InSecTT:
Intelligent Secure Trustable Things

InSecTT Industrial Demonstrators Y2

Document Type	Deliverable
Document Number	D5.51
Primary Author(s)	Lukasz Szczygielski | GUT
Document Version / Status	1.0 | Final
Distribution Level	PU (public)

Project Acronym	InSecTT
Project Title	Intelligent Secure Trustable Things
Project Website	https://www.insectt.eu/
Project Coordinator	Michael Karner | VIF | michael.karner@v2c2.at
JU Grant Agreement Number	876038
Date of latest version of Annex I against which the assessment will be made	2021-06-25

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, Sweden, Spain, Italy, France, Portugal, Ireland, Finland, Slovenia, Poland, Netherlands, Turkey

CONTRIBUTORS

Name	Organization	Name	Organization
Lukasz Szczygielski	GUT	Magnus Isaksson	RTE
Peter Priller	AVL	Leander Hörmann	LCM
Frank van de Laar	PRE	Francesco Pacini	LDO
Paulo Duarte	Capgemini Engineering	Łukasz Goncerzewicz	VEMCO
Raja Ramachandran	PRE	Esa Piri	KAI
Efi Papatheocharous	RISE	Ralph Weissnegger	CISC
Björn Leander	ABB	Fabio Bruno	CINI-UNICAL
Carmen Perez	INDRA	Francisco Parrilla	INDRA
John Barry	LCC	Liam O'Toole	UCC
Sergio Jimenez	INDRA	Mateusz Rzymowski	GUT
Dogancan Koruyucu	PAVOTEK	Yavuz Selim Bostanci	MarUn

FORMAL REVIEWERS

Name	Organization	Date
Marcin Cylkowski	VEMCO	2022-05-30
Jakub Kownacki	ISS RFID	2022-05-30

DOCUMENT HISTORY

Revision	Date	Author / Organization	Description
0.1	2022-04-21	Lukasz Szczygielski / GUT	First version of the document
0.2	2022-05-09	P. Priller /AVL	Added T5.3 demonstrators
0.3	2022-05-13	Paulo Duarte / CAP	Added T5.1 demonstrators
0.4	2022-05-17	Efi Papatheocharous / RISE	Added T5.12 demonstrator
0.6	2022-05-27	Lukasz Szczygielski / GUT	Integrated contribution from UCs
1.0	2022-05-31	Lukasz Szczygielski / GUT	Version after internal review

TABLE OF CONTENTS

1 EXECUTIVE SUMMARY 9

2 OBJECTIVES 10

3 DESCRIPTION OF WORK 11

3.1 Use Case 5.1 - Wireless Platooning Communications 11

3.1.1 Planned demonstrators 11

3.2 Use Case 5.2 - AI-enriched Wireless Avionics Resource Management 14

3.2.1 Planned demonstrators 14

3.3 Use Case 5.3 - Wireless Security Testing Environment for smart IOT 23

3.3.1 Planned demonstrators 23

3.4 Use Case 5.4 - Intelligent wireless systems for smart port cross-domain applications 28

3.4.1 Planned demonstrators 28

3.5 Use Case 5.5 60

3.5.1 Planned demonstrators 60

3.6 Use Case 5.6 - Location awareness for improved outcomes and efficient care delivery in healthcare 66

3.6.1 Planned demonstrators 66

3.7 Use Case 5.7 - Intelligent Transportation for Smart Cities 72

3.7.1 Planned demonstrators 72

3.8 Use Case 5.8 - Intelligent Automation Services for Smart Transportation 84

3.8.1 Planned demonstrators 84

3.9 Use Case 5.9 - Cybersecurity in Manufacturing 86

3.9.1 Planned demonstrators 86

3.10 Use Case 5.10 - Robust resources management for construction large infrastructure 89

3.10.1 Planned demonstrators 89

3.11 Use Case 5.11 - Smart Airport 94

3.11.1 Planned demonstrators 94

3.12 Use Case 5.12 - Driver Monitoring and Distraction Detection using AI 100

3.12.1 Planned demonstrators 100

3.13 Use Case 5.13 - Secure Industrial Communications System 103

3.13.1 Planned demonstrators 104

3.14 Use Case 5.14 – Secure and resilient Collaborative Manufacturing Environments 105

3.14.1 Planned demonstrators 105

3.15 Use Case 5.15 - Intelligent Safety and Security of Public Transport in urban environment 110

3.15.1 Planned demonstrators 110

3.16 Use Case 5.16 - Airport Security–Structured and Unstructured Flow of people in airports 112

3.16.1 Planned demonstrators 112

4 DISSEMINATION, EXPLOITATION AND STANDARDISATION 116

5 CONCLUSIONS 117

6 REFERENCES 118

A. ABBREVIATIONS AND DEFINITIONS 119

LIST OF FIGURES

Figure 1 Autonomous cars fabricated as part of the robotic testbed 11

Figure 2 V2V platoon MIMO model inside a semi-circular tunnel (lateral view) 13

Figure 3 Real life situation in the WAIC system. Transmitting device (Tx) mounted in the back of the airplane may encounter problems while communicating with receiver (Rx) because of intentional interference created by a jamming device (Jx) mounted outside of the outside of the airplane 15

Figure 4 WAICs 3D channel model (multi-ray and stochastic geometric) for avionics communications 15

Figure 5 Anechoic chamber testing 16

Figure 6 Node measurements topology 17

Figure 7 Simulator used by ISEP to use interference and channel measurements to evaluate the use of AI for interference detection and cancellation 18

Figure 8 Sensor wireless signal transmission experimental setup inside a Boeing 737 fuselage 18

Figure 9 Aircraft mechanical model for propagation analysis 19

Figure 10 Simulator used by ISEP to validate and verify wireless avionics intra-communications enhanced by artificial intelligence 20

Figure 11 Example of a passive switches application 21

Figure 12 Simulator used by ISEP to provide simulations of battery-less devices with energy harvesting capabilities in WAICs networks 22

Figure 13 Wireless and battery less avionics sensor, called Hermes that simultaneously enables piezoelectric energy harvesting as well as sensing 22

Figure 14 A network of 30 energy harvesting nodes and a gateway in a 4 m by 4 m area emulating multiple harvester events per second for showing TUD's MAC protocol 23

Figure 15 Experiment setup inside fuselage to test energy harvesting MAC protocol 23

Figure 16 Wireless embedded device testbed architecture based on ROS 25

Figure 17 Embedded host node (Raspberry PI) and connected device-under-test (nRF52840 development kit) 26

Figure 18 Current state of the OpenAPI of the wireless embedded device testbed 27

Figure 19 GUT Campus demo site 29

Figure 20 Screen shot of initial page of PSIM documentation 30

Figure 21 Part of RabbitMQ queues defined for integration between partner’s system and Vemco’s PSIM 31

Figure 22 Example measurement scenario 32

Figure 23 Mobile platform designed and developed by GUT 33

Figure 24 Identification device 33

Figure 25 App for configuration of identification device 34

Figure 26 Possible place for setting up a restricted zone at GUT campus 34

Figure 27 Demonstrating historical locations of tracked beacon in Vemco's PSIM platform – analysis of data integrated from GUT, after an alarm is raised (here a "Door breakage" example) 35
Figure 28 Simplified functional flow of data 36
Figure 29 Planned location of the demonstrator outdoors – restricted area highlighted in red 37
Figure 30 Example of alarm raised within Vemco's PSIM platform after unauthorized presence is detected by one of the systems 37
Figure 31 Kaitotek's measurement device equipped also with a results server 38
Figure 32 Heat map visualisation in the results server's web-portal 39
Figure 33 Simplified functional flow of data 39
Figure 34 Example of low QoS alarm raised within PSIM platform 40
Figure 35 Simplified functional flow of data 40
Figure 36 Example of abnormal network functioning detection alarm raised within PSIM platform 41
Figure 37 Simplified functional flow of data 41
Figure 38 Simplified functional flow of data 42
Figure 39 Demo site at Port of Gdansk 43
Figure 40 Block diagram of the system 44
Figure 41 Sensor data collection for m/v Tucana 46
Figure 42 High-level architecture for the complete predictive module 46
Figure 43 RTE specific software design (by M24) 47
Figure 44 RTE's prediction module event demonstrated as alarm in Vemco's PSIM 47
Figure 45 The Flexible payload on the test boat 48
Figure 46 Raw data visualization 48
Figure 47 Vessel tracking on Baltic Sea 50
Figure 48 Hardware set during tests 50
Figure 49 Test vessel 51
Figure 50 Vessel route monitoring 52
Figure 51 Concept of underwater barriers for perimeter monitoring 53
Figure 52 Underwater sensors and a multi-interface node used to monitor passages through harbour entrance channel 53
Figure 53 Architecture for the integration among underwater barriers (LDO), SDN-enabled wireless network (CINI-UNICAL) and VEMCO platform 54
Figure 54 Potential location outside the harbour to perform the tests 54
Figure 55 Magnetic sensor prototype (left) and control console (right) 55
Figure 56 Simplified functional flow of data 56
Figure 57 Demonstrator Integration Schema 57
Figure 58 Simplified functional flow of data 58
Figure 59 Example of abnormal network functioning detection alarm raised within PSIM platform 58

Figure 60 Software simulation of a container port 59
Figure 61 Software simulation (2) of a container port 59
Figure 62 Integrated Dashboard showcasing the integrated TBB: Length of Stay prediction 61
Figure 63 Use case Architecture aligned with InSecTT HLA 62
Figure 64 API based integration of 6 different scenarios 63
Figure 65 ECG synthesis and learning algorithm 63
Figure 66 Anomaly detection principle 63
Figure 67 AI based wireless access point control structure 64
Figure 68 Bed manager dashboard 65
Figure 69 Dashboard providing an overview for an MCI 66
Figure 70 QR master location tag and the extracted floorplan navigation data 67
Figure 71 Indoor localization app using multimodal deep learning 67
Figure 72 An example of explainable AI/ML is the classification of the most important Wi-Fi stations to determine on which floor a person (using his/her phone's sensors) is in a building 68
Figure 73 Dashboard for situational awareness 69
Figure 74 nRF board with Android triage App for MCI triage handling 69
Figure 75 Installed Gateways (yellow markers) in Copernicus Medical Facility, which detects medical equipment (red markers) 70
Figure 76 PIR/Thermopile localization module with case 71
Figure 77 Example of multiple devices accessing the same channel 72
Figure 78 Demonstrator A schema for UC5.7 74
Figure 79 ASFA Installation 75
Figure 80 Demo A cloud Dashboard during tests in September 2021 75
Figure 81 Demonstrator scenario in Loughborough (United Kingdom) 77
Figure 82 ACS integrated into INDRA's rack 78
Figure 83 APS box deployed at the end of the train 78
Figure 84 WSN deployed in the train 79
Figure 85 Dashboard showing INDRA's WSN GPS and accelerometer data reported during the tests 79
Figure 86 Part of the train composition, and one of the installed wireless sensor nodes 80
Figure 87 Installation of the Wireless Sensor Nodes in the rolling stock 81
Figure 88 Installation of the UWB solution for proximity detection 81
Figure 89 Installation of the GNSS equipment for enhanced reference positioning data 82
Figure 90 TRX R6 gateway computer with multiple modems 83
Figure 91 Graphical front end for connection management 84
Figure 92 Demo site - ACCIONA 90

Figure 93 Machinery tracking 91
Figure 94 UC5.10 demo data analysis 91
Figure 95 ACCIONA Demo A test site 92
Figure 96 Electric trains 93
Figure 97 Wireless hardware used for demo purposes 94
Figure 98 RFID Reader Prototype 94
Figure 99 RFID Reader incl. test antenna 95
Figure 100 RFID analytics dashboard 95
Figure 101 Mobile platform equipped with the sensor's payload 96
Figure 102 Lidar image obtained during inspection 96
Figure 103 GUT campus demo site 97
Figure 104 Layout for Marmara University Smart Intersection Testbed 98
Figure 105 Pavotek Edge Cluster Server 98
Figure 106 Vehicle CAPTAIN - Hardware with communication module carrier. Equipped with an ITSG5 module in the picture 99
Figure 107 Smart Intersection infrastructure and BBs mapping 99
Figure 108 Demo I High Level Architecture 101
Figure 109 Block diagram of the system 102
Figure 110 Demo High Level Architecture 103
Figure 111 Network topology update of demonstrator A 104
Figure 112 High-level architecture of the Use Case and connections with TBBs 105
Figure 113 Demonstrator A hardware 107
Figure 114 Decentralized network deployed for the Demonstrator B 108
Figure 115 Embedded attestations of neural network inferences 109
Figure 116 The MASA Dynamic Model Area 110
Figure 117 ETH's laboratory implementation of people counting sensor strips 111
Figure 118 Preliminary implementation of the board deployed for video-anomaly detection 112
Figure 119 The extra-Schengen area of Brindisi Airport Terminal 113
Figure 120 ETH's environmental station 114
Figure 121 Fosso Madonna drainage channel at one of its intersections with the airport perimeter 114
Figure 122 The design of the Magnetic sensor node 115
Figure 123 The present "portable" magnetic sensor prototype 115

1 EXECUTIVE SUMMARY

This document is a summary of InSecTT Demonstrators available after Y2 of the project. Each of the Use Cases described status of preparation of the demonstrators with detailed information about localization, presented scenarios as well as TBBs deployed.

It is worth to mention, that the consortium delivers the description of the demonstrators in each year of the project. The form of presentation of the information is different in each year – Year 1 deliverable was prepared as a brochure and this form is also to be used in Y3. This document that includes summary of demonstrators in Y2 is presented as a typical deliverable that follows official structure of such a document.

Keywords: demonstrators, InSecTT demonstrators, industrial demonstrators

2 OBJECTIVES

The overall objectives of InSecTT (as defined in Description of Work [1] (DoW)) are to develop solutions for (1) Intelligent, (2) Secure, (3) Trustable (4) Things applied in (5) industrial solutions for European industry throughout the whole Supply Chain (6). More precisely:

(1) Providing intelligent processing of data applications and communication characteristics locally at the edge to enable real-time and safety-critical industrial applications

(2) Developing industrial-grade secure, safe and reliable solutions that can cope with cyberattacks and difficult network conditions

(3) Providing measures to increase trust for user acceptance, make AI/ML explainable and give the user control over AI functionality

(4) Developing solutions for Internet of Things, i.e., mostly wireless devices with energy- and processing-constraints, in heterogeneous and also hostile/harsh environments

(5) Providing re-usable solutions across industrial domains

(6) Methodological approach with the Integral Supply Chain, from academic, to system designers and integrators, to component providers, applications and services developers & providers and end users

WP5 ensures fulfilment of listed objectives through different activities which are described in detail in WP5 deliverables.

Objectives of this deliverable are defined as follows:

- Present current status of demonstrator preparation in Y2
- Deliver detailed description of demo test sites
- Describe the scope of demonstrators
- Present deployment of Technology Building Blocks in different Use Cases
- Present key achievements in Y2 in terms of demonstrator preparation

3 DESCRIPTION OF WORK

3.1 Use Case 5.1 - Wireless Platooning Communications

3.1.1 Planned demonstrators

For use case 5.1, three demonstrators are planned: Demonstrator A, for demonstrate how 5G can reduce the latency for communications in scenarios of emergency breaking, Demonstrator B, to test the reliability of communications inside a highly multipath scenario such as a tunnel and finally Demonstrator C, to evaluate platooning protocols, reduce latency and improve reliability in scenarios of dense traffic such as an urban scenario.

3.1.1.1 Demo A – Single platoon BS scenario

3.1.1.1.1 General information

This demonstrator comprises of a single platoon and one base station (BS) where each vehicle as well the BS are assumed to have multiple antenna transceiver. A BS is assumed to be used to either assist or even replace V2V links. Different layers are shown in this demo from the operator's support systems to the physical and channel layer. Different physical and medium access control layer assumptions are used to model both the channel and the MIMO tool. A Connected Cars Digital Twin will be used demonstrate the vehicle manoeuvres and V2X communication, where are generated the platoons and road-side units. The main idea is to show how 5G reduces the latency for platoon communications in scenarios of emergency breaking. This demo is to be demonstrated in a simulator as well as in a real setup either with robotic elements or real-life vehicles.

Figure 1 Autonomous cars fabricated as part of the robotic testbed

3.1.1.1.2 Scenarios demonstrated

Latency emergency breaking scenario is considered where platoon entities follow a set of protocols that allow the breaking signal to be transmitted with high priority towards all the elements of the formation.

A second scenario considers the implementation of designed protocols and platoon manoeuvres on a robotic physical testbed.

3.1.1.1.3 TBBs demonstrated

TBB 2.2 - AI algorithms for wireless resource and obstacle prediction / Telco OSS's and 5G RAN simulator

TBB 3.5 - System level evaluation/Large scale emulator with digital twin entities

TBB 2.1 - Hardware emulation

TBB 3.2 - MIMO and wireless MAC-PHY, SIC-NOMA Algorithms and 802.11p communication

3.1.1.1.4 Progress summary – Y2

Most important information regarding Y2 **demonstrator A** preparation were presented above, nevertheless it is important to highlight following milestones that have been achieved:

- OSS framework allowing the orchestration and management of network elements.
- RAN simulator implementing the NR and LTE stack.
- Semi-blind signal processing algorithms for conflict resolutions and MIMO decoding.
- Channel estimation and prediction using AI.
- Integration of 802.11p technology into the cars for V2V communication.
- Physical testbed using robotic autonomous vehicles to collect network statistics about platooning protocols.
- Platoon simulation/validation framework study to verify platooning manoeuvres.

In Y3, is expected to improve the algorithms, implement the platoon coordination system and perform network slicing to prioritize the traffic network. Also is expected to make available a release of the developed platform for research activities.

3.1.1.2 Demo B – In tunnel propagation and testing

3.1.1.2.1 General information

This demonstrator is derived from Demo A. The objective is to test the reliability of communications inside a highly multipath reflective scenario under different situations. The tests will be conducted in a simulator with realistic propagation channels. This scenario will take advantage of the blocks build in the Demo A such as the OSS and RAN, the Connected Cars Digital Twin. A propagation electromagnetic model is to be used inside the tunnel for platoon communications. The main idea is to detect the transition from Manhattan line of sight to non-line of sight to prepare the network, sending commands to the platoon in order to be aware of this transition.

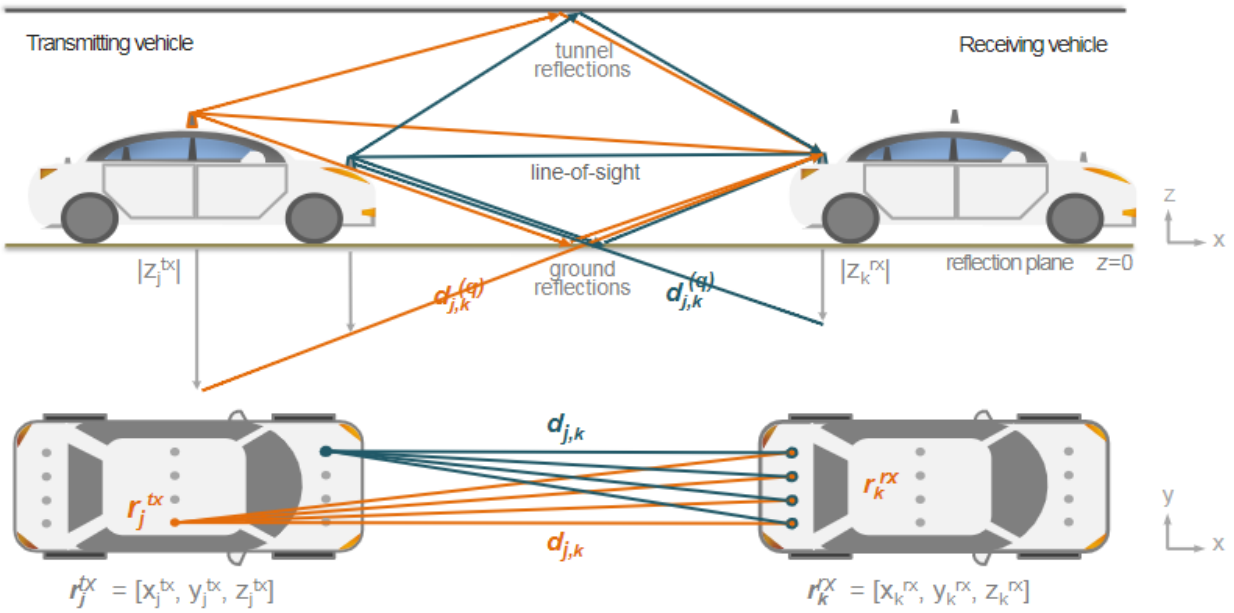


Figure 2 V2V platoon MIMO model inside a semi-circular tunnel (lateral view)

3.1.1.2.2 Scenarios demonstrated

Platoon coordination and wireless resource management in tunnels: this scenario considers the platoon management and coordination controls and communications when travelling inside a tunnel.

3.1.1.2.3 TBBs demonstrated

TBB 2.2 - AI Algorithms for wireless resources and obstacle prediction and telco OSS and 5G RAN.

T3.2: Wireless Resource Management and Spatial Authentication and interference reduction.

T3.5: Large Scale emulator with digital twin entities.

3.1.1.2.4 Progress summary – Y2

Most important information regarding Y2 demonstrator B preparation were presented above, nevertheless it is important to highlight following aspects:

- OSS and RAN sim will be derivate from Demo A.
- Extension of the Manhattan model, accounting for multiple order reflections experienced in environments such tunnels.
- For Y3, is expected the improvement of the algorithms and realize the integration the various components that compose the demonstrator.

3.1.1.3 Demo C – Platoon resource management system level

3.1.1.3.1 General information

This demonstration involves a system level simulation in a Manhattan grid network with hundreds of cars and/or platoons interacting with each other's. Realistic propagation models using BSs located at strategic positions will be used. Basic platoon operations with random vehicle arrival and platoon formation/destination processes. The objective is to evaluate platooning protocols, reduce latency

and improve reliability using different technics to optimize the network and the platoon management in dense traffic conditions.

3.1.1.3.2 Scenarios demonstrated

V2X Communications interference in a traffic congestion: this scenario considers a multiple cell site and multiple platoon network in urban or dense urban environments. The objective is to evaluate the performance of the V2V and V2X infrastructure in presence of interference of inter platoon and inter cell interference.

3.1.1.3.3 TBBs demonstrated

TBB 2.2 - AI algorithms for wireless resource and interference detection / Telco OSS's and 5G RAN simulator

TBB 2.4/2.5- Trustworthiness SLS

TBB 3.5 - Validation Framework for platoon behaviour and Large Sale emulator with digital twin entities

3.1.1.3.4 Progress summary – Y2

Most important information regarding Y2 **demonstrator A** preparation were presented above, nevertheless it is important to highlight following milestones that have been achieved:

- Channel Model and physical layer abstraction for MIMO operation is being developed.
- Manhattan simulator being developed with ability to coordinate multiple platoon environment.

In Y3, is planned to build the platoon control and operation system, integrate the different components such as Digital Twin with Manhattan Simulator, and validate the E2E demonstrator.

3.2 Use Case 5.2 - AI-enriched Wireless Avionics Resource Management

3.2.1 Planned demonstrators

3.2.1.1 Demo A

3.2.1.1.1 General information

This demonstrator consists of a set of measurement nodes located across different positions inside and outside a commercial aircraft. These nodes measure their interference fingerprints as well as channel variations according to different spatial positions. The objective is to create new data sets to be used in future WAIC systems to efficiently detect and minimize sources of interference using multiple antennas or other interference rejection AI (artificial intelligence) algorithms. Channel modelling will be also included to match the results of measurements (Figure 4).

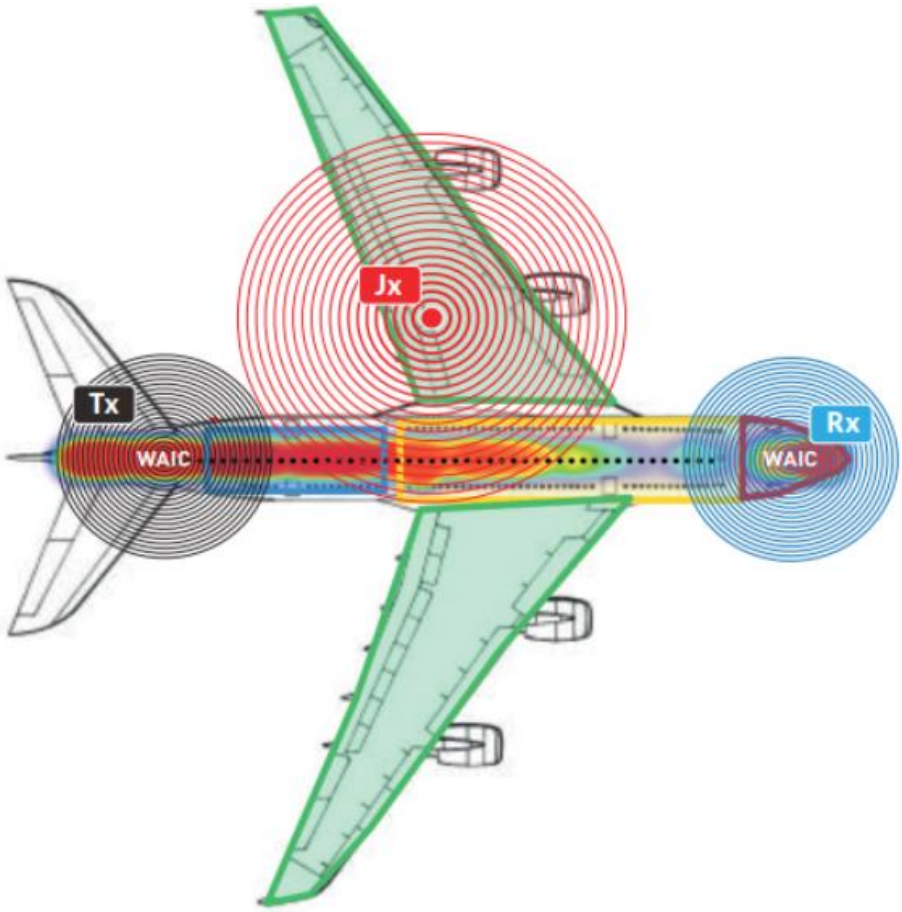


Figure 3 Real life situation in the WAIC system. Transmitting device (Tx) mounted in the back of the airplane may encounter problems while communicating with receiver (Rx) because of intentional interference created by a jamming device (Jx) mounted outside of the outside of the airplane

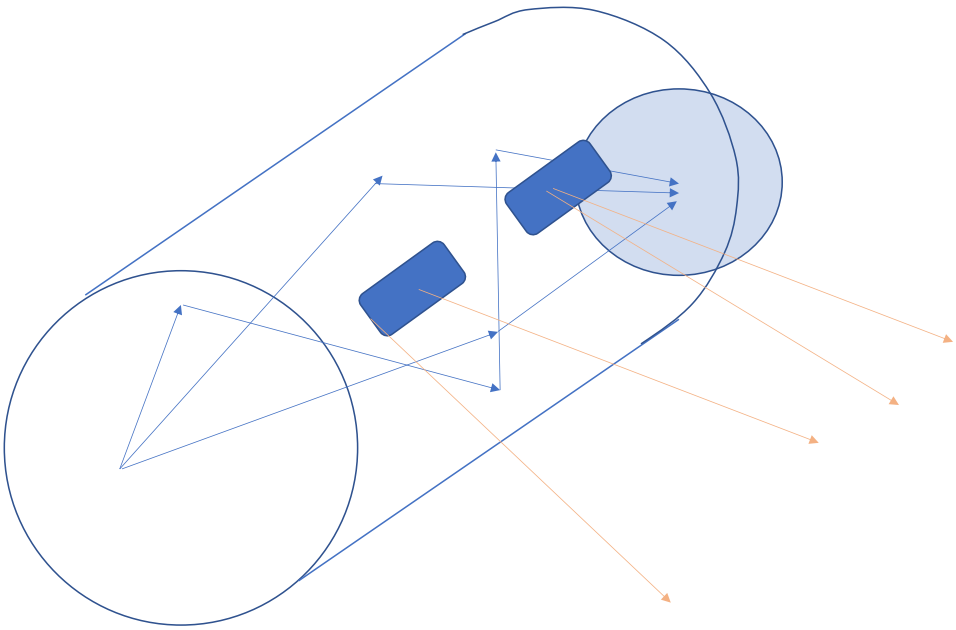


Figure 4 WAICs 3D channel model (multi-ray and stochastic geometric) for avionics communications

3.2.1.1.2 Scenarios demonstrated

GUT will perform measurements of interference on board commercial aircraft and interference detection/characterization algorithms.

ISEP demonstrates scenario 1 for interference characterisation and a set of AI tools for detecting and counteracting such interference. We also include the channel model for aircraft in different situations and the fitting with channel measurements. The idea of these measurements is also to feed the digital demonstrator of scenario 2.

TUD will provide support to the other partners for demonstrating scenario 1 and 2 by providing measurement data for making channel models. The nodes for the measurement are ready with TUD and the experiments will be conducted as part of Y3.

Scenario 1 is interference detection and cancellation. The scenario intense to generate new data sets to locate properly sources of interference across different locations of an aircraft and train models that can be used on board aircraft to supress jamming attacks.

Scenario 2 is verification and validation of WAICs using a digital demonstrator or other tools that will be used to simulate and emulate different layers of the protocol stack of WAICs

Scenario 3 is battery-less devices design, testing, implementation and verification and validation using a digital simulator.

3.2.1.1.3 TBBs demonstrated

TBB3.2 Channel modelling and measurements

TBB2.2 AI for wireless communications

3.2.1.1.4 Progress summary – Y2

GUT has performed measurements of interference on board commercial aircraft and interference detection/characterization algorithms in different settings (see Figure 5 and Figure 6).

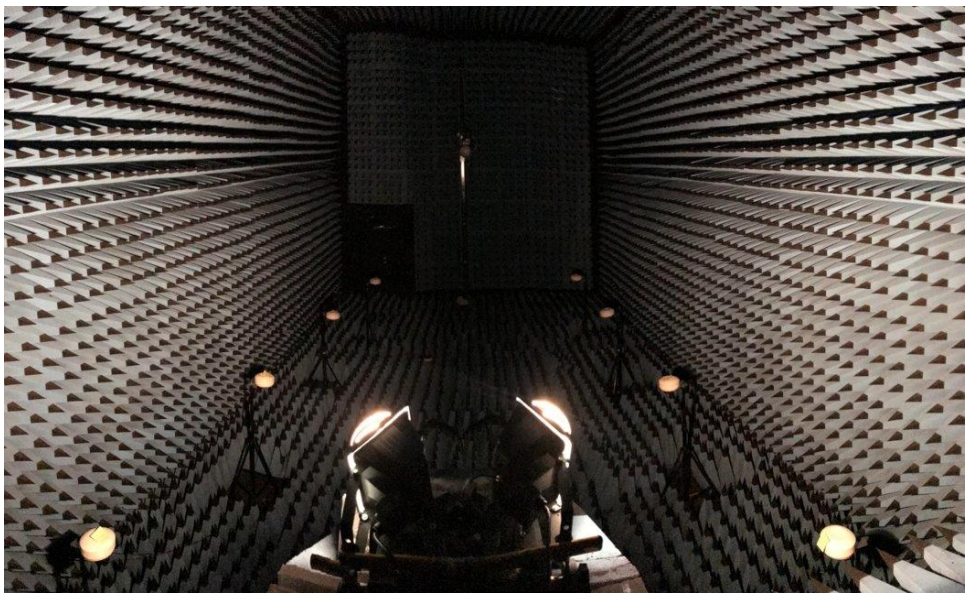


Figure 5 Anechoic chamber testing

Figure 6 Node measurements topology

ISEP has developed an aeronautical multi-ray and stochastic geometric channel model for any type of aircraft, considering propagation both inside the aircraft and the interactions with external nodes to the fuselage. We have improved the channel model to consider seats inside the aircraft and some human passengers introducing absorption models in the literature. In addition, we have improved the window aperture antenna model to calculate more accurately channel and interference models between external and internal nodes. The channel model considers reflections of multiple orders, which makes it an accurate electromagnetic model for multipath propagation. In addition, the channel model contains both deterministic and stochastic components that could be fitted with measurements. Therefore, we aim to refine the model based on realistic measurements in different types of aircraft and with different types of obstacles or in different scenarios. The simulator architecture used by ISEP to test interference detection and cancellation algorithms based on the models and measurements of this demonstrator is shown in Figure 7.

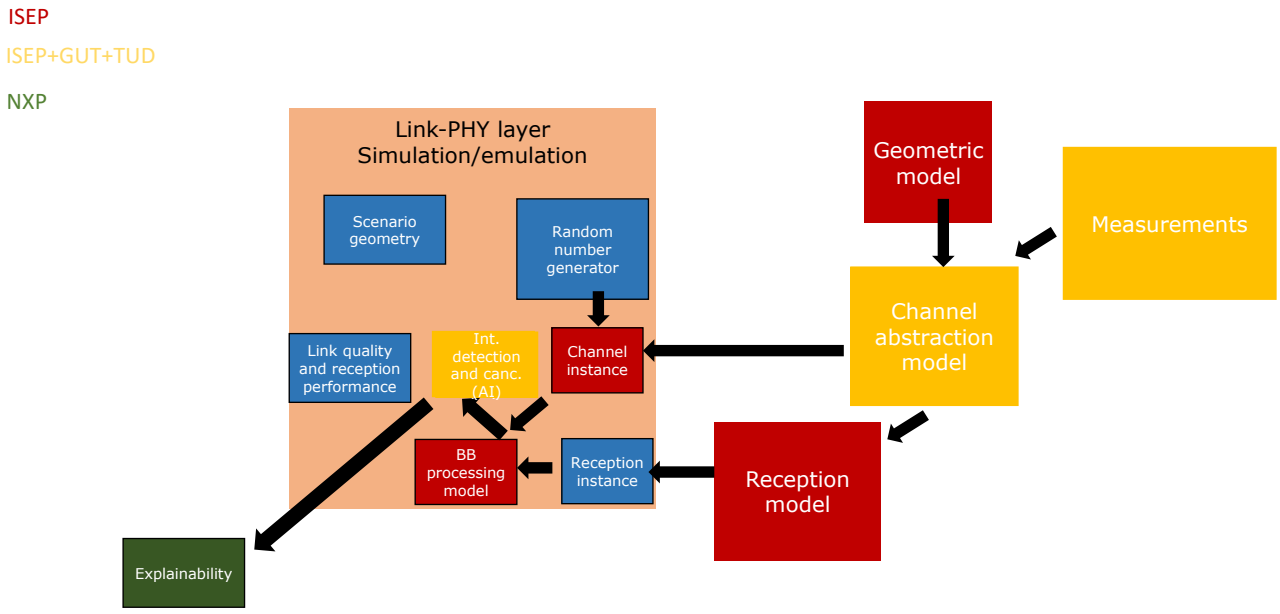


Figure 7 Simulator used by ISEP to use interference and channel measurements to evaluate the use of AI for interference detection and cancellation

For this demonstration, TUD is working in collaboration with ISEP to provide measurements for channel characterization. The wireless nodes will be placed inside a commercial 737 fuselage and measurements will be collected for varying transmission parameters both inside and outside the fuselage (see Figure 9). The aim of this data is to build channel abstraction models to be used for the simulator being developed as part of this demonstration.

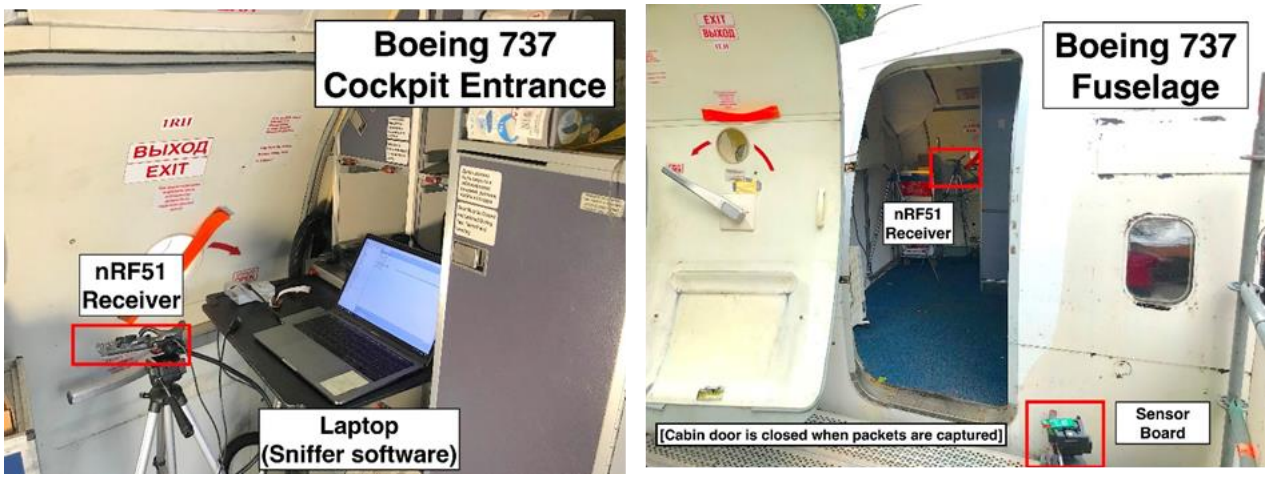


Figure 8 Sensor wireless signal transmission experimental setup inside a Boeing 737 fuselage

3.2.1.2 Demo B

3.2.1.2.1 General information

This demonstrator consists of replicating and emulating all the different physical processes involved in the design and management of a wireless avionics network onto a digital platform. This includes the use of a channel model fitted or completely replaced by measurement data, the interactions between the nodes, and the use of different signal processing algorithms to improve the operation of this type of network. The simulated environment is called system-level, because it aims to provide

a system wide overview of the scenario under test including the internal aeronautical network model, sensor and actuator models, channel propagation and mission scenarios in case of turbulence simulation. A model of the aircraft for simulation and emulation has also been developed as shown in Figure 9

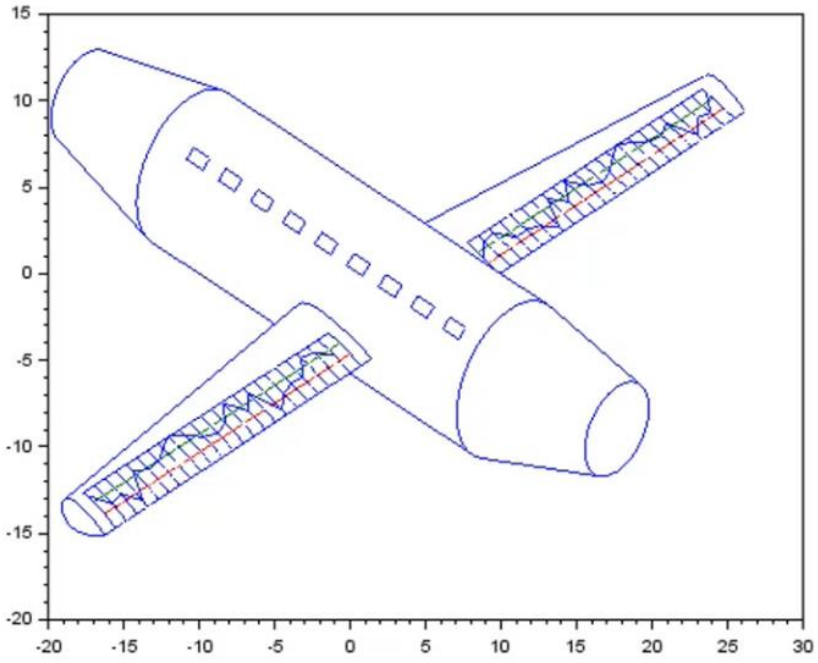


Figure 9 Aircraft mechanical model for propagation analysis

3.2.1.2.2 Scenarios demonstrated

The digital demonstrator will be used to address aspects of the three scenarios. In the first scenario, we will use it to test AI algorithms for interference detection and cancellation. In the second scenario, ISEP simulator is actually the core of all work to be demonstrated, but not only at the interference level, it also includes aspects of MAC (medium access control) and radio resource allocation level. In the case of the third scenario, we will use it also for including battery-less devices operational curves, showing performance in a realistic emulated environment.

The digital demonstrator will be used for the third scenario mainly for showcasing the integration of battery less devices into WAICs. The battery less wind speed and angle of attack sensor that is being created by TUD can be incorporated using the developed sensor model into the digital demonstrator. The sensor model is already developed as part of Y2 and the integration is planned for Y3.

3.2.1.2.3 TBBs demonstrated

TBB3.2 Channel modelling, TB2.2 AI for wireless, TB3.4 Real time wireless, TB3.5 Security testing, TB2.4 AI V&V

3.2.1.2.4 Progress summary – Y2

ISEP contribution

ISEP has built the main WAICs simulator with all the necessary pieces to emulate the different physical processes that are involved in the management and optimization of this type of networks. The simulator takes input from channel and interference modelling achieved in the demonstrator 1 to generate a virtualized space where more options can be studied and simulated. The simulator

architecture used by ISEP to perform the digital simulated demonstration of wireless avionics networks improved by AI is shown in Figure 10.

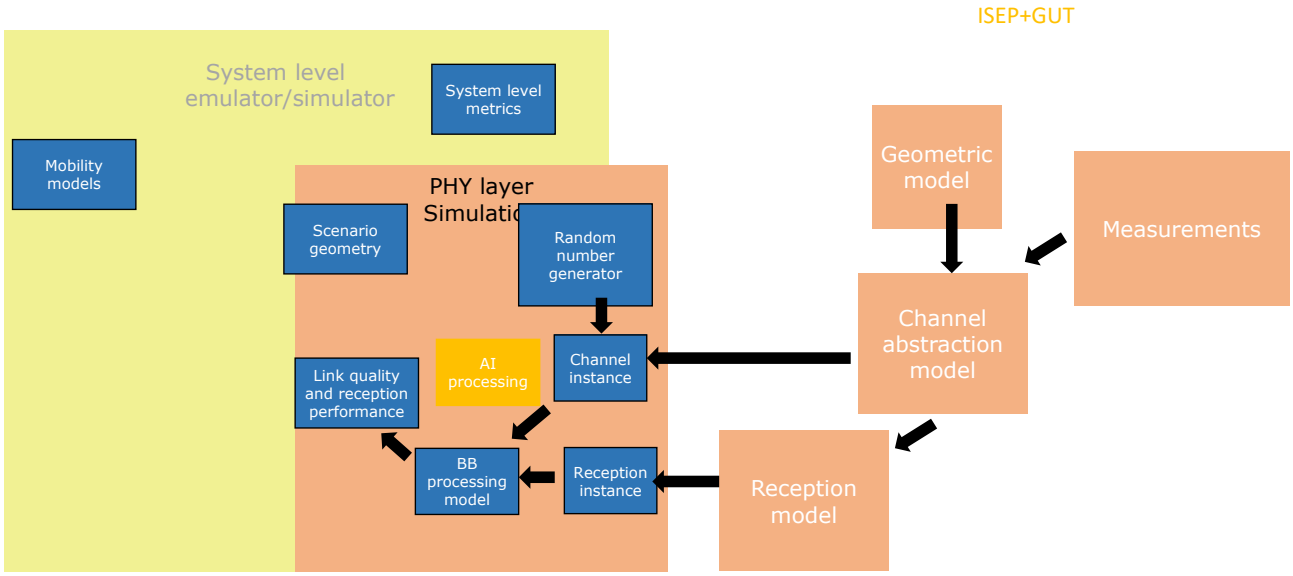


Figure 10 Simulator used by ISEP to validate and verify wireless avionics intra-communications enhanced by artificial intelligence

TUD contribution

For this demonstration, TUD in collaboration with ISEP will provide wireless channel measurements. Similar to demonstration 1, the wireless nodes will be placed inside a commercial 737 fuselage and measurements will be collected for varying transmission parameters both inside and outside the fuselage. Further TUD can provide sensor models based on the battery less wireless avionics sensor developed for measuring wind speed and angle of attack. The sensor data can be incorporated into the digital demonstrator to showcase working of the WAIC.

3.2.1.3 Demo C

3.2.1.3.1 General information

This demonstrator aims to show the benefits of energy harvesting technology to power battery-less devices on board an aircraft. The demonstrator will show how the performance can be optimized for this type of devices which promise to reduce energy consumption for wireless avionics intercommunications. An example of application is shown in Figure 11.

Figure 11 Example of a passive switches application

3.2.1.3.2 Scenarios demonstrated

ISEP contribution

ISEP will demonstrate all the scenarios with the system level simulator.

TUD contribution

This demonstrator will showcase scenario 3. The battery less wind speed and angle of attack sensor that has been created by TUD will be integrated into a WAIC using a gateway as part of Y3. The MAC protocol is being refined and experiments are being conducted to improve the performance and design of the network. As part of Y3, the gateway equipped with the MAC protocol will be integrated into the wider WAIC network.

3.2.1.3.3 TBBs demonstrated

TBB 3.5 Security testing, TB3.4 Real time wireless

3.2.1.3.4 Progress summary – Y2

ISEP contribution

The contribution of ISEP to this scenario is the realistic abstraction modelling of the battery-less devices to be included in detail in the simulator described in previous demonstrators. The idea is to perform a realistic system-level evaluation including realistic energy harvesting processes as well as Markov chains to show dependency on the current energy state of each node. The simulator architecture used by ISEP to test interference detection and cancellation algorithms based on the models and measurements of this demonstrator is shown in Figure 12.

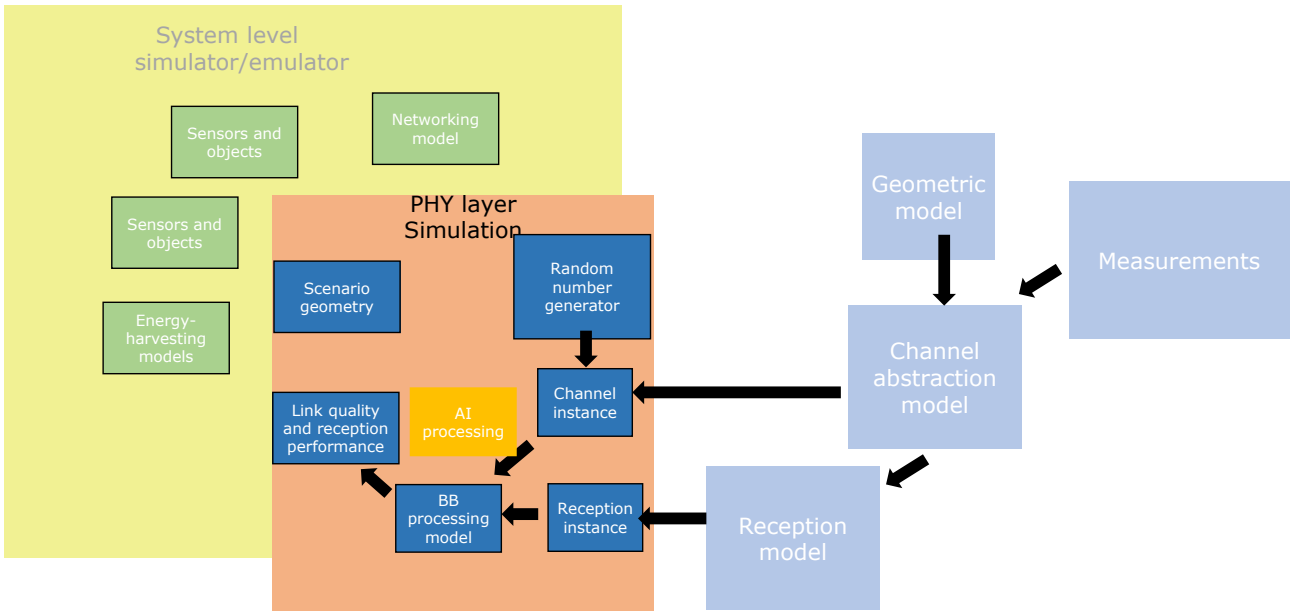


Figure 12 Simulator used by ISEP to provide simulations of battery-less devices with energy harvesting capabilities in WAICs networks

TUD contribution

For this demonstration, TUD will showcase the working of their wireless battery less wind speed and angle of attack sensor developed for avionics applications. The sensor readings are to be communicated wirelessly to a one hop gateway. This gateway will be integrated into the WAIC network. The sensors are shown in Figure 13.

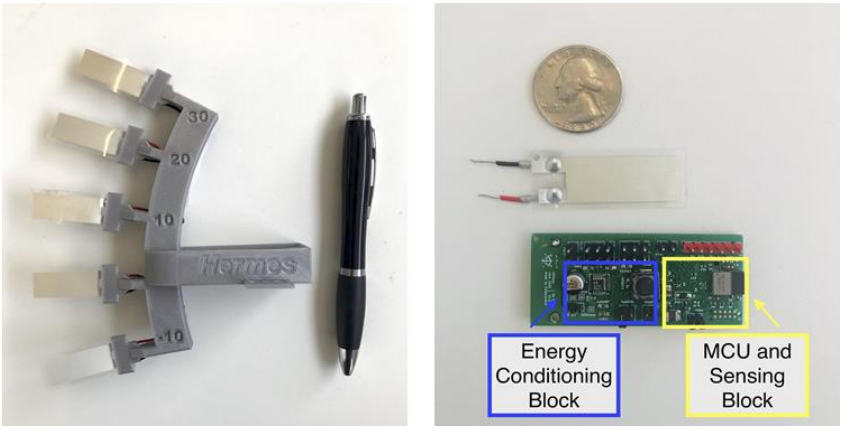


Figure 13 Wireless and battery less avionics sensor, called Hermes that simultaneously enables piezoelectric energy harvesting as well as sensing

Furthermore, TUD has developed a MAC protocol for such energy harvesting sensors and devices and a communication paradigm to demonstrate the working of such devices in a scaled-up setting (see Figure 13). This radiofrequency (RF) information harvesting based, channel sensing technique takes advantage of the energy in the wireless medium to detect channel activity at essentially no energy cost. This is being developed for event-driven energy harvesting wireless sensing applications like smart cabins, where wireless sensing is expected not only to contribute to better flying experiences but also to help airliners reduce costs. Our ultra-low-power MAC protocol, Radio

Frequency-Distance Packet Queuing (RF-DiPaQ) is being developed to this end. The MAC protocol will be showcased using Energy harvesting battery powered nodes to visualize the working of the protocol in a network of 30 nodes.

Figure 14 A network of 30 energy harvesting nodes and a gateway in a 4 m by 4 m area emulating multiple harvester events per second for showing TUD's MAC protocol

An example of the testing inside a real aircraft cabin is shown in Figure 15

Figure 15 Experiment setup inside fuselage to test energy harvesting MAC protocol

3.3 Use Case 5.3 - Wireless Security Testing Environment for smart IOT

3.3.1 Planned demonstrators

3.3.1.1 Demo A: Security Testing of Vehicle Access System

3.3.1.1.1 General information

Vehicle access systems are used to authenticate users, open doors and activate a vehicle. Security is critical as previous systems based on RFID or low-frequency communication have been hacked by intruders in the past.

This demonstrator consists of an Automata Learning (AL) setup that derives a behavioural model of the system under test (SUT), which is a novel vehicle access system based on Near-field

Communications (NFC). The learning algorithm, embedded in the test orchestration system, derives a model of the SUT that is used for security analysis and input for a model-guided fuzz tester that generates security tests for the SUT.

3.3.1.1.2 Scenarios demonstrated

Scenario 4: Testing a multi-radio vehicle access system

3.3.1.1.3 TBBs demonstrated

- BB2.4 (AI V&V): Integrate AI tools into the existing security testing core framework
- BB3.5 (Verification, validation, accountability): Test orchestration platform
- BB3.5 (Verification, validation, accountability): Track active Bluetooth Low Energy (BLE) connections

3.3.1.1.4 Progress summary – Y2

The learning setup has been established, and will be demonstrated at the Y2 Review. It will consist of the demo board (the system-under-test) and a learning setup, consisting of the learning software running on a laptop and a suitable NFC hardware (e.g. Proxmark3) that can be used to freely issue NFC commands guided by the learner. The outcome will be an abstract behavioral model of the system.

3.3.1.2 Demo B: Security Testing of V2x-based Truck Plattoning

3.3.1.2.1 General information

Demo B will show security testing of radio-guided truck platoons based on the Ensemble protocol.

For this, a a Platooning Simulation System will act as system under test (SUT) for the Automotive Security Testing Demonstrator.

The Platooning Simulation System consists of wireless communication subsystems combined with simulation nodes. The wireless communication subsystems are based on IEEE802.11p/ETSI ITS-G5, running an implementation of the secure platooning protocol, defined by the EU multi-brand truck platooning protocol Ensemble. The simulation nodes simulate parts of the behaviour of the trucks and the platoon.

The demonstrator shows a security test consisting of forged adversarial messages that forces the platoon disband and/or issues faulty commands to non-leading platoon members.

3.3.1.2.2 Scenarios demonstrated

Scenario 2: Testing V2X ITS-G5 interface and functionality

3.3.1.2.3 TBBs demonstrated

- BB3.2 (Dependable (reliable, robust, secure) wireless communication): Stacks and Verification environment
- BB3.5 (Verification, validation, accountability): Test orchestration platform
- BB3.5 (Verification, validation, accountability): Physical layer verification and validation framework
- BB3.5 (Verification, validation, accountability): Connected Cars Service Platform & Connected Cars Digital Twin

3.3.1.2.4 Progress summary – Y2

An initial version of this setup has been shown at the Y1 review. Since then, the security testing platform is being extended to inject attacks into an established platoon. This will be demonstrated by running the attack sequence on the adapted and integrated AVL attack platform.

3.3.1.3 Demo C: Wireless sensor network (WSN) test bed

3.3.1.3.1 General information

This test bed allows automated testing of typical WSN nodes (e.g. based on Bluetooth (BT) / Bluetooth low-energy (BLE) radios). An overview of the testbed architecture is shown in Figure 16. The wireless sensor nodes which will be tested are highlighted in dark blue.

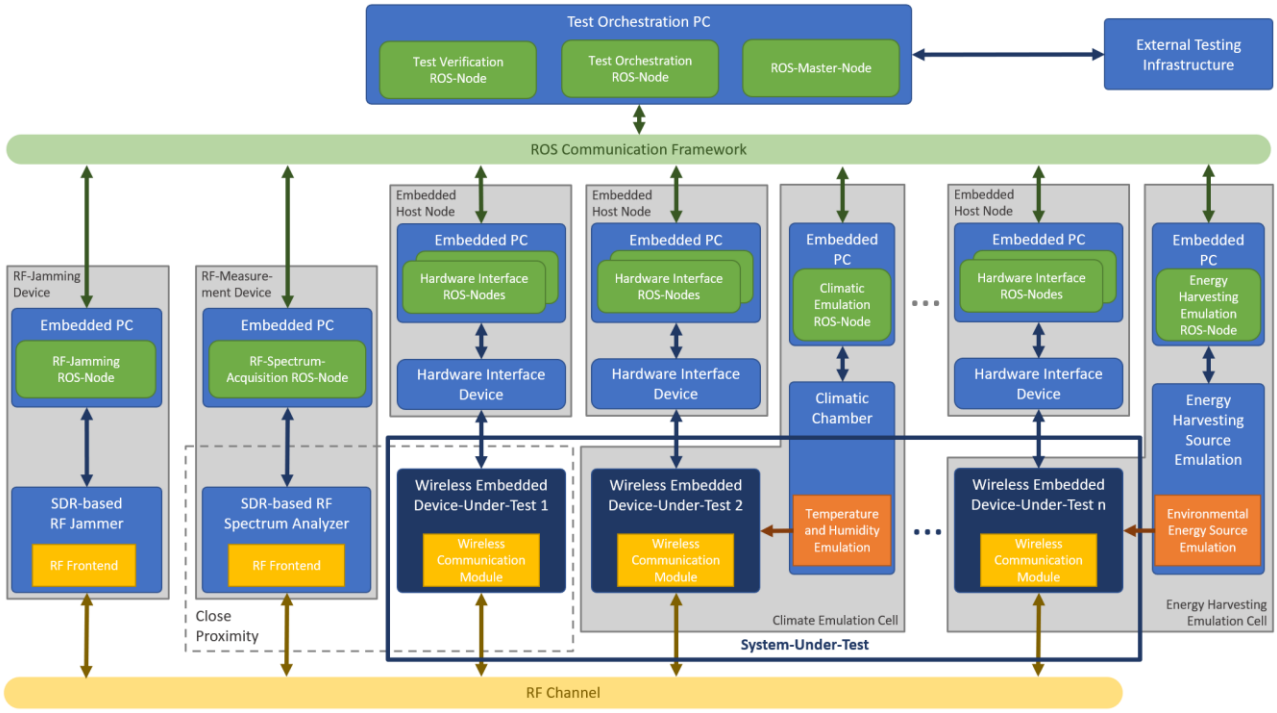


Figure 16 Wireless embedded device testbed architecture based on ROS

The wireless embedded device testbed consists of the test orchestration PC (Raspberry PI) including the ROS master node and an OpenAPI implementation to access and control the testbed. Besides the test orchestration PC, the current installation at LCM's laboratory consists of three embedded host nodes (Raspberry PIs) connecting one WNP (wireless sensor network base station) and two wireless sensor nodes. The three connected devices represents the system-under-test. One embedded host node and a connected device-under-test (nRF52840 development kit) is shown in Figure 17.

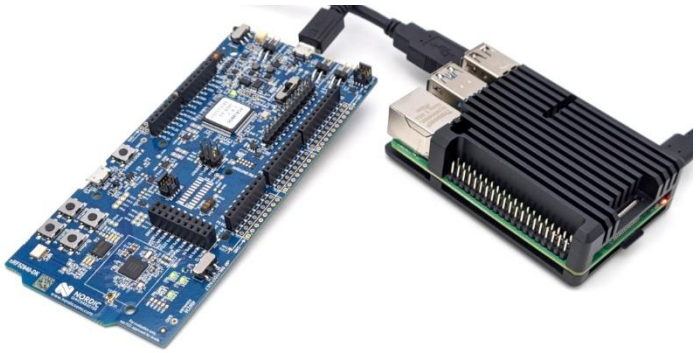


Figure 17 Embedded host node (Raspberry PI) and connected device-under-test (nRF52840 development kit)

The API is based on an OpenAPI specification and accessible for humans and machines. The current state of the testbed API is shown in Figure 18.

Figure 18 Current state of the OpenAPI of the wireless embedded device testbed

3.3.1.3.2 Scenarios demonstrated

Scenario 1: Testing BT/BLE wireless interface of a head unit

3.3.1.3.3 TBBs demonstrated

- BB2.2 (AI on communication level): Energy effi. comm. anomaly detection (req. 310)
- BB2.3 (AI on computational level): Device anomaly detection (req. 311)
- BB3.2 (Dependable (reliable, robust, secure) wireless communication): Secure communication / lifetime security concept (req. 312)

- BB3.2 (Dependable (reliable, robust, secure) wireless communication): Interference and jamming test (req. 435/313)
- BB3.5 (Verification, validation, & accountability): Automated wireless testbed (req. 316)
- BB3.2 (Dependable (reliable, robust, secure) wireless communication): Test Oracle
- BB3.3 (Real-time monitoring and response): Interference Detection / Wireless interference verification (req. 314)
- BB3.4 (RT critical communication): Routing algorithm

3.3.1.3.4 Progress summary – Y2

An initial version of the WSN TB has been shown at the Y1 review. Since then, it was extended by a communication architecture based on the Robot Operating System (ROS). ROS acts as a middleware to connect each device of the testbed and distributes the messages between the communication participants. This modular approach allows to add and combine different components for additional skills, like jamming, to be shown at the Y2 review. A special focus of the Y2 demonstrate will be on the interface of the testbed: first to test different devices under test (UWB wireless sensor nodes from JKU), second to integrate a jamming device (provided by GUT), third to integrate interference measurement nodes (from SAL) and to provide the possibility to control the testbed externally (test orchestration from AVL).

3.4 Use Case 5.4 - Intelligent wireless systems for smart port cross-domain applications

3.4.1 Planned demonstrators

3.4.1.1 Demo – GUT Campus

3.4.1.1.1 General information

All demonstrator scenarios will take place at GUT Campus – outdoor or indoor. The main area of testing is a parking lot with internal crossroads. The figure below shows a target area of measurement.

Figure 19 GUT Campus demo site

GUT has already prepared an infrastructure by mounting communication gateways on the roof of the building. The gateways connect to the system of data acquisition and visualization.

Gateways can communicate via various communication protocols, such as Bluetooth Low Energy, Wi-Fi, V2X, LORA, and LTE. A variety of wireless communication can be helpful for all partners to integrate their systems. The connectivity aims to monitor vehicles' movement and signal quality within the testing area, but possibilities are unlimited and depend on specific requirements.

According to many integrations with Vemco’s Physical Security Information Management platform – documentation was prepared to simplify and clarify integration with each possible partner.

Integration documentation

Contents

- Integration documentation
- Configuring external system
- **Stage #1.** Supporting health monitoring integration stage.
- **Stage #2a.** Supporting events types integration stage.
- **Stage #2b.** Supporting elements types integration stage.
- **Stage #3.** Supporting elements based integration stage.
- **Stage #4.** Supporting events based integration stage.
- **FAQ**

In the following documentation we describe how to integrate external system with Vemco's PSIM (Physical Security Information Management) platform. In case of any questions feel free to email **lukasz.gonc@vemco.pl**.

> **Note**
>
> Some graphics used within this documentation are mockups yet - user interface and the API are still being developed. The view on how to integrate is actual.

Initial step towards integrating an external system with Vemco's PSIM platform requires creating an external system object within Vemco's platform (done by Vemco). When the integrated / external system object is created, you will receive authentication information (via email) for your integrated system only.

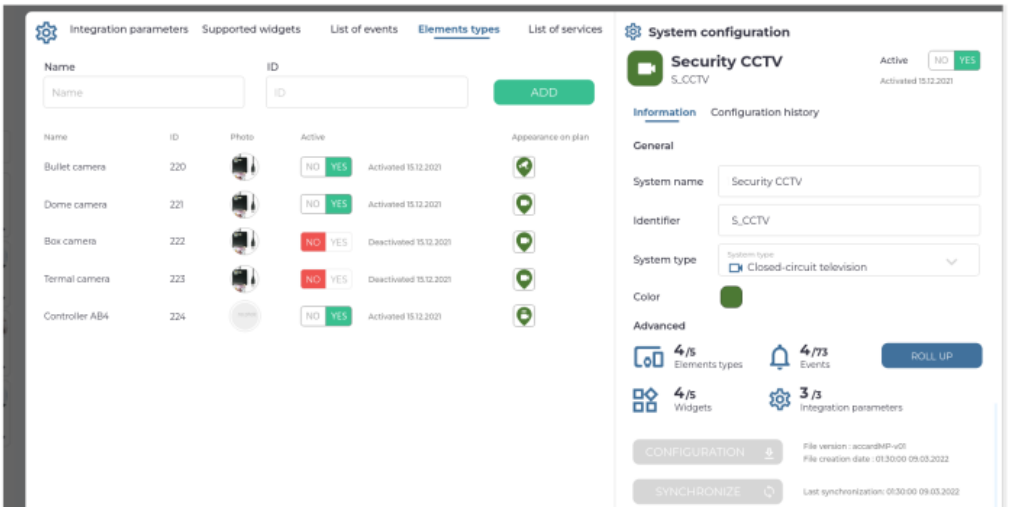
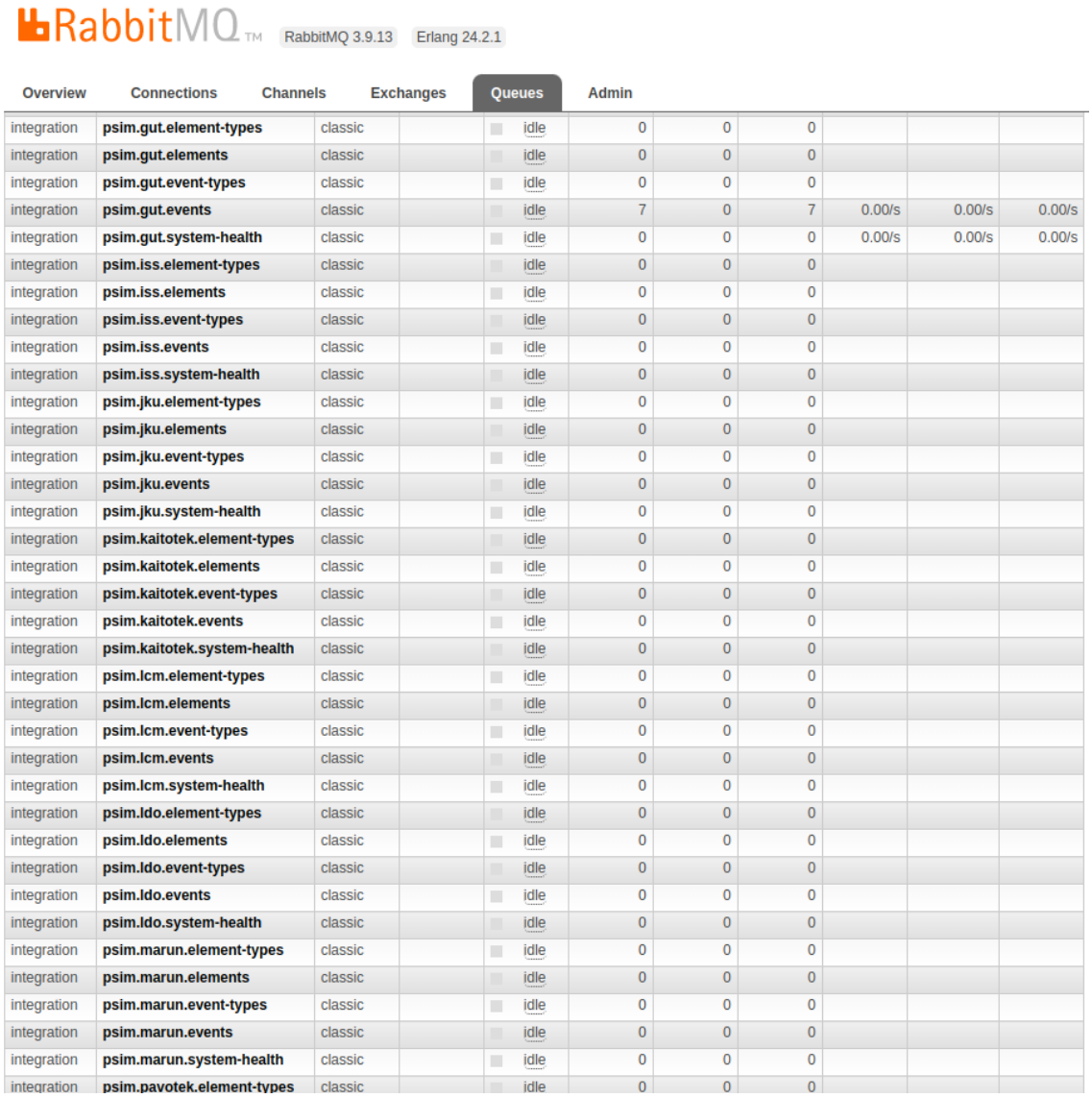


Figure 20 Screen shot of initial page of PSIM documentation

For each system integrating with PSIM platform, dedicated RabbitMQ queues were prepared to be used for sending data related to occurring events (alarms) and possible changes in used types of events and types of elements from the infrastructural point of view.



integration	psim.gut.element-types	classic		idle	0	0	0			
integration	psim.gut.elements	classic		idle	0	0	0			
integration	psim.gut.event-types	classic		idle	0	0	0			
integration	psim.gut.events	classic		idle	7	0	7	0.00/s	0.00/s	0.00/s
integration	psim.gut.system-health	classic		idle	0	0	0	0.00/s	0.00/s	0.00/s
integration	psim.iss.element-types	classic		idle	0	0	0			
integration	psim.iss.elements	classic		idle	0	0	0			
integration	psim.iss.event-types	classic		idle	0	0	0			
integration	psim.iss.events	classic		idle	0	0	0			
integration	psim.iss.system-health	classic		idle	0	0	0			
integration	psim.jku.element-types	classic		idle	0	0	0			
integration	psim.jku.elements	classic		idle	0	0	0			
integration	psim.jku.event-types	classic		idle	0	0	0			
integration	psim.jku.events	classic		idle	0	0	0			
integration	psim.jku.system-health	classic		idle	0	0	0			
integration	psim.kaitotek.element-types	classic		idle	0	0	0			
integration	psim.kaitotek.elements	classic		idle	0	0	0			
integration	psim.kaitotek.event-types	classic		idle	0	0	0			
integration	psim.kaitotek.events	classic		idle	0	0	0			
integration	psim.kaitotek.system-health	classic		idle	0	0	0			
integration	psim.lcm.element-types	classic		idle	0	0	0			
integration	psim.lcm.elements	classic		idle	0	0	0			
integration	psim.lcm.event-types	classic		idle	0	0	0			
integration	psim.lcm.events	classic		idle	0	0	0			
integration	psim.lcm.system-health	classic		idle	0	0	0			
integration	psim.ldo.element-types	classic		idle	0	0	0			
integration	psim.ldo.elements	classic		idle	0	0	0			
integration	psim.ldo.event-types	classic		idle	0	0	0			
integration	psim.ldo.events	classic		idle	0	0	0			
integration	psim.ldo.system-health	classic		idle	0	0	0			
integration	psim.marun.element-types	classic		idle	0	0	0			
integration	psim.marun.elements	classic		idle	0	0	0			
integration	psim.marun.event-types	classic		idle	0	0	0			
integration	psim.marun.events	classic		idle	0	0	0			
integration	psim.marun.system-health	classic		idle	0	0	0			
integration	psim.pavotek.element-types	classic		idle	0	0	0			

Figure 21 Part of RabbitMQ queues defined for integration between partner's system and Vemco's PSIM

3.4.1.1.2 Scenarios demonstrated

3.4.1.1.2.1 Real-time measurement and monitoring of V2X communications quality to enable safe and efficient operation of autonomous robot vehicles

Kaitotek's passive network QoS/QoE measurement solution, from TBB3.3, carries out continuous real-time monitoring of the network quality of the network in relation to mission-critical applications that need to work at all times. The measurement is based on lightweight measurement agents installed on network devices on which measurement is desired to be carried out. The measurement is passive, which means that the measurement is done for real active applications without creating any artificial test traffic that is being measured. The measurement does not have limitations on applications or network technologies over which measurement is carried out. It can be end-to-end or on any network path between that.

For measurement, a measurement controller is needed. The measurement will be carried out manually with a graphical measurement controller but also with a controller developed for automated management of measurements, which better suits continuous monitoring of network quality.

In the demonstration, the robot applications are being monitored for QoS/QoE. The measurement agent runs on the robot. The other end can then reside in the application server, or having an intermediate measurement point nearby that. Figure 22 Example measurement scenario illustrates an example measurement scenario where the quality of the network is monitored from the perspective of applications used by machines/robots on the field. The QoS measurement happens between two measurement agents as QoS measurement needs always be a two-point measurement. Measurement can be carried out between any two measurement points in the network that determines the measurement path.

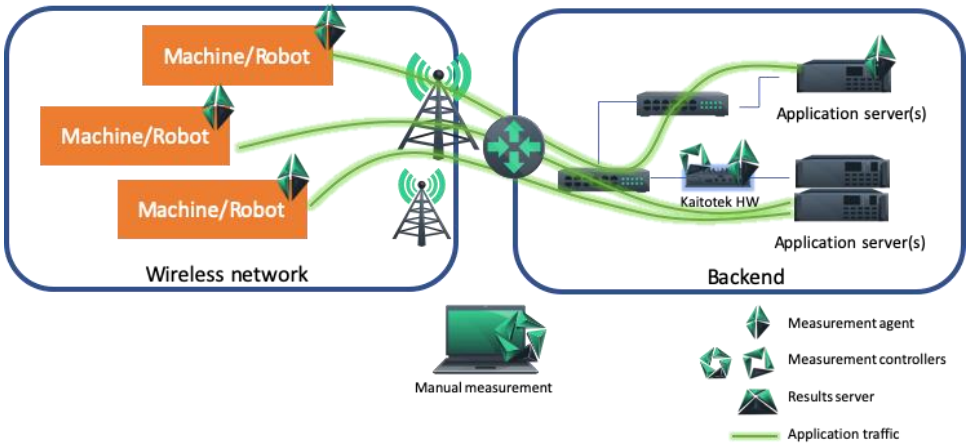


Figure 22 Example measurement scenario

This sub-scenario provides the basis for the sub-scenario on network quality situation awareness where the results are stored, analysed, and made accessible for further analysis and utilization.

GUT contributes by providing a mobile platform equipped with a V2X module. KAITOTEK's tool will analyse the link quality of V2X communication.

3.4.1.1.2.2 Localization and/or secure communication for mobile platforms

Mobile platform by GUT (figure below) will be equipped with dedicated sensors that allow to localize it and track with different accuracy dependent on application needs and available infrastructure.

Figure 23 Mobile platform designed and developed by GUT

JKU will provide UWB-enabled wireless sensor nodes for position estimation.

LCM contributes by providing LCM's UWB localization solution (infrastructure based).

3.4.1.1.2.3 Authentication & Authorization of autonomous units

This demonstrator will be taking place on the GUT campus parking place. An identification device providing authentication and authorization will be integrated into the autonomous unit of GUT. The device will be configured via mobile app and all credentials and permissions are synched with the device via cloud-connectivity and stored in a secure element. The identification device is able to communicate with the surrounding infrastructure e.g. parking or charging by using BLE v4. Currently also BLE v5 and UWB are analysed in this project. The identification device builds up a secure channel to the infrastructure/gateway device and checks their permissions. After the successful verification of the tickets the device send a command to the autonomous unit that the permission is valid, as well the infrastructure for further actions (like opening the gate). The owner of the autonomous unit can check all steps in the mobile App.

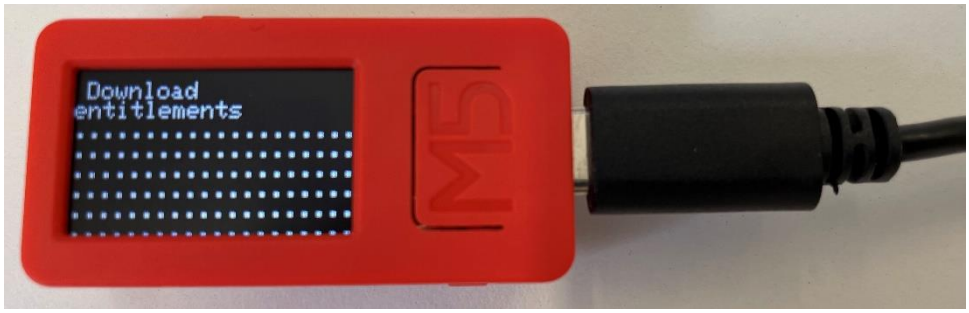


Figure 24 Identification device

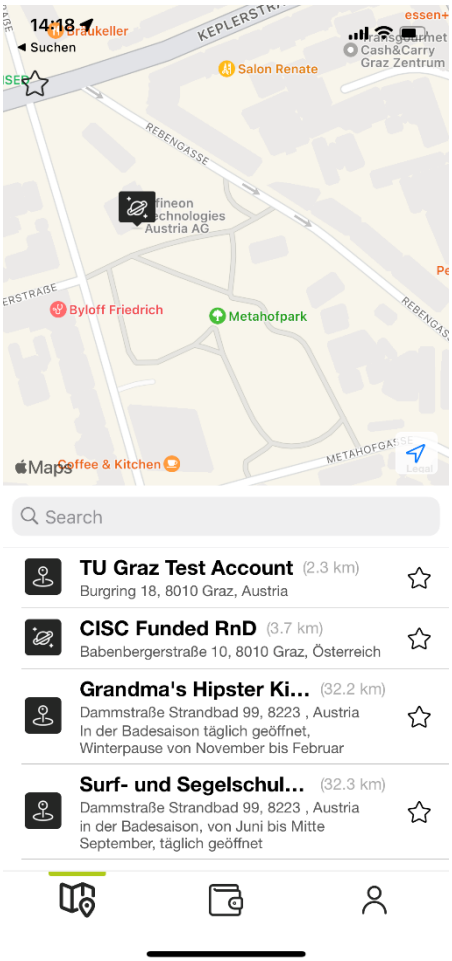


Figure 25 App for configuration of identification device

3.4.1.1.2.4 Asset tracking at the campus

This demonstrator will be taking place inside a building area on GUT campus. It aims at presenting how mobile robot (GUT) by entering the restricted zone causes triggering of an alarm which enables PSIM operator to analyse the whole situation, accessing past locations of the robot.

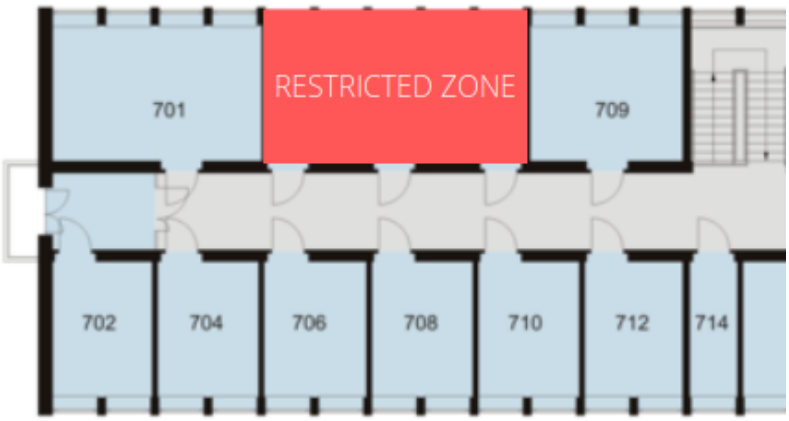


Figure 26 Possible place for setting up a restricted zone at GUT campus

Beacon tracking at the campus area enables real-time visualization using GUT's MPS. The data is saved for further historical usage by Vemco's Physical Security Information Management platform (PSIM). PSIM will allow for visualizing historical data of asset tracking for particular time frame, e.g., while analysing what was happening before an alarm was raised. Such a functionality will allow to search for specific causes of an alarm happening – analysing past location within a particular timeframe.

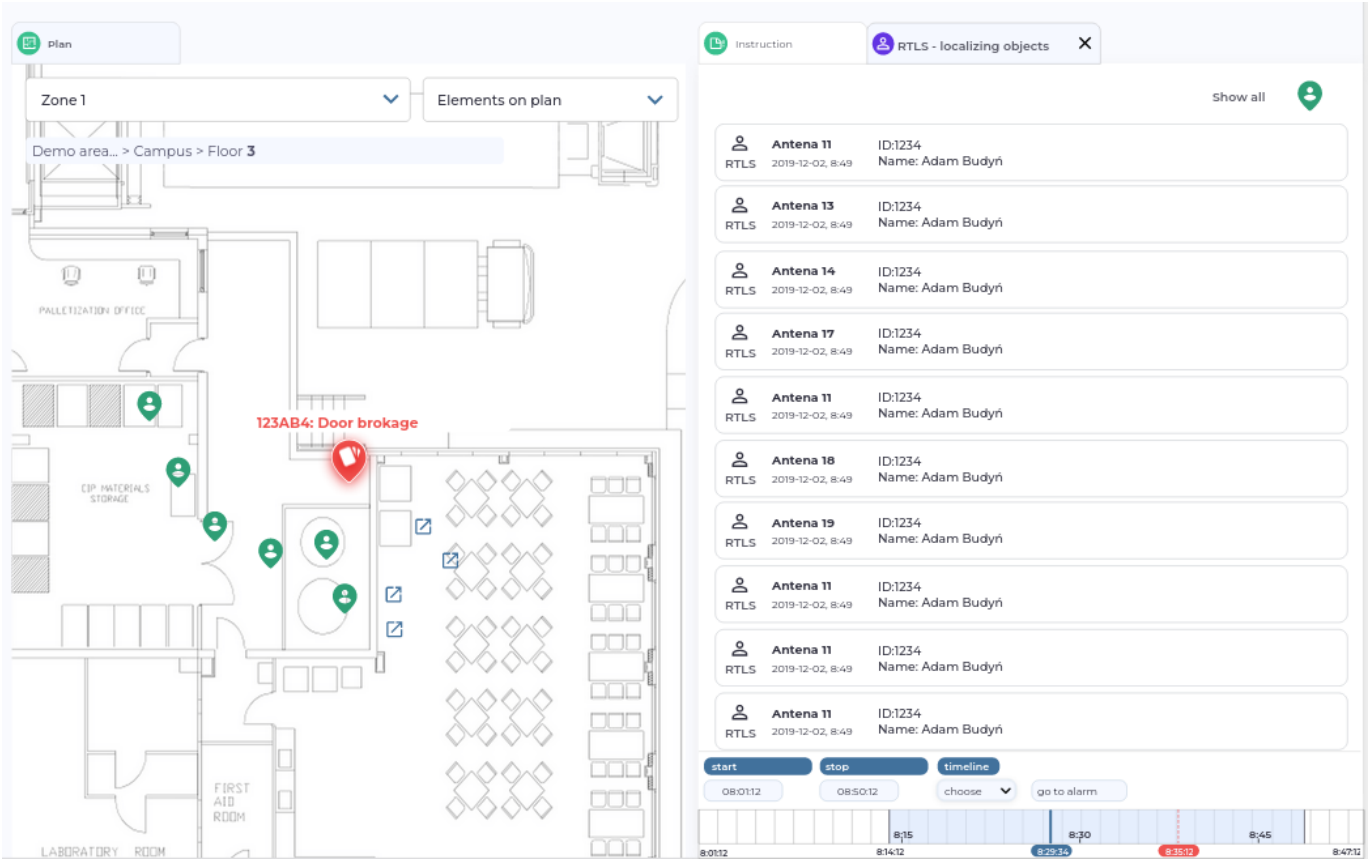


Figure 27 Demonstrating historical locations of tracked beacon in Vemco's PSIM platform – analysis of data integrated from GUT, after an alarm is raised (here a "Door breakage" example)

Below we present a flow of data through different components. Personnel with an asset is changing their location. The location data is being sent to GUT's MPS platform. After unwanted event takes place (here "Door breakage"), it is possible that PSIM's operator checks for historical asset's location changes for further threat causes analysis.

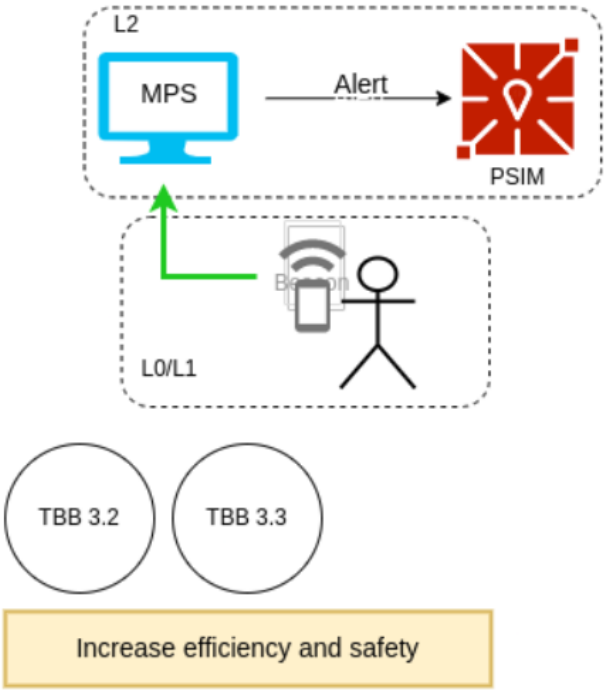


Figure 28 Simplified functional flow of data

3.4.1.1.2.5 Localization awareness – unauthorized presence in the area

The following demonstrator is an extension of “Asset tracking at the campus”, located outdoors.

Detection of personnel's unauthorized presence within restricted area. When the personnel enters the restricted area (setup zone), alarm is raised and presented to the PSIM operator.

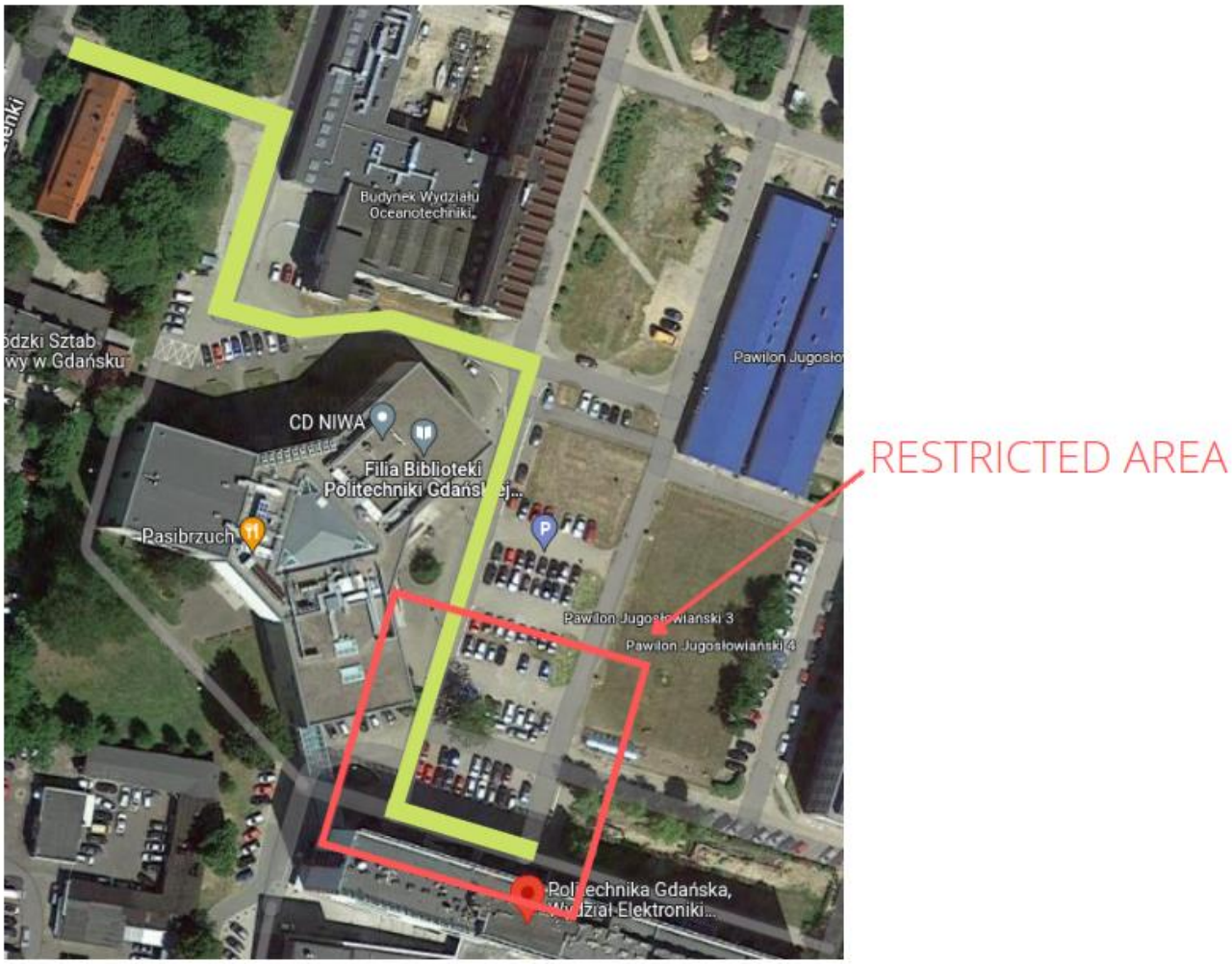


Figure 29 Planned location of the demonstrator outdoors – restricted area highlighted in red

LCM, JKU will provide UWB localization solutions to detect unauthorized access to a certain restricted area. Vemco is handling the alarm raised after detection of unauthorized presence, presenting it to the operator to let them decide on how to act. GUT will share their mobile robot and MPS as an additional source of localization system, to increase overall situational awareness – one system may detect unauthorized entrance in different conditions than the other one.

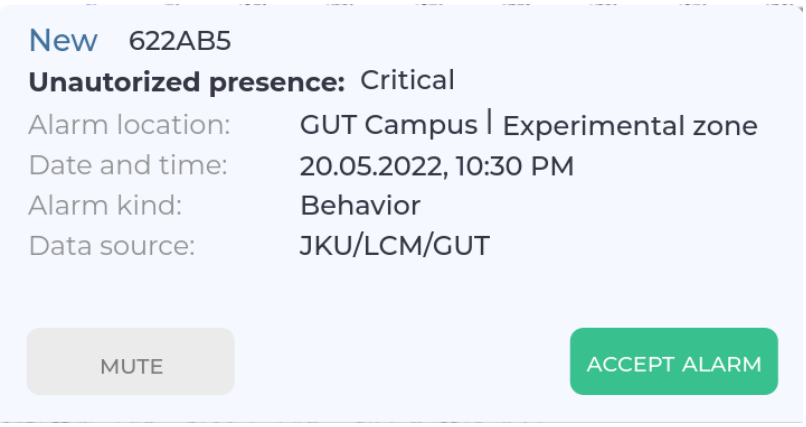


Figure 30 Example of alarm raised within Vemco's PSIM platform after unauthorized presence is detected by one of the systems

3.4.1.1.2.6 Network quality situation awareness

Results from passive network quality measurements carried out on the field are fed to a results server that creates a network-wide situation awareness, historical and current, of the network quality. A single measurement, related to sub-scenario 1.1, can be, e.g., the end-to-end connection quality of an operative machine (e.g., robot), focused on a mission-critical application(s), or all traffic. The results server stores results from every measurement in its local time-series database. The results are visualized as a heat map in the results server portal when geographical location information is tied with measurement results. Summary reports will be formed to help quickly analyse the network quality: when problems have happened, what connections have experienced connection quality problems, and where. The goal is to detect all connection quality problems before they harm operational efficiency and safety. Measurement results can also be downloaded for more detailed analysis.

The results server will run on a small-sized industry-grade PC shown in Figure 31. A heat map visualization of the results server is shown in Figure 32.

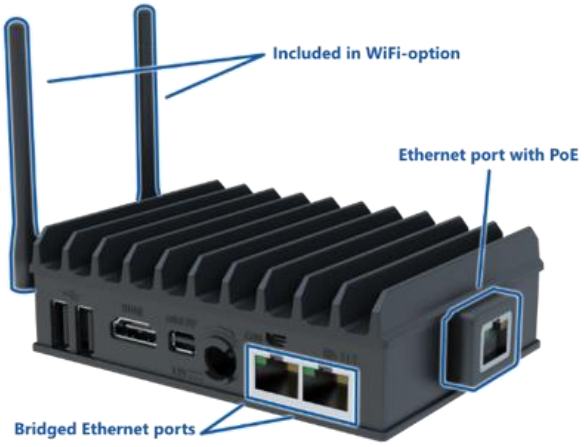


Figure 31 Kaitotek's measurement device equipped also with a results server

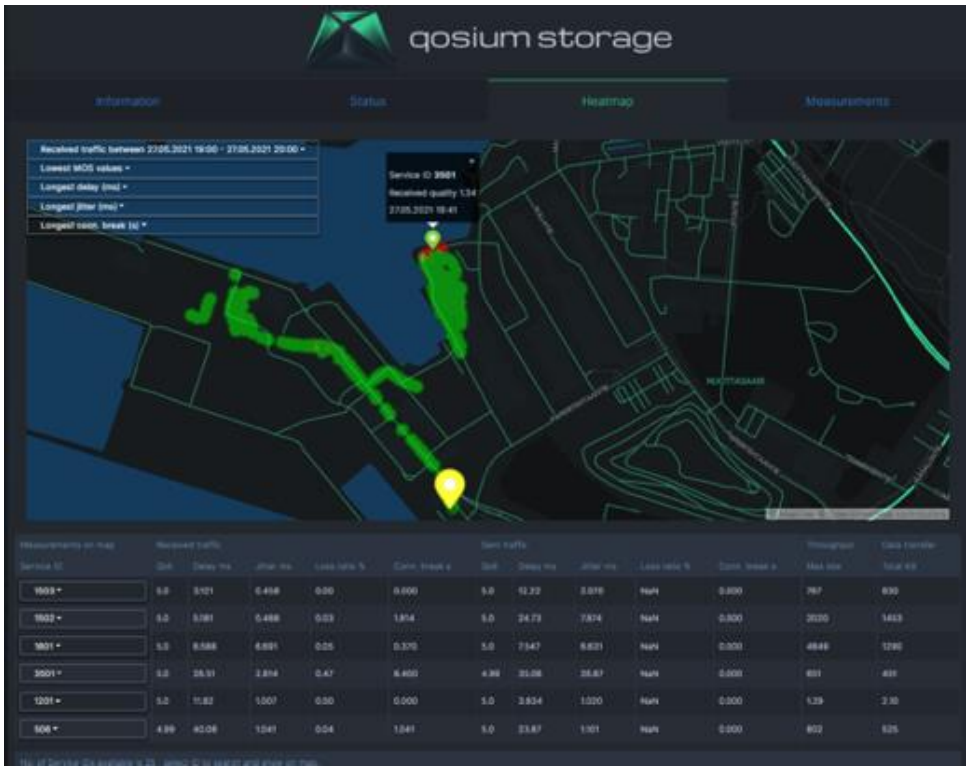


Figure 32 Heat map visualisation in the results server's web-portal

The results server triggers alarms of degraded connection qualities, e.g., due to increased delays, that are delivered to Vemco's PSIM platform and made accessible for different AI solutions through it. A simplified solution diagram is shown in Figure 32 and an example alarm depicted in Figure 33.

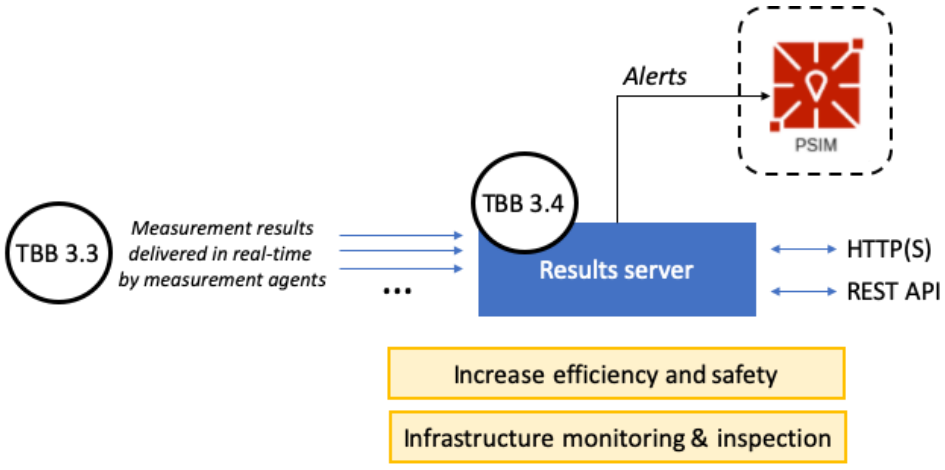


Figure 33 Simplified functional flow of data

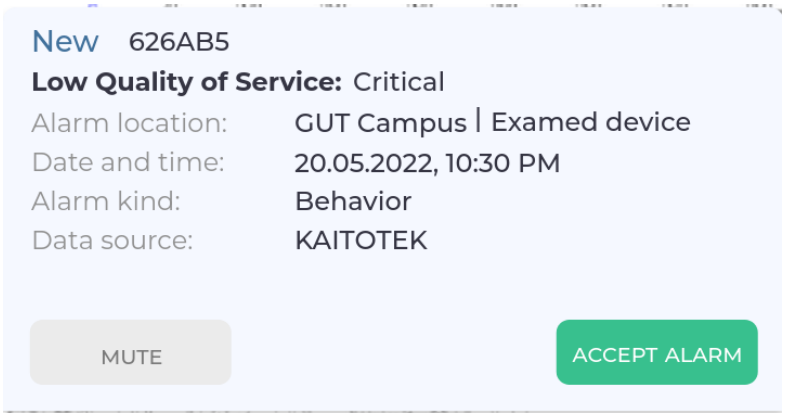


Figure 34 Example of low QoS alarm raised within PSIM platform

3.4.1.1.2.7 Network Anomaly Detection

The following demonstrator will present hybrid network anomaly detection via mirrored Ethernet interface in the edge field. If possible this will take place at GUT campus, in case of any problems with the setup, demonstrator location will include PAVOTEK's campus only.

PAVOTEK's PAVSEC will be analysing the network and providing Vemco's PSIM platform with detected anomalies.

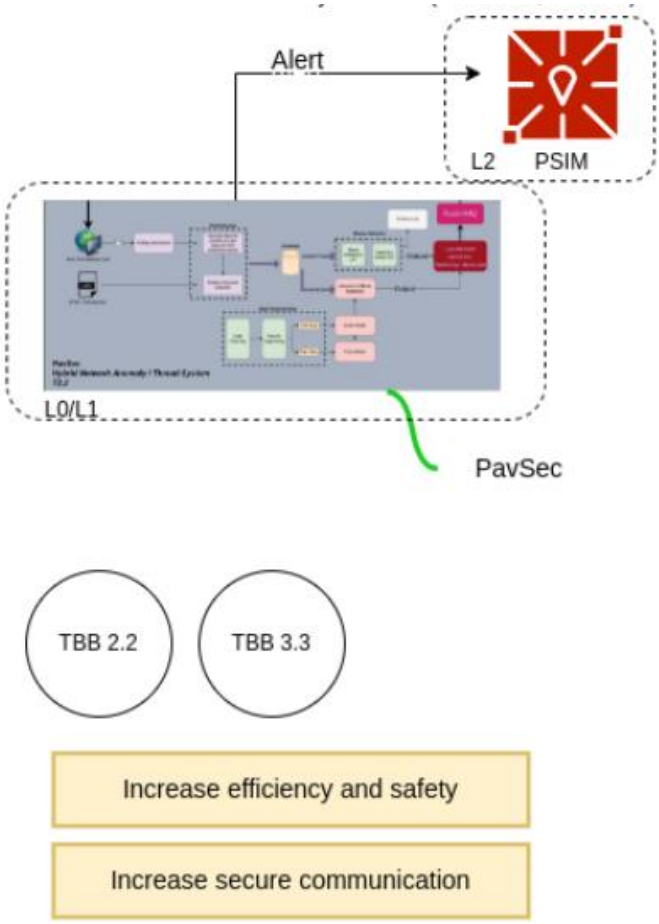


Figure 35 Simplified functional flow of data

The following event can be sent to PSIM platform, to inform the operator about potential risks.

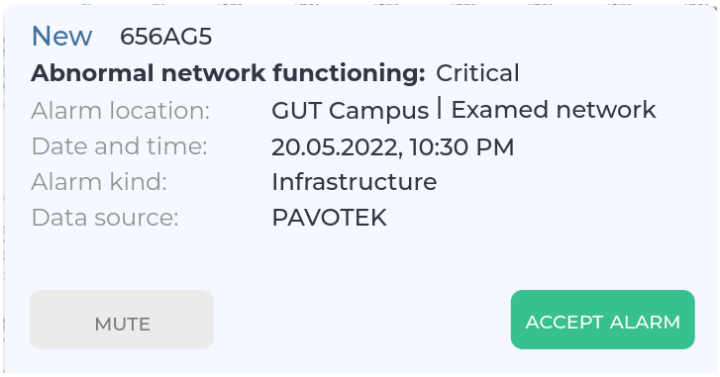


Figure 36 Example of abnormal network functioning detection alarm raised within PSIM platform

3.4.1.1.2.8 Image based monitoring

Machine vision-based event detection in smart environments – observing personnel / vehicles. Anomaly detection event will be sent to VEMCO's platform

For Y3 RabbitMQ integration with Vemco's PSIM is planned to take place. A dedicated events about detected anomaly will be sent to PSIM platform to inform the operator about potential threat.

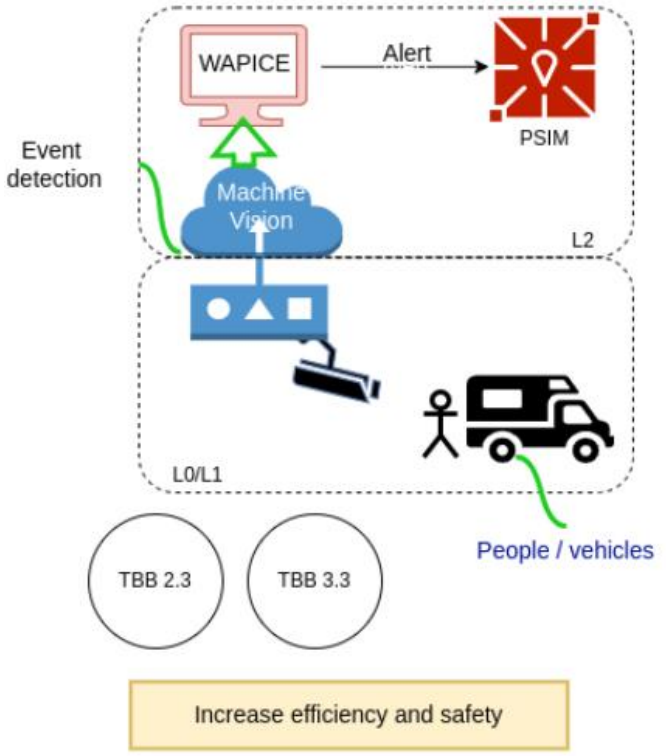


Figure 37 Simplified functional flow of data

3.4.1.1.2.9 Security seals monitoring

Security seals monitoring demonstrator focuses on monitoring ISS's seal status to increase reliability of overall functioning system and present a possible threat to the Vemco's PSIM operator. For Y2 demonstrator planned to take place at the campus, with final goal to extend it to other locations I.e. boat (as on the figure below) or Port of Gdansk. This scenario will be setup as part of "(semi)Autonomous vessel operations - Remote Inventory Management".

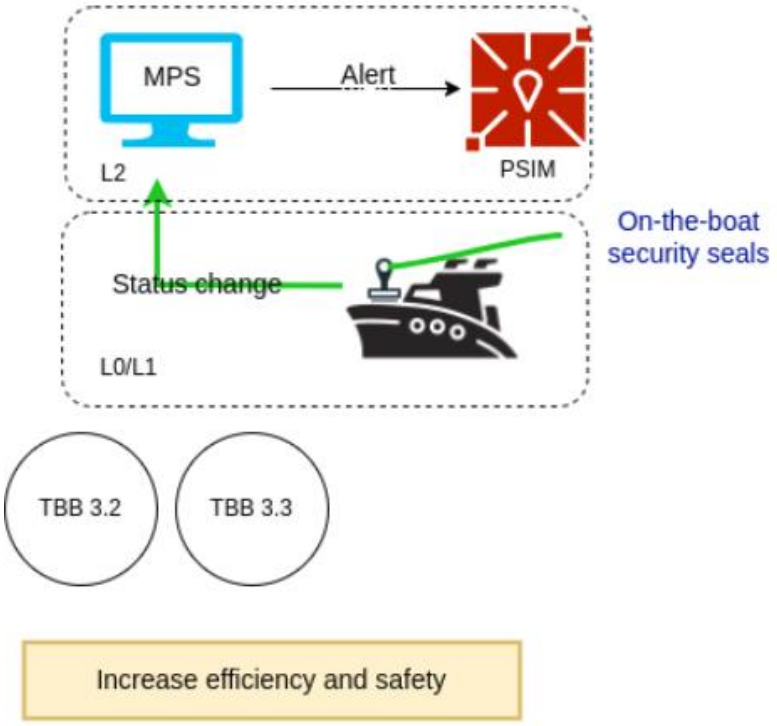


Figure 38 Simplified functional flow of data

The primarily recorded seal status will allow to provide a test demonstrational information to Vemco's RabbitMQ via GUT's MPS/ESPAR.

3.4.1.1.3 TBBs demonstrated

The work related to demonstrators located at GUT campus includes TBB 2.2 (PAVOTEK's PAVSEC), TBB 2.3 (WAPICE Machine Vision Software), TBB 3.2 (ISS's Security Seal), TBB 3.2 (GUT's Object localization), TBB 3.2 (GUT's Visualization and data acquisition application), TBB 3.2 (GUT's Wireless connectivity and security tools), TBB 3.2 (JKU's UWB and BLE-enabled wireless sensor node), TBB 3.2 (LCM's New WSN generation Proto22), TBB 3.3 (VEMCO's PSIM platform; KAITOTEK's real-time results delivery by agents), TBB 3.4 (KAITOTEK's results server).

3.4.1.1.4 Progress summary – Y2

After Y2 many of key functionalities in VEMCO's PSIM are ready for partners' systems integration. A document describing in details the integration process was prepared to simplify integrating with multiple partners simultaneously. VEMCO's RabbitMQ is hosted in private cloud – partners' access accounts with dedicated policies alongside queues were created for communication purposes with PSIM platform.

Security seal to be developed in next 12 months for final demonstrator – missing RF connection; tamper bit/seal status analysis in GUT localization system.

Improvement is still on progress for AI Model for the decrease false positive alarms (PAVOTEK).

There is at the moment no camera infrastructure in GUT campus that Wapice could utilize. Need to discuss with GUT later if we mount cameras there or utilize Wapice's infrastructure. RabbitMQ integration with Vemco during Y3.

GUT has prepared an infrastructure by mounting communication gateways on the roof of the building. The gateways connect to the data acquisition and visualization system. GUT has prepared

a mobile platform controlled by MQTT messages. In Y3 GUT will further work on testing V2X communication within its infrastructure. Also, the integration with other partners' system will take place.

3.4.1.2 Demo – Port of Gdansk

3.4.1.2.1 General information

Demonstrator will take place in Port of Gdansk, PG Eksploatacja Cargo Terminal, Gdansk, Poland. The aim is to deploy a localization system of vehicles and investigate radio propagation within such a harsh outdoor environment - a lot of reflections and interference. The main area of measurement (Szczecińskie Quay) is presented in the figure below.

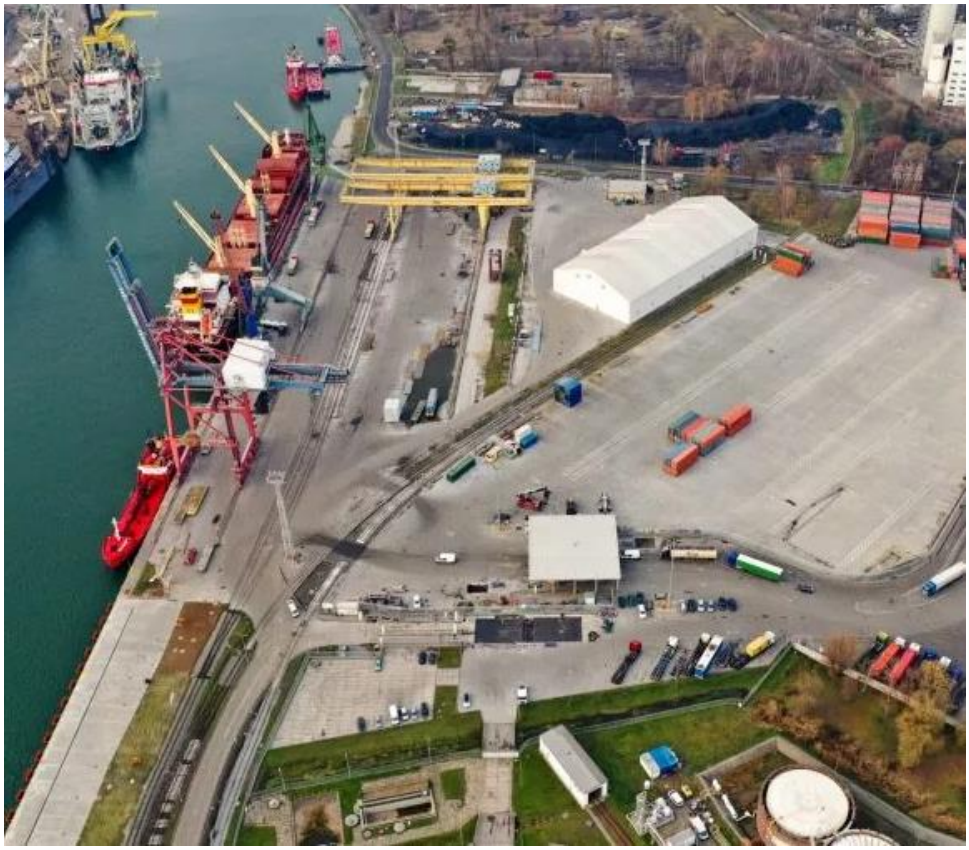


Figure 39 Demo site at Port of Gdansk[1]

3.4.1.2.2 Scenarios demonstrated

3.4.1.2.2.1 Vehicles localization within Port Infrastructure

The purpose of the scenario is to track the vehicles at the Port facility by exploiting two technologies, Bluetooth Low Energy (BLE) and GPS. The GUT will mount at one of the Port of Gdansk quaysides a master device equipped with dedicated ESPAR antennas for localization of the vehicles via Bluetooth Low Energy technology.

GUT will mount on several Port vehicles a BLE transmitter and GPS. BLE localization algorithms are under further development by the GUT. GPS will be a reference for the own localization algorithms.

[1] source: https://www.portgdansk.pl/en/about-port/terminals-and-quays/container_terminar_szczecinskie_quay/

A harsh propagation environment at Port quay may decrease the accuracy of the vehicle position estimation via BLE. Nevertheless, the total cost of a localization system would be much lower than basic GPS with LTE.

GUT has prepared a data acquisition and visualization system. Vehicle tracking would be available on the Grafana dashboard.

The block diagram of the system is in the figure below.

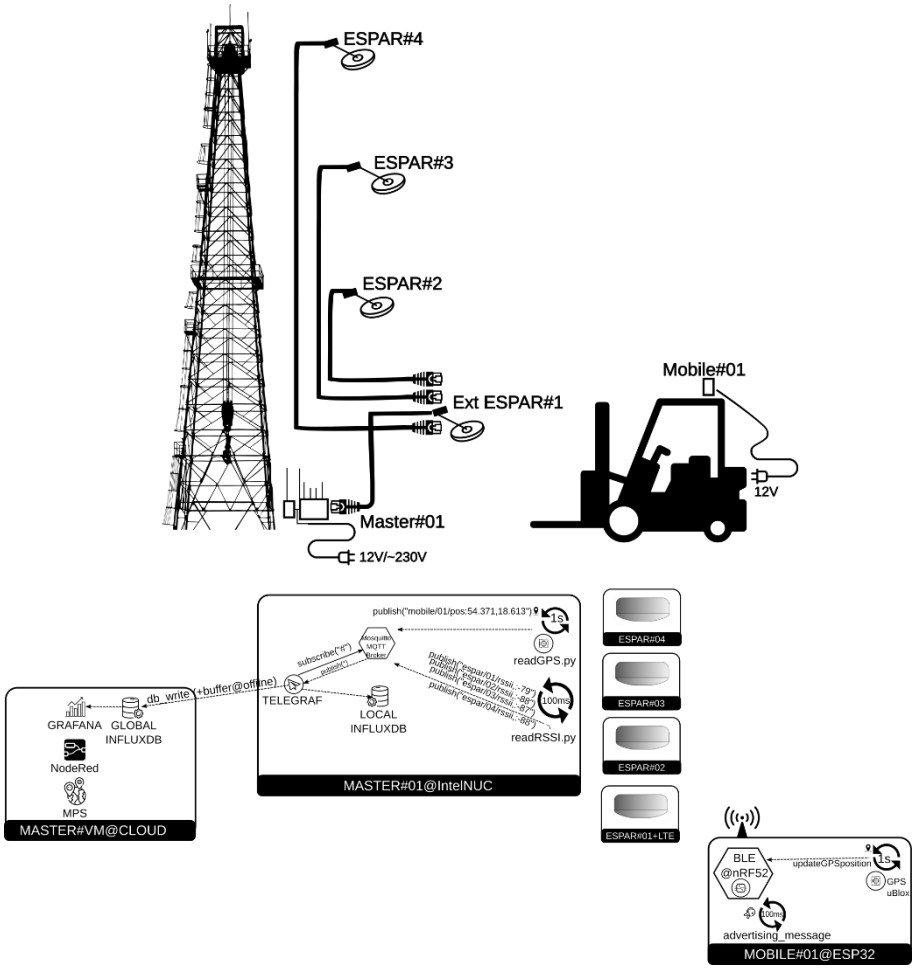


Figure 40 Block diagram of the system

3.4.1.2.3 TBBs demonstrated

TBB3.2 Dependable (reliable, robust, secure) wireless communication

- Objects localization. HW and SW for localization of objects, assets and vehicles
- Visualization and data acquisition application
- Wireless connectivity and security tools

3.4.1.2.4 Progress summary – Y2

Till Y2 GUT:

- agreed with Port authorities on the system requirements and deployment schedule
- developed localization gateways and localized nodes
- developed a localization algorithm

- prepared a system for data acquisition and visualization
- performed several measurements at test infrastructure at GUT Campus

In Y3 GUT will:

- mount hardware within Port Infrastructure and on the vehicles
- test within a port environment (RF measurements and localization accuracy)
- Analyse the measurements results and visualize vehicle tracking

3.4.1.3 Demo – Tucana Vessel

3.4.1.3.1 General information

Monitoring of Tucana Vessel on board systems has been updated with an AI based predictive maintenance algorithm. The algorithm will use the output data from the eleven deployed various sensors on m/v Tucana, e.g., for the ship engine and electrical batteries. RTE are for Y2 planned for development, testing and deployment of the predictive maintenance algorithm to be used for the on-board systems monitoring.

Besides onboard sensors, the Situational awareness system will be deployed on the ship. The system will provide additional information for the captain about all objects surrounding the ship both on and just below the surface of the water.

3.4.1.3.2 Scenarios demonstrated

3.4.1.3.2.1 Data analysis for predictive maintenance

A picture is shown below that describes the sensor collection setup.

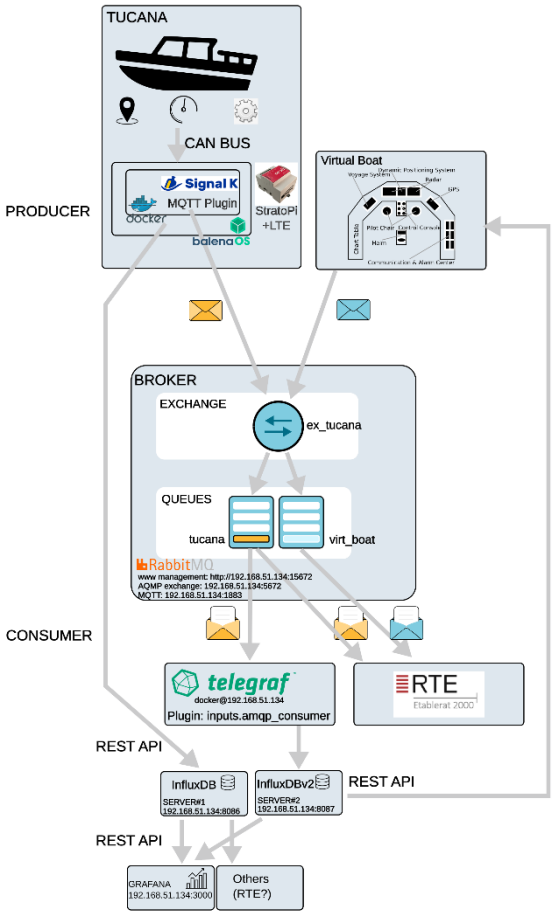


Figure 41 Sensor data collection for m/v Tucana

A high-level architecture for the complete predictive module is shown in the picture below.

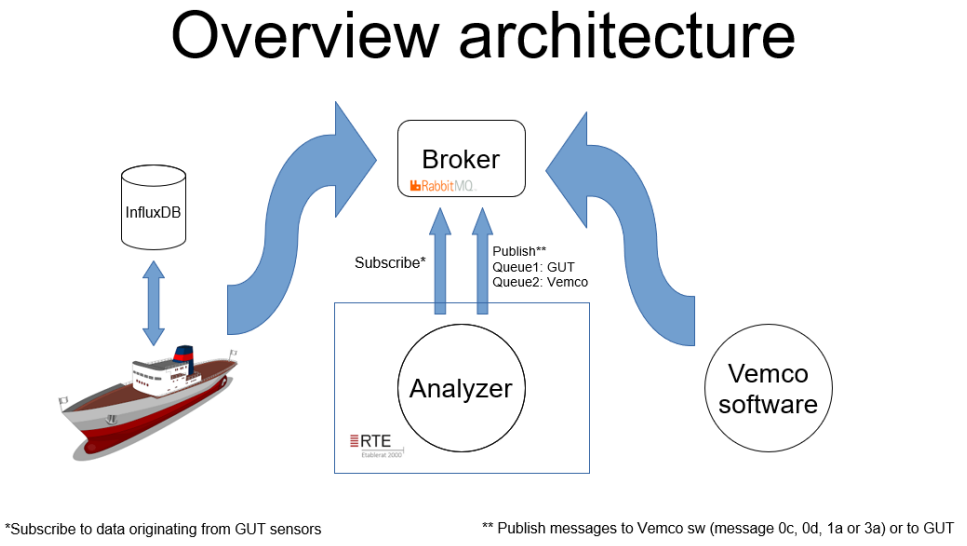


Figure 42 High-level architecture for the complete predictive module

As can be seen from the architecture diagram, the output of the predictive maintenance module is made available for the GUI as being developed and integrated by Vemco (alarming Physical Security

Information Management platform's operator). The RTE specific software design implemented so far is shown in the picture below.

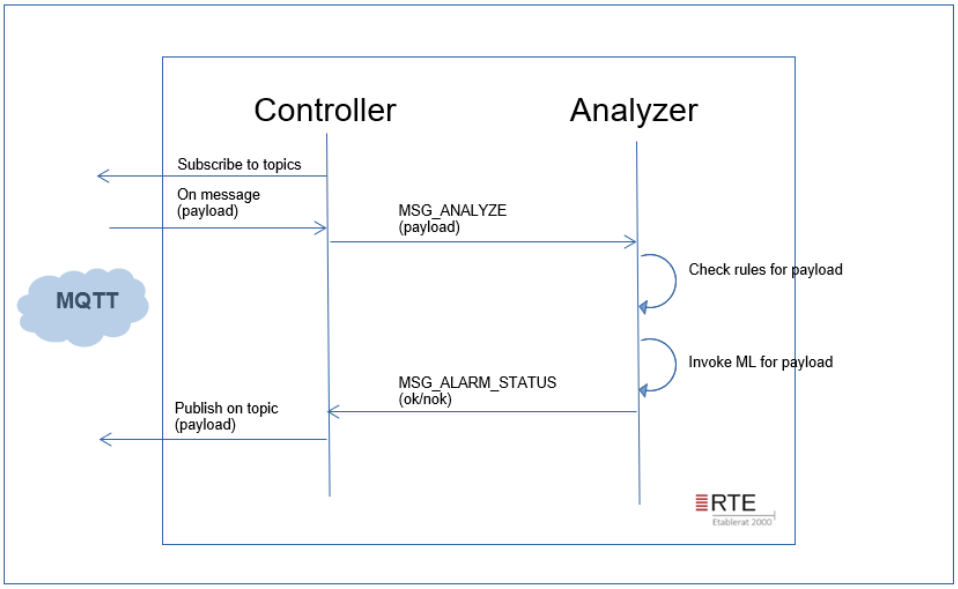


Figure 43 RTE specific software design (by M24)

An example of event (alarm) sent to Vemco's PSIM platform, after predicting abnormal condition.

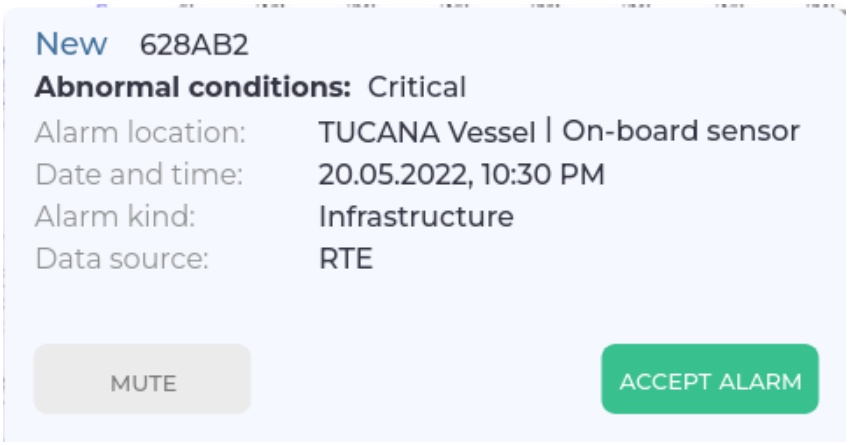


Figure 44 RTE's prediction module event demonstrated as alarm in Vemco's PSIM

3.4.1.3.2.2 Situational awareness system

The second part of the demonstrator will be the situational awareness system which is composed of the Flexible payload. The system in the default setup includes two lidars, two RGB cameras and a radar which are connected to the main box capable of analysing all data on the vessel. The Flexible payload can be seen in the picture below deployed on the motorboat as the intermediate step before the demonstrator on the Tucana vessel.

Figure 45 The Flexible payload on the test boat

All data collected in the system will be displayed for the captain of the ship in real-time to increase his situational awareness.

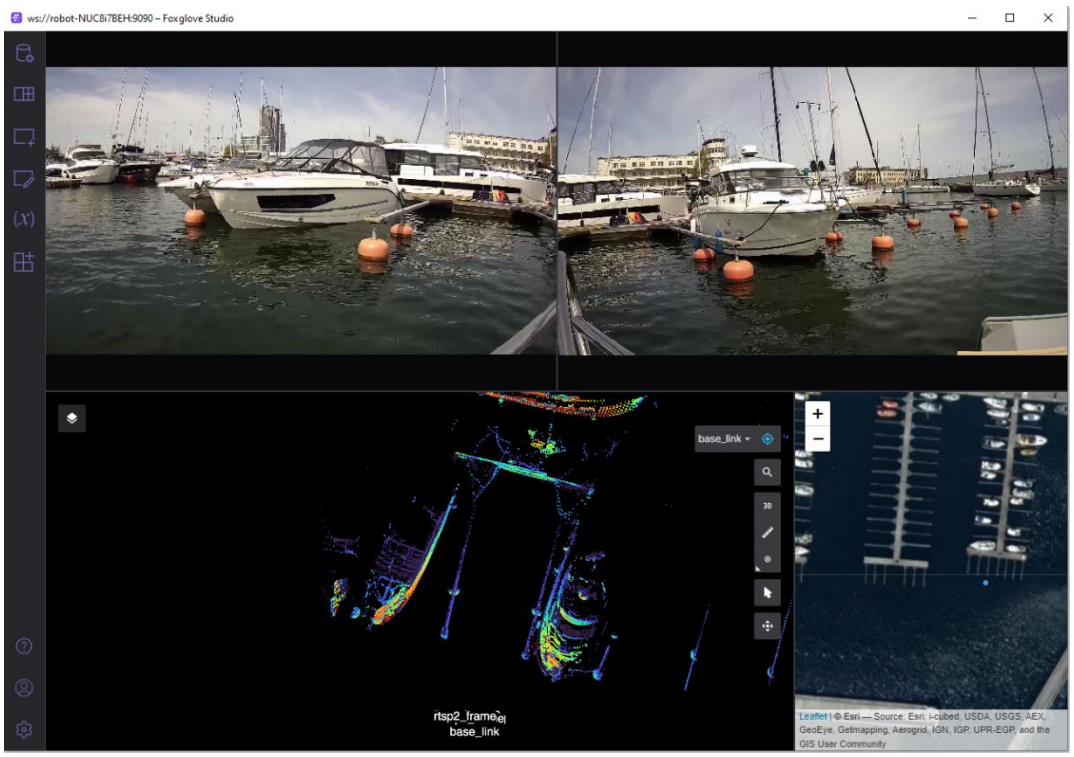


Figure 46 Raw data visualization

3.4.1.3.3 TBBs demonstrated

The basis on which to carry out the “Data analysis for predictive maintenance” work is from TBB2.1, where RTE has developed various machine learning-based algorithms for anomaly detection and classification that can be used for predictive maintenance. Anomaly detection mainly regards identifying certain predefined states for the on-board systems on the boat. For Y2, a simplification is done that will show that the principles work as intended, a so-called proof of concept. The simplification is done just to short cut the otherwise time-consuming task of labelling the data that are received from the on-board sensors.

Because of the integration with Vemco’s platform – work from TBB3.3 is also included (PSIM).

The situational awareness system include work from TBB3.2 (Flexible Payload)

3.4.1.3.4 Progress summary – Y2

Current status is that the information flow from the boat sensor controller has been setup and is working. All eleven sensors are active and send at regular intervals when the boat engine is active. Currently, the data is accessed through the local Influx database but this will be replaced by a Rabbit MQ queue as seen above. A first very basic predictive maintenance algorithm is being implemented. Two basic labels – “normal1” and “normal2” - will be used to simplify labelling in this stage of the development. The labels represent geographical location of the boat inside vs outside the port boundary. More elaborate states will be introduced during Y3. Depending on which state that is targeted for detection, there will be an associated ML-algorithm. In the simplest case, a deterministic algorithm would be the easiest way forward. RTE therefore foresees that the ML-algorithm will need to be re-designed and elaborated as the states for detection will change during Y3. RTE also prepares to synthesize data in order to achieve anomalies for the ML model to include in training. Integration with Vemco platform (GUI) is planned to be ready by M24. This will allow for a first demonstration to be made. The interface for the integration has been specified and consists of a set of JSON-formatted messages.

In the case of the situational awareness system in Y2 GUT fully tested the proposed solution on a smaller vessel. The hardware part of the system is complete and ready to be mounted on the target vessel.

3.4.1.4 Demo – ISS-RFID Test Vessel operating on Baltic Sea

3.4.1.4.1 General information

Main focus of this demonstrator is to show the security of assets and people on board, with real time asset monitoring based on active tags attached to the equipment located on the board. The system will also be able to monitor the crew. The idea is to ensure a safe and secure monitoring and information about the state of equipment and crew with necessary alarms when there are discrepancies.

The vessel will be operating in Gulf of Gdansk during summer season (form April to October) and gathering data.

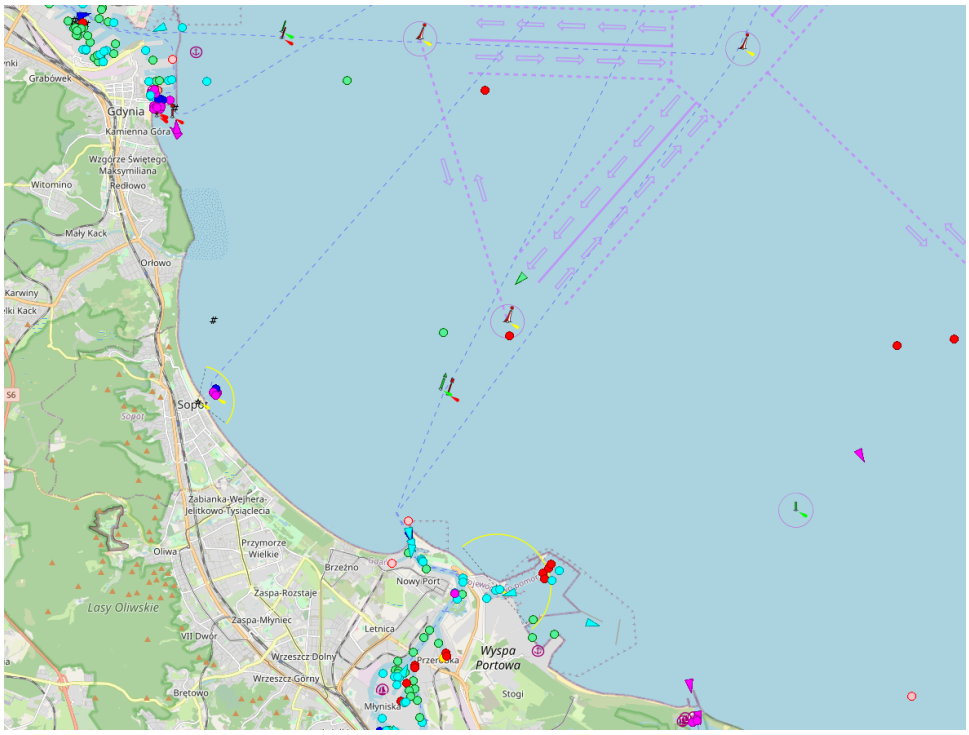


Figure 47 Vessel tracking on Baltic Sea

3.4.1.4.2 Scenarios demonstrated

3.4.1.4.2.1 (semi)Autonomous vessel operations - Remote Inventory Management

System uses and adapts GUT ESPAR antennas, which monitor the position and status of equipment and items being stored on vessels. Additionally, 2.4 GHz beacons are used to monitor and manage the inventory.

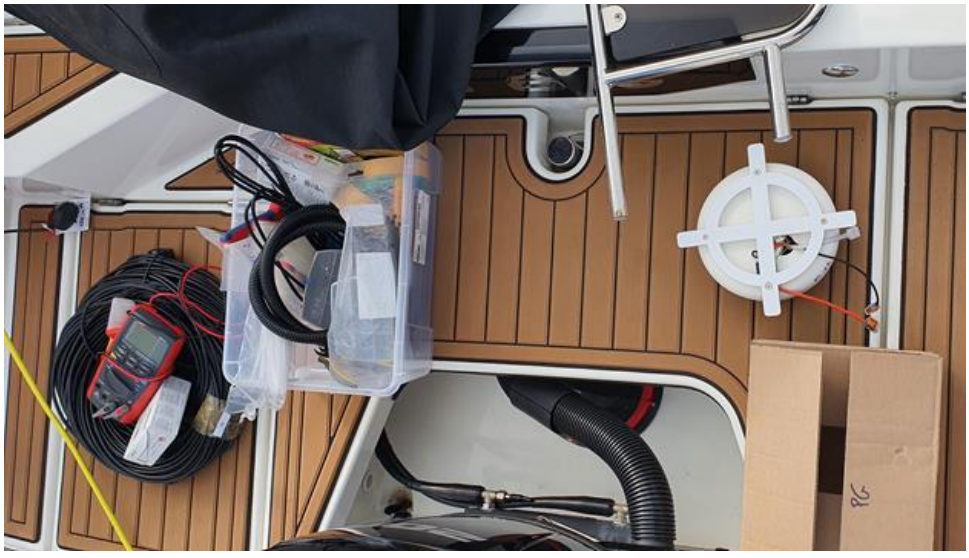


Figure 48 Hardware set during tests

System is equipped on small vessel – Parker 690 DC (7.24 m in length, 2.45 beam).

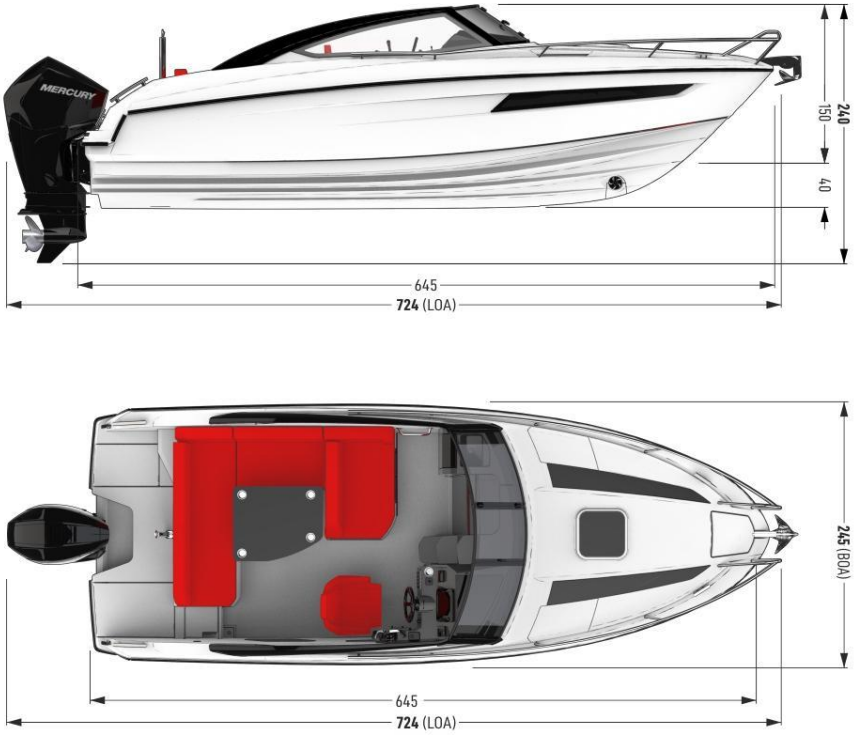


Figure 49 Test vessel

To boat operates in Gulf of Gdansk, with its main docking area in Gdynia Marina. There are planned trips from Gdynia to Gdansk, which will take at open sea and in channels around the city.

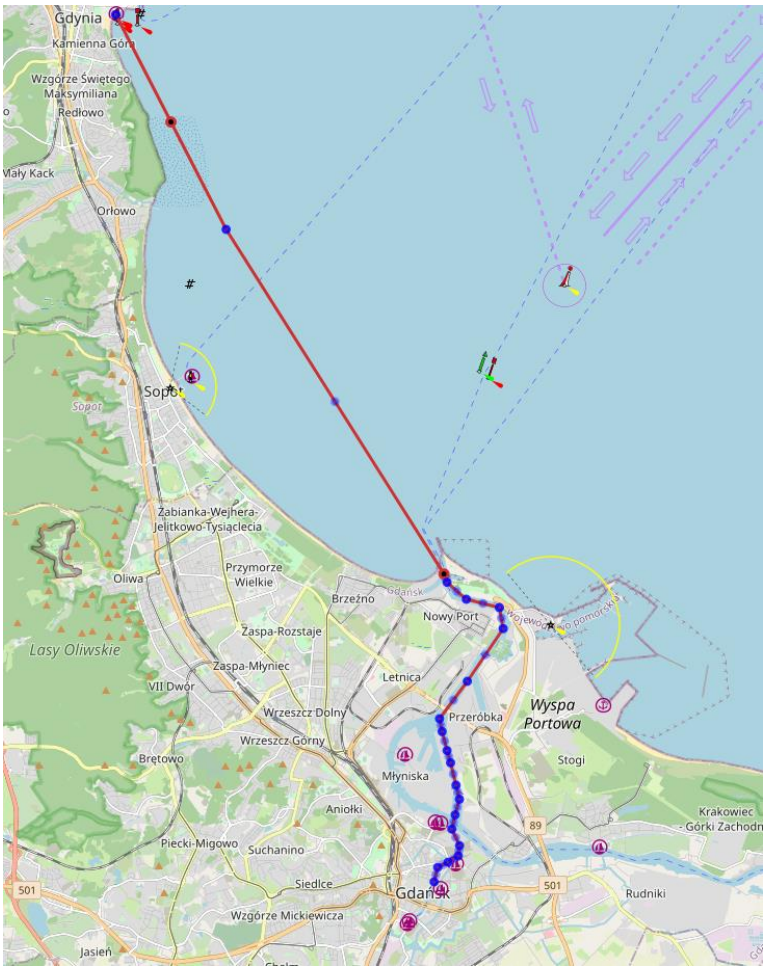


Figure 50 Vessel route monitoring

3.4.1.4.3 TBBs demonstrated

ISS RFID includes the work from TBB2.1, TBB3.2 and TBB3.3. All is directly linked to this specific scenario with regards for parameter collection, assets and crew monitoring and interfaces and integration.

3.4.1.4.4 Progress summary – Y2

Preparation for final demonstrator has begun. Initial tests and setups were done at end of Y2. The organization of demonstrator is according to plan. List of items that can be potentially tagged has been prepared. Items needed to be tagged and equipped with IoT trackers were verified in possibility of attaching trackers to them. Design of new IoT tags in form of security seals has been started.

Final demonstrator will be ready by M36.

3.4.1.5 Demo – Cetraro harbour (Italy)

3.4.1.5.1 General information

This demonstrator is relevant to the application of acoustic and magnetic barriers for the protection of maritime infrastructures. In particular, the proposed scenario is referred to the deployment of acoustic and magnetic sensors out of a small harbour to identify the passage of potential targets in the nearest volume of water. The theoretical concept is to build a monitored perimeter around the infrastructure, but in specific the sensors will be deployed near choke points (e.g., harbour entrance

channel). An SDN-enabled multi-interface wireless network will be also deployed in the Harbour to connect the underwater access control system with the remote harbour control room. It is able to detect DDoS/DoS, and MiTM attacks using an AI-based Intrusion Detection System (IDS) that is integrated into the ONOS controller of the network, and to provide a redundant and robust wireless communication based on the use of SDN-enabled multi-interface wireless network nodes, and on a software application on SDN Controller for automatic wireless interface selection (Reliability Module).

Figure 51 Concept of underwater barriers for perimeter monitoring

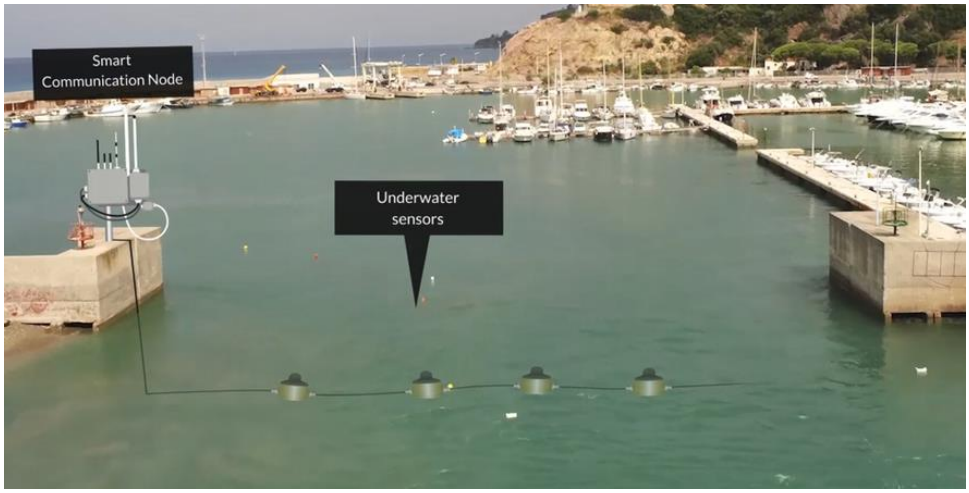


Figure 52 Underwater sensors and a multi-interface node used to monitor passages through harbour entrance channel

3.4.1.5.2 Scenarios demonstrated

3.4.1.5.2.1 Port surveillance

The scenario involved the use of (Figure 17):

- a magnetic barrier prototype composed of at least three sensors (first phase);
- an acoustic barrier composed by at least three sensors (second phase);
- An SDN-enabled multi-interface wireless network connecting the terminal of the barriers and the harbour control room.

- VEMCO's data management system.

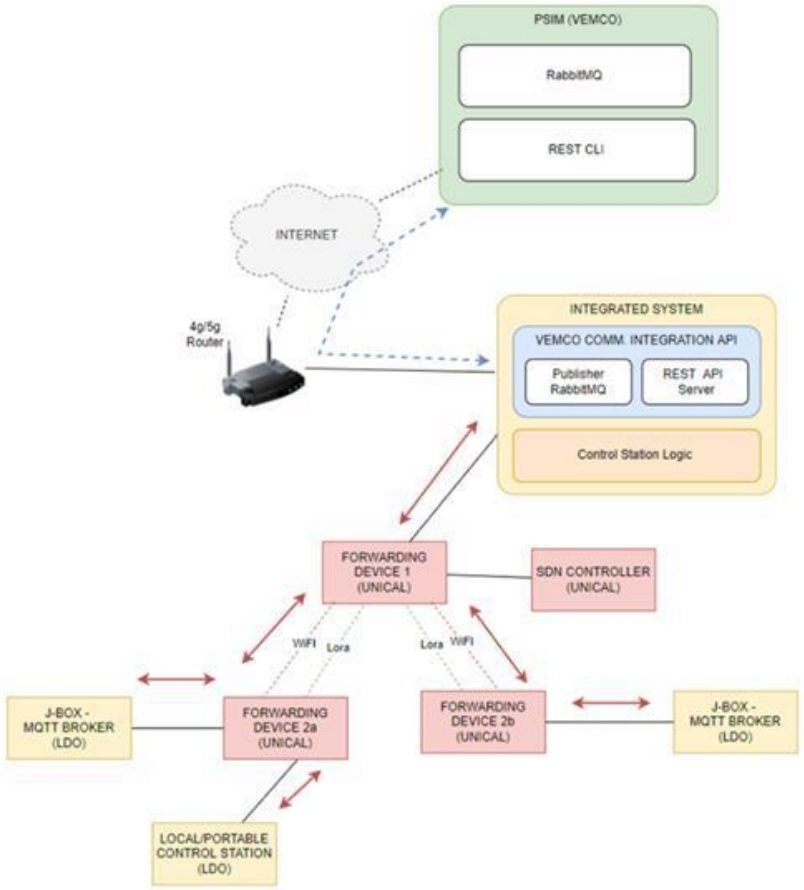


Figure 53 Architecture for the integration among underwater barriers (LDO), SDN-enabled wireless network (CINI-UNICAL) and VEMCO platform

The test activities shall not have impact on the daily activities of the harbour, thus the tests will be performed in a sea area outside the port.

This will also allow safety conditions during the runs of divers and underwater vehicles.

Figure 54 Potential location outside the harbour to perform the tests

3.4.1.5.3 TBBs demonstrated

The collaboration between LDO and CINI UNICAL allows to demonstrate BBs implemented in WP3. All functionalities and capabilities developed in BB 3.1, BB3.2 and BB3.3 will be verified during the live experimental activities performed at sea.

3.4.1.5.4 Progress summary – Y2

According to the planning, the organization of the trials is progressing well.

LDO completed the first prototype of magnetic sensor, prepared a portable version able to manage two set of transducers that have been integrated together. The magnetic barrier architecture has been defined and validated.

Figure 55 Magnetic sensor prototype (left) and control console (right)

The preparation of the prototypes for the sea trials is starting, to provide the barrier within M28, so to perform a first set of tests in M29 – M30.

CINI-UNICAL has prepared a first release of the SDN network prototype composed of 2 SCNs and 1 controller where the first release of the IDS and the Reliability module have been integrated. The first test campaign at the Cetraro Harbour has been planned at M25.

The architecture of the acoustic sensor and of the relevant barrier has been defined too, while the detailed design is proceeding with some months of delay. The goal is to complete the sensors within M32 and assemble the prototype barrier within M34, to perform the final sea trials in M35.

In addition, after the tests are performed, alerts about underwater threats will be sent to Vemco's PSIM platform, to inform the operator about potential danger (Y3).

3.4.1.6 Demo – VeNIT Lab (Marmara University Dragos Campus)

3.4.1.6.1 General information

Main focus of this demonstrator is to monitor the connectivity of IoT devices in real-time. The concept is to be aware of the changes in system performance or connectivity and alert the operator about these system changes. Lack of data due to communication problems is also taken into account in this demonstrator and more insights about connectivity problem is evaluated with developed components to provide processed information to the user.

The system includes software components that are implemented in both IoT device and the edge device to collect data about link quality, network traffic and run performance measurements. The data is transferred and stored using reliable network protocols on a database and the APIs for further

analysis on both real-time and along with historical data are being implemented. The diversity of the information processing is also enabled with the proposed architecture and will be tested using VEMCO's platform along with MarUn's provided platform.

3.4.1.6.2 Scenarios demonstrated

3.4.1.6.2.1 Network Quality Monitoring

Parameter/Data collection application is running on a device placed in the field to check access and measures performance to the APIs and services in the control center. When there is a connectivity problem or an issue regarding a service, the operator is alerted on graphical monitoring tool. The tool also provides warnings on performance changes on the network and alerts user per-device/per-application. Results will be integrated with VEMCO PSIM platform as presented on the figure below.

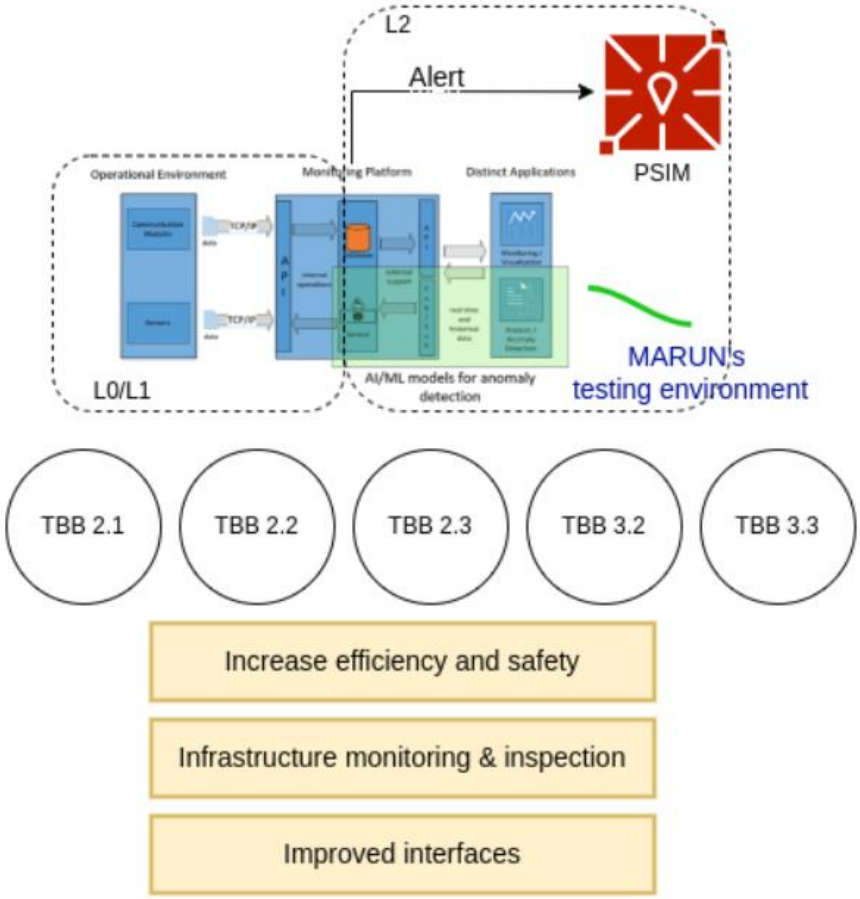


Figure 56 Simplified functional flow of data

3.4.1.6.3 TBBs demonstrated

BB2.1 - Parameter Collection Application, BB2.2 - Monitoring Platform, BB3.2 - Monitoring Tool, BB2.3 - Anomaly Detection Algorithm, BB3.3 - Anomaly Detection Application, BB3.3 - PSIM platform

3.4.1.6.4 Progress summary – Y2

A dedicated RabbitMQ account with dedicated policy and queues access was created for MARUN to allow to send alerts to VEMCO's PSIM platform.

The applications' integration, interface improvements and multiple devices/environment testing is ongoing. The demonstration can be made in MarUn Dragos Campus with current implementation.

Data management platform including MQTT and RESTful API is deployed on a VM in VeNIT Lab. Monitoring Tool is currently being deployed to a VM having Internet access to test the integration. The data collection application, anomaly detection algorithm and application are tested and currently being prepared for demonstrations. The demonstrator schema including building block components are provided below:

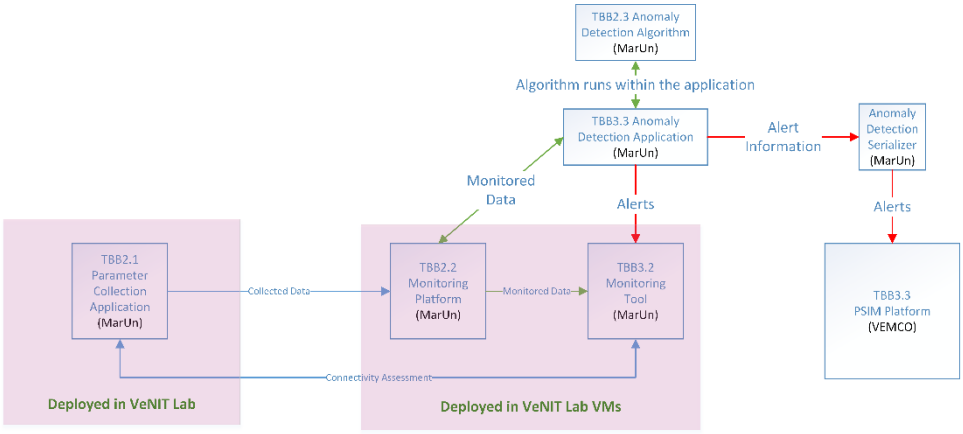


Figure 57 Demonstrator Integration Schema

3.4.1.7 Demo – Pavotek Campus (Teknopark Istanbul)

3.4.1.7.1 General information

This demo will show detecting network anomalies in the edge network with PavSec Hybrid Anomaly Detection software. In the campus there is several edge network cabinet in the campus, there will be a PavSec device for each cabinet. Each PavSec analysing edge network and if the system detect anomaly then sending alarm to VEMCO Platform with RabbitMQ.

3.4.1.7.2 Scenarios demonstrated

3.4.1.7.2.1 Network Anomaly Detection

The following demonstrator will present hybrid network anomaly detection via mirrored Ethernet interface in the edge field. If possible this will take place at GUT campus, in case of any problems with the setup, demonstrator location will include PAVOTEK's campus only.

PAVOTEK's PAVSEC will be analysing the network and providing Vemco's PSIM platform with detected anomalies.

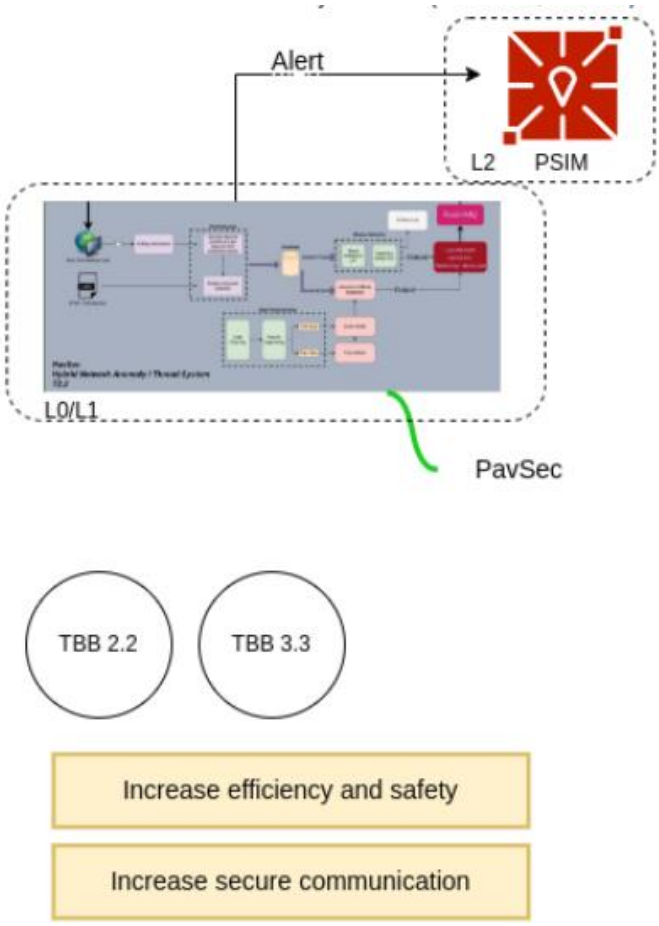


Figure 58 Simplified functional flow of data

The following event can be sent to PSIM platform, to inform the operator about potential risks.

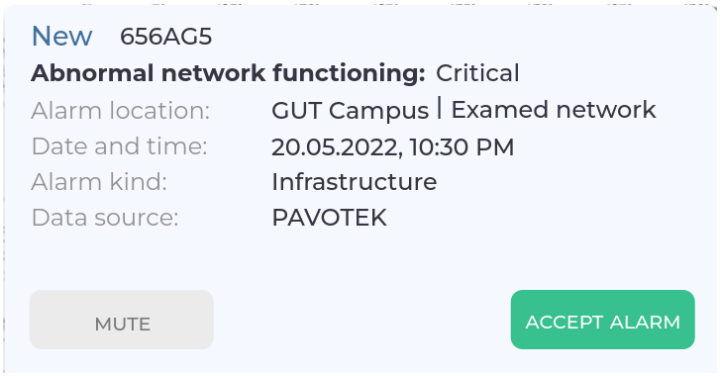


Figure 59 Example of abnormal network functioning detection alarm raised within PSIM platform

3.4.1.7.3 TBBs demonstrated

The main work in here is related to TBB 2.2 (PAVSEC).

In addition, because of integration with Vemco's PSIM, work from TBB 3.3 is included.

3.4.1.7.4 Progress summary – Y2

A dedicated RabbitMQ account with dedicated policy and queues access was created for PAVOTEK to allow to send alerts to VEMCO's PSIM platform.

Improvement is still on progress for AI Model for the decrease false positive alarms (PAVOTEK).

3.4.1.8 Demo – UCC Campus (University College Cork)

3.4.1.8.1 General information

This demo concerns the verification of video data streams obtained in an industrial setting, namely a ship-to-shore crane operating in a container port. See the figures below for a software simulation of the environment.

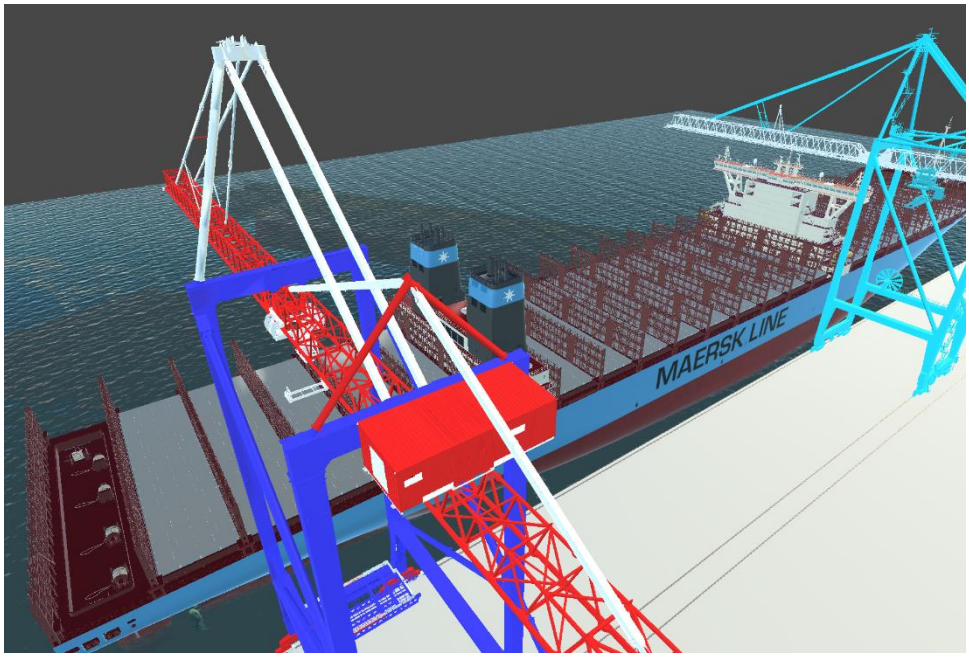


Figure 60 Software simulation of a container port

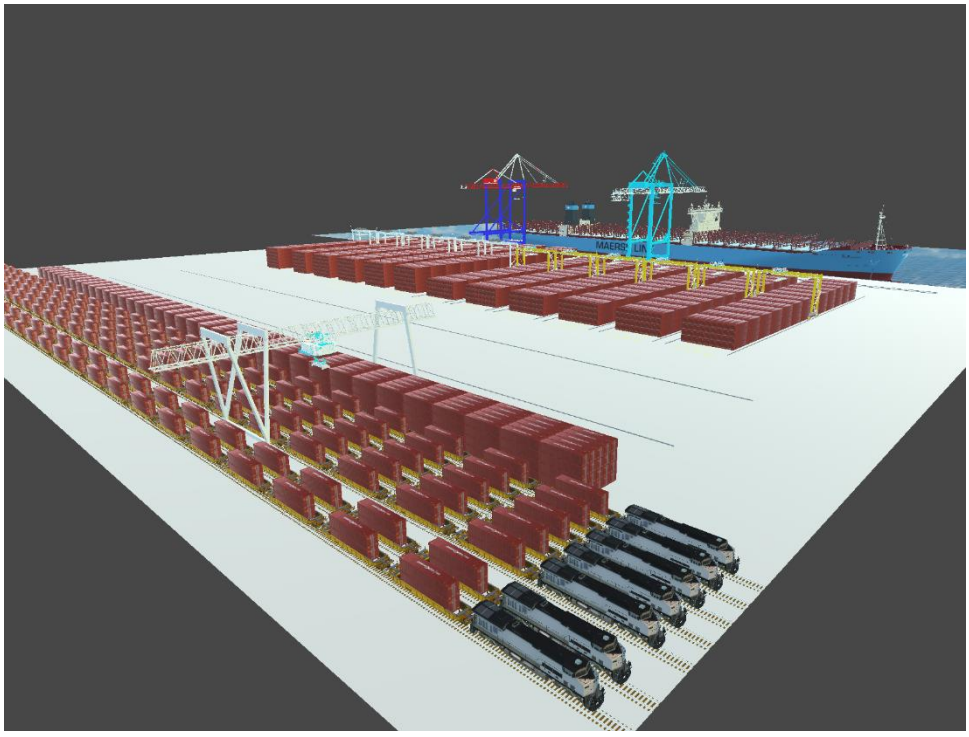


Figure 61 Software simulation (2) of a container port

The physical demo consists of a miniature replica of part of a container port, in which a model crane, containers and various vehicles are located. A number of cameras (one of which is mounted on a camera dolly for tracking shots) provide video data streams of the scene.

3.4.1.8.2 Scenarios demonstrated

The demo will show that anomalous video feeds can be detected by AI methods. An anomalous feed can be obtained when a user positions or orientates a camera incorrectly, either maliciously or inadvertently. Therefore, the demo falls into the category of secure port communications.

3.4.1.8.3 TBBs demonstrated

The work is related to TBB 3.1.

3.4.1.8.4 Progress summary – Y2

A literature search of anomaly detection applied to video streams has been conducted. A list of materials for the demo has been compiled. Initial real-world (container terminal) video streams have been collected and provided to UCC.

3.4.1.9 Demo – LCC Client Container Terminal(s)

3.4.1.9.1 General information

This demo concerns the predictive maintenance relating to steel wire rope bending cycle counting and damage model implementation. Bending cycle counting is executed on the basis of crane log file using specific algorithms and models developed within LCC and in collaboration with UCC (algorithm development is ongoing).

3.4.1.9.2 Scenarios demonstrated

The demonstration is intended to demonstrate the feasibility of AI-models for remaining rope life estimation, and ideally (historical data availability permitting), validation of the method. Therefore, the demo falls into the category of "AI on computational level (on device and edge)" and “Intelligent wireless systems for smart port cross-domain applications”.

3.4.1.9.3 TBBs demonstrated

The work is related to TBB 2.3 and Task 5.4.

3.4.1.9.4 Progress summary – Y2

Method to enable cycle counting direct from crane log files has been provided to UCC. An outline design of experiments has been conducted with target ports identified and discussions ongoing regarding the provision of sufficient (historical / regular) data for training and validation of the AI model (the objective being to include in the demonstrator the AI ‘damage’ model). A review of commercial sensors to provide high resolution ‘inspection’ data has been undertaken. IoT platform architecture has been developed.

3.5 Use Case 5.5

3.5.1 Planned demonstrators

The use case 5.5 is about smart and adaptive connected solutions across health continuum. The main focus of the use case is to improve operational efficiency by reducing the need of redundant

manual intervention in the operational and non-clinical tasks of a hospital workflow. Multiple technology building blocks developed by the partners are integrated to the dashboard. The integrated dashboard provides an overview of the workflow related to the patient. An IoT based hospital bed management solution is developed, which will provide an overview of hospital beds w.r.t their location and current status. Both these dashboards are adaptive such that the context of the dashboard is set based on the role of the person interacting with the device.

3.5.1.1 Demo A: Integrated dashboard

3.5.1.1.1 General information

The integrated dashboard provides an overview of the workflow in a hospital. Patient information and workflow related information are grouped under multiple tabs. Information in each tab is obtained from various technology building blocks via a REST API. A centralized overview of the patient, asset and workflow status is available in the integrated dashboard.

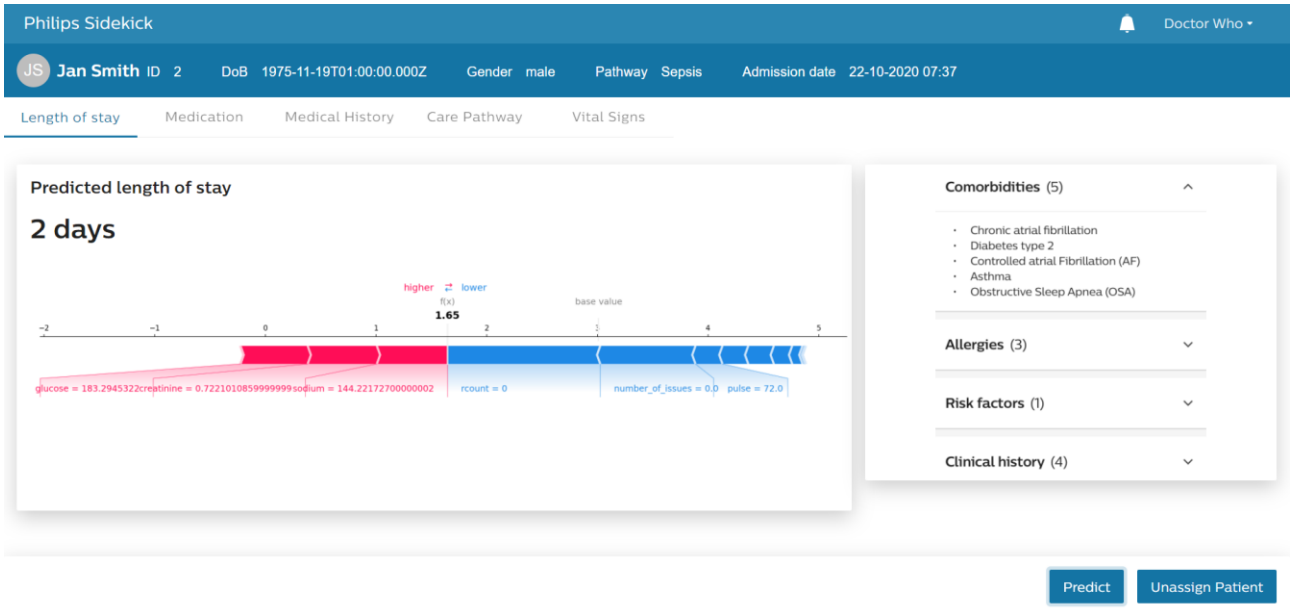


Figure 62 Integrated Dashboard showcasing the integrated TBB: Length of Stay prediction

A use case architecture aligned with the InSecTT HLA is defined, such that integration of the dashboard with multiple TBB is implemented at L2 layer.

3.5.1.1.2 Scenarios demonstrated

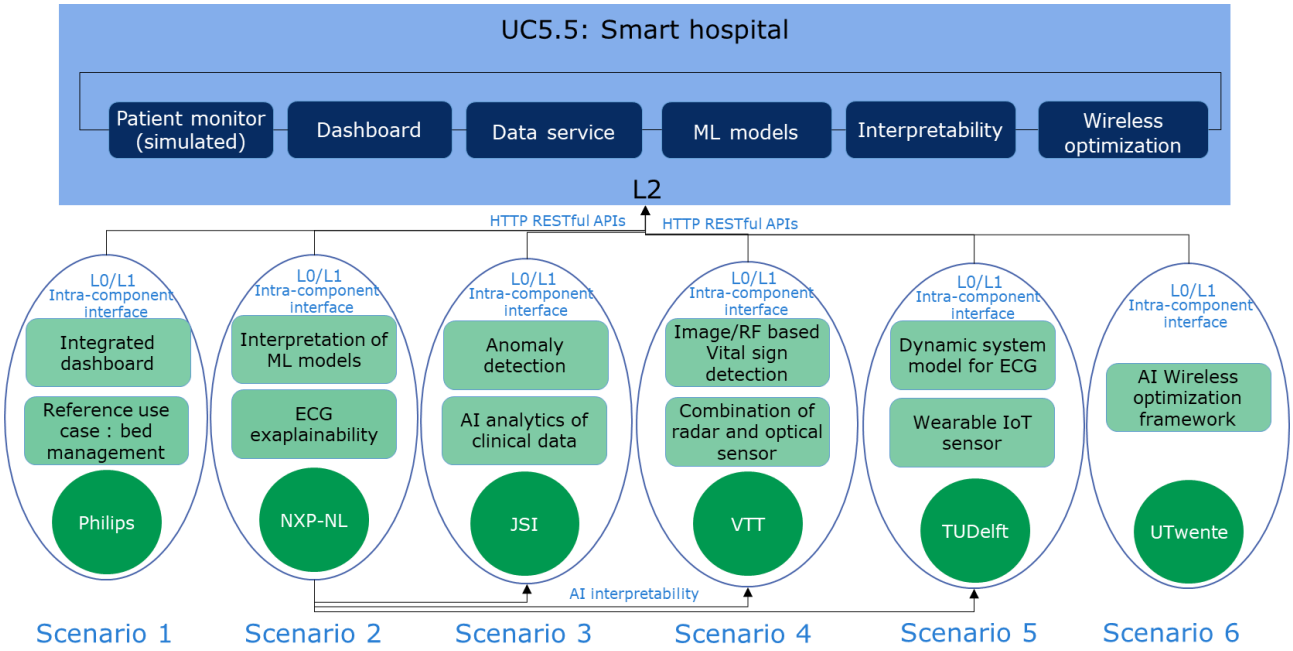


Figure 63 Use case Architecture aligned with InSecTT HLA

In the integrated dashboard, we demonstrate 6 different scenarios. Each scenario is demonstrated using TBBs developed by the use case partners. The scenarios demonstrated include:

- Scenario 1: Reference dashboard implementation with basic functionalities (TBB 2.1, 3.1, 3.3)
- Scenario 2: Length of stay prediction with explainability (TBB 2.1)
- Scenario 3: Anomaly detection in ECG and risk score prediction (TBB 2.1, 2.2)
- Scenario 4: Vital sign prediction using real-time camera and radar (TBB 2.1, 2.2, 2.3)
- Scenario 5: Wearable IoT sensor / dynamic ECG model (TBB 2.1, 2.2)
- Scenario 6: Throughput optimization (TBB 2.2, 3.1, 3.2)

3.5.1.1.3 TBBs demonstrated

Multiple TBB are developed within the use case that are demonstrated under the 6 scenarios as noted in Section 3.5.1.1.2. A common API format is used by all the TBB to demonstrate an integrated dashboard that interfaces with multiple TBBs as listed below:

- TBB 2.1: Explainability offline webserver, XGBoost inference engine, ECG risk assessment, ECG synthesis and learning algorithm, Remote vital signs monitoring
- TBB 2.2: Learning representations, RF based radar for vital sign monitoring, Automated wireless traffic modelling
- TBB 2.3: Camera based vital signs monitoring, Real-time ECG measurement and processing
- TBB 3.1: Distributed wireless optimization, Asset manager
- TBB 3.3: Scannable universal identifiers

Note that each scenario encompasses multiple TBBs which can be demonstrated individually. However, Demo A focusses on the demonstrating the functional integration of all the TBB into one central dashboard.

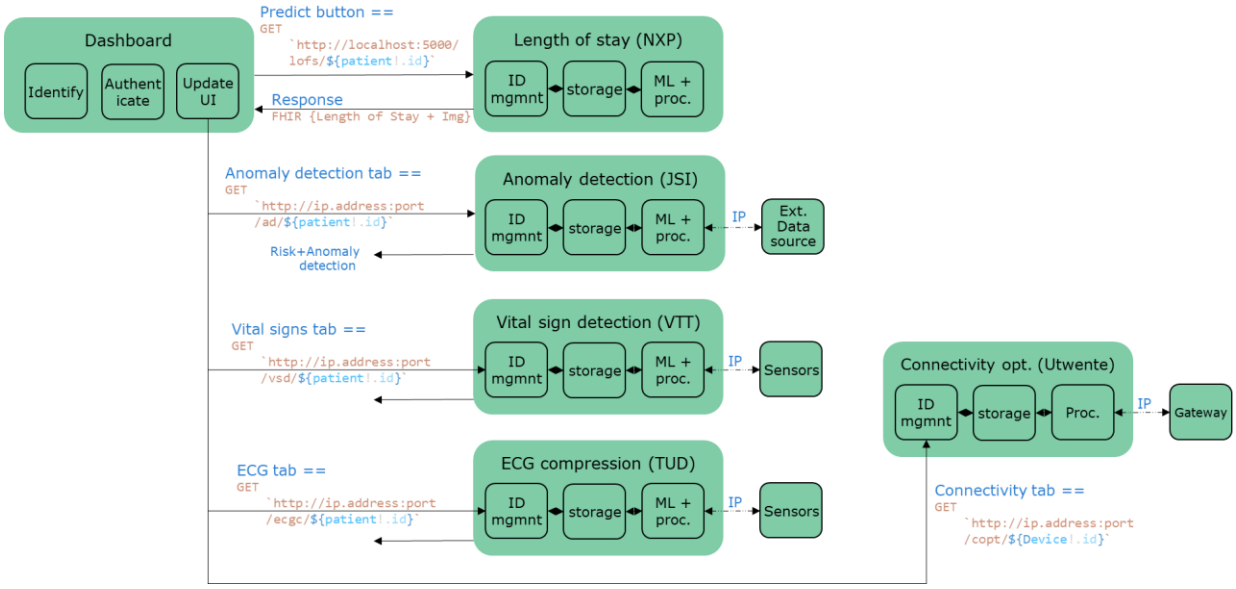


Figure 64 API based integration of 6 different scenarios

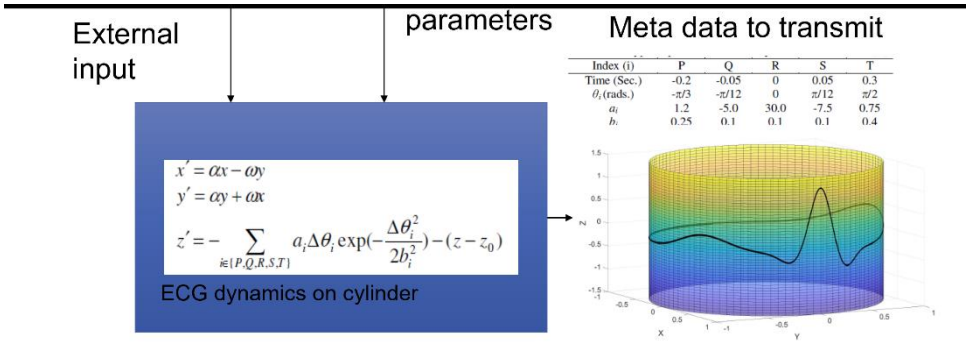


Figure 65 ECG synthesis and learning algorithm

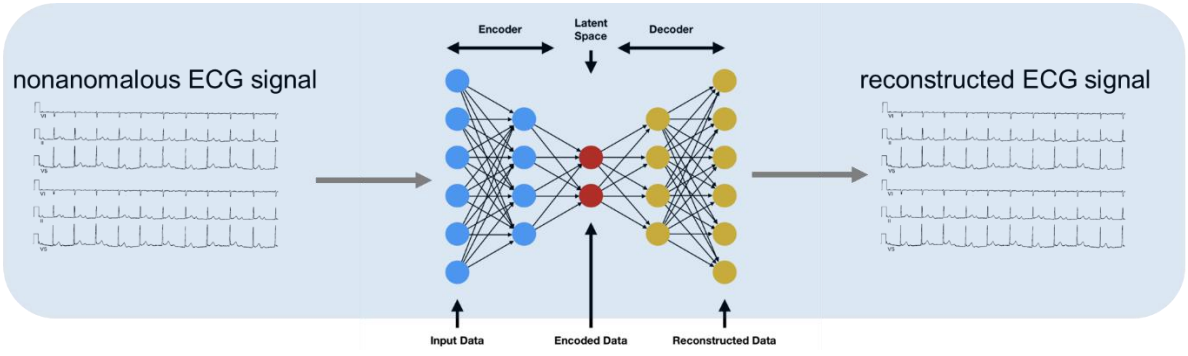


Figure 66 Anomaly detection principle

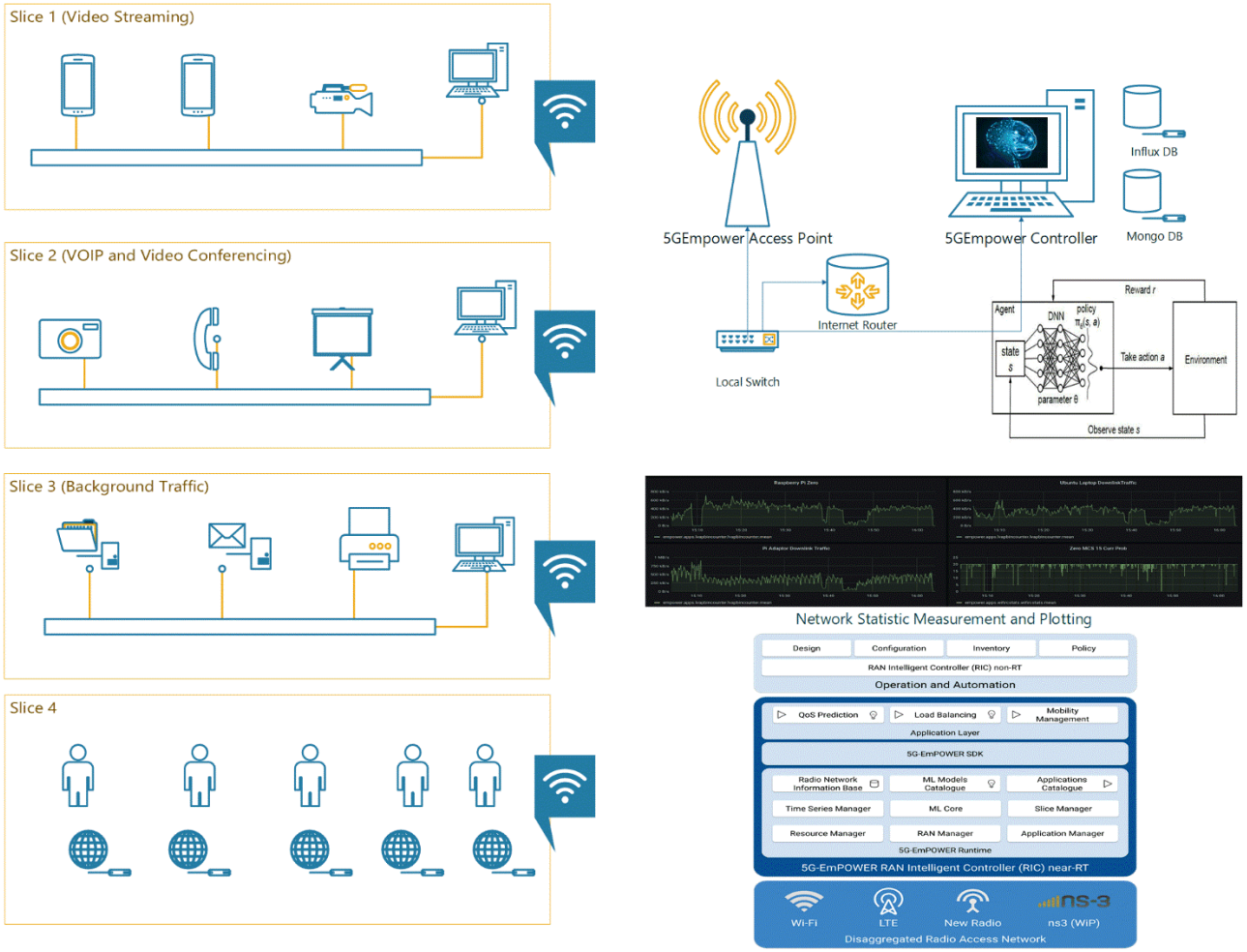


Figure 67 AI based wireless access point control structure

3.5.1.1.4 Progress summary – Y2

Significant progress has been made in two aspects, one in the technological improvements of TBB and two in the integration of TBB into the use case reference implementation. All the partners have contributed to both of these aspects via technology building blocks. A framework for the final demonstrator has been set and most of the TBB are integrated to the use case. Technical improvements made in year 3 will be integrated to this framework demonstrator. In year 3, the webserver is planned to be conditionally extended with a FHIR server as a technology component. Any TBB which produces data for the dashboard will interact using a FHIR API at L2 interface of the InSecTT HLA with the FHIR server. The dashboard will then fetch data or be pushed with the new data from the FHIR server and not directly from a TBB component as demonstrated in year 2.

3.5.1.2 Demo B – Asset manager – IoT based Bed management

3.5.1.2.1 General information

In year 2, the asset manager is fully focussed on bed as an asset. Current bed management systems heavily rely upon manual data entry. Asset manager is aimed at eliminating the need of manual data entry and automating the workflows surrounding the Hospital bed, such as scheduling of surgeries, bed cleaning, patient admission/discharge/transfer etc. The bed manager is implemented end-to-end in terms of microservice architecture, APIs, services, database and IoT device implementation.

As shown in Figure 68, in iteration 2 the bed manager dashboard is developed as a full-fledged solution which is almost compliant to be deployed in an hospital environment.

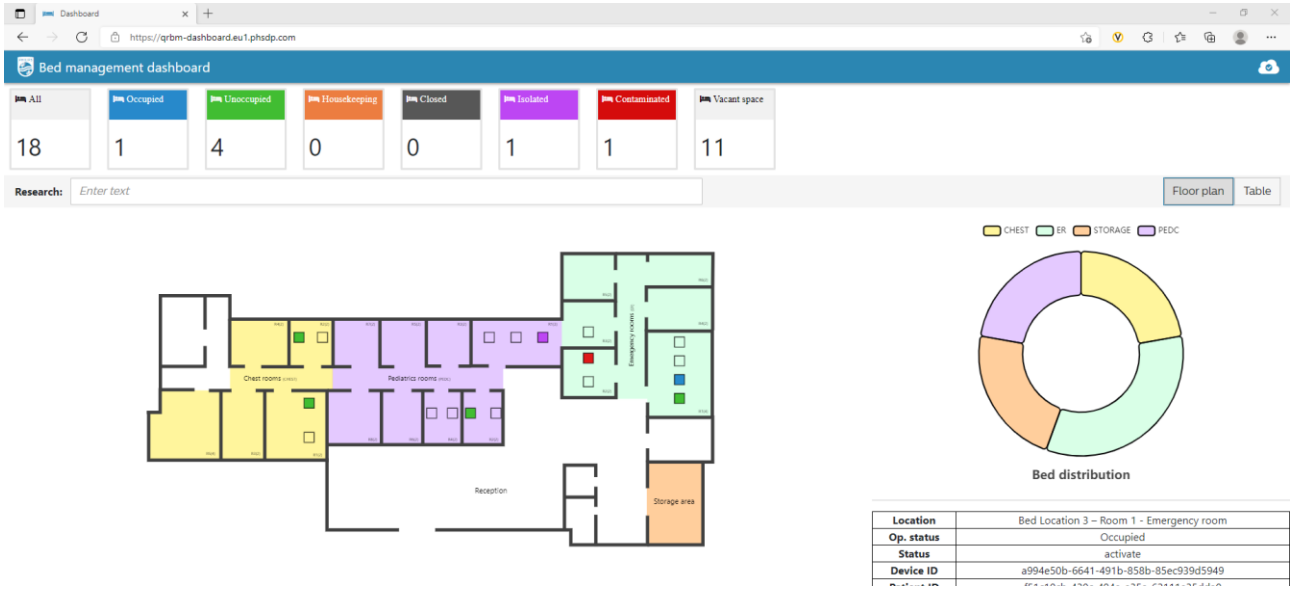


Figure 68 Bed manager dashboard

3.5.1.2.2 Scenarios demonstrated

This is a use case specific scenario demonstrated as reference implementation of an IoT solution in a hospital environment. This scenario will showcase the RESTful implementation of a microservice architecture in bed manager use case and the end-to-end implementation of an IoT solution compliant to be deployed in a healthcare environment

3.5.1.2.3 TBBs demonstrated

Multiple use case specific TBB are demonstrated as a reference implementation of the bed management use case, such as:

i. Location service

ii. Bed Status service

iii. Identity and access management service

iv. Patient data management service

In addition to these use case specific building blocks, TBB3.3: Scannable universal identifiers are demonstrated in this use case. The RFID tags used by the hospital personal are coupled with the IAM service such that their identity can be recognized across multiple hospital information systems.

3.5.1.2.4 Progress summary – Y2

A new reference use case of bed management using IoT components has been demonstrated in an end-to-end fashion. Progress beyond state of the art is clearly visible from the use case implementation w.r.t status detection using IoT sensors, reduction of manual data entry, bed availability as a service which converges role, location, and current status information into future status information of the bed as an asset. Further improvements of the bed management solution in terms of algorithm improvements, design improvements, security and safety of the patient data is planned to be investigated in the third year.

3.6 Use Case 5.6 - Location awareness for improved outcomes and efficient care delivery in healthcare

This use-case is about Location awareness for improved outcomes and efficient care delivery in healthcare.

3.6.1 Planned demonstrators

3.6.1.1 Demo A: Emergency Logistics SErvices for HealthCare

3.6.1.1.1 General information

This demonstrator covers a use-case for a digitized Emergency Logistics Service in case of a mass casualty incident (MCI). Logistics tags provided to the casualties show their triage status and provide their locations to a centralized server with a REST API. A dashboard connected to this server provides a list with the triage and transport status of all casualties and a map of their actual locations as well as the locations of nearby hospitals. A similar setup can be used for tracking of healthcare assets.

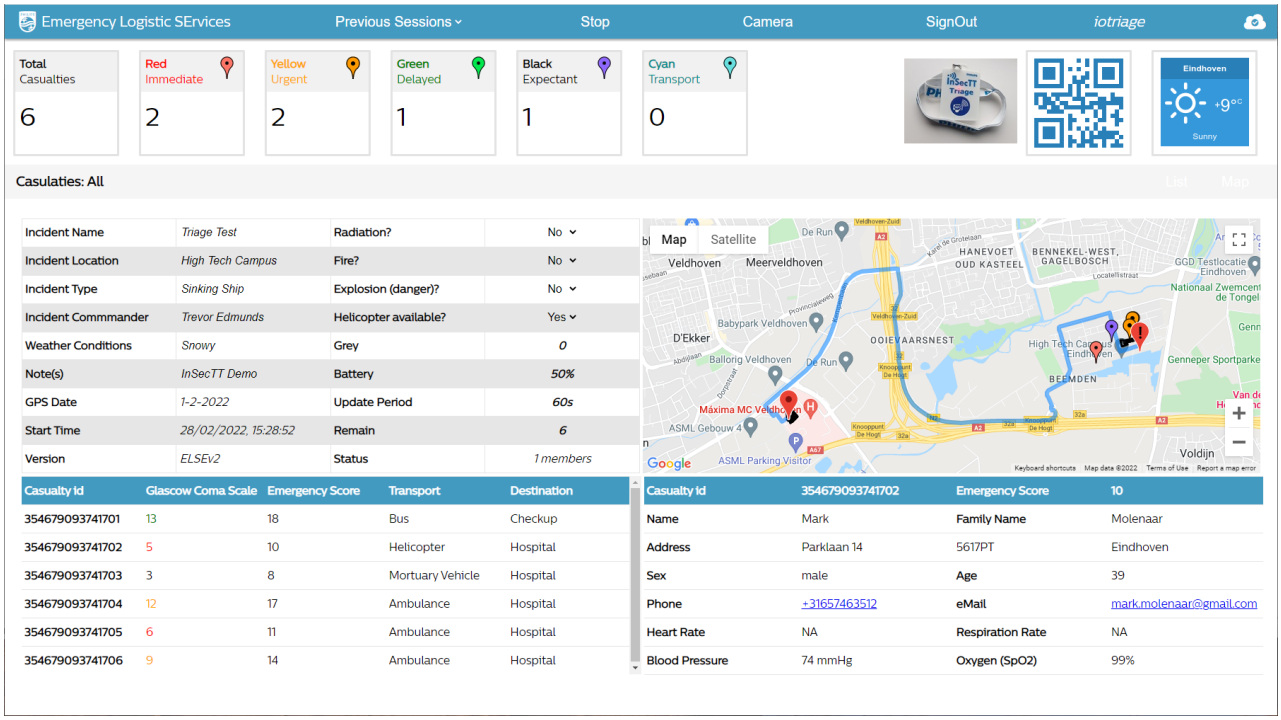


Figure 69 Dashboard providing an overview for an MCI

3.6.1.1.2 Scenarios demonstrated

The scenarios demonstrated include a logistics tag with GPS and cellular communication for outdoor localization as well as an innovative indoor localization method using printed (QR codes) location tags scanned by a smartphone. Another indoor localization method that can be demonstrated with the same setup is using a smartphone application using multimodal deep learning with various types of sensory signals (BLE, inertia movements).

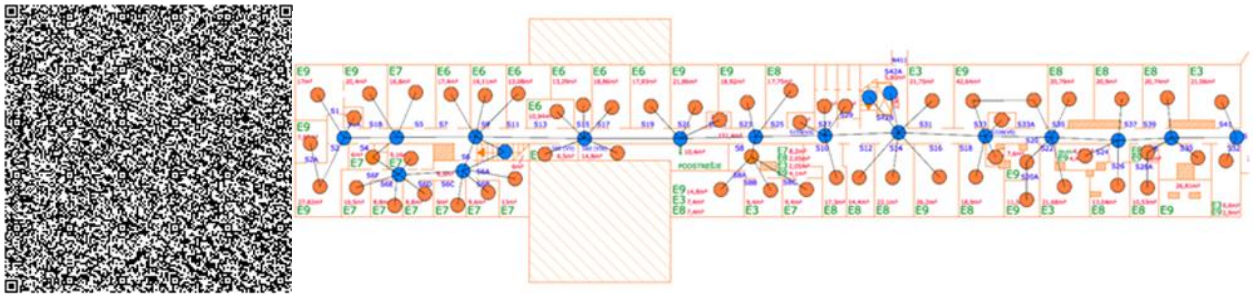


Figure 70 QR master location tag and the extracted floorplan navigation data

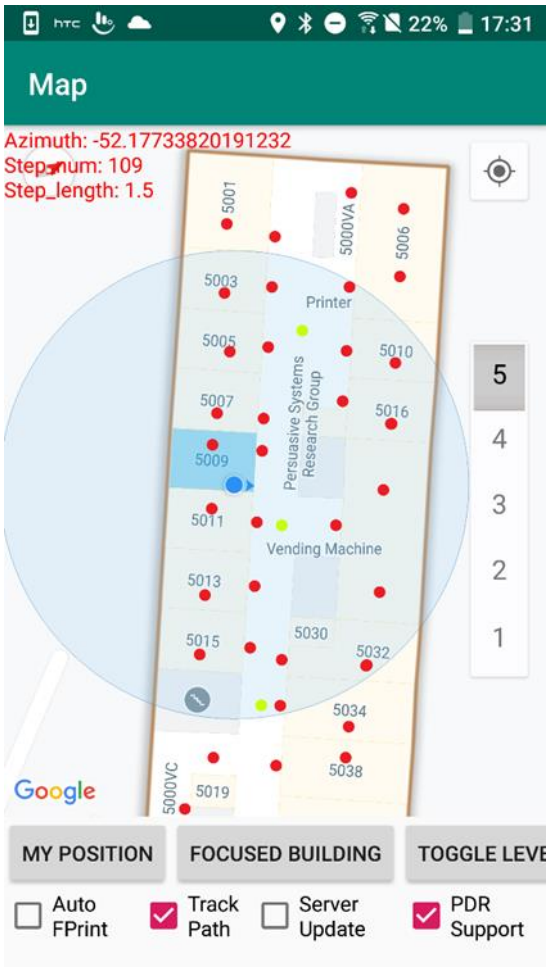


Figure 71 Indoor localization app using multimodal deep learning

3.6.1.1.3 TBBs demonstrated

TBBs included in this demonstrator include components from various partners from both universities and industries:

- An Explainability offline webserver (2.1 and 2.5)
- A smartphone App for indoor localization (2.3)
- An authentication service for IoT devices (3.1)
- Sensory data processing components (3.1)
- Component cellular IoT (3.4)

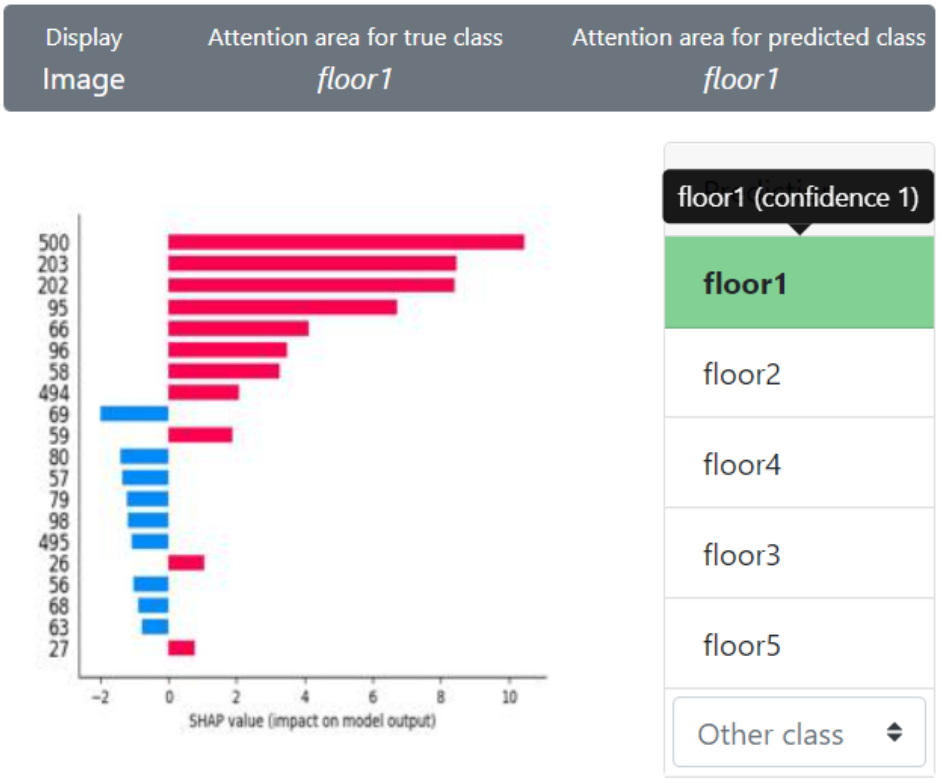


Figure 72 An example of explainable AI/ML is the classification of the most important Wi-Fi stations to determine on which floor a person (using his/her phone's sensors) is in a building

3.6.1.1.4 Progress summary – Y2

Main progress in Y2 has been on the integration of various indoor localization methods using a cloud server with a REST API and standardized geoJSON format for location reporting. Also the dashboard has been extended with support for indoor floorplans and new UI features. The smartphone navigation App for indoor localization using printed tags has been extended with an interface to the location server. The implemented explainability offline webserver provides insights on ML/AI as applied for localization using multimodal deep learning with multiple sensors. Most principle sensory data components (multimodal deep learning, unsupervised representation learning, and raw data encoded) as proposed for this have been implemented.

3.6.1.2 Demo B: Situational awareness in Emergencies

3.6.1.2.1 General information

This demonstrator covers a similar use-case providing situational awareness in case of indoor emergencies. Camera's or PIR sensors with AI processing provide information about occupancy of monitored areas in order to facilitate building evacuation. Occupancy information and optionally other detected characteristics are sent to a centralized server using MQTT. A dashboard based on the IoT ticket platform provides an overview of the actual situation showing the number and flow of people in each area.

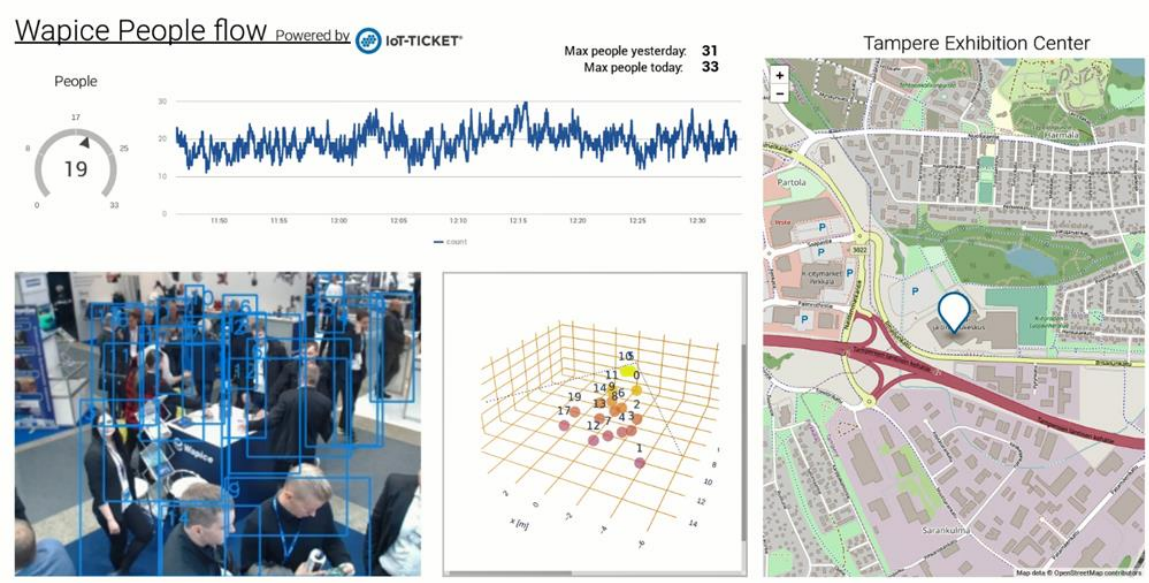


Figure 73 Dashboard for situational awareness

3.6.1.2.2 Scenarios demonstrated

The scenarios demonstrated include video cameras-based detection as well as detection using PIR/Thermopile sensors. Another demo scenario covers both MCI handling and medical asset tracking using GUT's MPS solution.

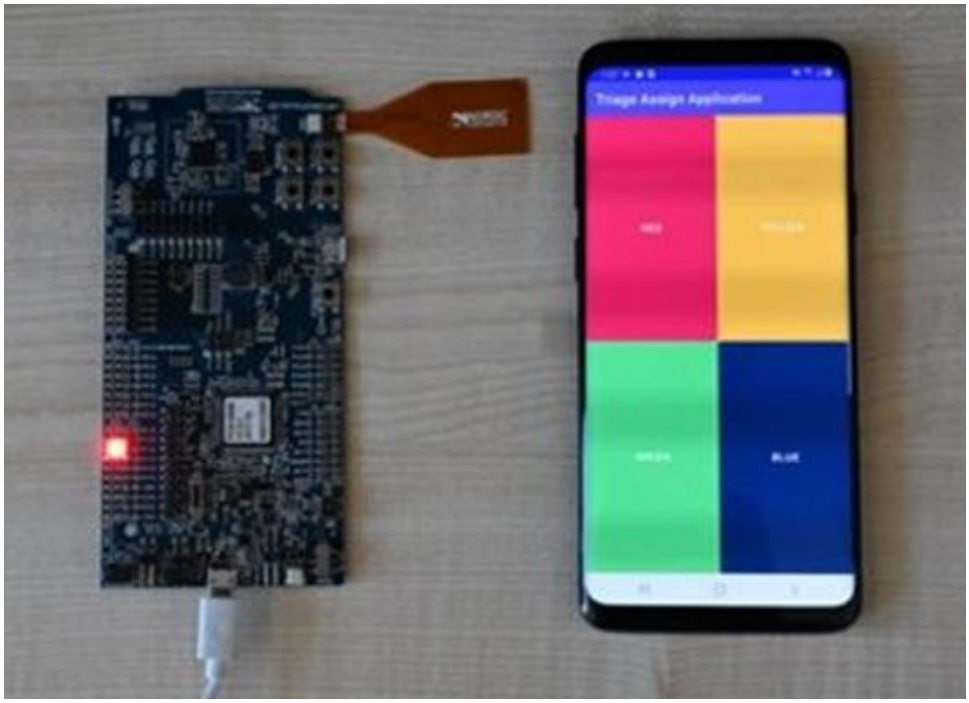


Figure 74 nRF board with Android triage App for MCI triage handling

GUT conducts medical asset tracking using MPS at Copernicus Medical Facility located in Gdansk. Due to agreement with Copernius Facility, phase I of installation has been prosecuted, which takes into account:

- Installation of 6 gateways in Emergency Room

- Installation of custom beacons adjusted to wheelchairs and hospital beds.

Figure 75 Installed Gateways (yellow markers) in Copernicus Medical Facility, which detects medical equipment (red markers)

3.6.1.2.3 TBBs demonstrated

TBBs included in this demonstrator include components from various partners from both universities and industries:

- AI-aided Localization Algorithms in MPS (2.2)
- Localization using PIR sensors (2.3)
- IoT platform with AI support for situational awareness (2.3)
- Component Multimodal Positioning System (3.2)

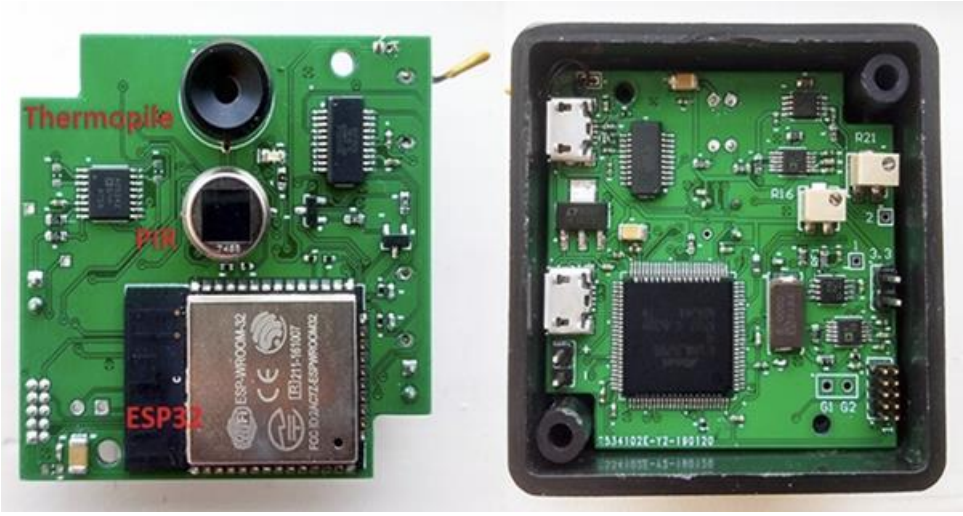


Figure 76 PIR/Thermopile localization module with case

3.6.1.2.4 Progress summary – Y2

Significant progress in Y2 has been on the integration of various location awareness methods using a cloud server with MQTT and standardized geoJSON format for location reporting. The IoT ticket platform has been provided to partners using the MQTT protocol, allowing them to setup their own dashboard. The possibility of utilization of AI to localization algorithms used in MPS is under research. An easy-to-use smartphone application has been developed for the MPS to support the MCI scenario. The hardware for the PIR/Thermopile has been developed and achieves localization of multiple persons with high accuracy.

3.6.1.3 Demo C: UWB system simulation

3.6.1.3.1 General information

This demonstrator shows how state of the art UWB communication schemes access the RF-channel and how likely collisions occur because of the nature of the user MAC protocol. The simulator is based on an event driven python simulator that acts similar to SystemC from a behavioural modelling perspective. (https://github.com/majvan/DSSim/)

The slides will show some use cases and the collision likelihood for some given examples.

Figure 77 Example of multiple devices accessing the same channel

3.6.1.3.2 Scenarios demonstrated

The slides will show different scenarios, how collisions can occur and what different collision resolving strategies will bring from a package error rate perspective.

3.6.1.3.3 TBBs demonstrated

TBBs included in this demonstrator include components from RT critical communication (3.4)

3.6.1.3.4 Progress summary – Y2

In Y2 bugs in the UWB simulator has been fixed and the level of detail has been increased. The simulator is now capable of simulating big networks and multiple different protocols. The simulation of the actual use case 5.6 has just started and some first results are expected in the next months.

3.7 Use Case 5.7 - Intelligent Transportation for Smart Cities

3.7.1 Planned demonstrators

The demonstrators carried out during this second year of the project cover transversally use cases UC5.7 and UC5.8 since the developments and deployment done are complemented ones with each other's. Considering this preliminary issue, the demonstrators described in the following sections can be assumed also for Use Case 5.8 (see section 3.7.1).

The aim of this UC is to continue covering and enhancing the management of areas where rail and automotive domains cross or interact. Once the safety level is guaranteed, it is vital to introduce a

system able to communicate between the railway domain and the road domain not only to manage traffic jams patterns, but multimodal jams.

The key objectives of this task are as follows:

- Increase the efficiency of the rail and automotive domain.
- Provide intelligence to the decision maker in order to control the critical areas.
- Manage traffic jams in shared areas making use of the Artificial Intelligence (AI) and IoT technologies.
- Develop safe and secure wireless communications, Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V), to connect the stakeholders involved.
- Minimize CAPEX (Capital EXPenditure) and OPEX (Operation EXPenditure) costs.
- Improve reliability, safety and security of the current system.

3.7.1.1 Demo A: APS test on real environment

3.7.1.1.1 General information

During three weeks, on three different locations and loco equipment, INDRA has tested and validated a first version of the Adaptable Positioning System (APS) and specific Wireless Sensor Network (WSN) for Train Integrity and Train Length determination, deploying a fully autonomous box containing the APS, the WSN, a 3G/4G equipment and a local Juridical Registration Unit (JRU) federated with a cloud JRU linked to a specific dashboard. These tests have demonstrated the first version of APS making use of Global Positioning System (GPS) and accelerometer fusion based on Machine Learning algorithms and Kalman filters. The main purpose of these tests is to test current developments and to collect new datasets to enrich the AI algorithms and ML modules in order to train them and improve the future developments. These demonstrators has been included on real deployments of national train protection system (Anuncio de Señales y Frenado Automatico - ASFA) validation and verification task for Red de Ancho Métrico (RAM).

3.7.1.1.2 Scenarios demonstrated

INDRA has tested the following scenario in a train with On Board equipment running as it is expected in the INSECTT UC scenarios. The scheme of the demo is shown in Figure 78.

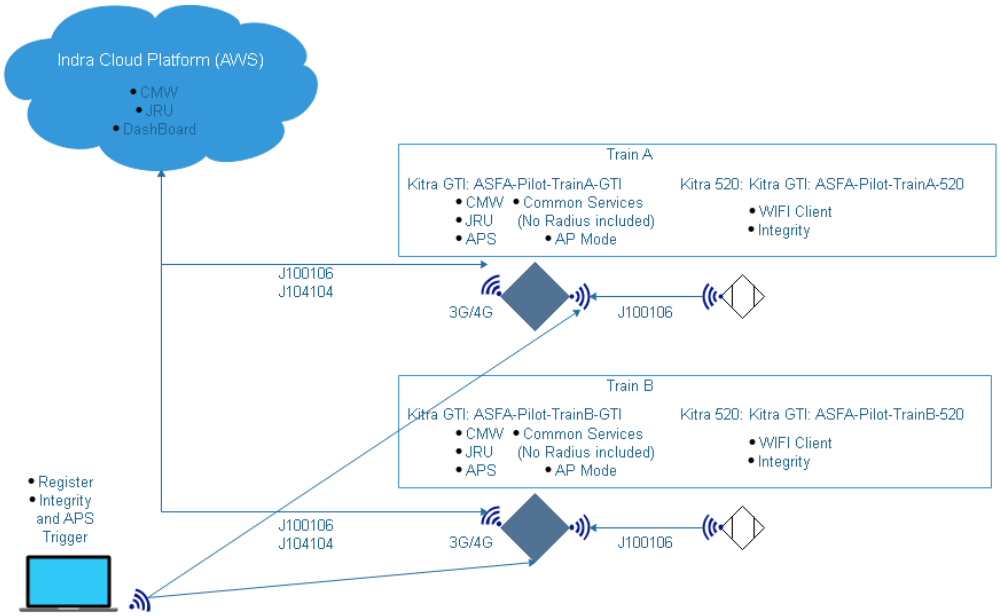


Figure 78 Demonstrator A schema for UC5.7

As it is observed, several entities participated on the demo. There is a computational entity that hosts several services that complements the provision and register of the APS data. Moreover, it provides the mechanisms to connect the accelerometer using the Integrity service, which has the accelerometer data embedded, thought a WiFi client.

The APS reports the positioning data aligned with the Integrity (accelerometer data) and it is treated to be represented in a dashboard at the Cloud.

This experiment has been tested in the following lines:

- Balmaseda – Bilbao: Cabin 3604, leave at 9:20am, arrive at 10:37am.
- Bilbao – Balmaseda: Cabin 3603, leave at 10:39am, arrive at 11:33am.
- Santander – Aranguren. Cabin 2422 leave at 8:54am.
- Aranguren – Santander. Cabin 2472 leave at las 12:41am.
- Cistierna - León, la Asunción Cabina 2616, leave at 8:42, arrive at 10:22 am.
- León, la Asunción - Cistierna Cabina 2615, leave at 10:51, arrive at 13:10 am.

The devices are installed in a box which is covered by the magnetics antennas to provide Global Navigation Satellite System (GNSS) and 3GPP. This implementation can be seen in Figure 79.

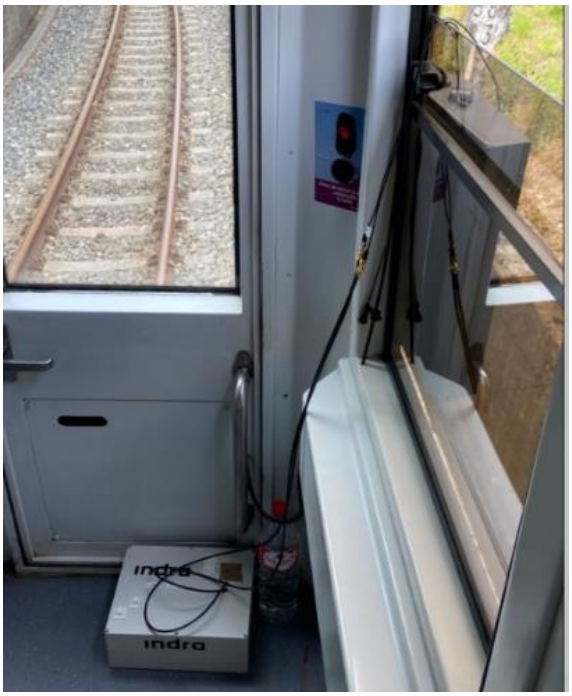


Figure 79 ASFA Installation

The cloud dashboard shows the following data representing the position and the accelerometer in x3 axis as seen in Figure 80.

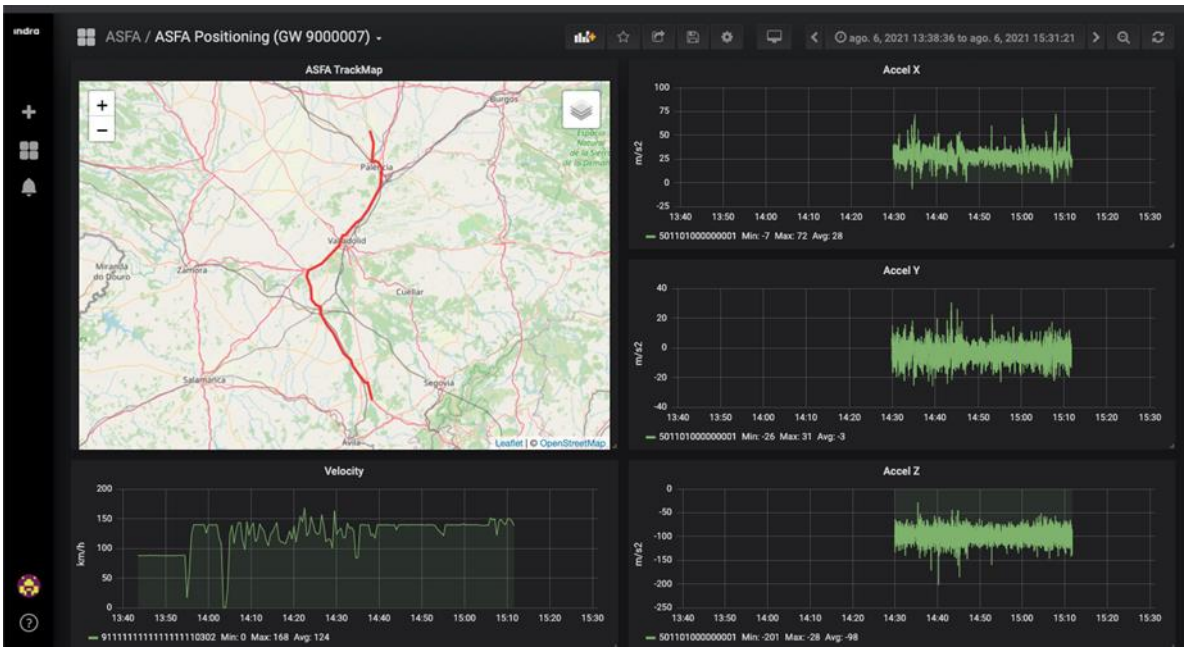


Figure 80 Demo A cloud Dashboard during tests in September 2021

3.7.1.1.3 TBBs demonstrated

Multiple TBBs are demonstrated within this demonstrator. Even they can be demonstrated by themselves, the idea is to integrate them together in order to have a more complete demonstrator in which all the data collected can be seen in a dashboard. The TBBs covered are:

- TBB2.1: AI on application level, explainable and traceable AI

- The accelerometers and the APS data are reported.

- TBB2.2: AI on communication level (AI enhanced wireless transmission, beam forming)
  - A 4G link and a WIFI link are selected for the services.
- TBB3.1: Methodologies, concepts & system solutions for safety and security
  - Train Integrity is covered making use of APS and WSN supported by other relevant systems.
- TBB3.3: Real-time monitoring and response
  - A 4G link and a WIFI link are chosen for the services and a dashboard is implemented to show real-time data recollected.

3.7.1.1.4 Progress summary – Y2

The progress on this area is remarkable as there is an On Board real demonstrator to show the results of the APS and the accelerometers. These are the main inputs for the smart APS. Moreover, the mentioned register permitted recording all the data reported for further training of the AI/ML modules. This dataset is really valuable as it was obtained in a real line, which combined with the previous datasets permits to improve the systems

3.7.1.1 Demo B: Evaluation of multiple AI modules for positioning and communication

3.7.1.1.1 General information

During one week and framed in the X2RAIL4[2] Project of the SHIFT2RAIL[3] program, INDRA has taken advantage of these tests making use of several wagons and two locomotives, to test and validate a second version of the APS and specific AI module for the developed WSN for Train Integrity and Train Length determination on this project. Two complete autonomous boxes were deployed in the train, containing the APS, the WSN, a 3G/4G equipment and a local JRU federated with a cloud JRU linked to a specific dashboard. One of them was located in the locomotive while the other was placed at the end of the composition.

These tests have demonstrated the second version of APS making use of GPS and accelerometer fusion based on Machine Learning algorithms and Kalman filters, as well as Ultra Wideband (UWB) solution for Train Integrity. This demonstrator has been included on real deployments in Loughborough (United Kingdom) in collaboration with the X2RAIL4 project.

3.7.1.1.2 Scenarios demonstrated

The scenario demonstrated focused on:

- Test current developments and collect new datasets to enrich the AI algorithms and ML modules in order to train them and improve the future developments for Train Integrity, Train Length determination and Positioning.

[2] https://rail-research.europa.eu/ The objective of Europe's Rail Joint Undertaking is to deliver a high capacity integrated European railway network by eliminating barriers to interoperability and providing solutions for full integration, covering traffic management, vehicles, infrastructure and services, aiming to achieve faster uptake and deployment of projects and innovations.

[3] https://projects.shift2rail.org/s2r_ip2_n.aspx?p=X2RAIL-4 Advanced signaling and automation system - Completion of activities for enhanced automation systems, train integrity, traffic management evolution and smart object controllers

- A first version of the Adaptable Communication System (ACS) with a single communication bear.

The ASFA test of the previous demo unify all the systems (CMW, JRU, APS, and ACS) in a little device that had limited computational resources. In this case a dedicated hardware with specific networking and dedicated devices for the CMW, JRU, APS and ACS was deployed in the final infrastructure approach to be equipped in the train.

The scenario is developed in the United Kingdom (UK) Grand Central Railway (GCR), a unique heritage railway located in the university town of Loughborough in the East Midlands of England between the cities of Leicester and Nottingham. The line where the tests were carried out is shown in the Figure 81.

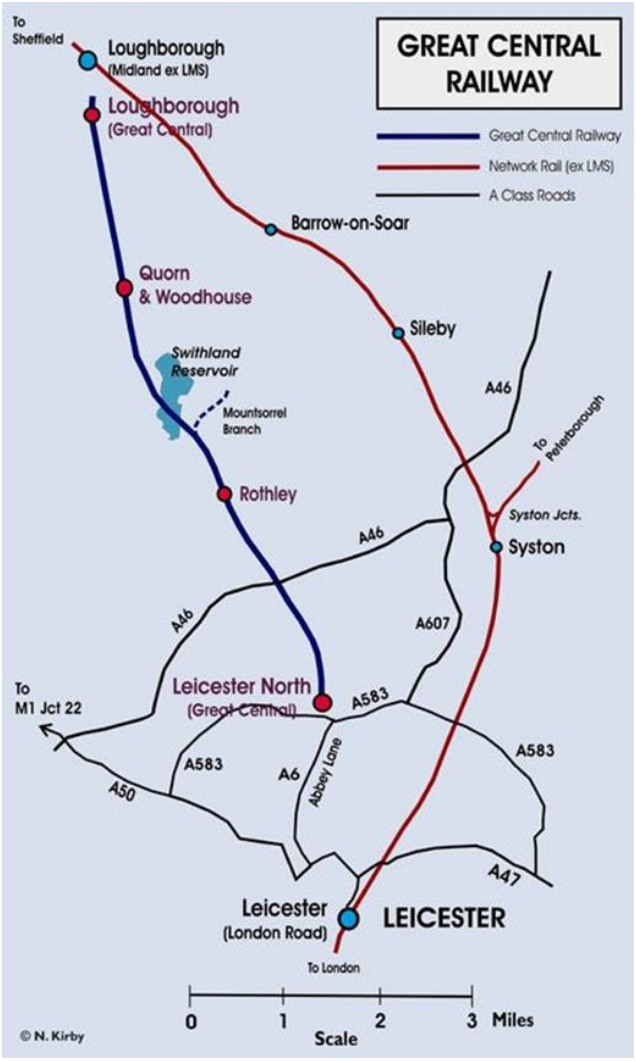


Figure 81 Demonstrator scenario in Loughborough (United Kingdom)

Regarding the ACS, the network infrastructure (OSI1 to 3) that will serve to the complete ACS functionality was tested. A 4G specific device is included to stablish the connection to the Cloud services for both management and for services purposes. The relevant point is that all the installation has been prepared and secured for any ACS implementation. For future implementations, the complete Multiple Access Management Services (MAMS) architecture will be implemented and deployed, the resultant ACS will be connected in a plug and play manner, covering one of the requirements defined in the project. The Figure 82 show the computation unit including all these mentioned functionalities except the WSNs.

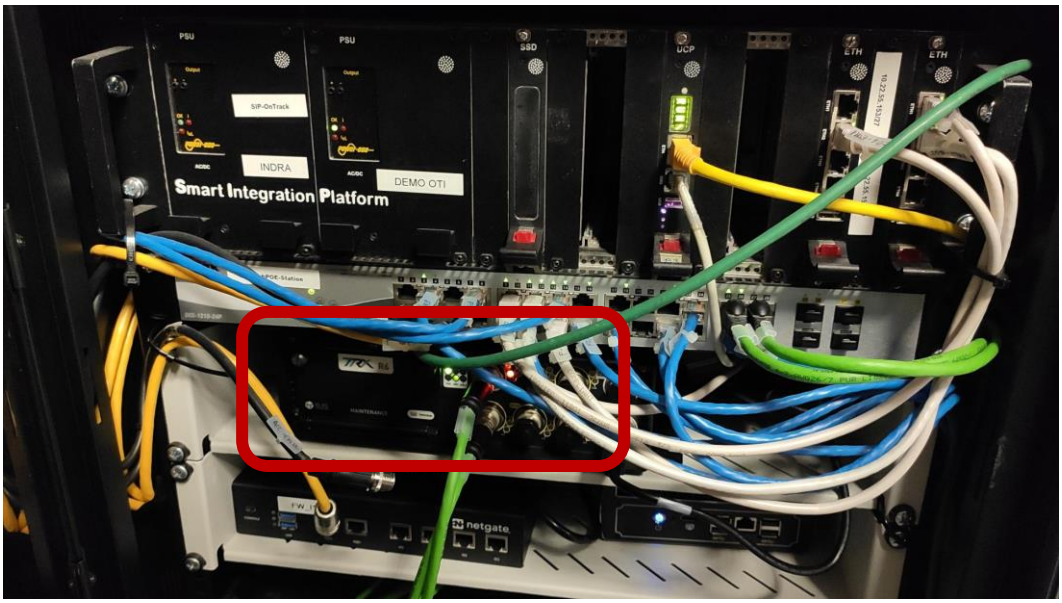


Figure 82 ACS integrated into INDRA's rack

The AI module developed during this year were included in the different nodes of the WSNs, deployed in different wagons to report the data continuously. This module collect GNSS data (GPS and accelerometer) in order to provide a more precise GNSS localization to be used by the Train Integrity system. The tests performed and the new datasets obtained confirmed the improvements on the positioning of each wagon based on AI modules. The two APS boxes deployed in the train were also tested with good results based on the developments made during this year and a huge dataset fussioning both WSN data collected and the two APS was obtained for future developments.

Figure 83 APS box deployed at the end of the train

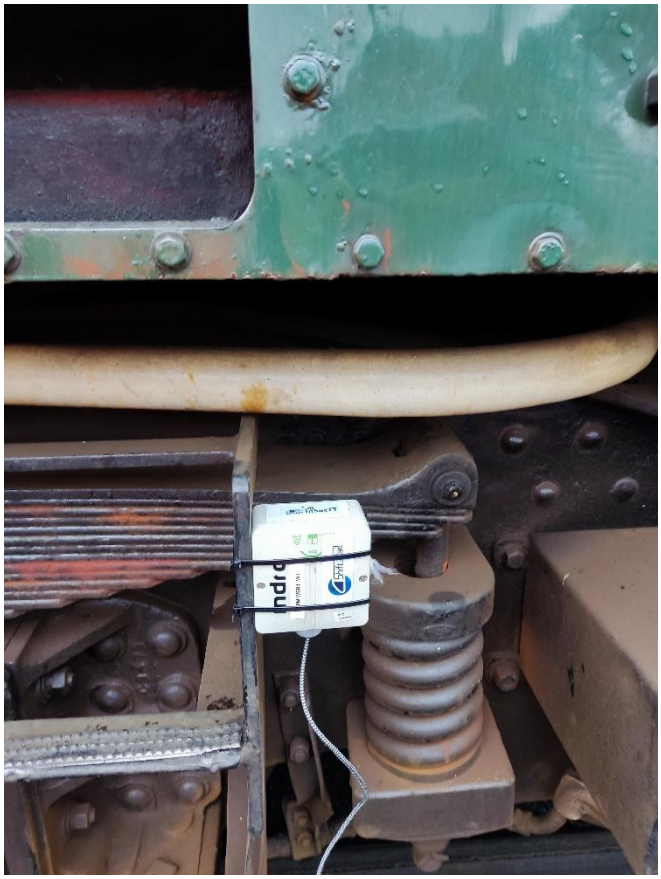


Figure 84 WSN deployed in the train

The data collected can be shown in a cloud dashboard in real-time, so that it can be checked remotely while the tests are being done. Figure 85 shows the data collected during the demonstrator related to INDRA's WSN improvements, which reported GPS positioning and accelerometer. It should be noted that the accuracy of the positioning sensor is quite good related with Figure 85 Dashboard showing INDRA's WSN GPS and accelerometer data reported during the tests.

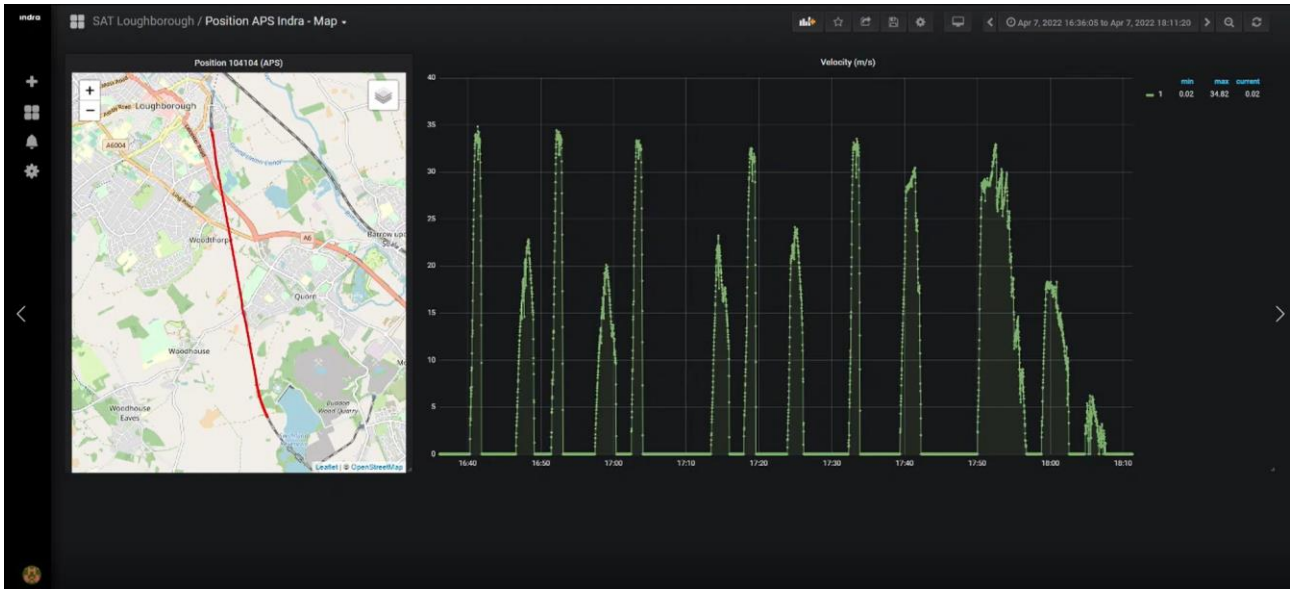


Figure 85 Dashboard showing INDRA's WSN GPS and accelerometer data reported during the tests

The UPM has been working in close cooperation with Indra to test the development progresses of Use Cases included in Tasks 5.7 and 5.8. In this way, the WSN technologies and related implementations have been put into real demonstrator and pilot contexts, highlighting in particular the one carried out in Loughborough.

For that purpose, three different WSN have been deployed in the rolling stock to test in conjunction with Indra the Train Integrity solution, as well as testing the distance measurement technology developed for the proximity solution. Figure 86shows a diagram of the GCR track used to perform the test in dynamic conditions, where different maneuvers during 5 consecutive days were carried out to test the deployed technologies. Figure 86 shows a capture of the locomotive and one of the wagons of the train used during the demonstrator tests.

Figure 86 Part of the train composition, and one of the installed wireless sensor nodes

The WSNs were composed of one coordinator node for every sensor network, 6 wireless sensor nodes in case of the first two networks that measure parameters related to positioning, acceleration and radio communication indicators, and the third network composed of two sensor nodes with the UWB solution for distance measurements between breaking points of the composition, so that the evolution of the distance during such maneuvers can be correctly detected. Figure 87 and Figure 88 show the installation of some of the devices in the real wagons.

Figure 87 Installation of the Wireless Sensor Nodes in the rolling stock

Figure 88 Installation of the UWB solution for proximity detection

The tests were carried out in moving conditions, performing several journey activities to verify the functionalities of the overall system and individual components, including the real measurements of the sensor technologies and the network performance. In fact, uncoupling maneuvers were planned and realized to evaluate in real time how the system can perform integrity break detections, and also the evaluation of the distance measurement capabilities based on UWB.

Apart from the data gathered by the WSNs, an additional GNSS equipment with enhanced precision capabilities was installed in the train to obtain an additional positioning information source that will allow analysing how the development algorithms for positioning refinement can be enhanced with reference location points. Figure 89 shows the installation location of the device on the train locomotive.

Figure 89 Installation of the GNSS equipment for enhanced reference positioning data

3.7.1.1.3 TBBs demonstrated

Multiple TBBs are demonstrated within this demonstrator. Even they can be demonstrated by themselves, the idea is to integrate them together in order to have a more complete demonstrator in which all the data collected can be seen in a dashboard. The TBBs covered are:

- TBB2.1: AI on application level, explainable and traceable AI
    - The WSNs are advanced and deployed in a real scenario. Further advances on the services that are served of them can be tackled after this tests based on the benefits and failures detected.
- TBB2.2: AI on communication level (AI enhanced wireless transmission, beam forming)
    - A 4G link and a WIFI link are selected for the services.
- TBB3.3: Real-time monitoring and response
    - A 4G link and a WIFI link are selected for the services.

3.7.1.1.4 Progress summary – Y2

The progress is aligned with the one indicated into the section 3.7.1.1.4.

3.7.1.2 Demo C: Mobile connection management

3.7.1.2.1 General information

The demonstrator showcases the management of multiple cellular connections in a vehicular onboard gateway. The hardware in use is a Klas Telecom TRX R6 rail certified gateway computer with multiple interfaces, as shown in Figure 90. In particular, it includes separate modems for 5G, 4G and 3G.

Figure 90 TRX R6 gateway computer with multiple modems

When the gateway is in a moving vehicle, the coverage and signal quality for each of the modems changes continuously, and machine learning algorithms assess the quality of each link and switch connections accordingly.

3.7.1.2.2 Scenarios demonstrated

In the demonstrator, it is intended to show the real-time management of the connections. The gateway is placed in a moving vehicle and it can be demonstrated through a web front end how the estimated link quality changes and connections are changed accordingly.

3.7.1.2.3 TBBs demonstrated

The demonstrator includes components from TBBs 2.2, 3.3 and 3.4:

- Connection management platform
- Machine learning methods for data rate estimation
- Machine learning methods for interface decision

3.7.1.2.4 Progress summary – Y2

The current status of the demonstrator is that data rate estimation and interface selection methods have been implemented in a virtual machine on the TRX R6, and a front end has been developed as well to display estimated data rates and interface decisions as shown in Figure 91, thereby creating a working setup that can be updated with improved estimation and decision methods as the project progresses.

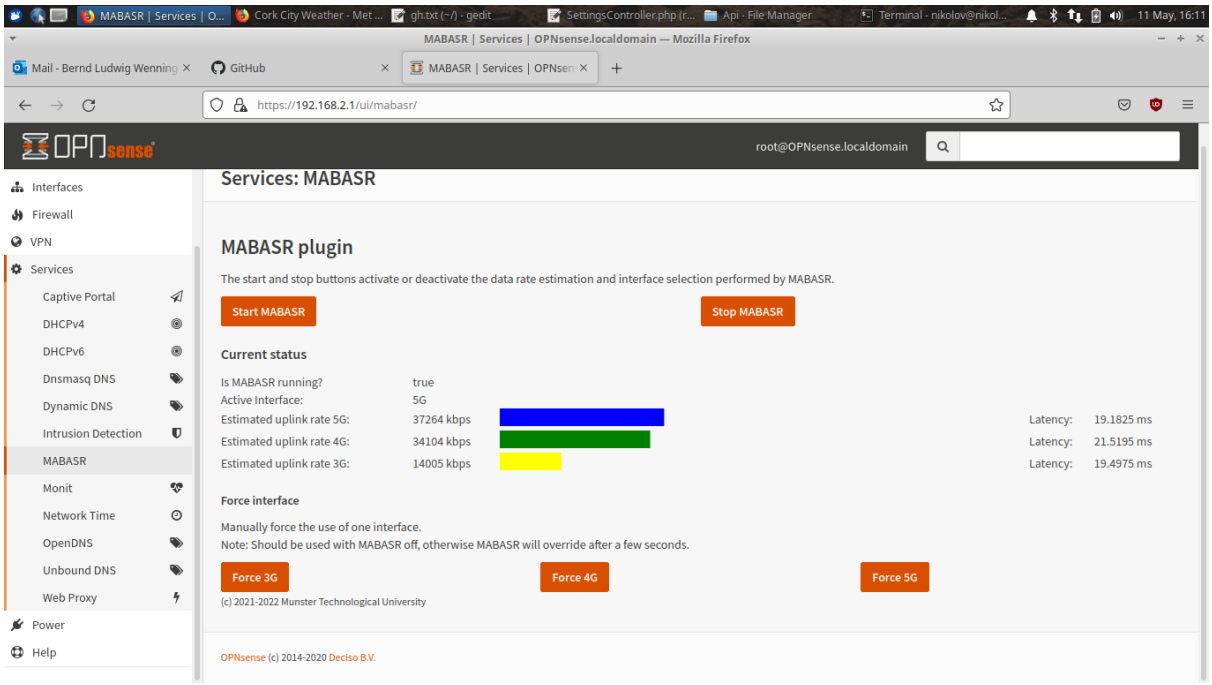


Figure 91 Graphical front end for connection management

3.8 Use Case 5.8 - Intelligent Automation Services for Smart Transportation

3.8.1 Planned demonstrators

This use case aims to improve upon the services defined in SCOTT[4] 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 a system able to make the different railway vehicles to communicate in a 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.

[4] Based on SCOTT Project results focus on Smart Train Composition Coupling. (see SCOTT D19.5 "*Smart Train Composition Coupling System Demonstrator Report*")

- 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 a distributed and collaborative environment.
- Providing an improving 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.

The demonstrators carried out for this UC during the second year of the project are contained in the demonstrators defined in section 3.7.1. Due to the nature of the use cases, these demonstrators group the developments of both tasks.

3.8.1.1 Demo A: APS test on real environment

3.8.1.1.1 General information

Refer to section 3.7.1.1.1.

3.8.1.1.2 Scenarios demonstrated

Refer to section 3.7.1.1.2

3.8.1.1.3 TBBs demonstrated

Multiple TBBs are demonstrated within this demonstrator. Even they can be demonstrated by themselves, the idea is to integrate them together in order to have a more complete demonstrator in which all the data collected can be seen in a dashboard. The TBBs demonstrated are aligned and complemented with the ones defined for UC5.7. The TBBs covered are:

- TBB2.1: AI on application level, explainable and traceable AI
    - The accelerometers and the APS data are reported.
- TBB2.2: AI on communication level (AI enhanced wireless transmission, beam forming)
    - A 4G link and a WIFI link are selected for the services.
- TBB2.3: AI on computational level (on device and edge)
- TBB3.1: Methodologies, concepts & system solutions for safety and security
    - Train Integrity is covered making use of APS and WSN supported by other relevant systems.
- TBB3.3: Real-time monitoring and response
    - A 4G link and a WIFI link are chosen for the services and a dashboard is implemented to show real-time data recollected.

3.8.1.1.4 Progress summary – Y2

Refer to section 3.7.1.1.4.

3.8.1.2 Demo B: Evaluation of multiple AI modules for positioning and communication

3.8.1.2.1 General information

Refer to section 3.7.1.2.1

3.8.1.2.2 Scenarios demonstrated

Refer to section 3.7.1.2.2.

3.8.1.2.3 TBBs demonstrated

Refer to section 3.8.1.1.3

3.8.1.2.4 Progress summary – Y2

Refer to section 3.7.1.2.4.

3.9 Use Case 5.9 - Cybersecurity in Manufacturing

3.9.1 Planned demonstrators

This Use Case focuses on developing secure, reliable, and trustable wired/wireless services for supporting the operation of industrial robots in manufacturing. It aims to:

- Develop new services and solutions with IoT-enabled components to increase connectivity and integrate these reliable and trustable solutions into legacy technologies and systems.
- Increase wireless security with AI-enhanced mechanisms against failures and cyberattacks for resilient wireless communication.
- Data collection in real-time and anomaly detection on the edge for fast response and forwarding to the cloud for comprehensive data analysis

One of the main objectives of this Use Case is to develop AI-based algorithms for detecting failures in wireless communication. Manipulation of data, attacks, and data loss can cause functional damage to the system or environment. Therefore, real-time monitoring of the state and edge computing is essential to detect and generate a fast response to the system. For this purpose,

- AI-based jamming detection and identification algorithm will be developed for wireless OPC-UA communication.
- AI-based anomaly detection mechanisms will be developed for failures and packet drops on wireless links and
- Data collection, continuous monitoring, and storage solutions for the wireless link data will be developed with the assessment of data in reliability and availability manners.

Another objective in this task would be providing authentication and network security between IoT devices. It is crucial to secure the integrity of the devices concerning incoming attacks. Devices must be protected from both network and device attacks. In this regard, we can separate the use case objectives into two main parts. These can be considered as:

- Network Security: Certification-based authentication mechanism will make sure that the edge device will only be allowed to connect and communicate with each other after authorization. After that, all network traffic will be encrypted.

- Device Security: There will be some AI-based detection routines that will be able to detect anomalies happening on the edge device. These will be comprised of both network and

3.9.1.1 Demo A

3.9.1.1.1 General information

The "Cybersecurity in Manufacturing" Use Case seeks to create a reliable, secure, and safe communication layer for both wired and wireless industrial networks as part of a manufacturing network infrastructure. Both use case scenarios in this demonstrator aims to show the effects of various kinds of cyberattacks on industrial equipment widely used in manufacturing environments. Because it is essential to maintain the continuity of production processes in plants, implementing a demonstration for the use case in real manufacturing conditions will not be viable. As a result, in Atolye 4.0's laboratory, which develops Arçelik's own Advanced Robotics and Automation applications in Arçelik's production facilities, a simulation of the production environment will be set up. Atolye 4.0 already has a basic model of production line infrastructure, which is controlled by a PLC and includes industrial robots, RFID receivers, and barcode readers that are all connected via an industrial network.

3.9.1.1.2 Scenarios demonstrated

Scenario 1:

Demonstrator A consists of an edge device and industrial robot that the edge device is tasked with continuously sending commands to robot for different positions and trajectories over wireless OPC-UA network. In this scenario, applications installed in both robot controller and edge device, will collect wireless link quality data, monitor and evaluates the data traffic between robot and edge device in real time and detects anomalies created by a series of simulated cyberattack such as wireless jamming.

Scenario 2:

In this scenario, an assembly operation, based on product information, is simulated with an industrial controller, edge device, remote I/O module and barcode reader. All equipment in this demonstrator will be communicating with each other via OPC-UA network. This particular scenario is about detecting anomalies happening over network communication. In order to eliminate the authorization and authentication type of attacks, NuRD will develop a certification-based authentication mechanism which will ensure the security of the IoT devices is not compromised by incoming network threats with respect to unknown entities inside the network. Furthermore, encrypting the communication over network after authentication ensures that it will not be intercepted by outside parties. On top of the proposed authentication system, AI-based authentication detection algorithms will be created to detect anomalies occurring within the network of the device. Several predetermined attack simulation cases (e.g., denial of service, scanning, brute force, man in the middle) will be used for the training data of the proposed AI solution.

3.9.1.1.3 TBBs demonstrated

The work is related to TBB 2.1, 2.2, 2.3, 2.4, 2.5, 3.1, 3.2 and 3.5.

3.9.1.1.4 Progress summary – Y2

Y2 concentrated on the technical aspects of the use case scenarios and their physical execution. ARCELIK worked with the partners on the development and integration of essential hardware and software for test scenarios as part of this effort. To the existing industrial robot and its communication infrastructure, wireless communication infrastructure has been introduced. In addition, physical

components for a wired communication system were purchased. On the other hand, the software development process for both scenarios is currently in progress. In Y3, the main focus will be on enhancing demonstration preparation and finalizing the demonstrator's physical implementation. The software development phase will be completed in particular. By organizing a visit of partners to the demo site, the initial deployment of the test scenarios will be done with their participation and contribution. In collaboration with partners, necessary improvements and modifications will be planned and implemented. Throughout the process, updates and next steps will be presented and discussed with partners at regular meetings.

3.9.1.1 Demo B

3.9.1.1.1 General information

MarUn constructed a local demonstrator in VeNIT Lab to execute jamming attacks using SDR on a Raspberry PI device. The components of the demonstrator infrastructure are:

- OPC-UA Server (Edge Device)
    - To replicate the server on manufacturing plant
- OPC-UA Client – Robot
    - Robot built by servomotors and a Raspberry PI as a controller
- USRP 2932 Radio – Spot Jamming
    - To transmit jamming signals
- LabVIEW application – packet transmission
    - To generate jamming attacks
- Jamming detection application
    - Running on both edge device and robot controller
- Leeds – indication of evaluation results
    - To indicate different Wi-Fi channels

MarUn tests the communication between robot controller and the edge device under different jamming conditions and on the normal condition to collect data and evaluate it to detect and identify anomalies and jamming. The data is transferred to the monitoring platform and can be monitored by the developed tool to inspect visually. Additionally, MarUn had meetings with Arçelik to create jamming scenarios to evaluate the effects of jamming on the operational environment.

3.9.1.1.2 Scenarios demonstrated

MarUn is investigating different jamming attacks and sources to identify those attacks. It is needed to find and create the jamming scenarios and data collection from a controlled experiment. We are currently working on developing the jamming scenarios using NodeMCU and USRP 2932 to build more accurate and effective jamming. We have currently implemented three different jamming scenarios:

Deauthentication Attack Description

a. An open-source ESP8266 deauther is used to send the jamming scenario.

b. When this jamming attack is conducted, it is observed that the devices under attack can't reconnect and continuously disconnect whenever the frame is sent by the deauther.

c. The network parameters collected also show an increase in TCP packets' retransmission compared to the normal operation.

d. Although, it is rather easy to detect this attack with significant increase in de-authentication and disassociation packets in monitoring mode.

Spot Jamming Attack Description

In the scenario, the robot is asking the server for different instructions. During the normal scenario, the server sends an acknowledgment and the asked instruction. When the communicating Wi-Fi channel is jammed, the delay of the application increases significantly. The robot keeps on asking the server for the same instruction until it gets the acknowledgment and the instruction in a constant loop. In the production line, it slows down the process and may lead to a decrease in production rate.

3.9.1.1.3 TBBs demonstrated

The work is related to TBB 2.1, 2.2, 2.3, and 3.2

3.9.1.1.4 Progress summary – Y2

MarUn had several meetings with Arçelik and had demo site visits to discuss the integration plan and detailing of the test scenarios. Firstly, the test cases are created on a small scale using the infrastructure and devices at VeNIT Lab. The experiments are conducted and initial tests are executed to evaluate the preliminary results.

MarUn is contributing to Scenario 1 with many components to detect jamming and monitor the network between the robot controller and the edge device. The Quality Monitoring Platform is a centralized platform that is used to store, collect and provide data in the built IoT system. It is developed in a containerized approach to be able to tackle compatibility issues between devices and planned to be deployed in the edge device in Atölye 4.0 Lab. The application for collecting the data, executing performance tests and jamming detection is going to be deployed on the robot controller. They are sending the data via the APIs that exist within the platform when the network is available and temporarily storing the data otherwise. The monitoring tool that is being used to visualize the data and provide warnings/alerts is either going to be deployed on the edge device or a device that shares the same network as the robot controller. The tool is developed as a web interface and visualizes the data and alerts from many devices via the APIs on the platform. The tool also conducts connectivity tests depending on the state changes of the devices.

3.10 Use Case 5.10 - Robust resources management for construction large infrastructure

3.10.1 Planned demonstrators

The global objective of the use case is to improve productivity and safety in construction sites of large civil infrastructure projects, e.g. construction of tunnels, railways, highways, etc. This shall be achieved by enabling cost-efficient and non-intrusive tracking of workers and machinery, combined with a fixed distributed monitoring infrastructure deployed on site, specifically designed for the case of tunnel construction projects.

Through the intelligent processing of all these data sources, the use case aims to provide insight into the real progress of construction tasks and of the resources employed to complete them. This shall support early identification of deviations or delays from the original project plan.

Furthermore, the data collected shall support identification and management of safety risks, and the implementation of optimized maintenance strategies to prevent losses of productivity associated to unexpected machinery breakdowns.

One of the main challenges of this use case lies in the complexity of the construction domain from the point of view of technology deployment, as it involves dynamic spaces and layouts that evolve in parallel with the progress of the project, and that usually have very harsh conditions for the deployment and operation of electronic equipment and wireless communications.

3.10.1.1 Demo A

3.10.1.1.1 General information

The first demonstrator of the use case is located in one of the construction projects of ACCIONA in Norway, where two tunnels, 2.3 and 2.7 kilometres long respectively, are being excavated with conventional methods (Drill & Blast).

This demonstrator shall support the validation of most of the use case planned components and functionalities, including:

- Tracking of workers and of machinery within the tunnel.
- Automated identification and measurement of the tasks executed within each tunnel construction cycle.
- Automated identification and management of safety risks, e.g. detection of intruders, detection of dangerous gases, evacuation management, etc.

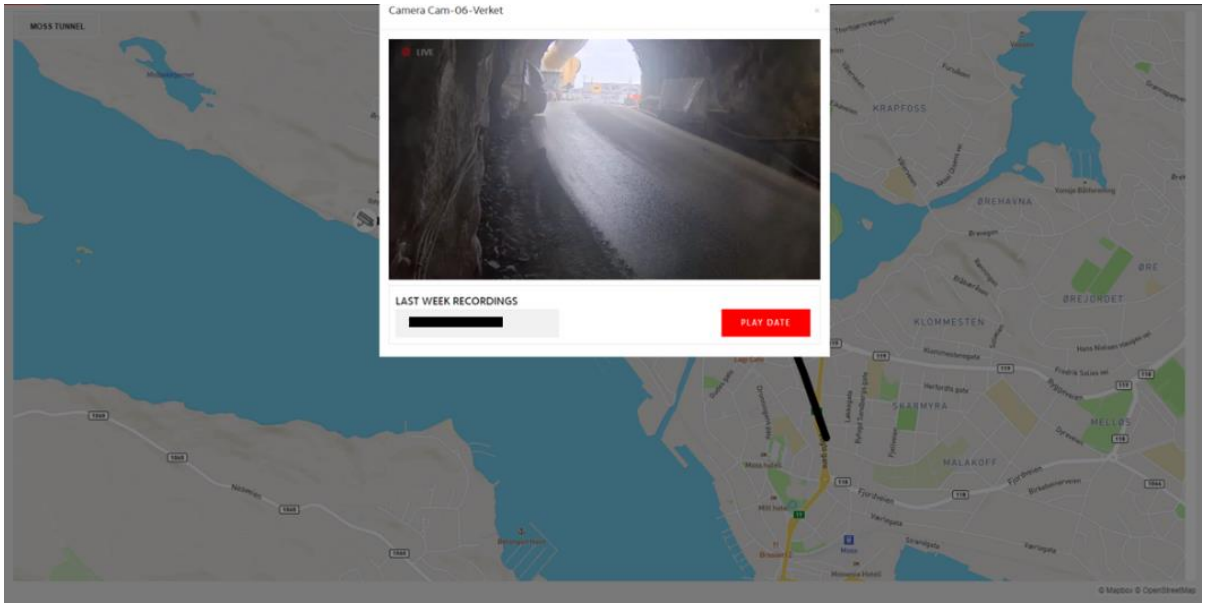


Figure 92 Demo site - ACCIONA

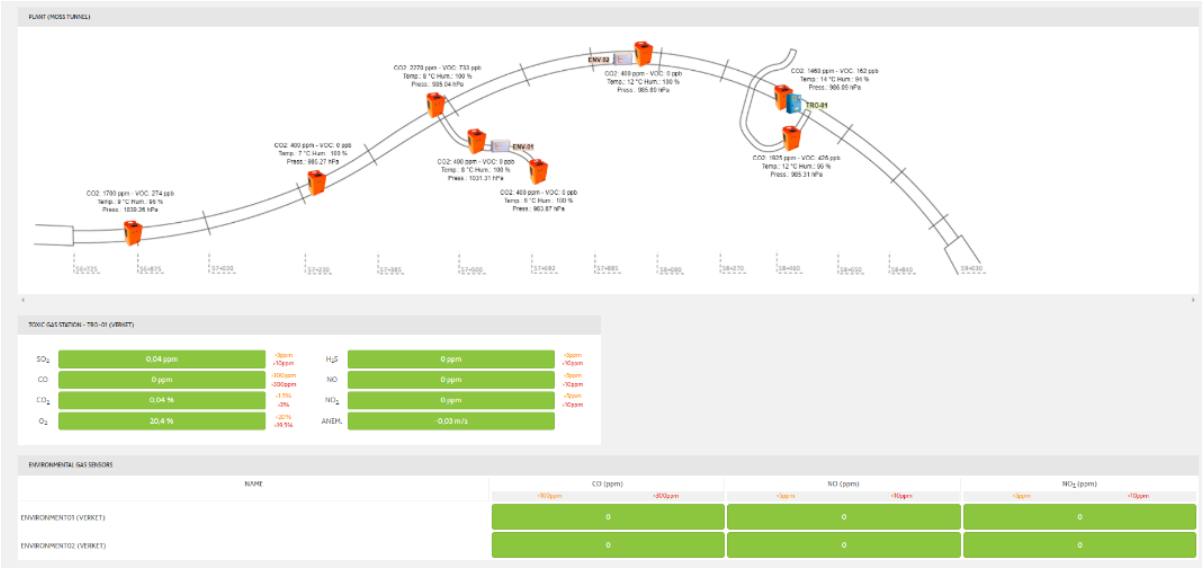


Figure 93 Machinery tracking

3.10.1.1.2 Scenarios demonstrated

Three scenarios are planned for validation in this demonstrator:

- **Tracking of tasks during the construction of large infrastructures:** the validation of this scenario in this demonstrator is done through the automated identification and measurement of the tasks carried out in each construction cycle of the tunnel (Drilling, Blasting, Mucking & Scaling, Rock Support, and Grouting). This is done through the intelligent processing of different data sources: worker tracking, machinery tracking, and electricity consumption profile.

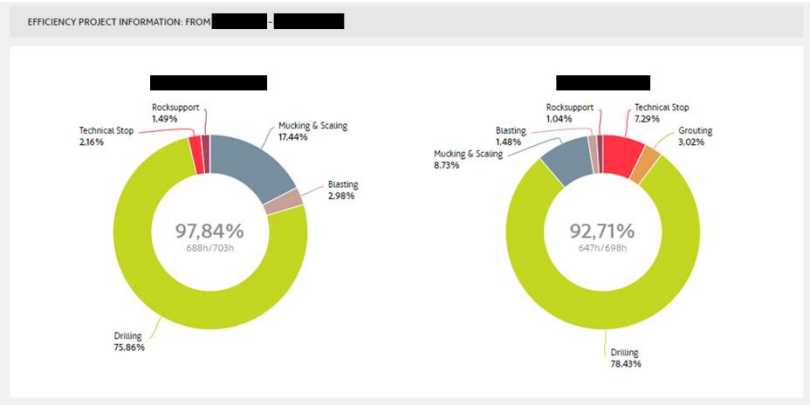


Figure 94 UC5.10 demo data analysis

- **Management of safety incidents:** this scenario is validated in this demonstrator through the identification and management of different safety risks/incidents, e.g. detection of intruders (detecting presence of people and/or machines without authorization to be within the tunnel).
- **Ensuring continuity of machinery operations:** this scenario is validated in this demonstrator through the collection of machinery tracking data that shall support the implementation of more optimized maintenance plans to avoid unexpected breakdowns.

3.10.1.1.3 TBBs demonstrated

The following Technical Building Blocks are planned to be validated in this demonstrator:

TBB3.3: For this TBB, this demonstrator contributes to the validation of the tracking of workers, the tracking of machinery, and the distributed monitoring infrastructure.

TBB2.1: For this TBB, the demonstrator helps to validate the automated identification and measurement of tunnel construction tasks, the identification and management of safety risks and incidents, and the implementation of optimized management strategies.

3.10.1.1.4 Progress summary – Y2

After the second year of the project, the demonstrator already implements a combined analysis of machinery tracking, worker tracking and distributed monitoring data to identify and measure the construction cycles of the conventional tunnels of the demonstrator, including the tasks within each construction cycle.

On the other hand, from the point of view of supporting safety risks/incidents identification and management, the demonstrator already implements the processing of machinery tracking and worker tracking data to analyse presence in each tunnel section. Furthermore, through the combined use of machinery tracking, worker tracking and distributed monitoring data, the demonstrator already implements the functionality for intrusion detection and management.

For the last year of the project, the demonstrator will focus on the following activities:

- Further improvement of precision in construction tasks identification and their correlation with the project plan to assess real progress of the project.
- Enable management of additional safety incidents or risks, e.g., detection of fire, too close distance between workers and machinery, etc.
- Implementation of predictive maintenance strategies for machinery.

3.10.1.2 Demo B

3.10.1.2.1 General information

This demonstrator was started during the 2nd year of InSecTT project, and it is located in another tunnel construction site of ACCIONA in Spain. Unlike the Demo A, this tunnel, 12.6 kilometers long, is built using a Tunnel Boring Machine (TBM).

Figure 95 ACCIONA Demo A test site

This project uses special electric train engines to transport the workers that need to enter or exit the tunnel. The use of this means of transport, combined with the considerable length of the tunnel, makes it necessary to have a proper tracking system to control what workers and engines are inside the tunnel and within which tunnel section they are located.

Figure 96 Electric trains

Thus, the main purpose of the demonstrator is to use it as a testbed for an alternative use of the worker and machinery tracking modules, that shall help to validate them in a different environment, while at the same time implementing hardware and software updates to achieve better robustness and reliability in terms of detection and of transmission of data.

3.10.1.2.2 Scenarios demonstrated

This demonstrator is focused on the scenario for detection and management of safety risks and incidents. The objective is to demonstrate the use of worker tracking and machinery tracking data to detect location of workers and wagons within specific sections of the tunnel.

3.10.1.2.3 TBBs demonstrated

The following Technical Building Blocks are planned to be validated in this demonstrator:

TBB3.3: For this TBB, this demonstrator contributes to the validation of an improved hardware and software for tracking of workers and tracking of machinery, in the context of transportation of workers with electric trains.

TBB2.1: For this TBB, the demonstrator helps to validate the identification and management of safety risks and incidents by monitoring the location of workers and trains within the tunnel.

3.10.1.2.4 Progress summary – Y2

During the second year of the project, works have focused on the preparation of the testbed for validating the new hardware and software for tracking of workers and trains within the tunnel. This testbed consists mainly of the following components:

- WiFi Access Points connected to the wired communications backbone already existing within the tunnel.
- BLE PoE Readers installed in the same locations as the Wi-Fi APs, as well as at the entrance of the tunnel and at the location of the TBM.
- BLE Wi-Fi Readers installed within the wagons for detecting the tags of the workers travelling inside the wagons and for transmitting those data to the Wi-Fi APs.

Once deployed, the aim for the last year of the project is to continue with the validation activities in order to improve the robustness and precision of the tracking system.

Figure 97 Wireless hardware used for demo purposes

3.11 Use Case 5.11 - Smart Airport

3.11.1 Planned demonstrators

3.11.1.1 Demo A

3.11.1.1.1 General information

In order to create the joined Asset Tracking Demonstrator, GUT and CISC have developed systems capable of estimating the objects localization based on RF signals. These two subsystems are partially independent, as they are meant to localize different classes of objects, however they are designed in such way that will be integrated within one overall, centralized system, which will merge the data from both sources, manage them and visualize the results through a common dashboard. The final demonstrator consists of two distinct sites, however the Y2 demonstrator will focus only on the CISC's part and their site.

CISC established an own demonstrator at their lab localized in Klagenfurt. Three gates have been built up to demonstrate the airport luggage detection. For this, 3 new developed RFID Reader devices have been mounted to the gates.

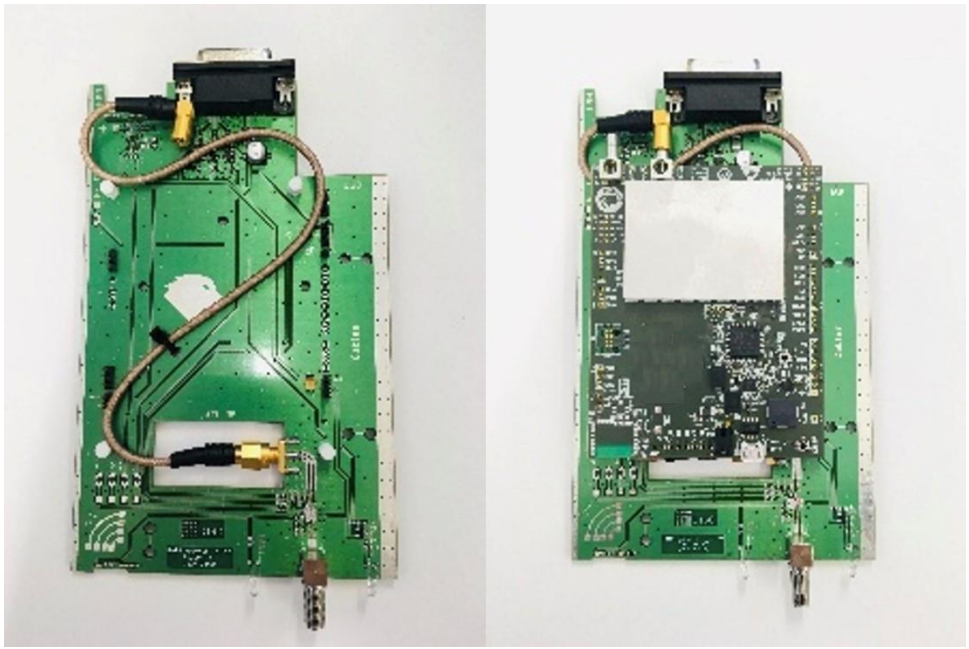


Figure 98 RFID Reader Prototype

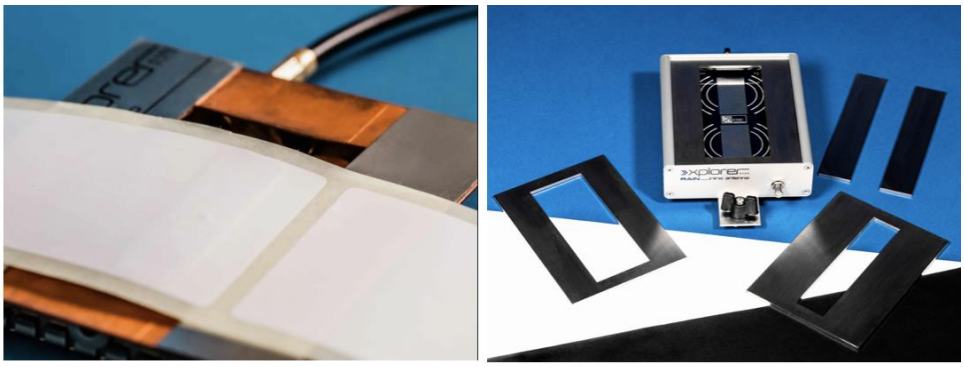


Figure 99 RFID Reader incl. test antenna

Moreover, the reader device is a tag performance test tool that additionally allows encoding of RAIN RFID tags and labels. The device is setup that it supports up to 100k UPH for testing the essential points of the tags resonance behaviour, which means 5 power/frequency pairs on EPC and reporting EPC and TID of each tag additional to the pass/fail result. The device consists of 2 elements, the reader device itself and a test antenna (Fig. 6). The results of the RFID measurements are collected in a cloud-based backend and visualized on a dashboard. The included performance test support mode supports reference tag measurements to easily extract performance criteria for the tags. These parameters are then used to define criteria for the high-volume quality assurance testing (Fig.7). Through the message broker we will connect to the backend of GUT to analyse the data together.

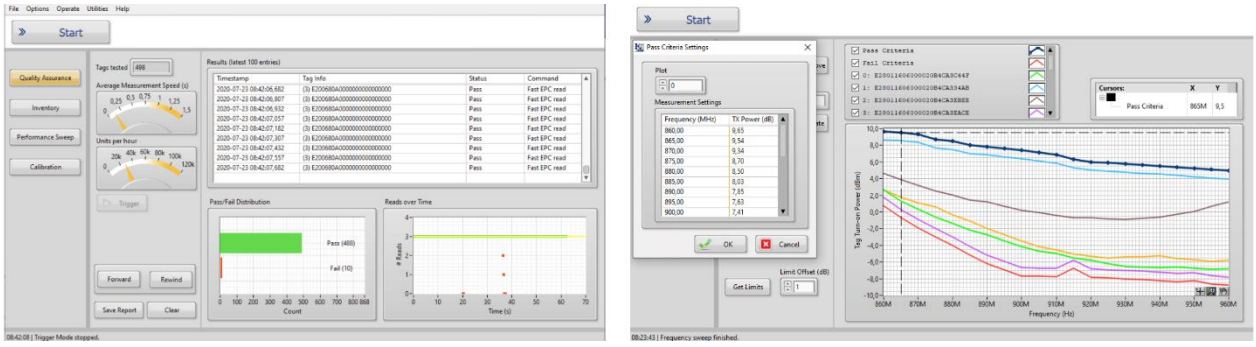


Figure 100 RFID analytics dashboard

The results of localization coming from both subsystems will be visualized through a mutual platform.

3.11.1.1.2 Scenarios demonstrated

This is meant to be a cross-scenario demonstrator, as it combines the features offered by the solutions proposed in Scenario 1: Asset tracking and Scenario 3: Securing mission-critical applications in airport, however this demonstrator will focus mostly on the Scenario 1's part. Y2 demonstrator will present the operation of CISC's RFID system and how it may be integrated with GUT's platform.

3.11.1.1.3 TBBs demonstrated

In the described demonstrator the main building block involved is TBB3.2 - "Using RF signals for the purpose of localization".

3.11.1.1.4 Progress summary – Y2

The subsystems contained in this demonstrator are already developed and will be ready for the integration until the end of Y2. Y3 will be dedicated to the integration purposes. Both GUT campus facility and CISC's lab are already prepared for conducting the final demonstrator.

3.11.1.2 Demo B

3.11.1.2.1 General information

GUT has developed an inspection robot, capable of performing an inspection and detecting anomalies along the airport boundaries following a predetermined route. Operator will have access to the image from both standard and infrared cameras. In addition to the vision-based solutions, the robot will be equipped with a radar in order to detect moving objects, even in poor vision conditions. However, such setup, which will be demonstrated, is just an example of what may be included within the robot's payload. In general, the system should be considered as two parts: the mobile platform and the flexible payload, which may be customized according to each use case, requirements and environment.

Figure 101 Mobile platform equipped with the sensor's payload

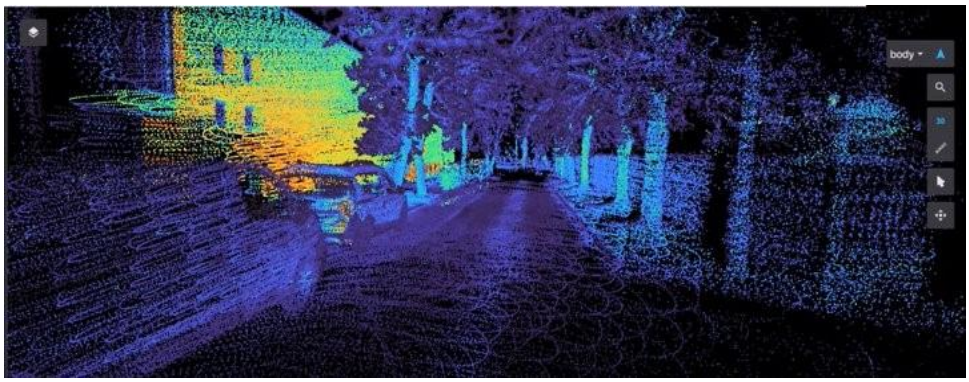


Figure 102 Lidar image obtained during inspection

In order to demonstrate the aforementioned features, the scenario will consist of robot following a given route and will face several obstacles/intruders what will result in specific alarms being triggered through the operator's application. The Kaitotek's Network Monitoring Application will keep track of the network performance during robot's operation.

The Y2 demonstrator is planned to present the working robot and present its perception of the environment based on sensors values contained within the payload. The network performance will be monitored using Kaitotek's application, as it will be integrated as a part of the demonstrator.

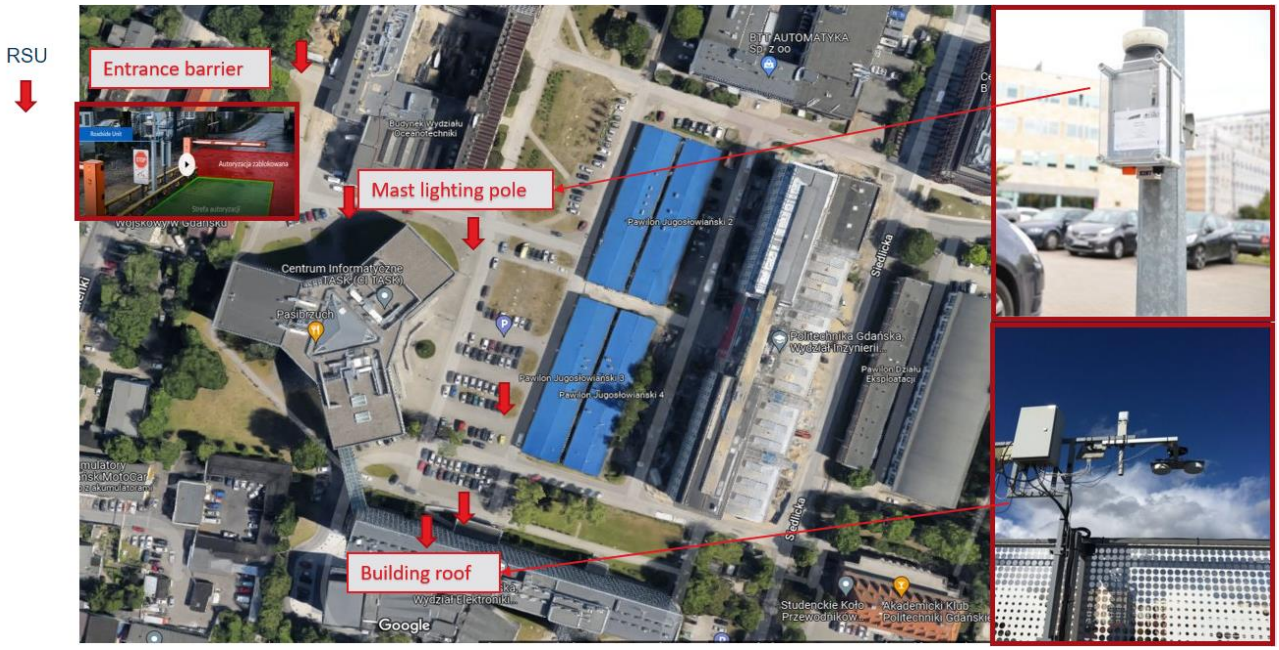


Figure 103 GUT campus demo site

3.11.1.2.2 Scenarios demonstrated

This is another demonstrator meant to be a cross-scenario one, as it combines the features offered by the solutions proposed in Scenario 2: Autonomous inspection and Scenario 3: Securing mission-critical applications in airport.

3.11.1.2.3 TBBs demonstrated

The building blocks involved in this demonstrator are:

- TBB3.2 - "Dependable Wireless Communication"
- TBB3.3 - "Passive QoS/QoE measurement"
- TBB3.4 - "Network quality situation awareness"

3.11.1.2.4 Progress summary – Y2

Most of the features have already been implemented, tested and are ready for the integration, which will be the main activity during Y3. The GUT campus facility is already prepared for conducting the demonstrator. Y2 demonstrator will present the integration of the GUT's robot and Kaitotek's network monitoring application. Y3 will focus on further development of the data fusion algorithms within the payload and will also be dedicated to integration the robot with V2X platform.

3.11.1.3 Demo C

3.11.1.3.1 General information

Marmara University provides a smart intersection testbed in Dragos Campus, İstanbul, in order to test and integrate the solutions developed by the partners. The infrastructure consists of a Road-side Unit (RSU), an edge processing device, traffic lights, and a traffic light controller. There will also be one or multiple cameras to demonstrate object detection applications. It is a T-intersection along with crosswalks and bicycle roads. The demonstrator enables VRU/vehicle detection applications at the edge and V2X communication and applications with real radios to be tested.

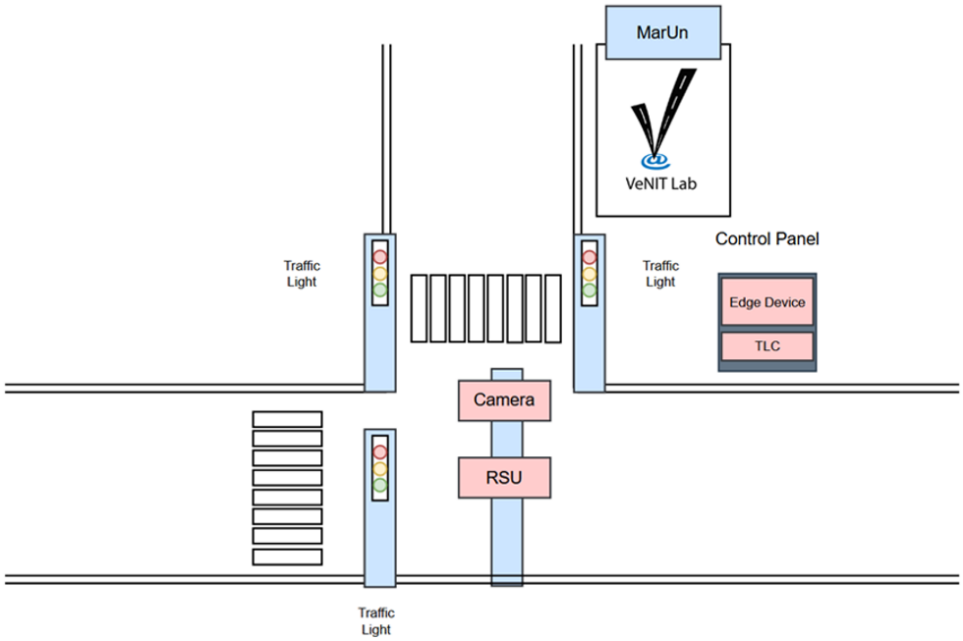


Figure 104 Layout for Marmara University Smart Intersection Testbed

Pavotek provides edge cluster server for the demonstrator. Pavotek's Servers has multiple GPU&CPU System on Module, which will be mounted to the control panel having network and electric connectivity. Marmara University will deploy and test the detection application in Pavotek edge server system on modules.

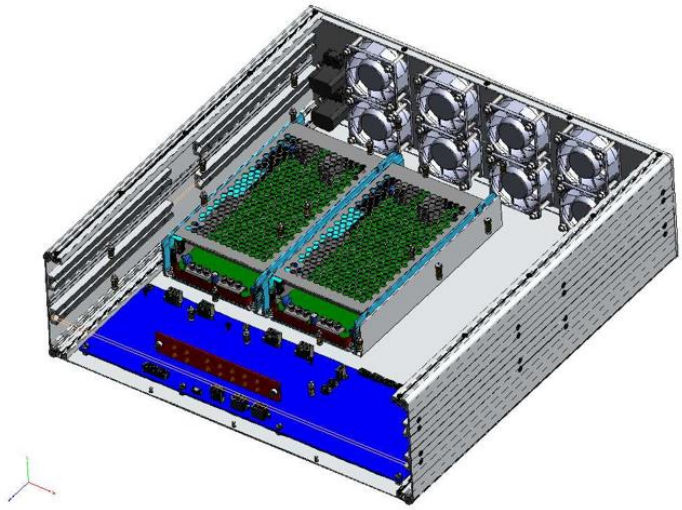


Figure 105 Pavotek Edge Cluster Server

ViF provides the V2X communication platform as OBU in the vehicles. The communication platform is called vehicle CAPTAIN (**vehicle c**ommunic**a**tion **p**latform **t**o **a**nyth**in**g) and will host an ITSG5 interface and a 5G interface. For the use case the focus is on the use of the ITSG5 capable communication. The vehicle CAPTAIN is shown in Fig. 14 with an equipped ITSG5 module.

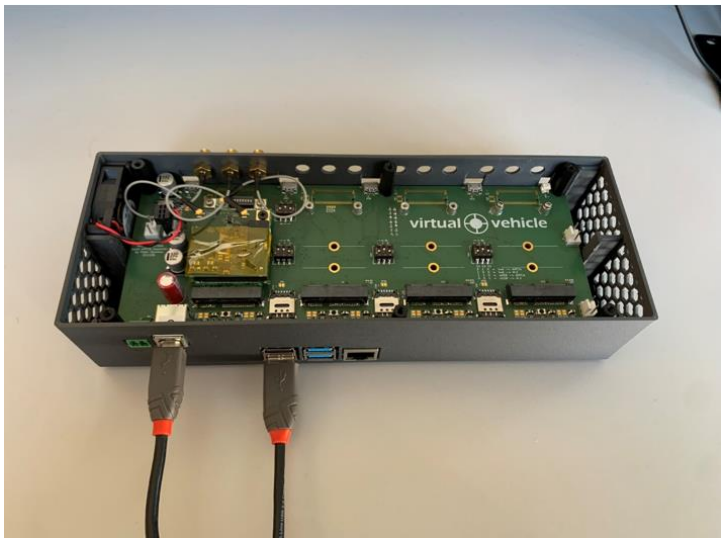


Figure 106 Vehicle CAPTAIN - Hardware with communication module carrier. Equipped with an ITSG5 module in the picture

3.11.1.3.2 Scenarios demonstrated

This demonstrator is planned to be used for Scenario 4 – Safety & Security in airport area in order to detect VRUs and other vehicles and provide this information to nearby vehicles via V2X communication. An object detection application detects 3D perceived object information from the camera feed about vehicles and provides the data to the RSU to be encapsulated in a Collective Perception Message (CPM). Feedback from the detected objects is delivered and stored to be used to further analyse the data in order to improve detection models.

3.11.1.3.3 TBBs demonstrated

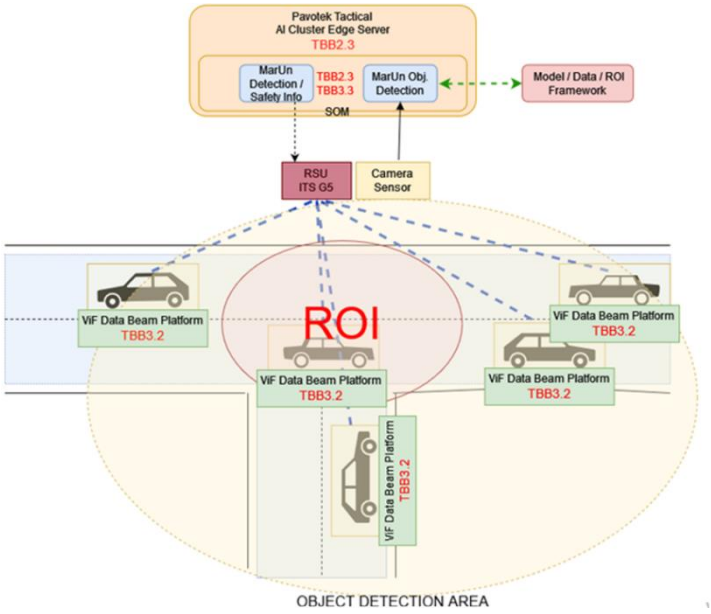


Figure 107 Smart Intersection infrastructure and BBs mapping

The Building Blocks involved in this Use Case are:

- TBB2.3 – Vehicle and VRU Detection Application (MarUn)
- TBB2.3 – Tactical AI Cluster Edge Server (PAVOTEK)
- TBB3.2 – Data Beam Platform (ViF)
- TBB3.3 – Model Framework (MarUn)

3.11.1.3.4 Progress summary – Y2

The demonstrator testbed infrastructure is constructed at Marmara University Campus. Data and electric connectivity have been provided to the infrastructure. RSU is mounted at the intersection to test V2X applications. A temporary Edge Device is mounted to test object detection application and performance. The integration between object detection application and CPM message broadcasting has been tested at the lab with real applications. A surveillance camera is not yet mounted, when the purchase and integration of the camera is done. The application is going to be calibrated to the camera and in Y3, real-site tests with integrated components are going to be demonstrated.

3.12 Use Case 5.12 - Driver Monitoring and Distraction Detection using AI

3.12.1 Planned demonstrators

3.12.1.1 Demo A

3.12.1.1.1 General information

The demonstrator comprises of a smartphone-based system that uses smartphone and smartwatch sensors to collect data about device usage during driving.

The TBBs developed are deployed in two stages (c.f. figure below):

- Offline demonstrator: The offline demonstrator which aims to detect at least one distraction event (e.g. moving the phone) using AI modelling.
- Online demonstrator: The online demonstrator which aims to detect at least one distraction event (e.g. moving the phone) using the AI modelling on the smartphone.

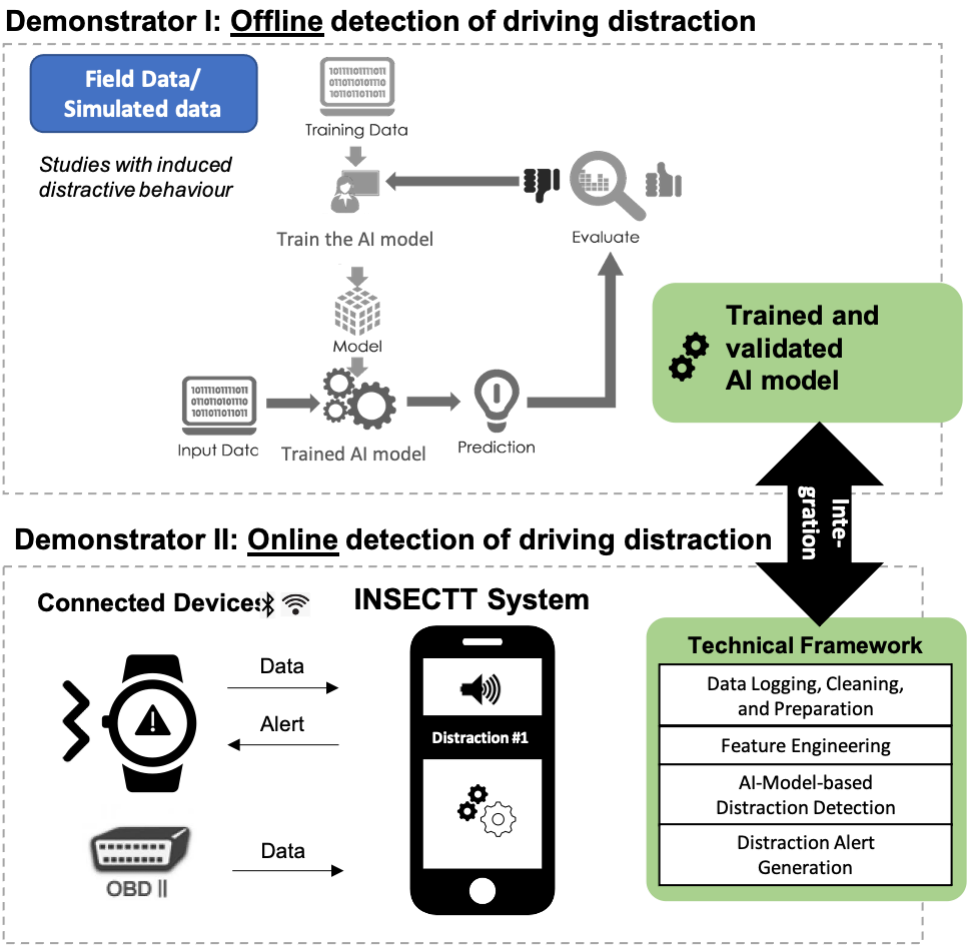


Figure 108 Demo I High Level Architecture

3.12.1.1.2 Scenarios demonstrated

A vehicle driver initiates driver monitoring and distraction detection for the current trip. Thus, opens the smartphone and the smartwatch application and starts the recording. Distraction events may be analysed in real-time or stored to be batch-processed after the trip is completed. A driving detection repository is created which can be chosen to be stored on the device.

Currently, sensor data from the smartphone and smartwatch sensors (i.e., IMU and GPS) is processed and used to create AI models that are used to classify the data into distractions or normal driving. Moreover, video recordings of trips are collected which are used to label distractions. The overall concept is shown in the figure below.

Figure 109 Block diagram of the system

3.12.1.1.3 TBBs demonstrated

Seven components were implemented by VIF, RISE and Tietoevry, namely (cf. figure below):

1) Smartphone application for data collection: Capable of collecting smartphone sensor data, which later will be used to develop an AI model. Collected data is, for example, IMU data, GPS data, screen state, and moving state (walking, running, driving, or biking). Data collection includes data cleaning, pre-processing and storing of the smartphone sensor data.

2) Smartphone data and AI modelling: Driver phone usage is detected via smartphone sensor data classification using an AI model directly on the phone. Data labelling is included to identify segments in the data which are distraction/inattention events, which are later used to train a Neuronal Network.

3) Smartwatch sensor data collection and fusion: A process is specified and developed to collect smartwatch sensor data while driving. The data is later used to develop an AI model. Data collection includes data cleaning, pre-processing, checking and storing the smartwatch sensor data.

4) Smartwatch data AI modelling: Driver smartwatch sensor data is used to train and evaluate an AI model which is used to classify data into normal driving and distraction.

5) Video labeller for distractions: A web-based tool is developed to create a labelled dataset from the collected sensor data and video trip recordings using smartphones. The output dataset is used to train the AI models.

6) Video data AI modelling: computer vision algorithms are used to detect distractions (such as texting, calling, reaching behind, etc.) from video images. This enables two use cases, one for predicting in real-time distractions and coupled with the AI models for smartphone and smartwatch. The second to ease and make the annotation process more efficient.

7) Smartwatch application for driver distraction: An initial draft smartwatch application has been developed to investigate steps needed to convert and include watch AI model in the watch app.

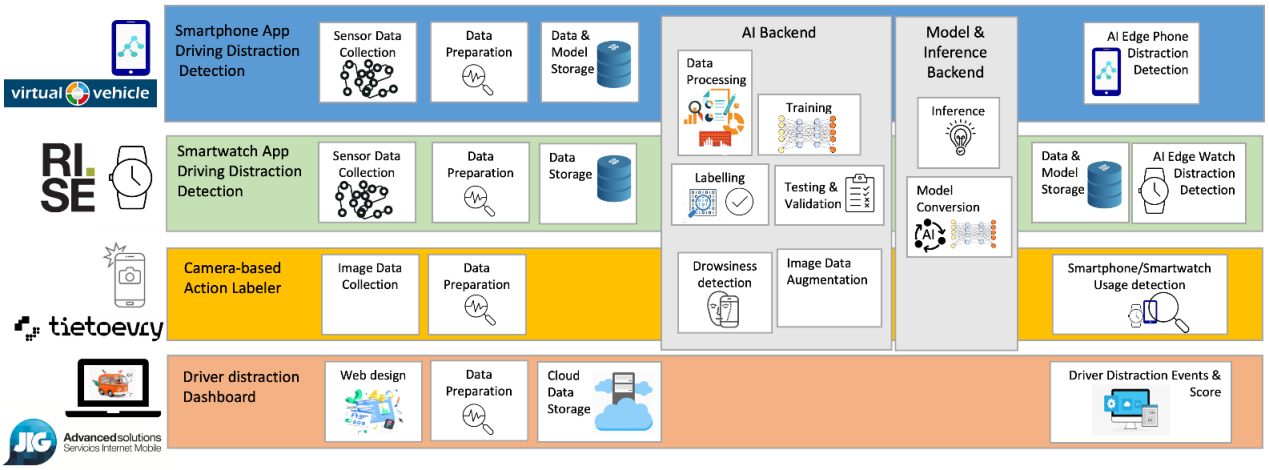


Figure 110 Demo High Level Architecture

3.12.1.1.4 Progress summary – Y2

During Y1 the offline demonstrator was developed and presented. In Y2 the progress had been respective to smartphones to develop AI models which are used on the smartphone to classify online (while driving and using the smartphone) distraction events. With respect to the smartwatch, the progress had been to collect smartwatch-related distraction data, label them (using the video labeller), and develop AI models to classify distraction events (offline). Finally, automatic video data labelling was developed in Y2 which uses computer vision algorithms to classify normal driving, using the smartphone (calling, texting) and using the smartwatch. As a result, videos get annotated with smart devices usage events. For Y3 a web-based application dashboard will be implemented based on the data collected, which will try to raise awareness to drivers regarding safety and distraction-related events.

3.13 Use Case 5.13 - Secure Industrial Communications System

Westermo designs and manufactures robust data communication devices for harsh environments, providing communication infrastructure for control and monitoring systems where consumer grade products are not sufficiently resilient. These products are central to a Secure Industrial Communications System (ICS). The realization that the needs of the industry are different from those of corporate IT creates growth in the requirement for industrial grade data communication. The main objectives of Use Case 5.13 are: first, to evaluate the resilience of the switches and by using AI in the edge or cloud investigate anomaly detection, but also to investigate architectural solutions for implementations of the additional functionality proposed for the switches, considering that switches are resource constrained.

3.13.1 Planned demonstrators

For Use Case 5.13, two demonstrators are planned. First, a virtual ICS Model simulated with GNS3, Docker and Qemu (Demonstrator A). Second, a data set that would represent parts of the traffic through part of the control zone of the ICS (Demonstrator B). We recently decided that we would like to extend the Use Case with demonstrator B, and work on it did not start in Y2, so this report covers only Demonstrator A.

3.13.1.1 Demo A - Virtual ICS Model

3.13.1.1.1 General information

Work on a digital twin for testing industrial control systems cybersecurity and Westermo software that builds up the core of a Virtual ICS Model, have progressed in Y2. The network architecture was previously implemented in the simplest star way topology with a single point of failure. The network topology is being extended in the demonstrator to a more realistic implementation, with a redundant ring network topology without a single point of failure. This better matches an actual ICS.

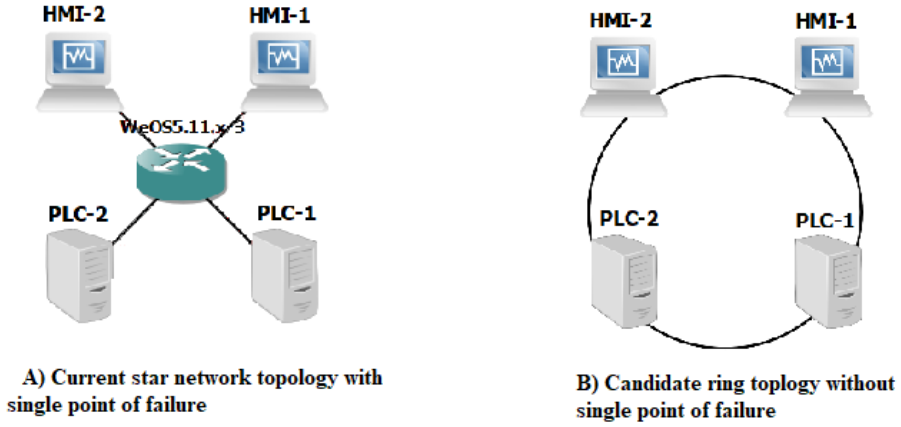


Figure 111 Network topology update of demonstrator A

3.13.1.1.2 Scenarios demonstrated

The core in Demonstrator A is composed of a Digital twin for testing industrial control systems cybersecurity and Westermo software. These can be seen as building blocks of the demonstrator, whereas the anomaly detection, intrusion detection, anomaly models and prevention systems have not yet been demonstrated with Demonstrator A.

Use Case 5.13 has three scenarios: Human Error, Control Components Connected to the Internet, and Intrusion via Remote Access. Work on defining and demonstrating these has only partially been conducted in Demonstrator A.

3.13.1.1.3 TBBs demonstrated

For Demonstrator A, the building block TBB3.1 on Methodologies, concepts and system solutions for safety and security is very central. The Use Case developed demonstrator A to produce ICS simulation testbeds, capable of meeting requirements for cyber security analysis. Possible future activities could be applying several types of attacks on simulated environment and study supervised and unsupervised anomaly detection methods to detect attacks.

3.13.1.1.4 Progress summary – Y2

During Y1, the use case was specified and work on demonstrator A progressed. During Y2, work on the test environment progressed, preparations and a first revision of an AI toolbox was completed. For Y3, we plan to refine demonstrator A, create demonstrator B, create one or several revisions of the AI tools using the updated demonstrators.

3.14 Use Case 5.14 – Secure and resilient Collaborative Manufacturing Environments

3.14.1 Planned demonstrators

For use case 5.14, two demonstrators are planned: Demonstrator A, for demonstrating security mechanisms related to access control and anomaly detection, using a modular automation system simulation environment, and Demonstrator B, for demonstrating results related to attestation and authentication of process data integrity.

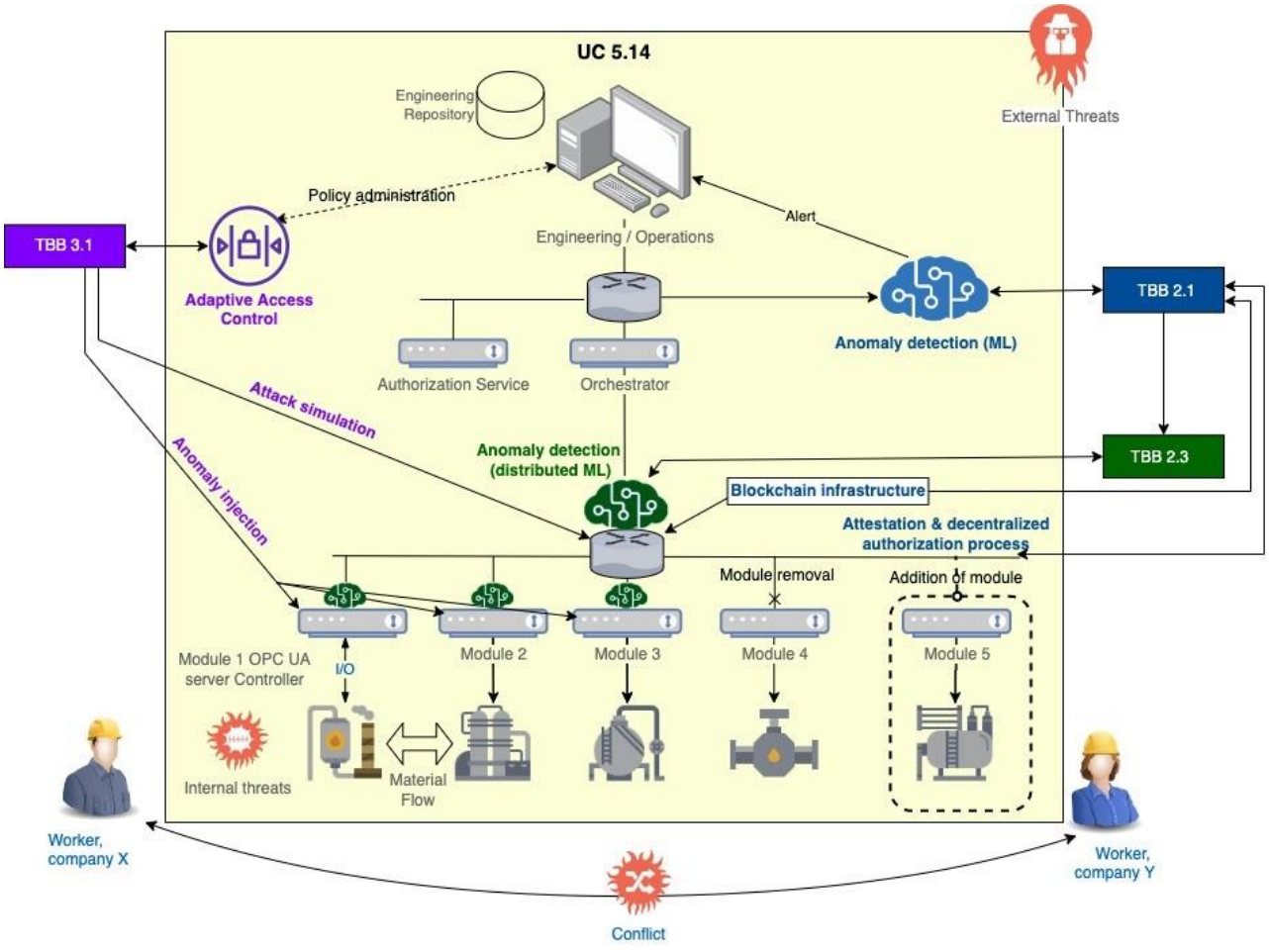


Figure 112 High-level architecture of the Use Case and connections with TBBs

3.14.1.1 Demonstrator A

3.14.1.1.1 General information

The demonstrator A consist of a simulated process industry, following the modular automation design strategy, with a set of individually controlled physical modules. The overall process is

synchronized using high-level recipes, being executed by an orchestrator unit. Everything in Figure 112, except the Block chain infrastructure, is part of Demonstrator A.

Demonstrator A is built using a bottom-up approach, with the focus during Y1 and Y2 on getting the mechanisms and functions related to module simulation, module detailed control, and orchestration running. The focus for Y3 will shift towards operator and engineer interactions.

The demonstrator system is built using COTS computing units. A standard Windows desktop computer is used for hosting virtual machines related to the 800xA core system, including engineering workstation, operator HMI, and related core services. The orchestrator and OPC UA service endpoint modules are in the form of ABB 800xA Control Services, executing on simple Raspberry Pi devices. The simulation engine is executing on a separate standard desktop. Interactions between components are TCP/IP-based, utilizing OPC UA for interactions between operations, orchestration, and module service endpoints, and MQTT for interactions between the modules and the simulation engine. Top threats will be implemented and used in attacks scenario execution toward the system to evaluate the effectiveness of its security measures. This will most likely lead to extensions of the demonstration system.

Demonstration A site is at MDH campus in Västerås, Sweden (Figure 113). As the equipment for the demonstrator is mainly in the form of regular desktop computers, Raspberry Pi devices, barebone/NUCs, and network equipment, the space needed is quite modest. The demonstrator is co-located with a laboratory containing simulators for heavy construction vehicles.

3.14.1.1.2 Scenarios demonstrated

The following scenarios are demonstrated: Scenario 1: Integration Engineering, scenario 2: Operational Engineering, and scenario 3: Process Execution are demonstrated in this demonstrator.

During the **integration engineering** phase, an integration engineer is formulating recipes, defining what module types are required and how they should interact in the physical as well as the digital world. This phase includes the tooling support and storage of recipes, as well as the act of making a recipe available for operational engineering. **Operational engineering** includes activation and deactivation of recipes, as well as plant supervision. During operational engineering the physical entities to be used for recipe execution are designated. **Process execution** in a Modular Automation plant is defined by a recipe, typically in the form of a Sequential Function Chart (SFC). The recipe contains high-level instructions to be carried out by the physical modules in the recipe. Coordination and execution of the SFC is driven by an orchestrator unit, typically a PLC or similar controller.

3.14.1.1.3 TBBs demonstrated

The components of technical building block 3.1, which are related to access control enforcement architecture and automated access control policy formulation, are to be demonstrated.

Some components of Technical Building Blocks 2.1 related to development of a reliable Intrusion Detection System (IDS) will as well be integrated in Demonstrator A. The building block that covers attacks simulations and anomaly injection, the work is done directly on the simulation engine (software) that will be connected to the Demonstrator A hardware components after all the functionalities are implemented and tested. Additionally, different ML algorithms for anomaly detection and classification are evaluated on well-known intrusion detection datasets.

Figure 113 Demonstrator A hardware

3.14.1.1.4 Progress summary – Y2

Equipment is purchased and installed. Physical access to the site requires MDH-employee access cards. The demonstrator setup is based on ABB Ability System 800xA with Modular Automation. Communication between modules / orchestrator / supervisory layers is based on OPC UA and Simulated modules (OPC UA Servers).

The simulation engine of the demonstrator is completed, and allows for easy configuration and control of separate, yet physically interconnected modules. Communication between controllers and resp. module I/O is utilizing the MQTT protocol. For recipe formulation and orchestration, a prototype is developed, which provide execution of recipes. This facilitates the creation of network data, as well as sensor log-data useful, e.g., for training in the anomaly detection components part of the use case.

Work on anomaly injections both on physical and network layer is on-going.

Related to the technical building blocks, the following are implemented and integrated:

- A proof-of-concept implementation of a tokens-based enforcement architecture is completed.
- Automated policy rule-inference based on recipe data is implemented and evaluated in a simulated Multi Agent System.

3.14.1.2 Demonstrator B

3.14.1.2.1 General information

The second demonstrator aims at focusing on attestation and authentication processes with different hardware architectures based on typical secure ARM platforms. Therefore, this demonstrator is related to device-level solutions by highlighting three components related to the BB2.1 (joint efforts with STMicroelectronics and AKEO PLUS):

- Block chain-based attestation process by cryptographically attesting the data issued from an AI-based application embedded in an IoT hardware platform.
- Authentication of the devices through smart contracts and decentralized application (dApp).
- Secure the history of the data produced by industrial applications embedded at the edge.

As illustrated below, the demonstrator is based on a decentralized network composed of a HUB and four IoT devices. The HUB is used as an access point to deploy a decentralized network with a star topology. Each device is connected to the HUB and can communicate with the others. Each stakeholder who participates to the ecosystem owns a personal computer with a copy of the ledger and is a member of the consortium for the governance of the block chain. The IoT devices are composed of a STM32MP157-EV1 board and a STPM4RasPI TPM Expansion Board including a secure element STSAFE-TPM ST33. For demonstration purpose, each embeds a different configuration concerning the access to the private key (clear or ciphered in the OP-TEE memory or STSAFE-TPM ST33).

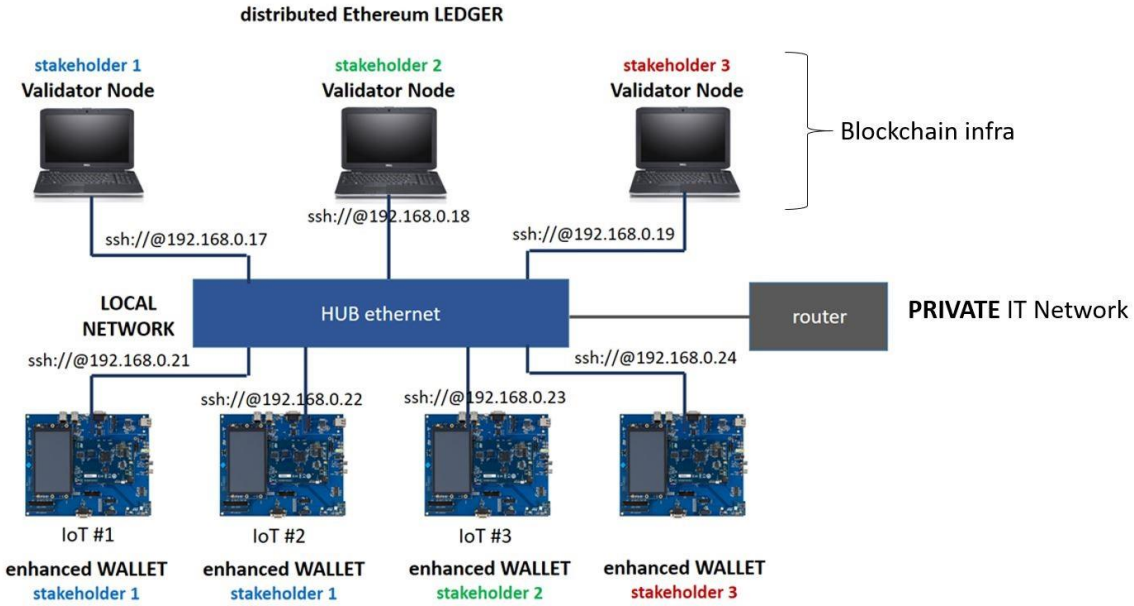


Figure 114 Decentralized network deployed for the Demonstrator B

3.14.1.2.2 Scenarios demonstrated

The demonstrator is focused on an audit-based scenario implying different stakeholders. A global scenario may be summarized as follows. IoT devices perform a task thanks to AI-based algorithm (inference of a neural network model) such as anomaly detection (or event classification). The embedded ML models have been protected against state-of-the-art attacks (theoretical as well as physical) that may threat their integrity of confidentiality.

A detected incident (such as intrusion) is linked to the detection timestamp that corresponds with a record in the ledger. Thus, an history of transactions since the detection timestamp is available. Each transaction/attestation embeds the authentication code (account address) of the device as well as the hashing of the data produced by this device at the transaction timestamp.

An independent auditor may ask each stakeholder (that owns devices included in this history) to provide the raw data, certified, produced by their devices. The auditor check that these data are authentic and not corrupted thanks to the transactions/attestations recorded in the ledger. These data can be safely used and exploited to further investigate the source of the incident and potentially unveil integrity or authenticity breaches.

3.14.1.2.3 TBBs demonstrated

The demonstrator is focused on the TBB of Task 2.1, 2.3 and 2.4. For task 2.1, the sub-BB related to the demonstrator is TBB2.1.1: *AI for audio-visual data* with the demonstration of works related to the development of block chain based authentication, as well as the security of the embedded machine learning models against API-based attacks. For task 2.3, the sub-BB is TBB2.3.4: *Privacy and security of distributed AI* with the demonstration of works related to the security of the embedded machine learning models against physical attacks. Finally, for the task 2.4, the sub-BB is TBB2.4.2: *V&V of AI-based systems* since the technologies proposed in the demonstrator will be evaluated according to methods, metrics, assessment recommendations proposed in the task 2.4.

3.14.1.2.4 Progress summary – Y2

During Y2, a neural network-based application has been embedded in the system-on-module. The neural network (NN) is integrated in the ARM Cortex M4 available in the board. When the industrial application needs an inference decision, it sends a request with the input data to the embedded model. The inference is transferred to the ARM Cortex A7 and added to the attestation process that builds a transaction compliant with the ethereum block chain to be register in the ledger. This transaction ensures the traceability of the inference decisions and authenticates the devices and the embedded application that produce the data. The scheme of the embedded design is presented in Figure below. Moreover, tools have been developed to write, compile, deploy, and use smart contracts in the ethereum block chain. A tamper-resistant historic of attestations of the data produced by all the IoT involved is available to all the stakeholders in the distributed ledger. Everyone sees and shares the same information, improving trust between the stakeholders and preventing litigations.

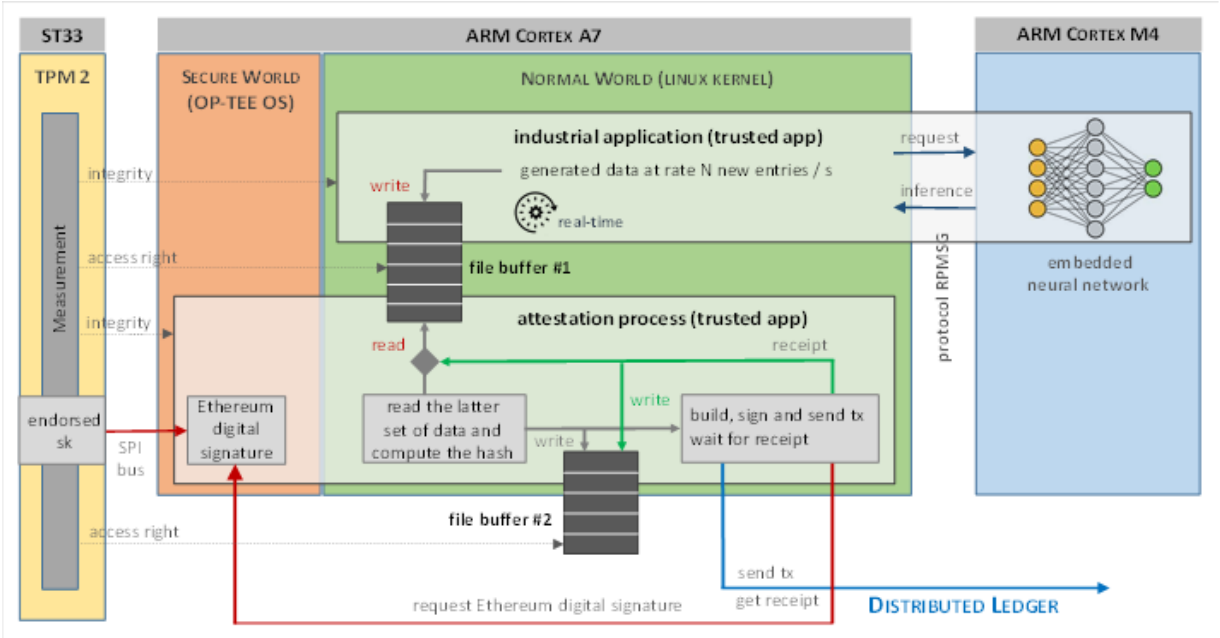


Figure 115 Embedded attestations of neural network inferences

3.15 Use Case 5.15 - Intelligent Safety and Security of Public Transport in urban environment

3.15.1 Planned demonstrators

3.15.1.1 Demo A

3.15.1.1.1 General information

The demonstrator of UC5.15 will consist of a SETA bus equipped with:

A Leonardo on-board unit together with a driver's terminal

- A NVIDIA board for pothole detection provided by LDO
- A frontal camera for the pothole detection provided by LDO
- A NVIDIA board to perform video anomaly detection provided by CINI
- 2 environmental stations for air-quality monitoring provided by ETH
- 1-2 Strips for people counting provided by ETH
- A gateway provided by ETH
- Array of microphones provided by CINI
- NVIDIA board for the coarse audio anomaly detection system provided by CINI

Moreover on the enterprise side there will be a dashboard implemented by ETH to collect and visualize the alerts as well as a separate tool for CAN bus data analytics.

Figure 116 The MASA Dynamic Model Area

The demonstration will take place either at the MASA Dynamic Model Area or at the MASA Smart Model Area. These are automotive specific test areas which have been thoroughly described in deliverable D5.15. The demonstration will be conducted using actors (most likely employees of the partners involved), having signed an informed consent to the data processing.

3.15.1.1.2 Scenarios demonstrated

We shall demonstrate Scenario 1 (video/audio anomaly detection, potholes detection) and 3 (environmental monitoring and people flow monitoring) during a bus ride in one of the two areas of the MASA to be determined. As specified earlier, the bus ride will not be open to public, but restricted to the actors involved in the demonstration. Scenario 2 is the one related to the predictive maintenance. Predictive maintenance is supposed to run over a long time on a wide fleet of vehicles and it is thus unsuited for a demonstration in a single bus ride. We will present the study of the dataset in our possession which comprises data from a large CNG bus fleet over a 3 months period. To have a feedback from the user and to get more insight regarding the algorithm we are thinking to plan maintenance checks of the SETA's vehicle interested by the project, in accordance to LDO's system alerts, over a period of a few months. The demonstration will thus consist of a report regarding both of the results obtained on the dataset, and the results of the application of the methodology to the specific SETA bus over the test period.

Figure 117 ETH's laboratory implementation of people counting sensor strips

3.15.1.1.3 TBBs demonstrated

The TBB demonstrated will be 2.1, 2.3, 3.2, 3.3, and 3.4. The precise TBB mapping is provided in deliverables D5.15, D5.31, D5.49. Each of these deliverables also contains a slightly more detailed description of how components are linked to TBB in the Link to BB Table.

3.15.1.1.4 Progress summary – Y2

Implementation of the SW components (AI algorithms and edge-cloud infrastructure) have been completed in their first release. Partners working on AI/ML algorithms are currently gathering additional data to enhance the performances of the different algorithms and/or dealing with explainability aspects. In particular, there will be a second round of data acquisition for video anomaly detection planned between M25 and M28, whereas we are planning with SETA an air quality data collection onto one of the SETA busses operating on Modena. At the moment preliminary SW solution are under testing on data from the SETA bus before the deployment planned in Y3. HW deployed in the forthcoming round of air quality data acquisition will be a prototypal one prepared by CINI -until ETH environmental stations will be ready for the on-site test and then deployed for the final demonstrator. ETH environmental stations have been assembled and are currently being tested to check the correct functioning of all the sensors mounted. A first implementation of the different

HW components is already available, CINI is now focusing on the embedded deployment of AI algorithms on the NVIDIA target platform. LDO's on-board unit will be mounted on the bus within M26 and will start to collect CAN bus data to be analysed by the predictive maintenance algorithms. ETH strips are slightly behind schedule for what concerns their integration and deployment on-board.

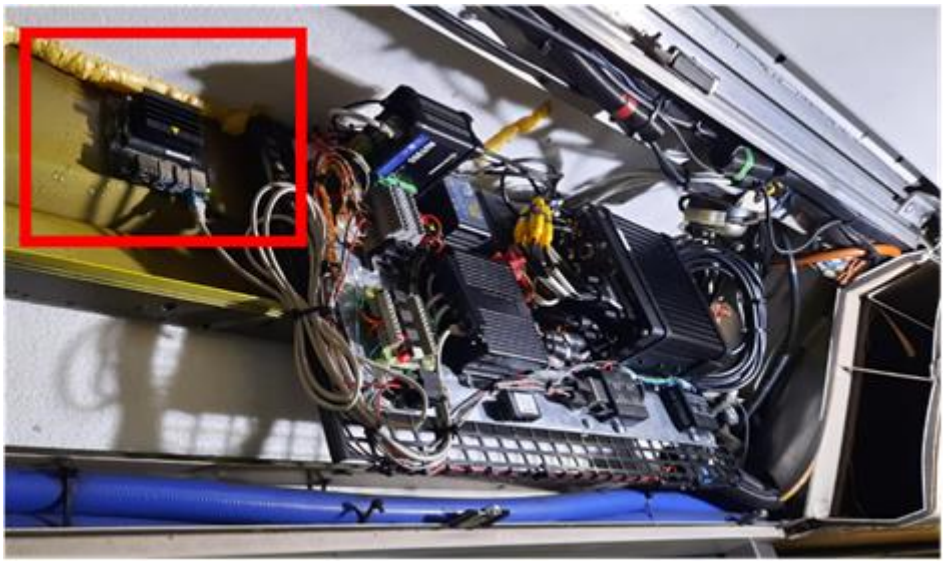


Figure 118 Preliminary implementation of the board deployed for video-anomaly detection

3.16 Use Case 5.16 - Airport Security–Structured and Unstructured Flow of people in airports

3.16.1 Planned demonstrators

3.16.1.1 Brindisi Airport Demonstrator

3.16.1.1.1 General information

Brindisi Airport Demonstrator will take place mainly in the extra-Schengen area of Brindisi's Airport Terminal. The demonstrator will comprise:

- 3-5 of surveillance cameras in the extra-Schengen area of the terminal;
- an API RESTful for video streams analysis which comprises several algorithms of crowd management: people counting, social distancing, man down;
- a second API RESTful for face re-identification;
- VPN connections
- 3-4 environmental stations provided by ETH
- Gateway provided by ETH for environmental monitoring system
- IoT infrastructure for environmental monitoring system
- Biometric recognition enrolment kiosk (infrared camera for hand-vein pattern recognition, camera for faces deep descriptors extraction)

- Biometric recognition check kiosk (infrared camera for hand-vein pattern recognition, camera for faces deep descriptors extraction)
- A software for Anomaly Tracking, to identify the person who is with reasonable probability the one responsible for triggering the alert of the environmental monitoring system; the result will be shown on dashboard.

Figure 119 The extra-Schengen area of Brindisi Airport Terminal

3.16.1.1.2 Scenarios demonstrated

Brindisi Airport demonstrator will allow to demonstrate Scenarios 1-3, according to the description in deliverable D5.16. Notice that, for all components involving the processing of personal data, tests and demonstration will be made using actors (most likely employees of the involved partners), having signed an informed consent describing the type of processing will be made of their personal data.

3.16.1.1.3 TBBs demonstrated

The TBBs demonstrated in Scenario 1-3 are 2.1, 2.3, 3.2, 3.3, 3.4. The way TBBs are linked to the different components are specified in the TBB mapping sections of deliverables D5.16, D5.32, and D5.50 and in the Link to BB Table in the same deliverables.

3.16.1.1.4 Progress summary – Y2

At the moment the components has been designed and implemented and we are working on the different components. The area of the Brindisi Airport interested by the demonstration has been identified and a data acquisition on field for what concerns environmental sensor (gaseous pollutants and dangerous chemical element) is starting within the next weeks.

We are currently discussing with ETH and ADP the best way to demonstrate Scenario 2 and 3, which is intended for detection of dangerous substances and tracking of the carrier inside the airport. The introduction of an amount of such substances sufficient to activate ETH's sensors is out of question as it poses bureaucratic and security issues. The solution envisaged would be to prove the technology using semi-radioactive seed with very low level of radioactivity.

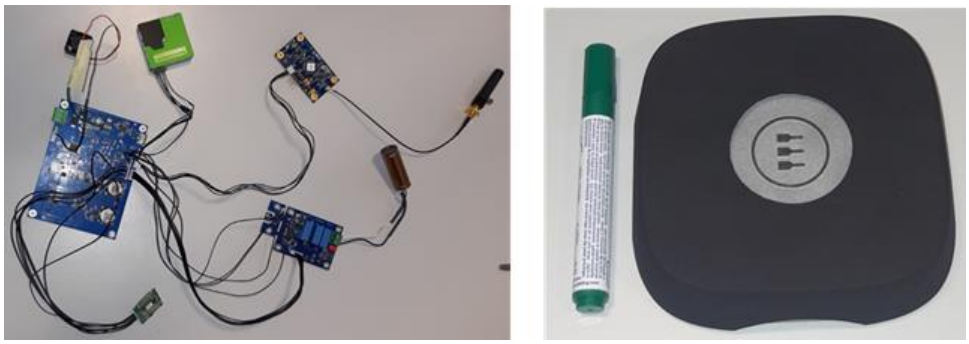


Figure 120 ETH's environmental station

3.16.1.2 Taranto-Grottaglie Airport Demonstrator

3.16.1.2.1 General information

The Taranto-Grottaglie Airport Demonstrator will take place in the Taranto-Grottaglie Airport area, and in particular it will interest one of the drainage channels which cross the airport area in proximity of the airport perimeter. The demonstrator will comprise

- Magnetic barrier sensing node
- Magnetic barrier terminal node
- (Wireless link)

Figure 121 Fosso Madonna drainage channel at one of its intersections with the airport perimeter

3.16.1.2.2 Scenarios demonstrated

Taranto- Grottaglie Airport demonstrator address demonstration of Scenario 4, and will thus permit to validate the deployment of this technology for the monitoring of drainage channels crossing the airport perimeter. This scenario has been added in D5.34, and is intended to demonstrate the validity of the component “Magnetic barrier”, developed for the maritime domain (UC5.04), in the context of smart infrastructure / aeronautics.

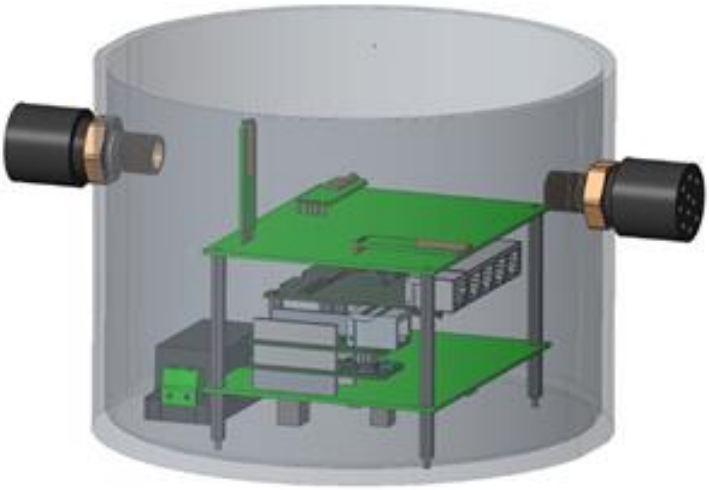


Figure 122 The design of the Magnetic sensor node

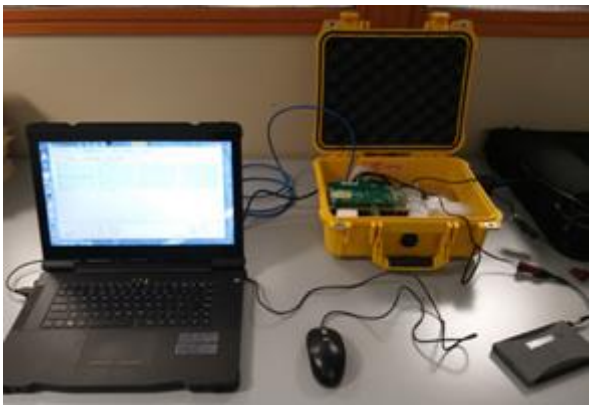


Figure 123 The present "portable" magnetic sensor prototype

3.16.1.2.3 TBBs demonstrated

The TBBs demonstrated in Scenario 1-3 are 3.2, 3.3. The way TBBs are linked to the different components are specified in the TBB mapping sections of deliverables D5.34, D5.50 and in the Link to BB Table in D5.50.

3.16.1.2.4 Progress summary – Y2

The first magnetic sensor prototype has been designed, implemented and tested in laboratory, including the integration of two sets of transducers measuring in parallel (emulation of a minimal barrier).

LDO and ADP are programming their deployment in the airport areas in the last half year of the project, after LDO will have conducted its tests at sea for UC5.04.

The set-up for the demonstration has already been defined, with the exception for the wireless link, which is somewhat accessory in the demonstration.

4 DISSEMINATION, EXPLOITATION AND STANDARDISATION

Specific, Use Case related dissemination, exploitation and standardisation actions are described in individual Use Case Y2 Progress Reports.

5 CONCLUSIONS

This document provides detailed description of status of InSecTT Use Case demonstrators. Together with individual Use Case progress reports, it creates comprehensive and transparent report on current status of development of both Use Cases and demonstrators.

As it was explained in D4.1 [2], each Use Case has defined scenarios for demonstrators during Use Case specification phase. This scenarios are constantly updated with details and reported in individual Use Case progress reports.

During second year of the project, all of the Use Cases have achieved planned progress in terms of demonstrator preparation. InSecTT is following an approach, where early results presented in a form of demonstrators are verified and validated in order to gain feedback from various entities engaged in the project – demonstrator hosts, Partners that integrate their solutions in particular demonstrators as well as external stakeholders.

During Y3 following activities related to Use Case demonstrators are to be performed:

- Final validation of Use Case and demonstrator scenarios,
- Integration of components as specified in individual integration plans,
- Deployment of components in designed locations,
- Preparation of Use Case demonstrator booklet,
- Dedicated dissemination and exploitation activities related to the demonstrators.

In critical areas that can be affected by the COVID-19 restrictions such as airports, ports, public buildings, reserve locations for demonstrators have been set up.

6 REFERENCES

[1] „InSecTT Description of Work Part A Part B, 2021-06-25”.

[2] „InSecTT Deliverable "D4.1 Use Case management methodology"”, v1.0, 2020-08-25

A. ABBREVIATIONS AND DEFINITIONS

Term	Definition
ACS	Adaptable Communication System
APS	Adaptable Positioning System
AI	Artificial Intelligence
AL	Automata Learning
BER	Bit Error Rate
BLE	Bluetooth Low Energy
BS	Base Station
CAN	Controller Area Network
CAPEX	Capital EXPenditure
CMW	Communication Middleware
COTS	Component of the shelf & Commercial Off-The-Shelf
CSH	Central station Harbour
DB	Distance Bounding
E/O	Electro Optic
ESPAR	Electronically Steerable Parasitic Array Radiator
FHIR	Fast Healthcare Interoperability Resources
GCR	Grand Central Railway
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HLA	High Level Architecture
HW	Hardware
IACS	Industrial Automation & Control Systems
I2V	Infrastructure to Vehicle
IoT	Internet of Things
ITS	Intelligent Transportation Systems
JB	Junction Box
JRU	Juridical Registration Unit
KPI	Key Performance Indicators
LIDAR	Light Detection and Ranging)
LORA	Long Range
LTE	Long Term Evolution
MAC-PHY	Medium Access Control - Physical Layer
MAMS	Multiple Access Management Services
MB	Magnetic Barrier

MCI	Mass Casualty Incident
MIMO	Multiple Input Multiple Output
MIPS	Maritime Infrastructure Protection System
ML	Machine Learning
MPS	Multimodal Positioning System
MQTT	Message Querying Telemetry Transport
NFC	Near Field Communication
OBU	On-board Unit
OPC-UA	Open Platform Communications United Architecture
OPEX	Operation EXPenditure
OSS	Operations support systems
PER	Packet Error Rate
PHY	Physical Layer
PMS	Portable Monitoring Station
QoS	Quality of Service
RAN	Readiness Assessment Network
RF-DiPaQ	Radio Frequency-Distance Packet Queuing
RFID	Radio-frequency identification
RSSI	Received Signal Strength Index
SC	SDN Controller
SCADA	Supervisory Control And Data Acquisition
SCN	Smart Communication Node
SD(W)N	SW Defined (Wireless) Network
SDN	Software Defined Network
SUT	System Under Test
SW	Software
SWND	SDN-enabled Wireless Network Device
TBB	Technical Building Block
TBM	Tunnel Boring Machine
TCP	Transmission Control Protocol
TDOA	Time Difference of Arrival
TN	Terminal Node
TOA	Time of Arrival
Tx	Transceiver
UC	Use Case
UUV	Unmanned underwater vehicles
UWB	Ultra-wide band

V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2X	Vehicle to X
WLAN	Wireless Local Area Network
WNP	Wireless Sensor Network base station
WP	Work Package
WSN	Wireless Sensor Network