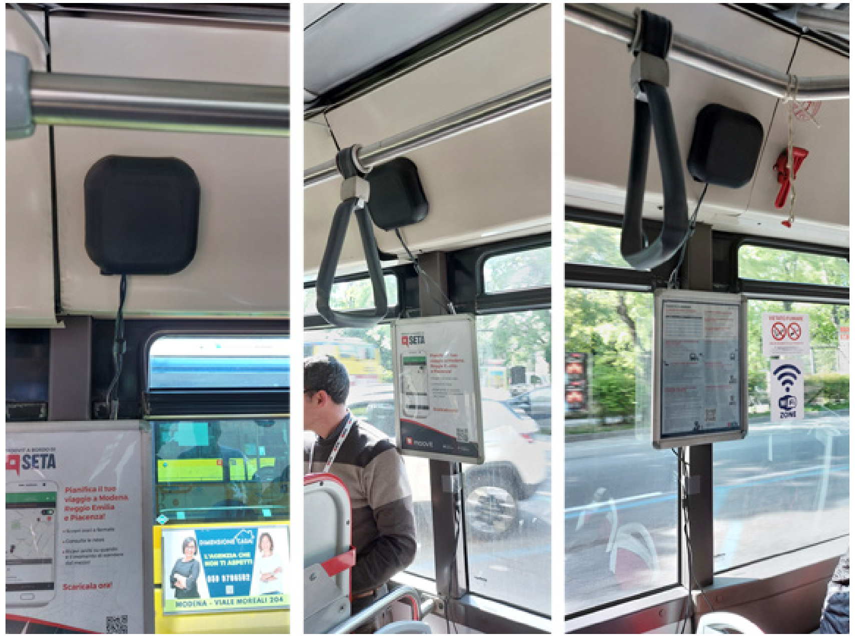


Figure 72: ETH's environmental sensors for air-quality monitoring system

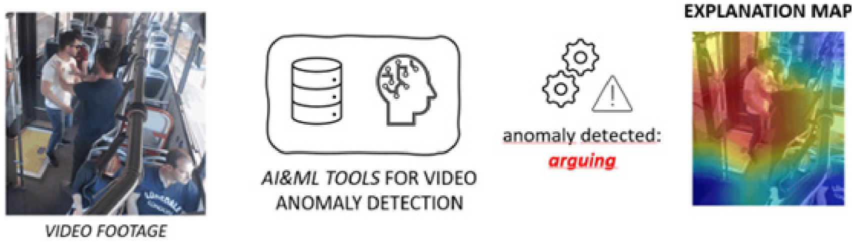


Figure 73: Video anomaly detection: production of explaination map

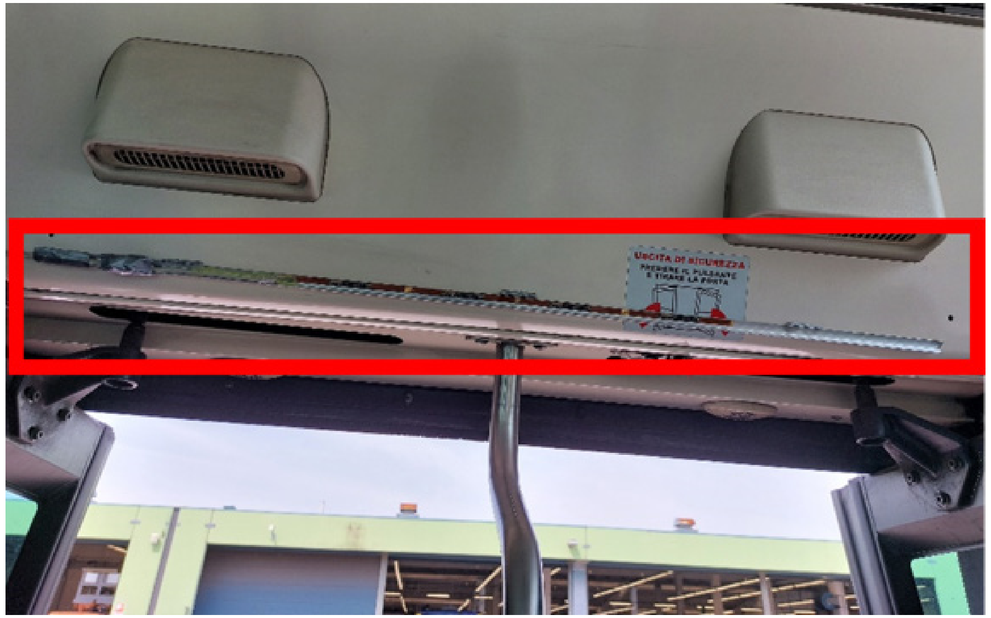


Figure 74: ETH's people counting strip

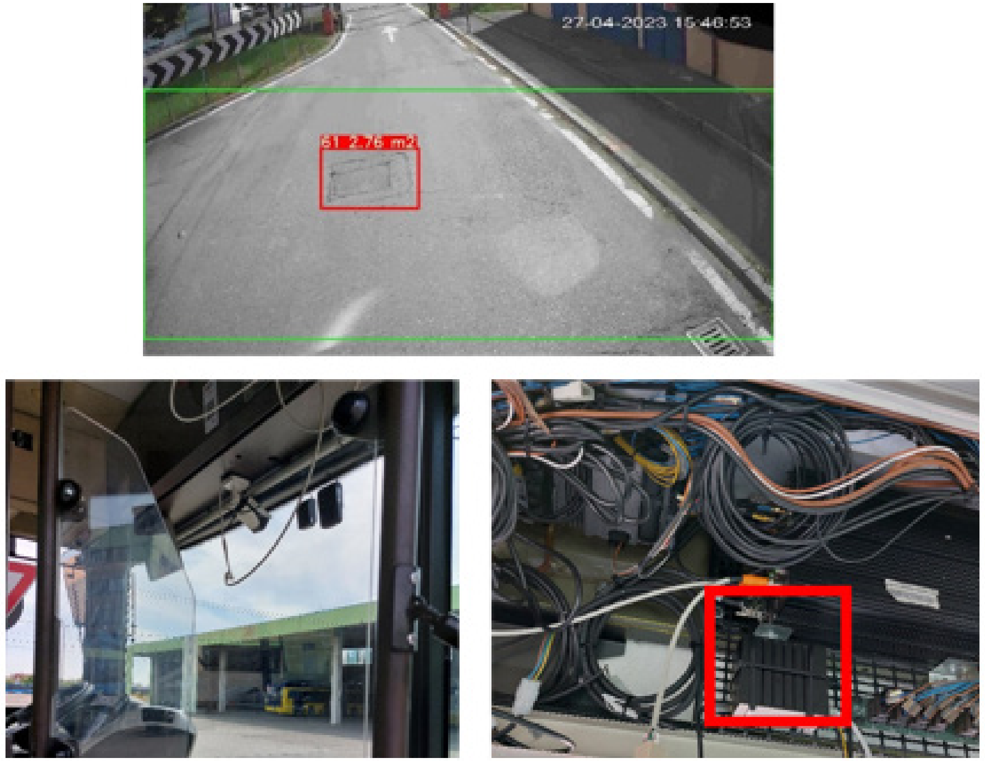


Figure 75: Potholes detection HW setup and sample frame for event detection

Exploitation plans

Potholes detection component has been successfully validated in an operative scenario by LDO. The component needs some refinement in order to avoid detection of manholes which are often present on the road surface but has been evaluated effective and worth of further investigation from the product management and the engineering department devoted to public transportation solutions. On the other hand, similar topic emerged in another program, where the component was developed by an academic partner and further activities are expected after end-user validation. Regarding predictive maintenance the topic is of interest. The activities conducted in InSecTT allowed for proof-of-concept of recurrent neural network approach to failure prediction, though based on assumptions in absence of list of maintenance intervention. The opportunity of further development activities in this direction are under evaluation.

ETH's work within the project led to two major results. First an advanced prototype for new generation of environmental sensing stations, much more compact and IoT ready than the previous ones. Such development, especially compactness of the sensors allows for new use cases (such as the one represented by the bus environment) and potentially new commercial opportunities. Regarding people counters, the developments achieved during the InSecTT project has been significant allowing to pass from proof-of-concept to prototype to sensor much closer to the final product that ETH has in mind. Privacy preserving approaches to counting are certainly of great interest for all companies which aim to have GDPR compliant way to count accesses, such as the public transportation companies.

Academic partners involved in the UC published several scientific papers reporting the results obtained in InSecTT. Among exploitable items available to the public, besides scientific publications we mention two dataset published by CINI-UNIMORE (one of them in collaboration with SETA):

- MOTSynth dataset: huge dataset for pedestrian detection and tracking in urban scenarios created by exploiting the highly photorealistic video game Grand Theft Auto V developed by Rockstar North. https://aimagelab.ing.unimore.it/imagelab/page.asp?IdPage=42

- INSECTT Anomaly detection SETA Dataset: long, untrimmed real-world surveillance videos with 11 realistic anomalies recorded with series of CCTV cameras placed inside SETA buses. https://aimagelab.ing.unimore.it/imagelab/researchActivity.asp?idActivity=79

We also mention here the intention of CINI-UNIPR and SETA to release dataset regarding air quality data collected on SETA bus operating in Modena for several months.

SETA besides having the opportunity to test several new technologies in an operative scenario contributed to the realization of the aforementioned dataset. Moreover, the experience gained during the InSecTT project and the interest towards digitalization and exploration of new services allowed SETA to become the end-user for the project "NextWare" where also CINI (UNIMORE and UNIPR) together with ETH will push forward the combined use of IoT and AI in the context of public transportation.

Use Case 5.16

In order to provide demonstration of the results achieved in UC5.16 partners contributing to the UC will prepare three distinct videos. Multi-biometric recognition system demonstrator will provide demonstration of the multi-biometric recognition system by CINI-UNIROMA3. The multi-biometric recognition system has been integrated and deployed on ADP's premises in Brindisi (in the extra-Schengen boarding area of Brindisi Airport terminal). Footage for the demonstration has been recorded in Brindisi, and it represents the results of tests conducted in M37. Crowd management system demonstrator will provide demonstration of LDO's crowd management system (an algorithmic suite comprising people counting, social distancing and man-down detection) processing three footages trimmed from longer footage recorded in Brindisi in M36 in dedicated area for the test. Thermal screening demonstrator will describe the results obtained in laboratory environment for what concerns infrared-domain only thermal screening algorithm developed by LDO. Finally Anomaly Tracking system demonstrator will provide demonstration of the results obtained for the anomaly tracking system tested in Brindisi.

Demonstrator Key Components

The Multi-biometrics demonstrator consists of an identification system based on the fusion of biometric data such as hand-vein patterns and face deep descriptors captured by deep learning techniques by means of infrared cameras (hand-vein patterns) and cameras (face descriptors). The system is composed of an enrolment kiosk and verification kiosk communicating with laptop, positioned at the enrolment kiosk, where GUI allows the user to insert its data and perform the enrolment for both types of data. The verification kiosk is responsible for identity verification and is endowed with STOP/GO signal to prevent un-enrolled people to access the area.

The Crowd-management demonstrator shows the platform for security control enhanced by the use of deep learning algorithms. The system will show the functionality of three algorithms: people counting, social distancing and man-down, all applications based on the same detector (YOLOv5) but responding to different logic. In particular the people counting system allows to count people on given scene, providing also the user to set virtual fences on the scene, to count the number of people crossing them, or to circumscribe specific polygonal area to count the number of people inside it; the social distancing algorithm, building on the detector, tracking system and by means of calibration procedure allows the security operator to check the respect of social distancing measure and/or get qualitative sense of the risk due to the absence of the social distancing; finally the man-down detector, which is YOLOv5 based binary classifier to identify automatically man-down situation. The platform is able to work both with live streams from IP cameras or with streams from file stored on the client's side of the architecture and allows the user to choose the kind of processing to be performed on the video source.

The Thermal screening demonstrator shows the results of tests conducted in laboratory setup of an algorithm for thermal screening which is based on routine which approximate the correct location of the eye canthus of people on the scene. The thermal screening algorithm interacts with the thermal camera API and works exclusively in the thermal domain, thus protecting the privacy of involved subjects; the algorithm first estimate the location of the face key points (eyes, nose tip, ears), using those key points which are used for 3D head pose estimation and the 3D-to-2D projection; afterwards first approximation for the eye canthus region is obtained and an iterative procedure which looks for the warmest pixel in the current estimated eye canthus region and recompute the current estimated eye canthus region until convergence.

The Anomaly tracking demonstrator shows the result obtained in tests conducted in the extra Schengen boarding area of Brindisi Airport terminal, of module which leverage on knowledge graphs to correlate alerts coming from two different subsystems. face re-identification module based on deep learning for feature extraction and matching and an environmental monitoring system integrated thanks to the IoT framework of Eclipse Kura and Kapua. The system "counts" the number of almost simultaneous occurrences of matches from face gallery and the alerts coming from the environmental monitoring subsystem to identify the person which is supposed to carry the dangerous substance (alcohol, in the demonstration).

Security and quality of service are two main concerns of companies providing services and airports management. Security, despite having always been of capital importance in airport management, has been the principal concern in Europe since the rise of ISIS related terrorist actions in 2016 (mainly in France, Belgium and Germany). In UC5.16 we demonstrate some solution related to some situation which may occur in airport management. Namely:

- Multibiometric recognition demonstrator shows new method based on multibiometric data, much more resilient to spoofing attacks, and with reliability superior to the one guaranteed by fingerprints. Such system, which only requires an initial enrolment which takes one minute, may allow airport to reduce personnel devoted to identity checks and speed up boarding procedures and even control procedures, being able to work "on-the-move".

- Crowd management system demonstrator respond to the need of security operators of large infrastructure to monitor several screens at time. With an ever increasing number of monitoring devices it is paramount for security operators to have way to monitor streams of data from several sources in an automated manner. The system proposed allows to extract useful information and send alerts on the basis of parameters which may be selected by the operator, in relation with the functionality described above (people counting, social distancing and man-down detection). In particular, social distancing (as the thermal screening) was designed keeping in mind the evolution of the response to the COVID-19 pandemic, where social distancing, together with use of DPIs such as masks, has been reasonably effective countermeasure before the introduction of vaccines.

- Thermal screening demonstrator respond to need which has become even more common during the COVID-19 pandemic, from malls to airports, to train station, to post offices, the temperature check has become an everyday life experience (nowadays largely dismissed thanks to lift of safety measures consequent to the diffusion of effective vaccines). Commercial solution for temperature estimation are often unreliable, and they may have problems in estimating the temperature when several people appears on the scene. The solution proposed in the UC by LDO allows, thanks to an iterative procedure making use of face keypoints and 3D head pose estimation to correctly locate the region of the inner eye canthus – which is the region of the face with higher correlation with body temperature. The feature of working exclusively in the thermal domain represent distinguishing feature as it minimizes the risk related to transmission of personal data.

- The ability to identify set of of persons which are responsible of anomalous events detected by some monitoring system (an environmental monitoring system in the case of the anomaly tracking demonstrator) and to track their movements along security cameras would represent relevant enhancement of the capabilities of threat mitigation and containment of security operators. The logic implemented in the anomaly tracking demonstrator makes use of knowledge graph to temporally correlate alerts coming from ETH's environmental monitoring system with the "matches" obtained from face re-identification module, progressively increasing an index of dangerousness of the subject.

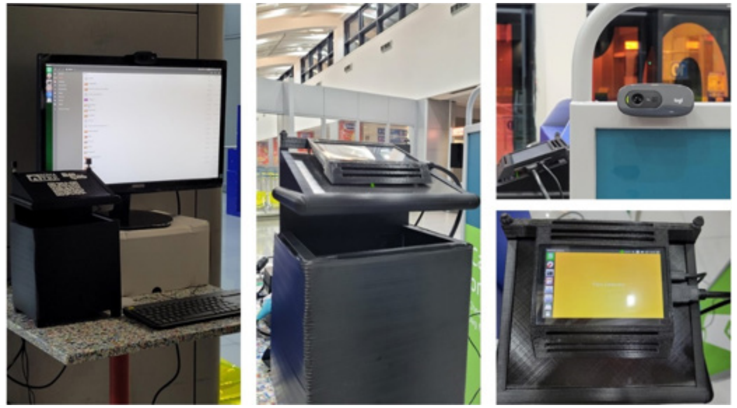


Figure 76: CINI UNIROMA3 Multibiometric recognition setup in the extra-Schengen boarding area of Brindisi terminal, enrolment and verification kiosk

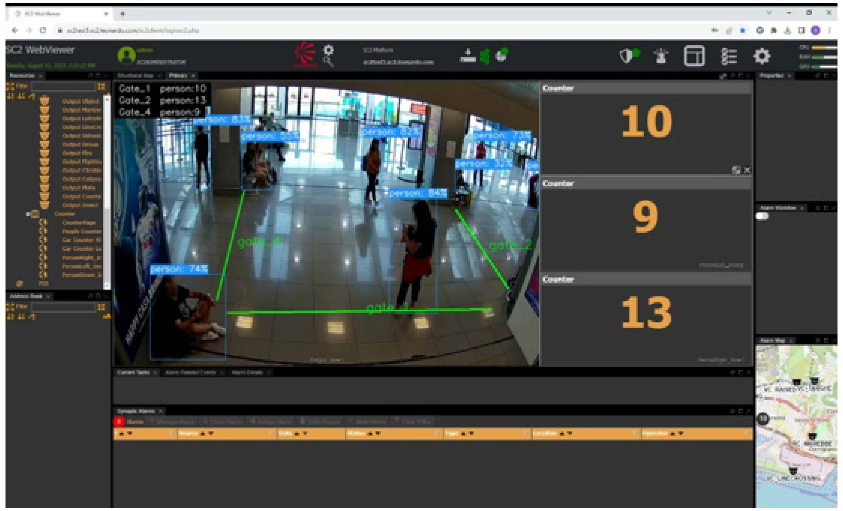


Figure 77: Crowd management system: SC2 cockpit for people counting tested over Brindisi airport footage taken in dedicated and advertised area. Faces have been blurred for anonymization purposes in compliance with GDPR according to the data protection agreement

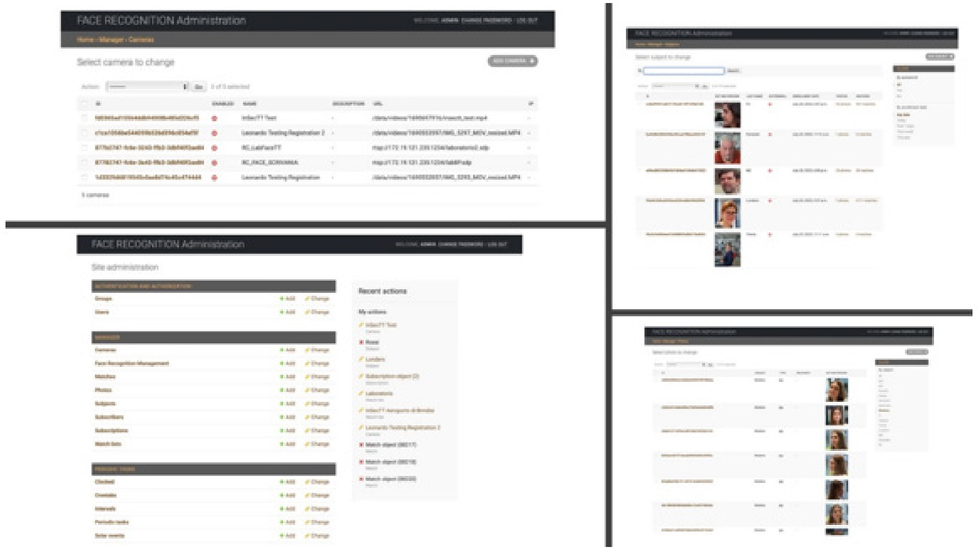
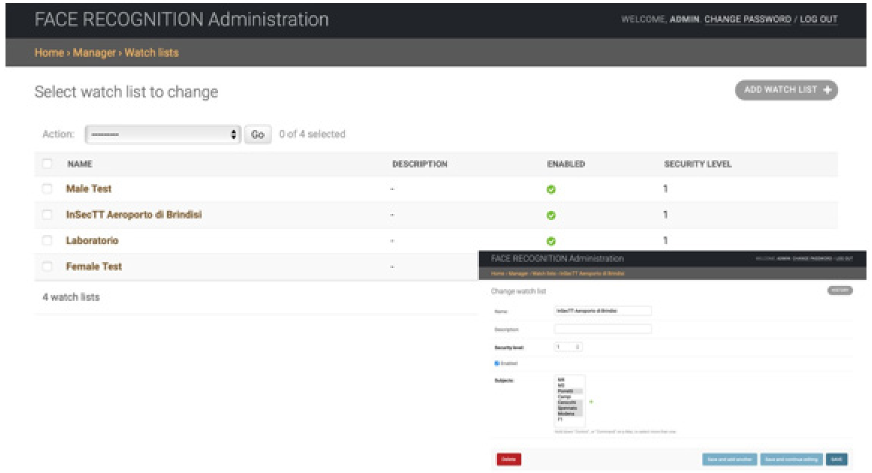

FACE RECOGNITION Administration
Select camera to change
FACE RECOGNITION Administration
Site administration
Recent actions

Figure 78: Face re-identification admin homepage plus some possible settings including watch lists



FACE RECOGNITION Administration

WELCOME, ADMIN. CHANGE PASSWORD / LOG OUT

Home › Manager › Watch lists

Select watch list to change

ADD WATCH LIST +

Action: --------- Go 0 of 4 selected

	NAME	DESCRIPTION	ENABLED	SECURITY LEVEL
□	Male Test	-	✓	1
□	InSecTT Aeroporto di Brindisi	-	✓	1
□	Laboratorio	-	✓	1
□	Female Test	-		

4 watch lists

FACE RECOGNITION Administration

Change watch list

Name: InSecTT Aeroporto di Brindisi

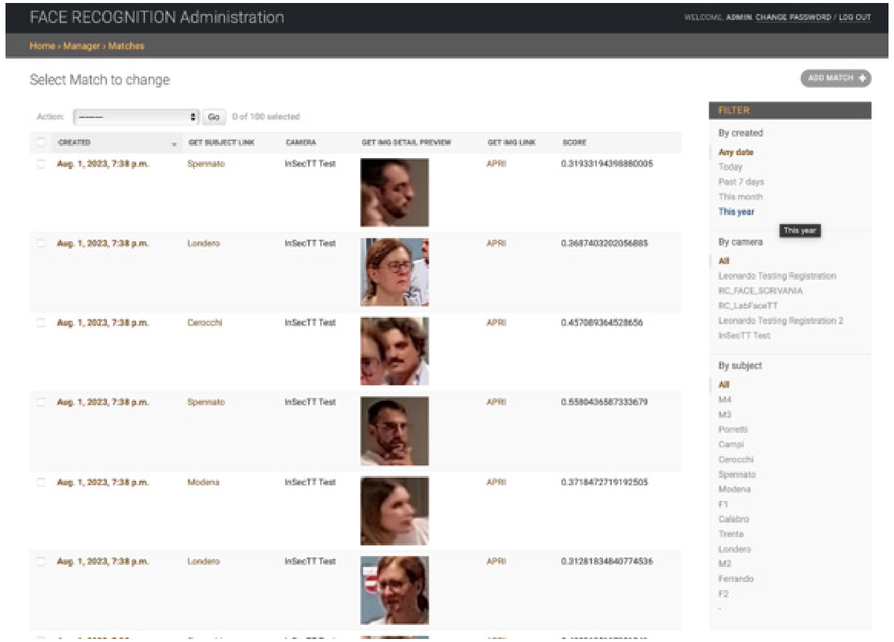
Description:

Security level: 1

☑ Enabled

Subjects:

Figure 79: Face re-identification watch list creation



FACE RECOGNITION Administration

WELCOME, ADMIN. CHANGE PASSWORD / LOG OUT

Home › Manager › Matches

Select Match to change

ADD MATCH +

Action: -------- Go 0 of 100 selected

	CREATED	GET SUBJECT LINK	CAMERA	GET IMG DETAIL PREVIEW	GET IMG LINK	SCORE
□	Aug. 1, 2023, 7:38 p.m.	Spennato	InSecTT Test		APRI	0.31933194398880005
□	Aug. 1, 2023, 7:38 p.m.	Londero	InSecTT Test		APRI	0.3687403202056885
□	Aug. 1, 2023, 7:38 p.m.	Cerocchi	InSecTT Test		APRI	0.457089364528656
□	Aug. 1, 2023, 7:38 p.m.	Spennato	InSecTT Test		APRI	0.5580436587333679
□	Aug. 1, 2023, 7:38 p.m.	Modena	InSecTT Test		APRI	0.3718472719192505
□	Aug. 1, 2023, 7:38 p.m.	Londero	InSecTT Test		APRI	0.31281834840774536

FILTER

By created

- Any date
- Today
- Past 7 days
- This month
- This year

This year

By camera

- All
- Leonardo Testing Registration
- RC_FACE_SCRIVANIA
- RC_LabFaceTT
- Leonardo Testing Registration 2
- InSecTT Test

By subject

- All
- M4
- M3
- Porretti
- Campi
- Cerocchi
- Spennato
- Modena
- F1
- Calabro
- Trenta
- Londero
- M2
- Ferrando
- F2
- -

Figure 80: Face re-identification matches from Brindisi test

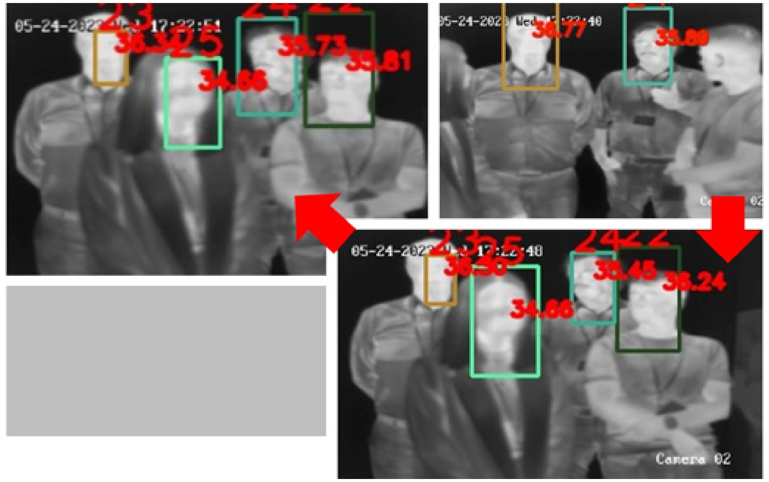


Figure 81: Thermal screening through eye inner canthus location: laboratory test with multiple subjects

Exploitation plans

Both the crowd-management system and the face re-identification module represent features which have been integrated in LDO's offer regarding control rooms. The enhancement of monitoring ability via artificial intelligence applications is of capital importance for LDO's Cyber and Security Solutions reference market, which is mainly constituted by blue lights, first responders and critical infrastructures. The InSecTT project and UC5.16 has contributed to accelerate the integration of the new services into our offer, and to test those solution in challenging environment such as ADP premises in Brindisi. Thermal screening has also achieved satisfactory development level, nevertheless the interest of the application has changed with the evolution of the pandemic. Anomaly tracking is an interesting topic which will be further explored internally; however new regulation by the EU (the AI act) poses concerns regarding the identification of business relevant scenarios.

The sensing solutions developed by ETH in the project and tested in the extra Schengen boarding area of Brindisi Airport will contribute to increase the product offer of environmental monitoring stations. Indeed, ETH has been able to provide evolved prototypes of environmental sensing stations which are smaller and less "intrusive" multi-sensor autonomous devices.

The research and development activities on the IoT integration platform allowed to improve the capabilities and the autonomy of current solutions, in regard to data collection, data processing, device fleet monitoring and management. The results of the project will influence the evolution of Eclipse Kura and Kapua, the open-source solutions developed and promoted by Eurotech and Red Hat for the IoT gateway management and system level integration. As consequence, we expect to see an influence also on the Eurotech Everywhere Software Framework (ESF) and on Eurotech Everywhere Cloud (EC), the commercial version of Eclipse Kura and Kapua respectively.

CINI-UNIROMA3 realized working prototype of the multibiometric recognition system, comprehensive of the kiosk for hand-vein pattern images collection, cameras, as well as the algorithms for feature extraction and data fusion. This led to several scientific papers which are public as well as number for demonstration during academic events. We mention that it is the intention of CINI-UNIPR (together with ADP) to release the dataset for air-quality gathered during data collection campaign of several months in Brindisi Airport terminal.

CONTACT INFORMATION

PROJECT COORDINATION

Michael Karner

email: michael.karner@v2c2.at

https://www.insectt.eu

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

InSecTT has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876038. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Finland, France, Italy, Ireland, Netherlands, Poland, Portugal, Slovenia, Spain, Sweden, Turkey.

The document reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains.