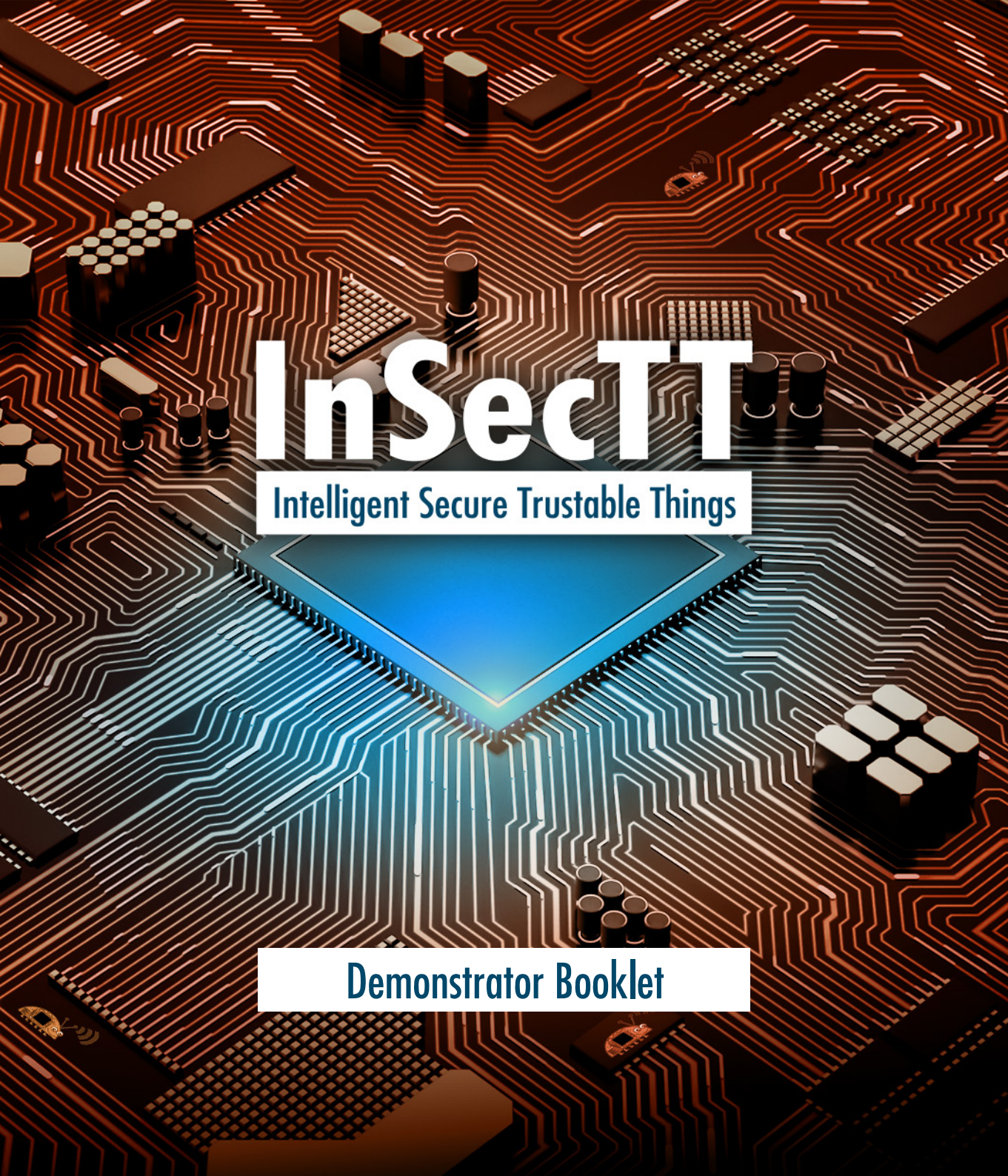

InSecTT
Intelligent Secure Trustable Things
Demonstrator Booklet

Wireleless platooning communication based on AI-enhanced 5G

General demonstrator information

The use case of wireless platoon intra-communications aims to show the benefits of artificial intelligence in the control and connectivity of sets of vehicles arranged in the form of platoons.

The demonstration of the use case for wireless intra-platoon communications relies mainly on a system level simulator/emulator for all the technical building blocks. A robotic demonstration connected to the main system level simulator/emulator is also considered to show specific platoon manoeuvres and real-time control. Three scenarios will be demonstrated with different instances of the main system level simulator/emulator or the robotic testbed:

1. V2x communication interference in traffic congestion.
2. Latency mitigation in emergency braking.
3. Replication of platoon behaviour in physical testbed.
4. Platoon coordination and wireless resource management in tunnels.

Functionalities

The main functionalities to be demonstrated in this use case are related to how wireless modern technologies enhanced by AI algorithms can provide a reliable, low-latency and secure medium for the exchange of control and operation of platoons of vehicles in challenging conditions.

The wireless connectivity functionalities are one of the main objectives of the use case to provide reliable and real time communications between all elements of the architecture. The control functionalities for the platooning functionalities located across different entities of the architecture are the other main pole of functionalities targeted by the AI algorithms developed in this use case.

The InSecTT reference architecture adopts a functionality model that combines the benefits of multiple other standards. This functionality model is displayed in its high-level view in the figure below, using 4 main horizontal layers (device or DL, network or NL, service or SL and application layer or AL). Two vertical layers account for cross-layer and security management. Each use case will organize their specific functionalities in a functional stack model as the one shown in the figure below. For the platoon use case the model shows a preliminary overview of the different functionalities expected associated to all communications and control/operation of the different platoon scenarios.

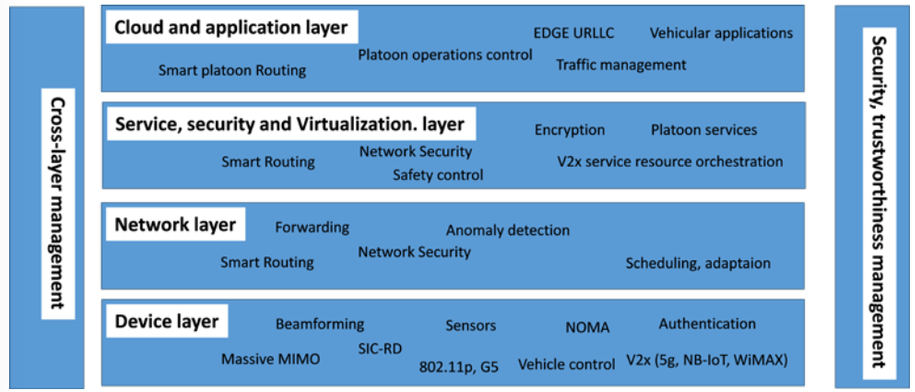


Figure 1.1

Key components

The components of the demonstrator are aligned with a modern system level simulator/emulator for performance evaluation and testing of secure wireless IoT solutions. Emphasis is given to the reliable channel emulation due to the challenging V2X propagation conditions, AI used for wireless signal reception, and the platoon control/mobility and resource allocation/orchestration and traffic management system. A prototype robotic testbed can be integrated into this platoon emulation framework. The simulator also has dedicated components to test security solutions for platooning and

platoon communications. The technical building block involved are T32 for dependable wireless, T2.2 for AI-based improved wireless reception, T3.4 for real time scheduling over reliable wireless, T3.5 for V&V of secure wireless, and T2.5 for trustworthy AI systems.

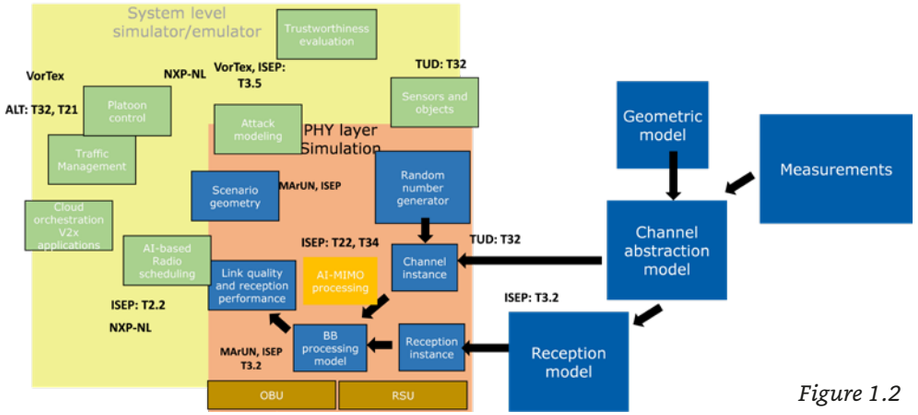


Figure 1.2

System architecture

Each element or vehicle of a platoon is considered as a node of the InSecTT reference architecture. The Bubble concept has two possible implementations in this use case. In the first option, ech platoon can be considered as a Bubble, with the leader being the Bubble Gateway. The Bubble Gateway uses a 5G link to connect to the Cloud. In addition, each node of the Bubble has also a link with the 5G BS/RSU. In this case, we can consider that the 5G RSU/BS is a direct connection with a virtual Bubble Gateway, as the 5G Base Station (BS) acts as relay and assistant of the main Bubble GW. This leads to an interesting modification of the Bubble and InSecTT architecture. In the predecessor project architecture, the Bubble GW was the unique access point to the Bubble Nodes from the external world. In the new InSecTT architecture, nodes can have another link to the outer bubble space using another interface.

The platoon-BS architecture can also be adapted in a different way to the InSecTT reference architecture by considering that nodes can communicate with two WSN gateways over two different L0 technologies. The 5G link can be regarded as L1 technology, and the Bubble GW is represented by the 5G BS. This is also illustrated in the figure below (the bottom sub-figure). This last option implies that the 5G BS or RSU are included in the Bubble, and therefore it can be inadequate for high mobility scenarios.

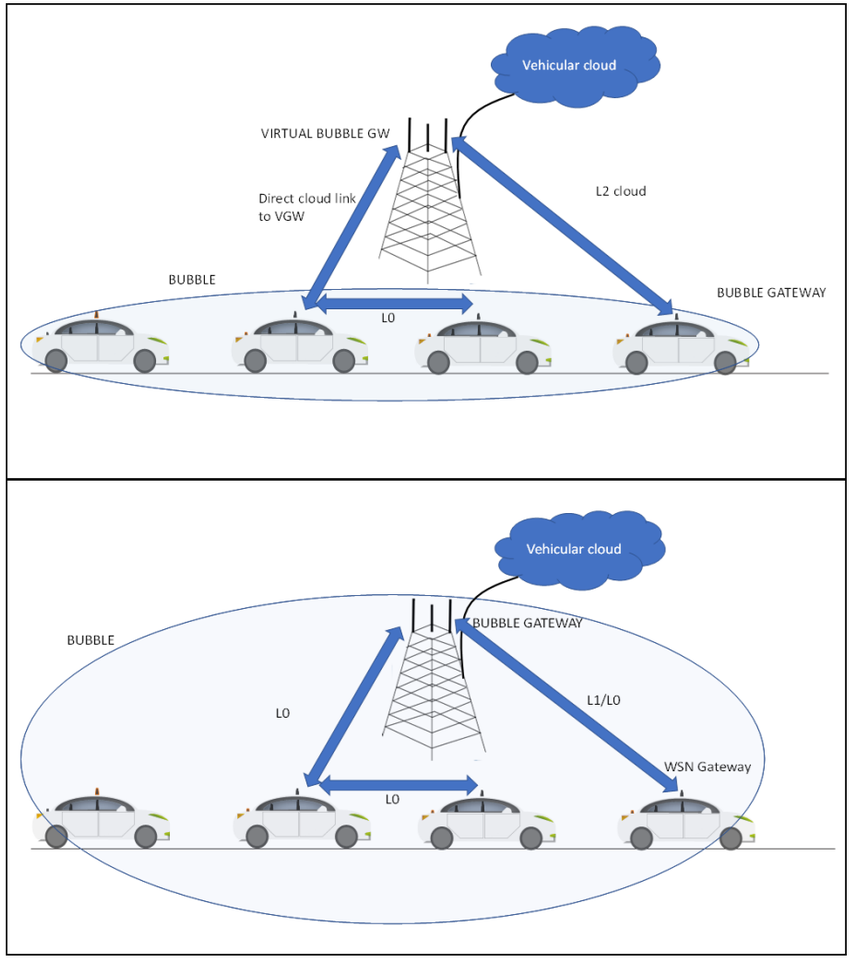


Figure 1.3

This use case also considers a multiple platoon scenario with multiple 5G BSs located in an urban environment. The objective is to evaluate the performance of all transmission systems with multiple antennas in a highly demanding and challenging interference environment with realistic platooning manoeuvres and traffic flows. This setting is displayed in the figure below using a Manhattan rectangular network deployment and multiple platoons.

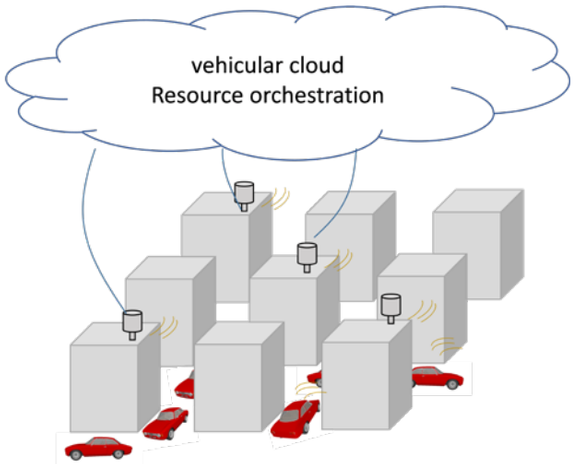


Figure 1.4

The mapping of the entity and functionality models for this use case allows us to split the overall functionalities over the main physical entities. The preliminary division of functionalities is shown in the figure below.

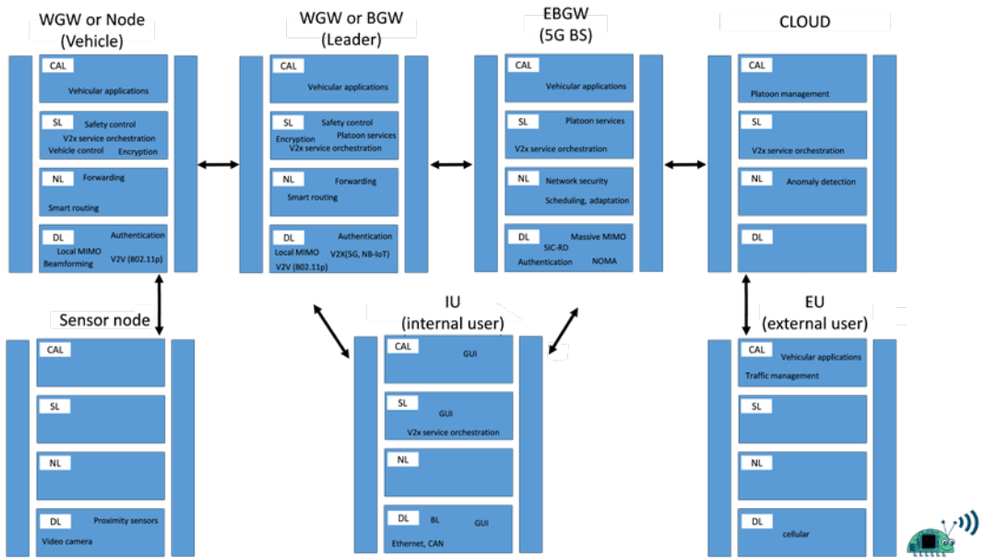


Figure 1.5

AI-enriched wireless avionics resource management and secure/safe operation

General demonstrator information

The use case of avionics aims to show the benefits of artificial intelligence in the reliability, real time operation and security against attacks (mainly jamming) of an emerging application of wireless technologies known as wireless avionics intra-communications (WAICs).

The demonstration of the use case wireless avionics intra-communications relies mainly on a system level simulator/emulator for all the technical building blocks. A testbed in a real aircraft prototype is also being considered for interference characterization. Three scenarios will be demonstrated with different instances of the main system level simulator/emulator or the aircraft testbed:

1. Interference detection and cancellation.
2. Verification and validation of WAICs.
3. Sensor flow management.

Functionalities

The main functionalities to be demonstrated in this use case are related to how wireless modern technologies enhanced by AI algorithms can provide a reliable, low-latency and secure medium for the exchange of control and operation of aircraft operational and senor information.

The wireless connectivity functionalities are one of the main objectives of the use case to provide reliable and real time communications between all elements of the architecture. The control functionalities for the avionics functionalities located across different entities of the architecture are the other main pole of functionalities targeted by the AI algorithms developed in this use case.

The InSecTT reference architecture adopts a functionality model that combines the benefits of multiple other standards. This functionality model is displayed in its high-level view in the figure below, using 4 main horizontal layers (device or DL, network or NL, service or SL and application layer or AL). Two vertical layers account for cross-layer and security management. Each use case will organize their specific functionalities in a functional stack model as the one shown in the figure below. For the avionics use case the model shows a preliminary overview of the different functionalities expected associated to all communications and control/operation of the different platoon scenarios.

Key components

The components of the demonstrator are aligned with a modern system level simulator/emulator for performance evaluation and testing of secure wireless IoT solutions. Emphasis is given to the reliable channel emulation due to the challenging avionics propagation conditions. The simulator also has dedicated components to test security solutions WAICS communications. The technical building block involved are T32 for dependable wireless, T2.2 for AI-based improved wireless reception, T3.4 for real time scheduling over reliable wireless, T3.5 for V&V of secure wireless, and T2.5 for trustworthy AI systems.

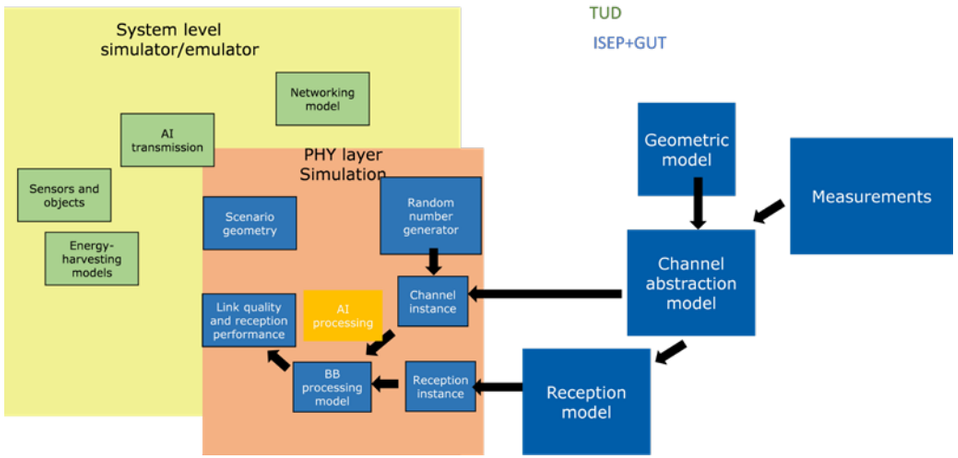


Figure 2.1

System architecture

The ITU recommendations define two types of WAICs network topologies depending on the location: internal or external to the cabin. The gateways are positioned in places to provide good coverage for the intended applications. The entities of a WAICs network can be rearranged as a Bubble of the InSecTT reference architecture. Sensors or groups of sensors can constitute an InSecTT Bubble node. Several Bubble Nodes can form a Wireless Sensor Network (WSN) which is assumed to be controlled by a WSN Gateway (WGW). One or more WSNs can be designed to operate in different parts of the aircraft, using different channels or different frequency bands (in case of FDM allocation) or different hoping or spreading sequences (in case of CDMA deployment). This reduces the interference between WSNs. All the WSNs that belong to the same Bubble are assumed to be controlled by a unique InSecTT Bubble Gateway (BGW). The Bubble gateway is therefore the central control entity of all Bubble Nodes and WSNs inside the aircraft information system. The WSNs are thus interlinked to each other and to the Bubble GW using the internal aeronautics bus network. The most used standard is ARINC 664 or the commercial version called AFDX (Avionics Full-Duplex Switched Ethernet). This technology is a modified version of the Ethernet standard based on the concept of virtual links that ensure real-time and deterministic deadline allocation. The concept of Bubble is especially fit for aeronautical applications, where L1 is the internal, real time and highly reliable aircraft network, L0 is the wireless links, and L2 is the cloud external connection of the aeronautical Bubble. We should emphasize that there are other ways of configuring the aeronautical infrastructure to have different deployments of the InSecTT bubble. For example, different bubbles can be operating in the same aircraft using an external L2 technology to achieve communication between bubbles. The use of one bubble per aircraft is illustrated in the figure below.

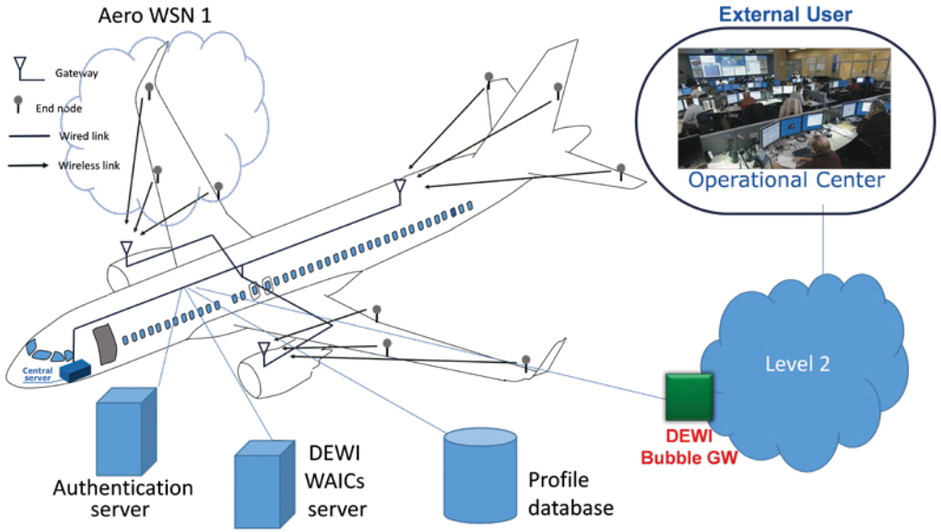


Figure 2.2

The functionality model of the reference architecture can be used also in WAICs. This generic functionality model is depicted in the figure below. The horizontal functional layers can be abbreviated as DL (Device Layer), Network layer (NL), Service and virtualization Layer (SL), and Cloud and Application Layer (CAL) or also abbreviated as ECAL (Edge and Cloud Application Layers). The vertical sublayers shown in the figure are the Cross-Layer Management and Security and Layer Management (CLM and SLM, respectively). The current functionality model for the WAICs use case is shown below.

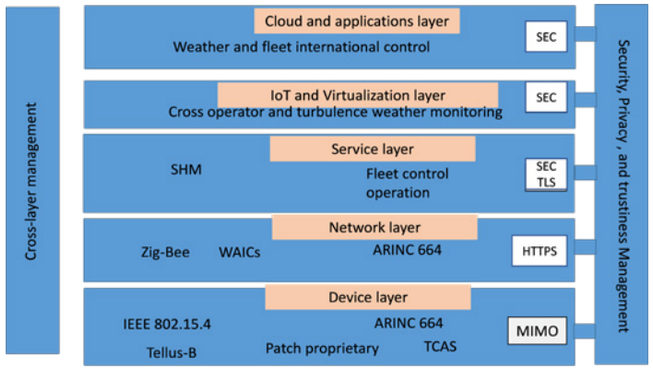


Figure 2.3

The mapping between the physical and functionality model of the WAICs use case is shown below.

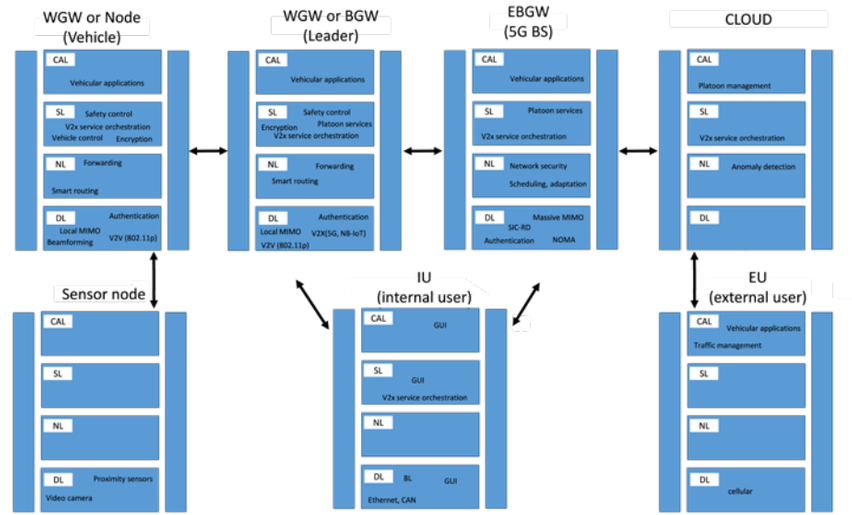


Figure 2.4

Wireless security testing environment for smart IoT

General demonstrator information

In this use case, a highly automated wireless cybersecurity test system will be developed. The novel approach will allow to greatly extend the number of tests within the same (or even lower) time and budget.

We plan to have three demo sites:

- **Demonstrator A:** Automated cybersecurity testing environment for wireless IoT in vehicles:
  - **Lead implementer:** AVL,
  - **location:** AVL vehicle test bed in Graz, Austria,
  - **Components:** simulation platform (AVL); test case generator (AVL); test automation (AVL); channel simulation (PhyWise - GUT); platoon simulator (NXP-NL); V2x simulation (digital twin - MarUn);
- **Demonstrator B:** Testbed for Embedded Wireless Devices:
  - **Lead implementer:** LCM,
  - **Location:** LCM in Linz, Austria,
  - **Main components:** Test orchestration, jamming simulation, test automation (all: LCM),
- **Demonstrator C:** Testbed for automotive keyless entry systems:
  - **Lead implementer:** NXP-AT,
  - **Location:** Graz, Austria,
  - **Main components:** vehicle equipped with keyless entry system under test (SUT / NXP-AT); UWB sensor nodes (JKU);

Current status: all three demonstrators are being built at the moment (M13) and shall be shown (either physically or documented via movies) as planned in the Y1 review meeting September 2021.

Functionalities

Vehicles need to be tested under real-life conditions, while still being in the controlled environment of an automotive test bed. For such a realistic context, all relevant aspects need to be simulated in high fidelity: environment, traffic, movements, passenger interaction, connectivity with external systems etc. The diversity of wireless systems requires the support of a wide range of technologies and, again, being able to simulate the exact physical conditions available (channel models, interference, etc.)

Cybersecurity testing tries to find (hidden) vulnerabilities in systems before the “bad guys” find them. Thus, our focus is on algorithms (both classical and AI-based) to come up with relevant test cases (attacks). This is closely linked to monitoring all systems and trying to detect any inacceptable behaviour caused by the attacks. Finally, it is important to highly automate cybersecurity testing, in order to drive down costs and time needed.

Key components

A wireless Security Testing Environment for smart IOT consist of a Test Case Generation (TCG), a Test Automation System (TAS), the test bed (TB) itself with the system under test (SUT), appropriate simulators (e.g. channel, traffic, …) to create appropriate environment for operating the SUT, and a test oracle.

System architecture

All demonstrators relate to the basic HLA agreed upon by the partners in T5.3 as depicted in the following diagram:

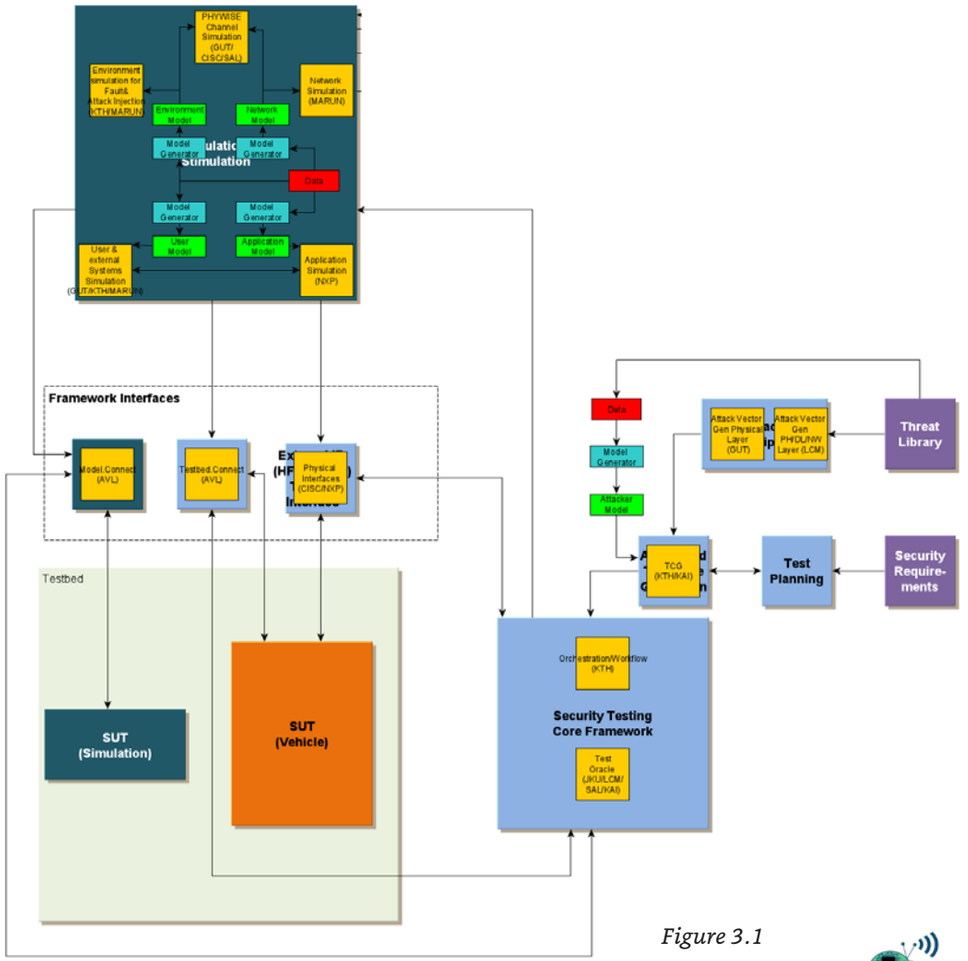


Figure 3.1

Intelligent wireless systems for smart port cross-domain application

General demonstrator information

As a part of cooperation between Port of Gdansk and InSecTT consortium, Port will host a demonstrator located in areas managed by the company Port of Gdansk. This is one of the largest ports in Baltic Sea, specialized in a.o. feeder services, ferry terminals as well as liquid and bulk cargo management.

Figure 4.1

The second main location is the Cetraro harbour in the south of Italy as the best location to perform the demonstration activities. UNICAL has its own support base for maritime activities in this port, so this is helpful from a logistic point of view. The harbour is mainly used for touristic and fishery purposes, so test activities will marginally interfere with the normal port activities allowing the execution of the demonstration without too many restrictions.

Figure 4.2

Functionalities

The demonstrator functionalities are grouped around Use Case scenarios:

Scenario 1 – V2X communication

The basis of the scenario is to provide communication between the vehicles and the roadside units to track the vehicles and monitor the behaviour of the vehicle's driver. Communication in a smart environment can take place using various communication protocols, including V2X (802.11p), BLE, LORA, 802.15.4, and others. The solutions need to focus on wireless communication security and the use of AI techniques. The target environment is the Port of Gdansk with harsh infrastructure, with a lot of possible reflections and interferences. The communication system should improve the daily work and increase efficiency in the Port of Gdansk.

Scenario 2A – Intelligent wireless systems for smart port cross-domain applications

Acoustic underwater sensors can be deployed to monitor movements near maritime infrastructures (e.g. at port entrance), while magnetic underwater barriers are deployed close to the piers, pylons, and anchors. Such set of sensors provide measurements that can be locally implemented by a terminal node to extract alarms. This component is placed "near" the barriers and it is "typically far" from the port control room. A communication gateway shall connect it to the wireless communication network, so to distribute the acquired information (raw data/alarms) to the security personnel in charge of harbour monitoring.

Scenario 2B – Objects monitoring and inventory check

Vessels items are equipped with IoT tags – each tag is paired with the item. System is able to locate items and read their status. It should allow to show: item ID, item status (parameters from eventual sensors, tamper status etc.), item location, signal strength from the item, item lists, location lists, user lists, reports, last time of correctly checked items, notifications, alerts.

Scenario 3 – AI-enhanced situational awareness solutions

This scenario involves multiple AI-enriched IoT systems working together to increase safety and security in the port area. Data from all the systems is collected and presented in real-time to the operators in the port authority control room to increase their situational awareness, support decision making and threat response. Moreover, this scenario covers tracking assets, vehicles, and people (without jeopardizing privacy).

Scenario 4 – Port Maintenance management

The scenario involves the creation of wired and wireless sensors network on the port crane, which will provide data about its actual state and potential faults for the supervisor. The crane supervisor will have access to real-time and historical data through a web-based application. Additionally, there will be the possibility to generate statistical reports about crane operation from the chosen period.

Key components

Below listed components are considered as the most important in terms of use case demonstration:

- Multimodal Positioning System.
- AI algorithms for Predictive Maintenance.
- Embedded software for AI-enriched objects positioning.
- Quality Monitoring Platform and Tool.
- Predictive Maintenance System.
- Security of the Access Control System Edge node.
- Crane Monitoring System.
- V2X communication within Smart Infrastructure.
- Software solution to measure the quality of critical applications and connection.
- Security Information Management Platform.
- Large-scale testbed/emulation platform for V2X Communication with ITS-G5 interface and functionality (including V2V, V2I and V2P).

System architecture

The early stage of Use Case architecture is presented below:

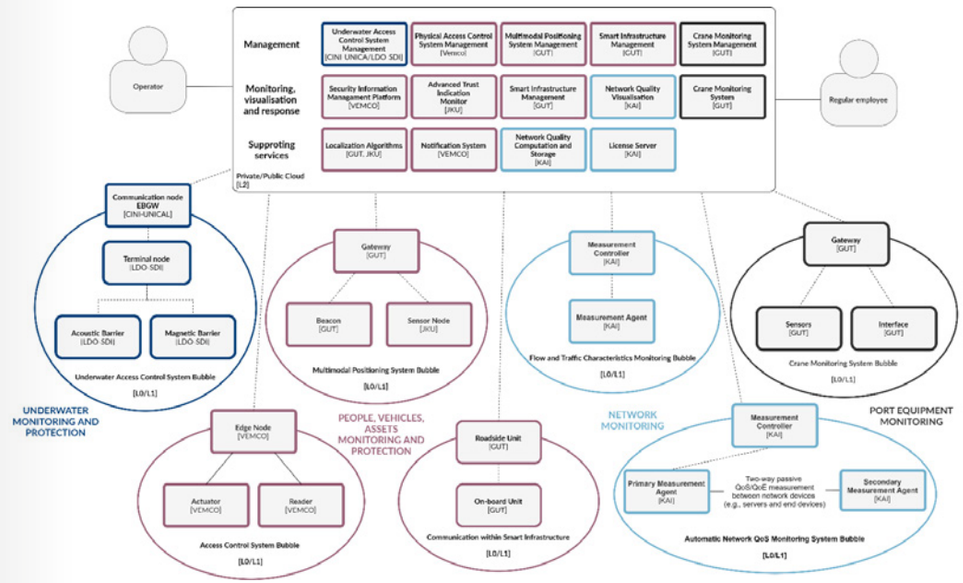


Figure 4.3

Smart and adaptive connected solutions across health continuum

General demonstrator information

In total, 7 different demonstrators are expected in use case 5.5 addressing various aspects of IoT and AI in healthcare context, namely:

1. Use case concept demonstrator.
2. Length of stay with explainability.
3. AI analytics and anomaly detection.
4. Image/RF based vital sign detection.
5. Dynamic system model for biomedical signals.
6. Wearable IoT sensor.
7. AI based wireless optimization.

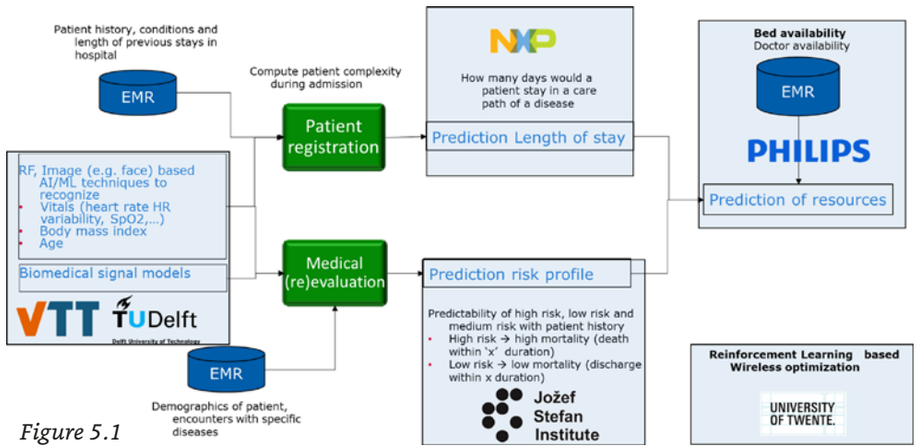


Figure 5.1

Currently, individual demonstrators are prepared in Year 1, demonstrating the ability of 17 different technical components involved in 7 different demo sites/scenarios.

In the upcoming period, integration of 7 different scenarios and 17 different technical components will take place. Upon integration, an overall use case demonstration will be showcased towards the end of the project.

Integration and technical component development are planned to be done in an iterative approach, with a yearly cadence.

Functionalities and key components

1. Use case concept demonstrator: A integration point for 17 different technical components developed by 6 different partners for 7 different demo scenarios.

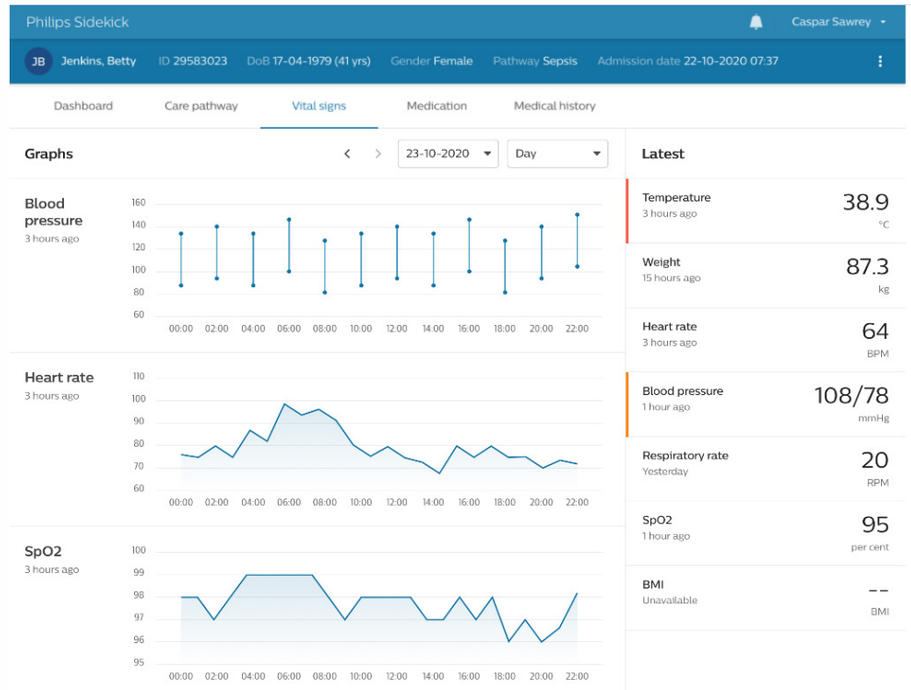


Figure 5.2

2. Length of stay prediction: prediction of the duration for which a patient will be admitted in a hospital based on the patient information available in the hospital information systems.

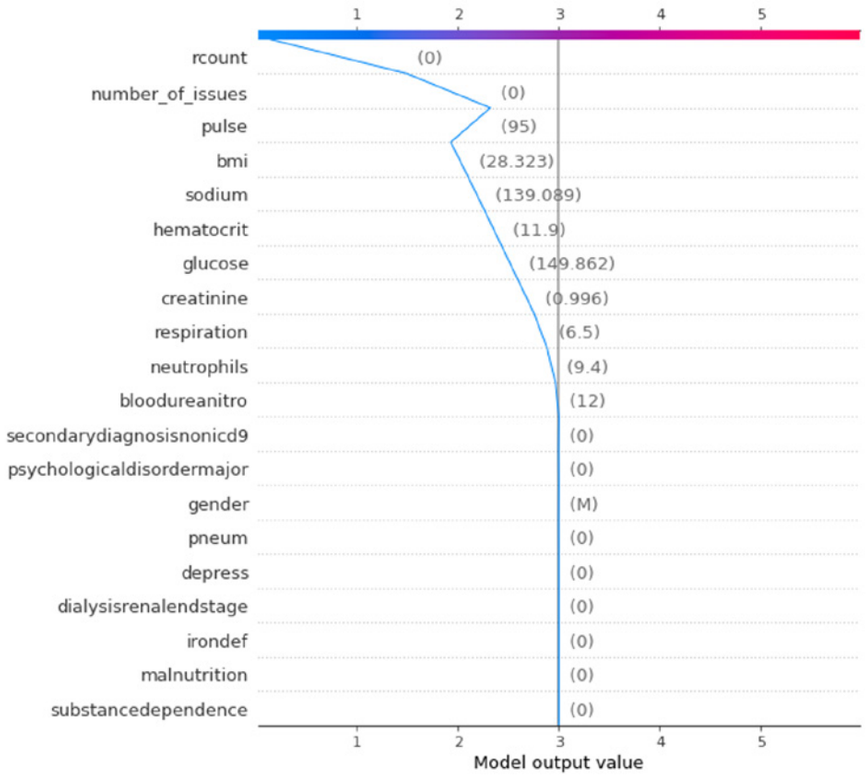


Figure 5.3

3. AI analytics and anomaly detection: detect anomalies in vital sign with explainable AI.

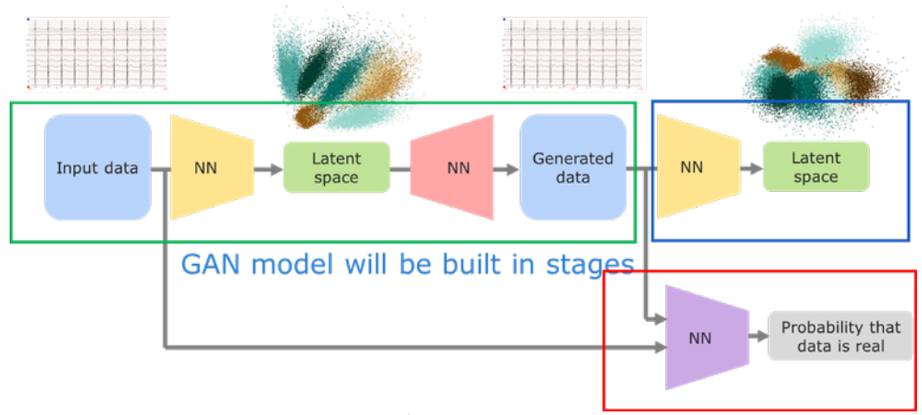


Figure 5.4

4. RF/Image based vital sign detection: Detect vital signs of a patient based on RF Radar and images. Potentially combine the technologies in the later stage.

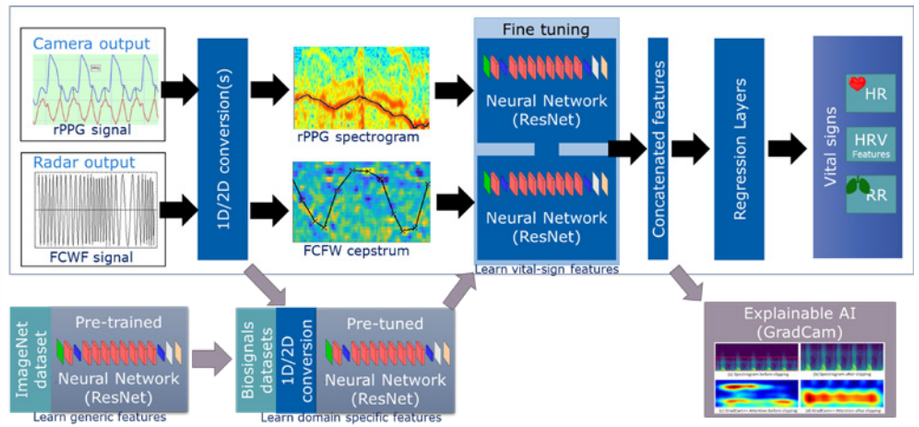


Figure 5.5

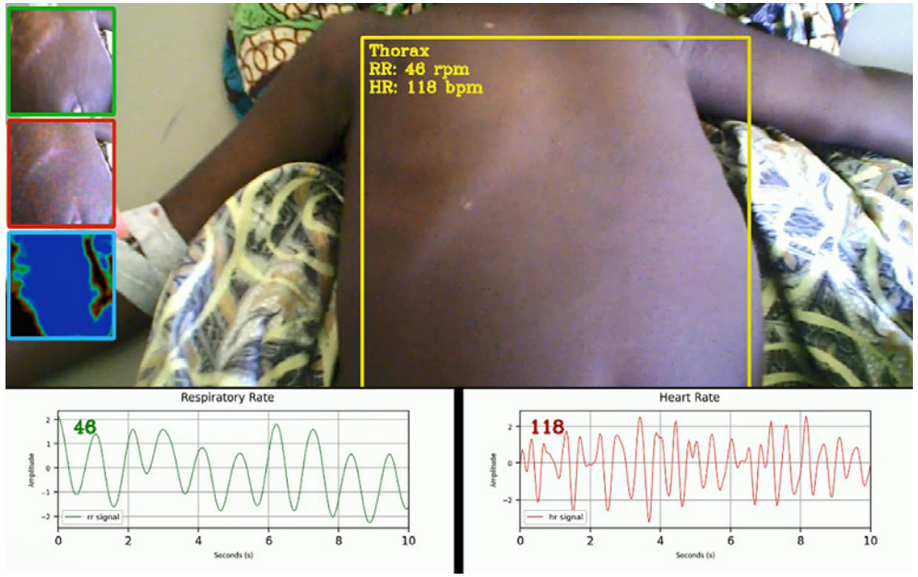


Figure 5.6

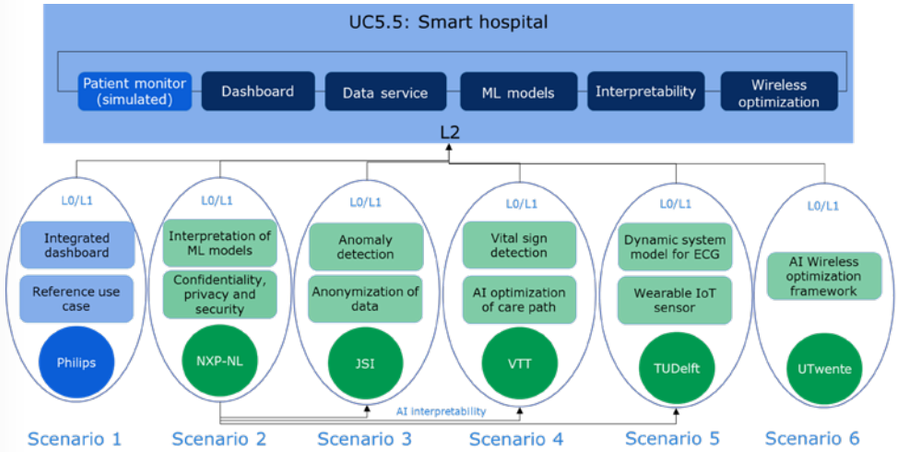
5. Wearable IoT sensor: detect vital signs of the patient using wearable sensors

Figure 5.7

Figure 5.8

System architecture

Early stage architecture of the demonstrator (InSecTT HLA)



PHILIPS · Jožef Stefan Institute · NXP · TUDelft · UNIVERSITY OF TWENTE. · VTT

Figure 5.9

Location awareness for improved outcomes and efficient care delivery in healthcare

General demonstrator information

A use-case concept demonstrator “Emergency Logistics Services” (ELSE) for Mass Casualty Incident (MCI) handling has been developed for use case 5.6 “Location awareness for improved outcomes and efficient care delivery in HealthCare”. The first version has a local running dashboard, but an upcoming version will also run on the web. A second use-case demonstrator is for medical asset tracking in a hospital to improve operational efficiency. Both use-cases address both indoor and outdoor localization and may (re)use similar components for tracking and communication. Various indoor localization solutions are investigated and supported by stand-alone demonstrators from industry and university partners. Prototype implementations for each of these are expected to be available in June (M12). Most of these will be integrated in the use-case concept demonstrators in the next phase (Y2).

Functionalities

A use-case concept demonstrator has been made using a GPS (outdoor) location sensor with a cellular IoT connection to a cloud server using a REST API. An HTML dashboard provides views for general event and triage information, a geographical map, a list of casualties and individual information. It has been connected to the server to provide access to location and personal (including clinical) information obtained from devices at the incident location. Other dashboard features may be added on a further need basis. This concept demonstrator may be used for both demonstration and validation purposes.

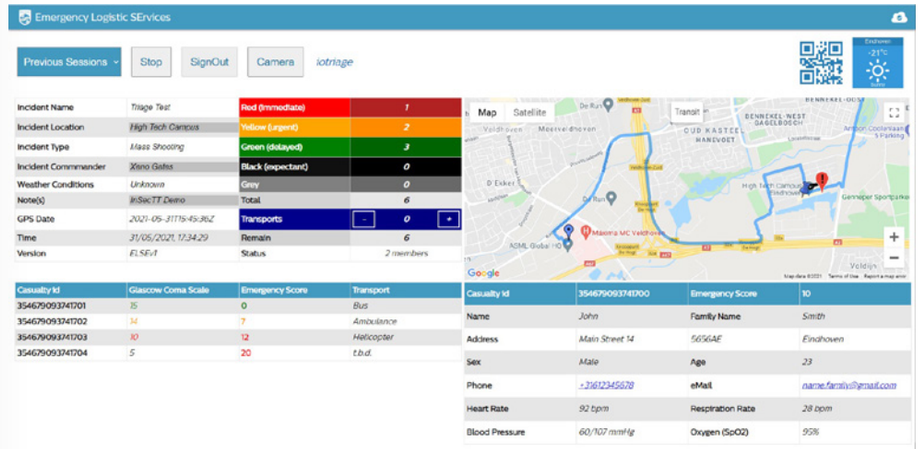


Figure 6.1: Screenshot of the Dashboard for Emergency Logistics Services.

In addition to this, separate demonstrators are under development by each partner in this use-case, corresponding to various (indoor) localization methods as described in the next section. Some of these methods include (X)AI/ML. One example of this is shown in the example below. Integration of these demonstrators in the use case concept demonstrator will be done in a 2nd iteration (Y2).

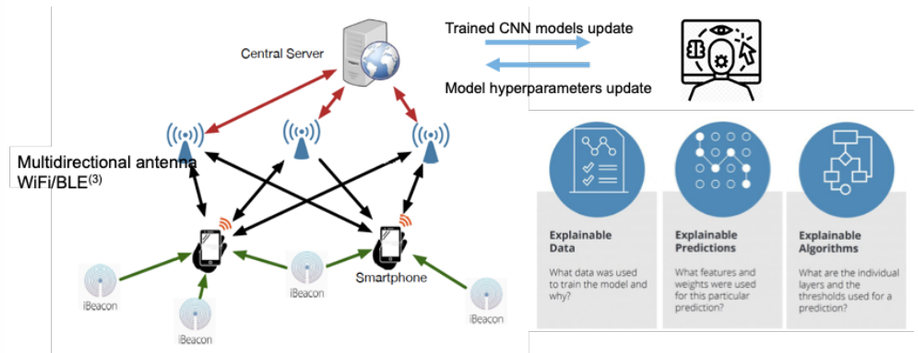


Figure 6.2: Demo’s system architecture for indoor localization using multimodal deep learning with explainability.

Key components

The following components for the demonstrators are under development with status as indicated.

- A dashboard providing an overview of the incident containing an incident information view, a map view, a casualty list-view and a (selected) casualty data view. A working prototype with basic functionality is available.
- A cloud server supporting secure authentication, a map API and a repository for storing data. A demo version has been setup using Google maps. Secure authentication methods and a common repository are still under consideration.
- Logistics tags for showing triage status and reporting casualty location. A prototype for outdoor (GPS) localization is available using cellular IoT communication with the server. Another prototype using MPS is under development (GUT).
- An indoor navigation system using a smartphone App with printed navigation tags is under development by JSI.
- An indoor location system using PIR/Thermopile sensors with optional support for LoRa communication is under development by TU Delft.
- A Multimodal indoor positioning system using a.o. a Multi-directional Bluetooth Antenna is under development by U Twente.
- An explainable AI solution to build a map for the multimodal indoor navigation system is under development by NXP-NL
- A simulation framework for multi-node UWB is under development by NXP-AU.
- A situational awareness solution for building evacuations using image data analytics is under development by WAPICE.

System architecture

The picture below shows the High Level Architecture (HLA) of the use-case demonstrator. Each partner's contribution is included as a separate use-case scenario. The L2 interface is based on the standardized GeoJSON format.

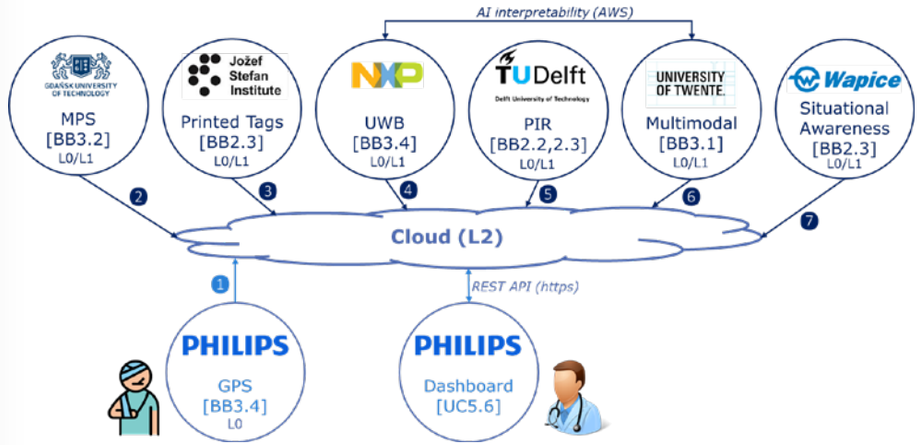


Figure 6.3

Intelligent transportation for smart citites

General demonstrator information

During the first stage of the project and based on SCOTT project results, the data obtained from the different pilots in real environments have been analysed. This detailed analysis of the different data sets has been prepared for each of the components involved. This available information is enough for the developments of the second year of the InSecTT project.

Nevertheless, several pilots have been analysed and managed – based on INDRA collaboration in Shift2Rail program –to fulfil with future requirements due to the project developments improvements.

These will be use to collect the dynamic data needed for the second part of the InSecTT project for each of the components. The data gathered and the results of the developments in the simulators will determine the need for future pilots.

Functionalities

A first approach of the key functionalities of the demonstrator includes:

- Collect and report in real time the position though the wireless sensor actuator network (WSAN). This network is composed of:
  - Galileo GNSS data,
  - GPS GNSS data,
  - Other GNSS data.
- Collect and report proximity information from the wireless sensor network:
  - UWB data,
  - LIDAR data.
- Collect and report in real time information from the train integrity network that consist in a combination of:
  - Accelerometer data,
  - GNSS data,
  - RSSI data,
  - Train Length data.
- Collect and report obstacle information from the wireless sensor network at the critical area:
  - Weight data,
  - Volume data,
  - Composition data,
  - GNSS,
  - Speed.
- Secure wireless communications Vehicle-to-everything (V2X).

Key components

The following components are involved:

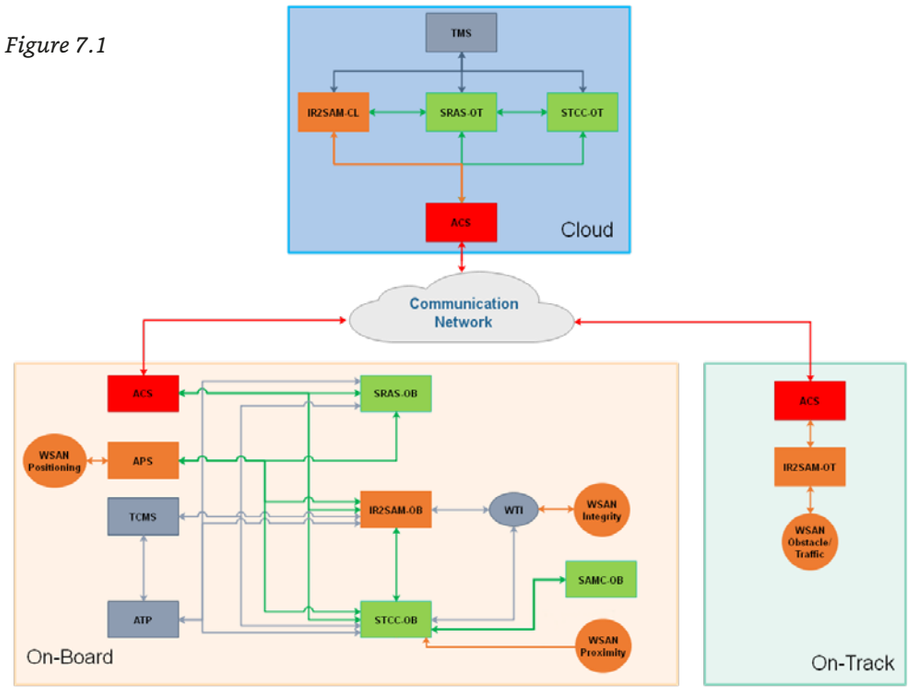
- GNSS Measurements correction and adaptation evaluator (defined for the TBB2.1),
- Train Positioning supervised decisor (defined for the TBB2.1),
- Proximity supervised evaluator (defined for the TBB2.1),
- Proximity supervised decisor (defined for the TBB2.1),

- Train Integrity supervised evaluator (defined for the TBB2.1),
- Train Integrity supervised decisor (defined for the TBB2.1),
- ML Measurements Correction Module and Object Selector (defined for the TBB2.1),
- Object/Priority Decisors (defined for the TBB2.1),
- Private/Public V2X Communication Systems ML Online Models evaluation (defined for the TBB3.3),
- Real-time monitoring and QoS control for IR2SAM (defined for the TBB3.3),
- Intelligent Routing Platform (defined for the TBB3.4).

System architecture

The high-level architecture of the UC5.7 is shown in the figure below.

Figure 7.1



Intelligent automation services for smart transportation

General demonstrator information

During the first stage of the project and based on SCOTT project results, the data obtained from the different pilots in real environments have been analysed. This detailed analysis of the different data sets has been prepared for each of the components involved. This available information is enough for the developments of the second year of the InSecTT project.

Nevertheless, several pilots have been analysed and managed – based on INDRA collaboration in Shift2Rail program –to fulfil with future requirements due to the project developments improvements.

These will be use to collect the dynamic data needed for the second part of the InSecTT project for each of the components. The data gathered and the results of the developments in the simulators will determine the need for future pilots.

Functionalities

- Collect and report in real time the position though the wireless sensor actuator network (WSAN). This network is composed of:
  - Galileo GNSS data,
  - GPS GNSS data,
  - Other GNSS data.

- Collect and report proximity information from the wireless sensor network:
  - UWB data,
  - LIDAR data.
- Collect and report in real time information from the train integrity network that consist in a combination of:
  - Accelerometer data,
  - GNSS data,
  - RSSI data,
  - Train Length data.
- Secure wireless communications Vehicle-to-everything (V2X).

Key components

The following components are involved:

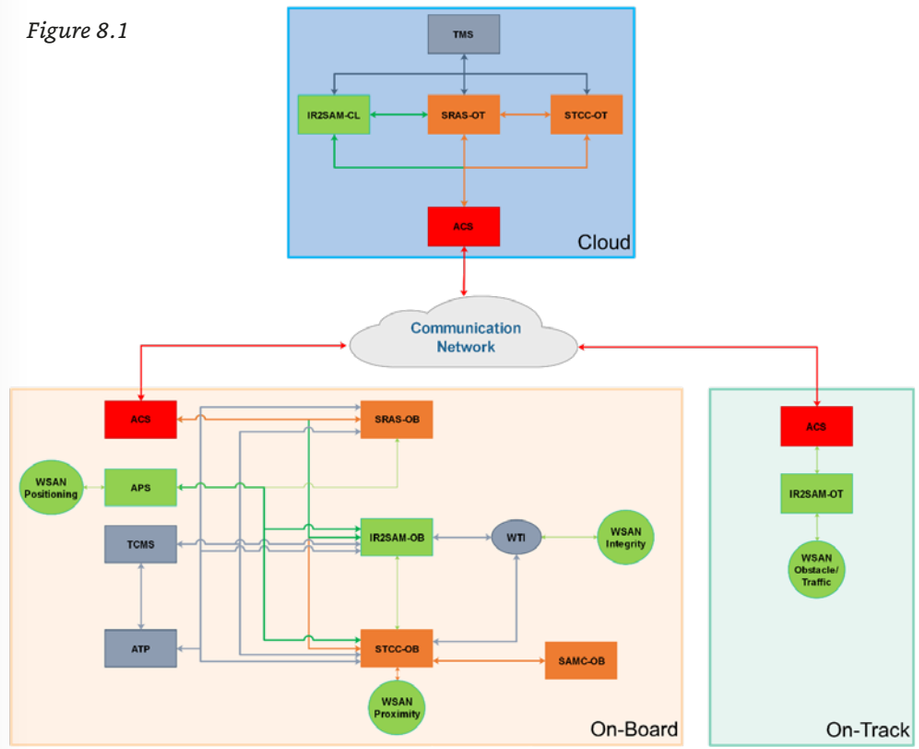
- GNSS Measurements correction and adaptation evaluator (defined in TBB2.1),
- Train Positioning supervised decisor (defined in TBB2.1),
- Proximity supervised evaluator (defined in TBB2.1),
- Proximity supervised decisor (defined in TBB2.1),
- Train Integrity supervised evaluator (defined in TBB2.1),
- Train Integrity supervised decisor (defined in TBB2.1),
- Private/Public V2X Communication Systems ML Online Models evaluation (defined in TBB3.3),

- Real-time Monitoring and QoS control for adaptative coupling distance control (defined in TBB3.3),
- Real-time monitoring and QoS control for platoon level strategy (defined in TBB3.3),
- Real-time monitoring and QoS control for vehicle model (defined in TBB3.3),
- Intelligent Routing Platform (defined in TBB3.4).

System architecture

The high-level architecture of the UC5.8 is shown in the figure below.

Figure 8.1



Cybersecurity in manufacturing

General demonstrator information

The use case (UC) “Cybersecurity in Manufacturing” aims to develop a reliable, secure, and safe communication layer for both wired and wireless industrial networks within a manufacturing network infrastructure. Implementation of a demonstration for the use case in real manufacturing conditions will not be suitable because of the maintain the continuity of the production processes in plants. Therefore, a simulation of the production environment will be set up in the laboratory of Atolye 4.0 that develops Arçelik’s own Advanced Robotics and Automation applications in Arçelik’s production facilities. Atolye 4.0 already has a minimal model of production line infrastructure controlled by a PLC and equipped with industrial robots, RFID receivers, and barcode readers which are interconnected with each other within an industrial network. Below the components in the physical simulation of the production line are listed:

PLC: A Siemens S7-1500 series controller that is tasked with the main control of the Flexlink line, mechanical equipment like stoppers and centering pistons, and coordination of robot movement cycles. Also provides ProfiNet industrial network infrastructure for all equipment on the production line to be interconnected with each other.

Flexlink Line: A model of production line actuated with a single AC(Asynchronous) motor to simulate a continuously running assembly line.
Industrial Robots: ABB, Kuka, and Fanuc robots performing adaptive flexible part assembly, laser measurement, and pick&place tasks on the production line.

RFID Receiver: Industrial-grade RFID receivers on each station for storing product data on RFID tags placed inside pallets for sharing product information across stations.

Barcode Reader: Industrial grade laser barcode reader installed on a station for reading 1D and 2D barcodes installed on pallets.

Currently, the components listed above are already physically present and powered in Atolye 4.0 laboratory. The ProfiNet network is also up and running, communication between devices in the network is already established.

In the next steps, an edge device will be integrated into the communication network for running test scenarios and wireless connectivity will be adapted between industrial equipment and edge device.

Figure 9.1: Atölye 4.0, Arçelik Advanced Robotics Lab.

Functionalities

The functional purpose of the demonstrator is to implement test scenarios generated for the “Manufacturing in Cybersecurity” use case. These test scenarios aim to develop secure connectivity within the wireless and wired OPC-UA networks. Test scenarios will test the security of network connection between an edge device and industrial equipment with a series of simulated cyberattacks which consist of wireless jamming, denial of service, and man in the middle attacks, monitor the network traffic continuously to detect the ongoing cyberattacks and provide a security measure for protecting the devices and communication infrastructure from these attacks.

Key components

Parameter Collection Application for extracting information from network regarding anomalies occurring in the communication network, AI-enhanced Anomaly Detection System for identification of link quality and detection of jamming in wireless network using AI/ML models, Link Quality Monitoring Tool for providing real-time

monitoring of wireless link quality on web-based user interface and Edge Anomaly Detection System for detecting network anomalies with AI-based algorithms on wired communication infrastructure.

System architecture

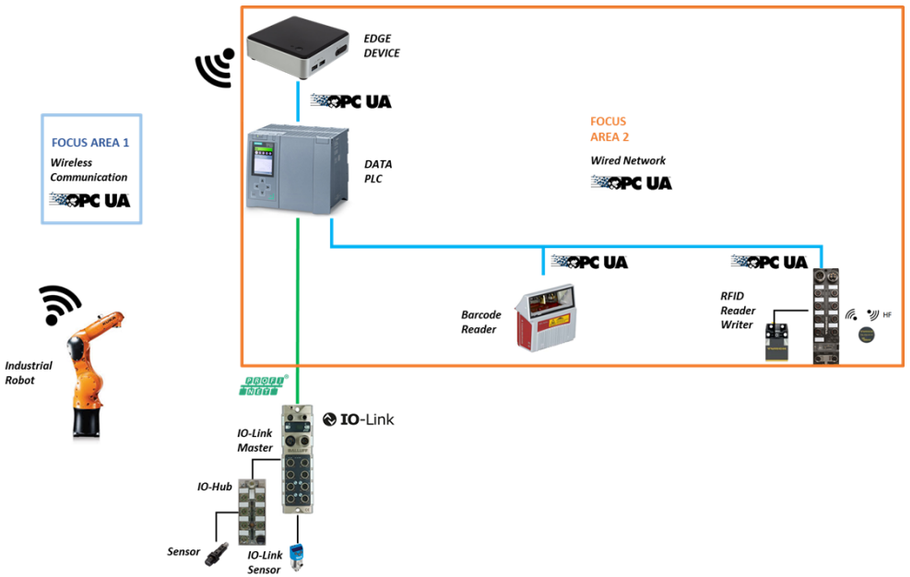


Figure 9.2

Robust resources management for construction of large infrastructures

General demonstrator information

Figure 10.1

At the current stage, the outcomes of the use case "Robust Resources Management for Construction of Large Infrastructures" will be demonstrated in a currently ongoing tunnel construction project of ACCIONA using conventional methods (Drill & Blast). The execution of this project is scheduled to be completed by May 2025, so it encompasses the whole duration of the InSecTT project. Nevertheless, the precise planning of the tunnel construction tasks will be constantly monitored in order to ensure their suitability for demonstrating the successive iterations of the use case. Other construction projects could be selected as alternative / complementary demonstration sites in case there is any risk of incompatibility with InSecTT planning, or if it is considered useful for validating additional functionalities of the use case.

Figure 10.2

The tunnel construction site has already in place a significant ICT and monitoring infrastructure that can be reused for deploying the InSecTT building blocks. Among the main infrastructure and technological components available, the following ones can be highlighted:

- Communications Network: it consists of an optical fibre backbone and a Wi-Fi mesh network, with base stations installed every 500 m of tunnel.

- Closed-Circuit Television (CCTV): it consists of IP rugged cameras and a NVR (Network Video Recorder).
- Gas and Environmental Sensors: it integrates gas measurement stations, distributed environmental/air quality sensors, and personal (portable) gas sensors.
- Tracking System: it is based on Bluetooth Low Energy (BLE), and it consists of fixed readers and tags attached to machinery or worn by workers. Each reader can detect both the presence of a tag and its direction of movement.
- Power Analysers: they are deployed at the power lines in the work zones of the tunnel, in order to measure electricity consumption of the machines and other elements powered by electricity.
- Other Safety and Security Systems: additional safety and security systems are available in the tunnel, e.g. Push-To-Talk (PTT) handsets and vehicle radios communicating through the Wi-Fi network, fixed phones, LED displays, and visual/acoustic alerts for evacuation.

The next main steps planned for the demonstrator are the following:

- Analysis of alternative/complementary location and communication technologies and sensors to cover a wider range of implementation scenarios for workers / machinery tracking and for distributed environmental monitoring.
- Preliminary implementation of the project tracking, safety management, and maintenance management components.

Functionalities

According to the communications and monitoring infrastructure available in the demonstrator, the following main functionalities will be implemented:

- Near real time location of workers, machinery and other assets. Detection of potential interference between workers and machinery.
- Automated identification of project construction tasks, starting from basic detection of the main phases of the working cycle of tunnel construction through the Drill & Blast method (Drilling, Blasting, Mucking & Scaling, Rock Support, Grouting, and Stops).
- Tracking of real project progress based on identified and measured tasks.
- Detection of safety/security related incidents within the tunnel (e.g. dangerous levels of toxic gases, the start of a fire, etc.) and management of emergencies.
- Prevent unscheduled stops of machinery by anticipating the need of replacing spare parts or implementing other maintenance strategies.

Key components

According to the current version of the use case architecture, the demonstrator will integrate 3 main components devoted to real time monitoring, 4 components for advanced processing of data applying AI/ML, and a Graphical User Interface (GUI) in order to access to data and functionalities of the different components.

The real time monitoring components include a worker tracking system, a machinery tracking system, and a distributed environmental monitoring system.

Currently, the worker tracking component of the demonstrator is based on the BLE system previously described. BLE readers are installed every 500 meters of tunnel, therefore it is possible to detect the workers present within each 500 meter-long section. The machinery tracking component currently implemented in the demonstrator is also based on the BLE system and provides similar performance as the worker tracking component. Lastly, the distributed environmental monitoring component deployed in the demonstrator consists of the CCTV cameras that already integrate some built-in intelligence for pre-processing raw video streams, the power analysers that are able to support the analysis of electricity consumption profiles, and the gas and air quality sensors.

The components for AI/ML processing include an activity tracker, a project tracker, a safety manager, and a maintenance manager.

The activity tracker component currently deployed in the demonstrator allows the detection of the main phases of the working cycle of tunnel construction through the Drill & Blast method, using the inputs from real time monitoring components (presence of workers, presence of machinery, and consumption measured by the power

analysers). The rest of components for AI/ML processing will be implemented during the next iterations of the demonstrator.

System architecture

The following figure presents the current specification of the demonstrator architecture, integrating all the components previously described.

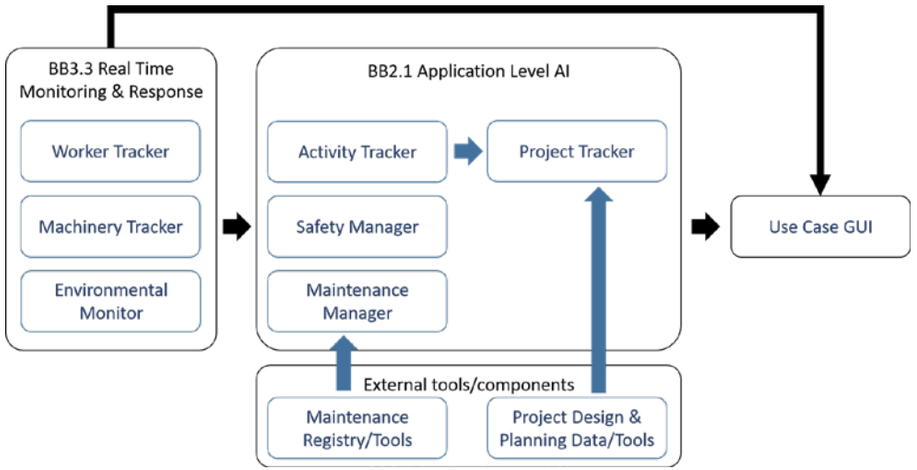


Figure 10.3

Smart airport

General demonstrator information

The use case will have both on site demonstrator, located at Gdansk Lech Walesa Airport, as well as local Partner demonstrators, integrated via e.g. web services. Representatives of Lech Walesa Gdansk Airport are engaged in the verification and validation of both on site and local demonstrators. During the first year of the project, Airport authorities have prioritized their expectations and selected two key technologies with highest business value. First of them is the inspection robot allowing to perform autonomous inspection at the airport area and capable of detecting anomalies through the robot's payload containing multiple sensors. The payload will be characterized by high flexibility as the on-board sensors may be easily swapped in order to adjust the sensing capabilities to the current demands and conditions.

Secondly, GUT will provide the Multimodal Positioning System (MPS), which allows to track assets (in this case baggage trolleys) and notify the administrator if prohibited behaviour is detected. In order to maintain privacy, localization functionalities are based on radio signals measurements done by GUTs reconfigurable antennas.

Lech Walesa Airport is a critical infrastructure, thus only verified, validated and highly reliable components and systems may be deployed on site. Therefore, as a first step, GUT has set up a test environment at its own campus, where prototypes will be tested, verified and improved. The test environment is meant to mirror the actual airport conditions as accurately as possible. Such an approach gives a possibility to validate other InSecTT component in a mirrored, industrial environment.

Partners involved in the Use Case (VIF, KAITOTEK and PAVOTEK) will utilize the test environment in order to validate the Building Blocks. Furthermore, the Airport representatives are to be engaged in the validation and the assessment of the technologies deployed at test demonstrator location.

Functionalities

The demonstrator functionalities are grouped around use case scenarios:

Scenario 1 – Monitoring of the location of luggage trolleys and suitcases

The MPS system provides information about the location of the airport luggage trolleys, based on the RF signals. Furthermore, the luggage itself can be tracked within different zones, e.g. airport gates. Modules used for this purpose are characterized by low power consumption, therefore they should run on a single battery for at least 3 months. The obtained position of the trolley will be displayed via a web application that will be accessible only for authorized users. It will be possible to define specific rules and set alarms when they are broken, for example in case of a trolley leaving the allowed area. Additional metrics like the number of suitcases within a certain area can be displayed and tracked.

Figure 11.1

Scenario 2 – Autonomous inspection of the airport area

The robot can perform an inspection and detect anomalies along the airport boundaries. It will follow a given 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.

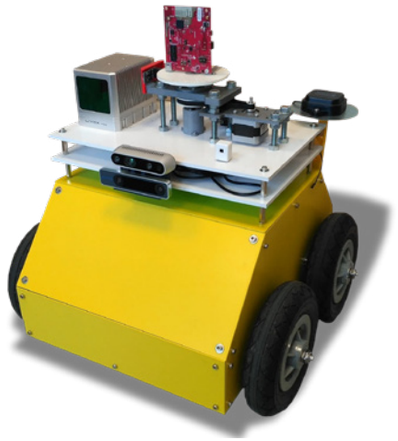


Figure 11.2

Scenario 3 – Securing mission-critical applications in airport

This scenario focuses on implementation and demonstration of a solution to ensure that critical connected applications enable safe and efficient airport operations. The main idea behind the scenario is that the quality of the application's connections over the network are measured and monitored continuously in real-time. If exceptions happen, they are detected and reported with no delay, and recovery actions can be initiated early on.

Figure 11.3

Scenario 4 – Safety & security in airport area

This scenario describes how the Camera & MEC unit helps increasing awareness of vehicles with V2X communication through object detection to improve safety and security at certain locations or to determine the safety of intended action of the vehicle. This is meant for locations such as intersections where vehicles can't receive information from other vehicles in the area due to sensor unavailability or communication insufficiency.

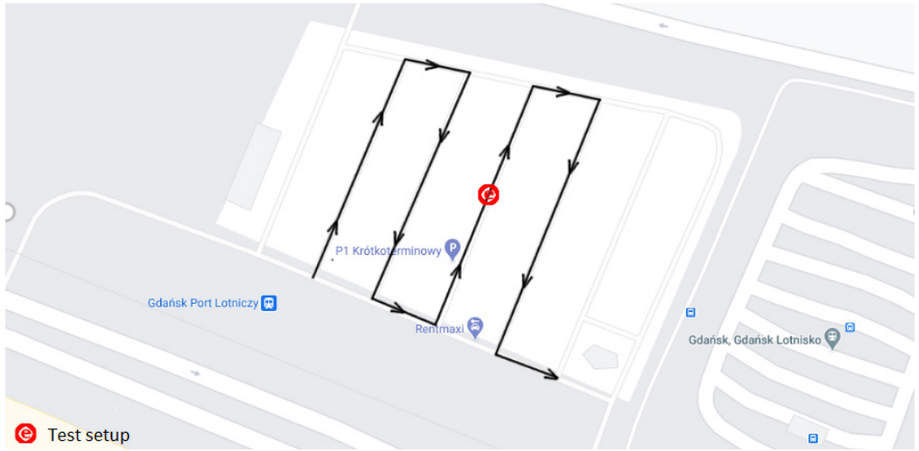


Figure 11.4

Key components

Below listed components are considered as the most important in terms of Use Case demonstration:

- V2X Communication Platform.
- Continuous Learning and Model Improvement Framework.
- Automated Network Measurement.
- Passive QoS/QoE measurement.
- RAIN RFID System.
- Multimodal Positioning System.
- Autonomous Inspection Robot.
- Device Management Platform.

Driver monitoring and distraction detection using AI

General demonstrator information

The use case plans to develop a demonstrator to collect and analyse driver behaviour with particular focus on driver inattention and distraction. The implementation includes the detection of at least one driver distraction event (e.g. smartphone usage) using AI modelling. A dashboard will be used to show the driver distraction events within a given distraction dataset.

The planned demonstrator is a smartphone-based system that uses smartphone sensors to collect data about smartphone usage during driving.

The development will be deployed in two stages:

1. Offline demonstrator: The offline demonstrator aims to detect at least one distraction event (e.g. moving the phone) using AI modelling.

2. Online demonstrator: The online (live) demonstrator aims to utilize an input data stream of smartphone sensor data to detect live at least one distraction event (e.g. moving the phone) using pre-developed AI models on the smartphone.

The destinated locations of deployment will be at the research institutes of Virtual Vehicle Research GmbH (Graz, Austria) and RISE (Kista / Stockholm, Sweden).

The current work is focused on the offline demonstrator and the next steps will be to start the work in the online demonstrator.

Functionalities

The use case plans to develop a demonstrator to collect and analyse driver behaviour with particular focus on driver inattention and distraction. The implementation

includes the detection of at least one driver distraction event (e.g. smartphone usage) using AI. A dashboard will be used to show the driver distraction events within a given dataset – a trip of the driver.

Key components

Four components are planned to build the demonstrator:

1. Smartphone application for data collection: Capable of collecting smartphone sensor data, which later on will be used to develop an AI model. Data collection includes data cleaning, pre-processing and storing of the smartphone sensor data.

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

3. Evaluation of the AI model in the smartphone application: The component includes: i) evaluation of the accuracy of the AI model; ii) evaluation of the feasibility and thresholds of the computation.

4. Usability evaluation of the smartphone application: Evaluating the usability of the driving distraction application taking into consideration trustworthy and explainability aspects, as well as limits of the cognitive load of the driver.

The status of the development is that we have achieved to complete:

1. software architecture design,

2. initial sensor data collection, and

3. a first smartphone application design concept,

4. smartphone application proof-of-concept to connect to vehicles' on-board diagnostics (OBD) system for data collection.

System architecture

Present early stage architecture of the demonstrator (InSecTT HLA) Figure 1 presents the high-level use case architecture, including the physical devices used in the use case.

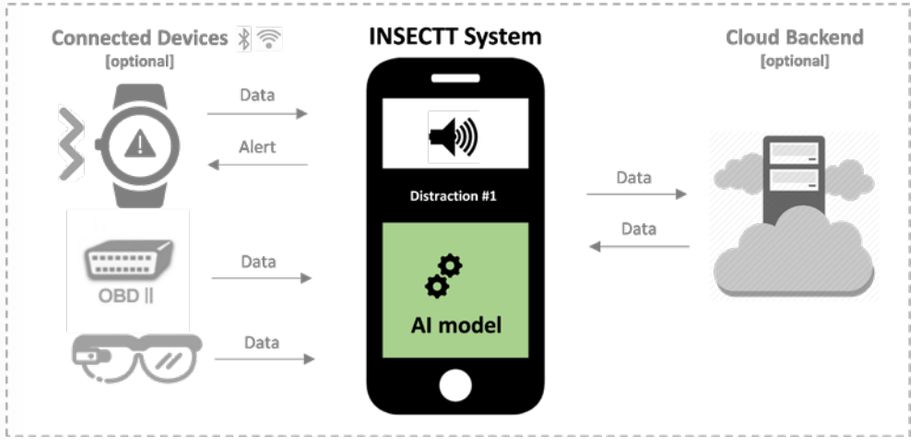


Figure 12.1: High-level use case architecture around the main device: The smartphone.

Secure industrial communication system

General demonstrator information

We will create our ICS testbed to test and validate our cyber-security solutions, including IDS methods. To achieve high fidelity, we emulate both network traffic and controlling plant in our testbed. Currently, we designed a plan for the 'Beta Version' of the testbed. The next step would be the construction of the testbed which will include the following components:

- **Plant instruments**: To simulate the plant process and instruments, we will use open-loop controlling problems to show the miniaturized version of a plant. We may use any open-loop controlling problem in the future, however, we nominated three scenarios for initial implementation which include a water tank scenario, a conveyor belt scenario, and a ball and beam scenario.

- **Controlling system:** Controllers, as the heart of controlling systems, are responsible for sending control commands based on sensor signals and user stimuli. Control engineers use high-level languages such as SFC, FBD, ST, and Ladder to generate control logic for controllers. To create a control logic for the testbed we could use open-source applications such as 'open PLC' software to develop logic commands, but it is a complicated and time-consuming approach. As an alternative, we could write simple C++ or Python scripts to generate control commands. For the beta version of our testbed we use simple scripts, however, we may choose to use control logic programming languages in later versions.

- **Network:** The network emulation will realize with container technology, where each ICS component will be deployed in a container. Containers let us simulate any type of network connection include of hard-wired connections and IP-aware connections. This setup facilitates integration of our partners' devices to this testbed, as long as their code would be available on the container technology. Several Technologies support containers, of which Docker and GNS3 are the most famous.

- **Observer & Management Network:** Generates data to be used further for intrusion detection and prevention modules.

- **Attack Generator:** Responsible to act as an intruder and generate cyber-attacks, such as Command injection, False data injection with IP Spoofing, and Denial of Service (DoS).

Functionalities

This use case develops a testing environment for ICS to integrate and validate different components, such as IDS. This environment includes digital twin to model a physical process. This allows operators to analyse each component of a physical process and detect issues before they occur, including issues that may impact the quality of products. Moreover, other components will be added to this environment including AI-based IDS to detect and classify attacks and intrusions. There have been several testbeds developed for ICS, however, our solutions will be easy to develop based on container technology and facilitates integration of our partners' devices to this testbed.

Key components

We presented testbed components in the general demonstrator section. We also have a component for each of our approaches toward cyber-security.

- Intrusion Detection in Digital Twins for Industrial Control Systems (defined for the TBB2.1),

- Anomaly detection by ML algorithms (defined for the TBB2.1),

- Distributed Intrusion Detection Systems at the edge level (defined for the TBB2.3),

- Distributed Learning methods (defined for the TBB2.3),

- Federated Learning algorithms (defined for the TBB2.3),

- Digital twin for testing industrial control systems cybersecurity (defined for the TBB3.1),
- Virtual environment for testing ICS cybersecurity (defined for the TBB3.1),
- Anomaly models and assurance cases (defined for the TBB3.1),
- Intrusion detection and prevention system (defined for the TBB3.1).

System architecture

The high-level architecture of the UC5.13 is shown in the figure below.

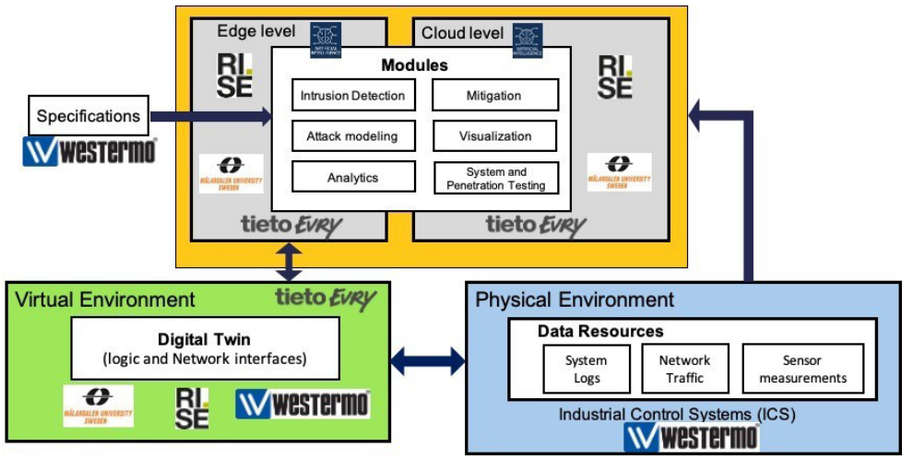


Figure 13.1

The physical environment in this figure is realized through our testbed. We designed the reference architecture of our testbed based on the "Purdue Enterprise Reference Architecture". which includes an enterprise zone (Tier 5), Demilitarized Zone or DMZ (Tier 4), and control zone (Tier 1, 2, and 3). The Below figure shows the logical network architecture and the tiers of our testbed.

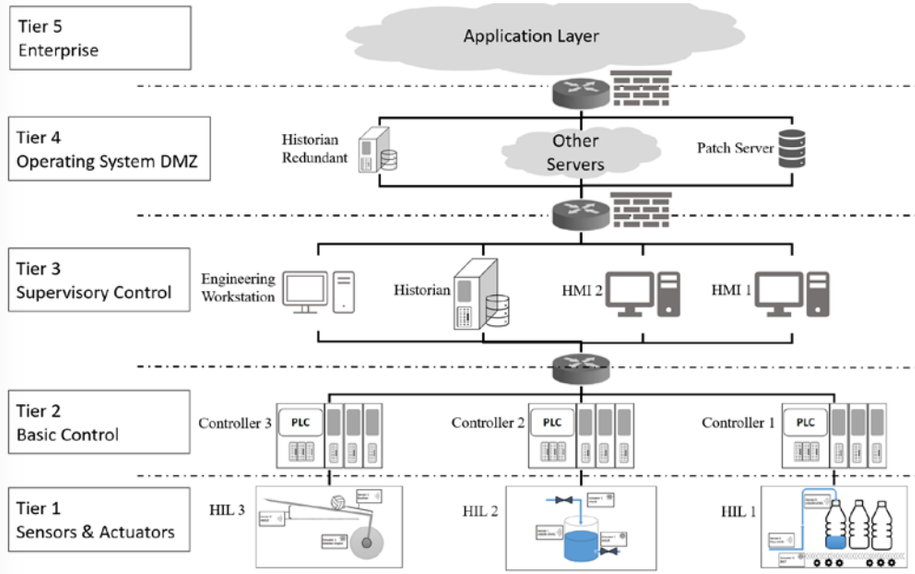


Figure 13.2

Secure and resilient collaborative manufacturing environments

General demonstrator information

The demonstrator is connected to use case 5.14 on secure and resilient collaborative manufacturing systems. There are currently plans for one demo site, located at Mälardalen University (MDH), in the form of a simulated modular ice cream factory. In the demo site all the key components of use case 5.14 will be demonstrated, including access control policy generation, authorization enforcement architecture and methods for anomaly detection.

The first batch of equipment for the demo site is purchased and is currently being set up for proof-of-concept studies. When confidence in the technology choices is built, there will be a scale-up of the equipment.

Functionalities

The functional scope of the demonstrator is to produce ice cream in a modular plant where each module has independent internal processes but is interconnected with neighbouring modules in the physical flow of material. The activation of each module is controlled by an orchestrator according to an engineered SFC recipe in a secure way. An authorization service will provide enhanced security with an enforcement architecture model for access control.

Key components

DCS system – Engineering and Operations

In an automated manufacturing system, there is need for supervision and operations of the process, as well as engineering upon required system changes. In the demonstrator system, this is done using standard components of the ABB Ability 800xA DCS system.

Recipe Orchestration and Module Control

For recipe orchestration, being the high-level synchronization and execution of the process, an orchestrator unit able to execute recipes formulated as part of integration engineering. In this system this is done by ABB 800xA Control Services. The same type of control logic execution engine will most likely be used for the detailed module control, with the addition of a connectivity service able to interact with process simulation engine.

Process simulation

The modules of the modular automation system will be individually controlled, but yet operate in the same physical environment with material flow and physical constraints between modules. To facilitate that, a framework for simulation of the physical modules in the factory is developed, along with basic control-logic for the end-to-end proof of concept studies. During the summer and fall of 2021 the physical simulation environment is planned to be finalized, including nodes for engineering and operations, orchestration of workflows as well as control and physical behaviour of modules.

Authorization enforcement and policy generation

An initial implementation of the policy generation algorithm is completed, and integrated in a simple proof-of-concept simulation. Plans for fall 2021 – spring 2022 is to implement a policy enforcement architecture to integrate into the demo site, using the policy generation algorithm for a subset of the policy inferences.

OPC UA and network infrastructure

The interactions within the system will utilize the OPC UA communication protocol, as current standardization efforts mandate. This implies requirements on certificate handling, data models, etc., which will make the proposed solutions interoperable with other system types utilizing OPC UA.

System architecture

The high-level architecture of the demonstrator system, illustrated in Figure 1, is aligned with the InSecTT DEWI bubble architecture in the following way: Each module is at layer Level 0, containing the physical module, including detailed control and an OPC UA server for northbound interactions. The operations, supervisory control and orchestration of one physical process is at layer level 1. Central monitoring and optimization are at layer level 2.

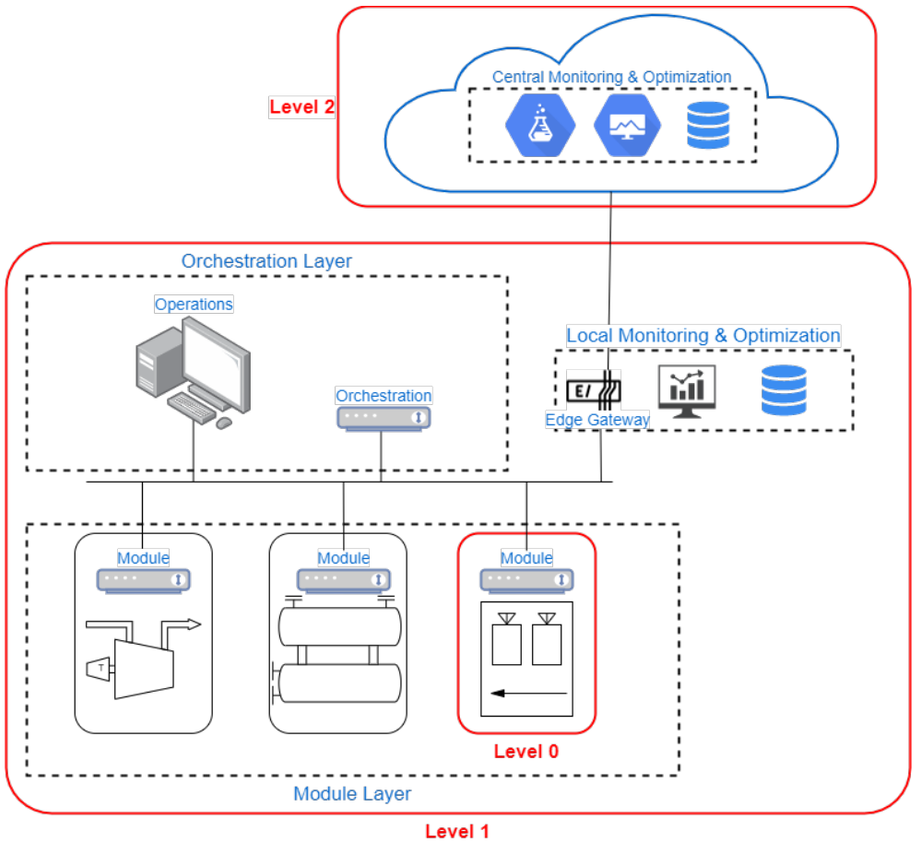


Figure 14.1. UC 5.14 High-level architecture

Airport security – structured and unstructured people flow in airports

General demonstrator information

The outcomes of the UC will be demonstrated at Taranto-Grottaglie Airport, a remarkable example of integration between air transport and aerospace industry. Already integral part of the program for the production of the fuselages of the Boeing 787 "Dreamliner", and already authorized by ENAC (the Italian Civil Aviation Authority) as a "testbed" for the research and testing of unmanned aircraft, the airport is currently involved in further development as a strategic infrastructure for Europe, having been identified by the Ministry of Infrastructure and Transport as the first Italian spaceport destined to accommodate suborbital flights.

With reference to the infrastructural equipment, Taranto Grottaglie airport is equipped with a runway with RWY 17/35 orientation, having a length of 3.200 meters and a width of 45 meters. The terminal area (passenger terminal and aircraft aprons) is centred with respect to the runway and located west of it. The passenger terminal, in particular, has an area of about 3.500 square meters, distributed over three levels, and is equipped with 6 check-in desks and 2 boarding gates.

The use case presents three different Scenarios, two of them dealing with monitoring of structured (Scenario 1) and unstructured (Scenario 2) flow of people within the Airport area and one concerned with the tracking an anomalous situation (Scenario 3). These Scenarios will be demonstrated through the implementation of the following components:

- Multi-biometrics recognition on-the-move (Scenario 1),
- Environmental monitoring: people flow monitoring and anomalous substances detection (Scenario 2),
- Social Distancing monitoring (Scenario 2),
- Thermal Screening (Scenario 2),

- Audio Recognition for anomaly detection (Scenario 2),
- Multi-Interface Gateway (MIG) (Scenario 2),
- Tracking of a person-of-interest (Scenario 3).

At the moment only a preliminary inspection of the demo site has been done due to the pandemic limitations. However the information gathered were sufficient to establish the HW to be deployed in the demonstrator. The High Level Architecture (HLA) of the UC has been defined; partners have been working together to make the HLA compliant with the Reference Architecture Guidelines of the InSecTT project.

Functionalities

For what concerns Scenario 1 the demonstrator will provide evidences of the accuracy and efficiency of the multi-biometrics recognition on-the move by installing two gates, one for the passenger enrolment and another one representing an access gate.

For Scenario 2 we will use AI/ML algorithms and sensors to prevent/react to overcrowded situation and anomalous events (social distancing, thermal screening and audio recognition) as well as the presence of hazardous chemical agents (environmental monitoring) and people counting within the terminal area, enhancing a prompt response from the Security Operators. The efficiency of the proposed solutions in the different cases presented in Scenario 2 will be tested. Finally, the Multi-Interface Gateway will continuously check and possibly improve the reliability and continuity of service of the wireless communication within those entities that rely on this communication technology.

Concerning Scenario 3, we will show that, triggered by the alerts provided by the environmental monitoring, the tracking of a person-of-interest will be able to identify a suspect. This functionality will provide an efficient tracking system which will allow security operators to take a prompt action on the basis of strong premises without over-alerting the rest of the passengers in the Airport.

The following table depicts the various scenarios and the functionalities that will be demonstrated.

Scenario 1: Enrolment & Gate crossing on the move (Structured Flow)	
Actors	► Travelers in the airport ► A legitimate traveler (named Alice) ► A non-legitimate traveller (named Bob) ► Control center operator(s)
Description	► Alice goes to the airport to take a flight. In order to speed up the security check, Alice enrols herself at the airport biometric recognition system. ► Enrolment is carried out at a dedicated site, where Alice provides an identifier, an informed consensus, and two biometric data, namely face and hand vein patterns, following the shown instructions. ► Once enrolled, Alice moves to the dedicated security check area, where her identity is checked while requiring minimum interaction from her side. ► Upon correct identification, Alice can proceed towards the secure areas of the airport. ► Without being enrolled, Bob moves towards the security check area, where his identity is checked. ► Bob is not recognized and consequently he is stopped at the e-gate.
Trigger	► Alice presents herself at the enrolment site ► Alice arrives at security check area
Flow of the events	► Alice arrives at the airport ► Alice presents herself at the enrolment site ► Alice provides the required data (identifier, consensus, biometric traits) ► Alice moves towards the security check ► Alice passes through the security check area and is recognized. ► Bob moves towards the security check area ► Bob passes through the security check and is not recognized.

Scenario 2A: Anomaly Detection (Unstructured Flow)	
Actors	► Passengers at the airport ► A passenger carrying a dangerous substance ► Control center operator(s)
Description	A typical day at the airport starts with a few people entering the main hall, starting to check-in luggage and scanning their IDs at the checkpoints. They later stroll around the airport's open spaces until the gates open. The airport's open spaces are equipped with a sensing infrastructure composed of passenger counters, people flow monitors and environmental monitoring systems installed at strategic positions. The situation is under control both in terms of number of passengers and in terms of anomalous substances detected. Later on, while approaching flights departure, more and more people are entering the airport, passengers are queuing in front of the check-in desks and at the security checkpoints. They also start clustering inside restaurants and cafes. This situation may be potentially harmful in terms of epidemic spreading and, in general, in terms of security and safety because of overcrowding. The data collected from the flow monitoring system and from the environmental sensors is constantly analysed by a dedicated intelligent software (based on AI) installed on the multi-service IoT gateway. At this point the software detects the overcrowded situation and generates an alert event which is sent to the control center operator. The operator quickly decides if additional check-in desks or security checkpoints need to be opened (when available), and sends out a general announcement encouraging people to respect social distancing. In the meanwhile, the presence of an anomalous substance at the airport is recognized. Three sensors hosted on the environmental stations reach a peak in sequence, as the carrier moves through the open spaces. The peaks pinpoint the presence of a dangerous substance. The software installed on the environmental station detects the situation and immediately sends an alarm to the control center operator. The operator alerts the security who is immediately sent on the spot with detection dogs to check the situation.
Trigger	► Abnormal people clustering or overcrowding ► Detection of anomalous substances in the air

Scenario 2A: Anomaly Detection (Unstructured Flow)	
Flow of the events	► A few people enter the airport early in the morning, they start the identification procedure and finally they stroll around the main hall. ► The sensing infrastructure installed in the airport's open spaces detects no anomalous situation. ► Close to the departure time, more and more people enter the airport and form clusters at the check-in area, at the security checkpoints and inside restaurants. ► A critical situation is reached in terms of overcrowding in correspondence of those areas. ► A passenger is walking through the main hall with a dangerous substance in the luggage. ► A set of 3 environmental stations detect the presence of the substance as the carrier moves. ► The software installed on the IoT gateway continuously analyses the data coming from the sensing infrastructure. ► The IoT gateway sends an alert to the control center operator to indicate the presence of overcrowding. ► The IoT gateway sends an alert to thxe control center operator to report the presence of a dangerous substance. ► The operator decides if additional check-in desks and security checkpoints need to be opened. ► The operator makes an announcement inviting people to respect social distancing. ► The operator sends the security with detection dogs to check the passengers for potentially dangerous substances.

Scenario2B: Anomaly Detection (Unstructured Flow)	
Actors	► Passengers ► A group of friends ► Security control center operator(s)
Description	Passengers are approaching the security checks. Here they are spotted by cameras monitoring the security check lanes for social distancing and counting. Currently only a couple of security check points are open, but the flow of passengers is increasing and the lines are growing. People counter module detects this situation and triggers an alert to the security control center where the proper countermeasures can be activated (eg. open further security check points). At the security check passengers are also screened for fever using AI-based algorithm applied to thermal camera streams. None positive case is detected and all the passengers can continue their way to the boarding gates. In the meantime, at a boarding gate a group of 6 friends are standing too close while waiting for boarding. That area is monitored by cameras on which social distancing algorithm has been configured. The security control center operator is notified about the social distancing violation and he can send the security personnel to the gate to manage the situation.
Trigger	► Too many people in the security check line ► A group of friends violates social distancing
Flow of the events	► Passengers go through security checks. ► People counting module detects too many people in security check line. ► Anomaly is signalled to the security control center in order to take the appropriate countermeasures (eg. open a further security check point). ► A group of friend waiting at another gate for boarding is continuously violating the social distancing. ► The information is signalled to the security control center. ► Security personnel is sent to the gate to manage the situation.

Scenario 3: Anomaly Tracking	
Actors	► A passenger carrying a dangerous substance ► Control center operator(s)
Description	The system detects and tracks both suspicious and unsuspicious persons, using graphical, easy to spot indicators/images to avoid confusing the two types in a rather complex scene. When the dangerous person is detected (see Scenario 2A), the system starts the tracking activity in the area surrounding him/her. This action is taken in order to: immediately allow security people to stop and check the suspicious subject, allow to catch the suspicious subject and keep it under control and to recognize the path of the suspicious subject seeking for partners.
Trigger	Event of hazardous substances from the system operating in Scenario A.
Flow of the events	► The system automatically enrols all the people entered the airport. ► A trigger comes from the hazardous detector system, defining the area of interest. ► The area is highlighted in a cartographic viewer made available to the control center operator. ► The system tracks all the people inside the area over the entire airport in order to allow the control center operator to deduce the path of the suspicious subject. ► The system allows the control center operator to re-identify the enrolled people on biometric basis over the recorded data.

Key components

As mentioned earlier the components that constitute the demonstrator are the following:

- Multi-biometrics recognition on-the-move (Scenario 1),
- Environmental monitoring (Scenario 2),

- Social Distancing (Scenario 2),
- Thermal Screening (Scenario 2),
- Audio Recognition (Scenario 2),
- Multi-Interface Gateway (Scenario 2),
- Tracking of a person-of-interest (Scenario 3).

The HW needed for the different components has been identified, as well as the design of the MIG and of the environmental sensors. A preliminary inspection of Taranto-Grottaglie airport has been conducted, in order to understand where the HW can be installed. The location of the HW components however is still to be determined. Most of the AI/ML algorithms have been designed and wait to be trained with properly constructed datasets. The algorithm for tracking of a person-of-interest is still under design.

System architecture

As previously stated, partners involved in this UC made concrete efforts in order to be compliant with the Guidelines proposed for the Reference Architecture of the InSecTT project. The current high level design of the solution, described in terms of the InSecTT Reference Architecture Guidelines is presented in the Figures below. The first Figure represents the Architecture of Scenario 1, the second instead corresponds to the Architecture for Scenarios 2,3:

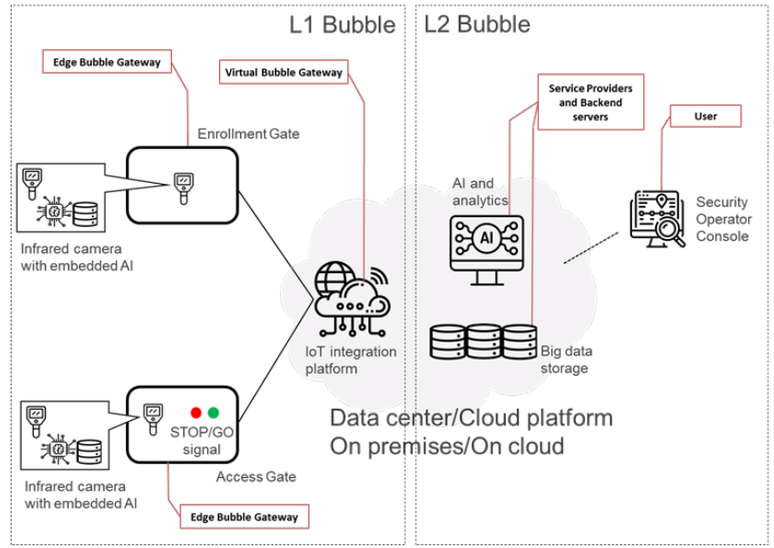


Figura 15.1 - Architecture for UC16, Scenario 1: Structured flow of people within the Airport

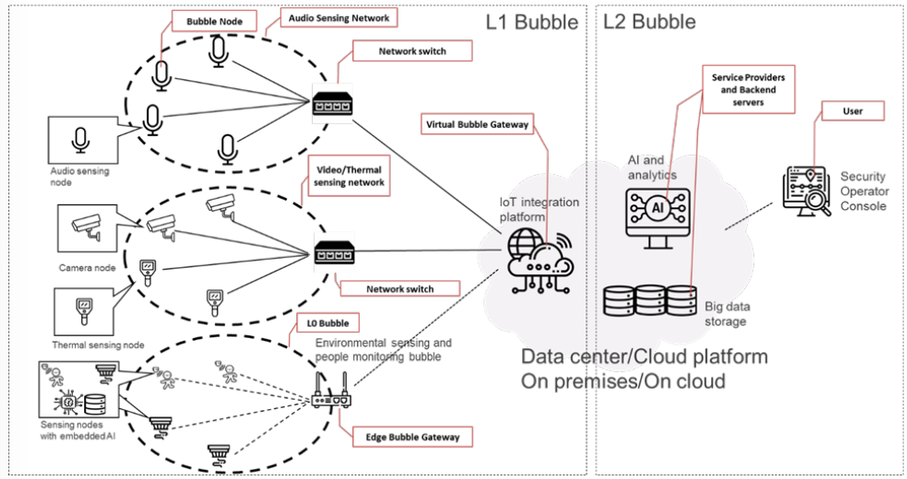


Figure 15.2 – Architecture for UC16, Scenarios 2,3: Unstructured flow of people within the Airport & Anomaly Tracking

CONTACT INFORMATION

PROJECT COORDINATION

Michael Karner

email: michael.karner@v2c2.at

PROJECT MANAGER

Manuela Klocker

email: manuela.klocker@v2c2.at

https://www.insectt.eu

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

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