InSecTT

Intelligent Secure Trustable Things

Use Case Booklet

3

Wireleless platooning communication based on AI-enhanced 5G

Generic use case description

We can define a platoon as a formation of autonomous or semi-autonomous vehicles that make decisions and coordinate their movements as a single entity. Vehicles of a platoon usually have similar routes or destinations. This makes traffic-flow and network management (V2X) more efficient as vehicles arranged in platoons can reduce processing complexity by offloading functionalities to lead cars and/or edge/cloud vehicular servers, as per illustrated in the following figure:

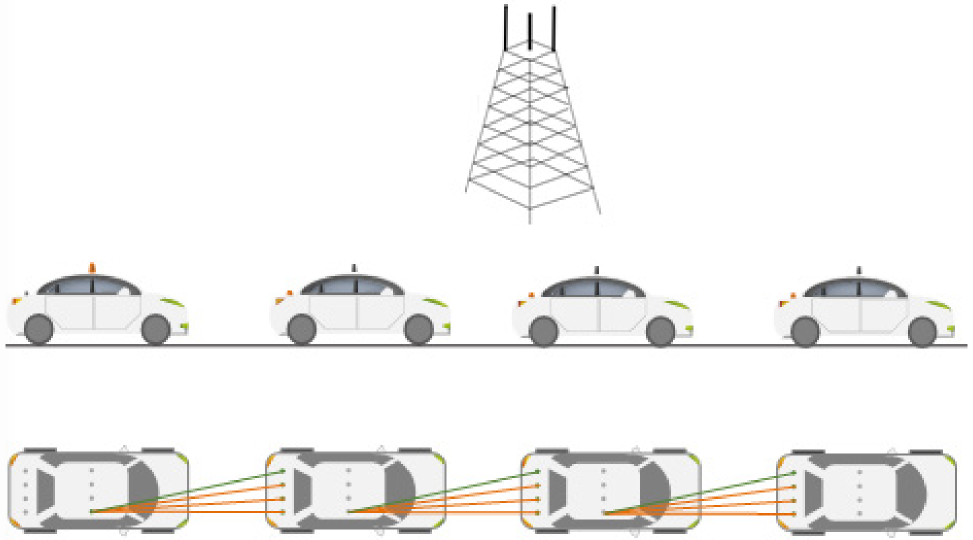


Figure 1.1

Platoons are thus the basis of future automated e-transportation systems (including, trucks, fleets, freightliners, etc). One key enabler of platoons is the coordination and reliable (real time) exchange of information between contiguous cars or between cars and edge/cloud servers.

This use case aims to improve the operation and control of platoons by using artificial intelligence to improve the control of the platoon operations and also to increase the reliability of V2X and V2V communications, reducing risks and increasing the trust of the end users on this type of smart transport applications. The platoon systems are assumed to use a mix of V2V and V2X (cellular) technologies to ensure the low latency and high reliability of critical control messages between the vehicles of the platoon. Advanced securities features for platoon scenarios will also be considered.

The use case will use innovative technologies and develop solutions which will be demonstrated through the following four scenarios:

Scenario		Short description
1	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 of this scenario is to evaluate the performance of the V2V and V2X infrastructure in the presence of inter platoon and inter cell interference. Another central objective is to evaluate platooning protocols and manoeuvres in challenging traffic conditions. AI algorithms will be used to detect/reject interference, reduce latency, improve reliability, and optimize platoon management in dense traffic conditions.
2	Latency mitigation in Emergency Braking	This scenario considers a stress test for both the platoon communications links and the platoon coordination management protocol. An emergency braking scenario is considered where the platoon entities must engage in a set of protocol steps that allow the braking signal to be transmitted with high priority towards all the elements of the formation with the lowest possible delay. The performance of this communication critical protocol defines the ability of the platoon to stay safe in case of a near collision event.
3	Replication of platoon behaviour in physical testbed	This scenario considers the implementation of designed protocols and platoon manoeuvres on a robotic physical testbed. The designed protocols or solution will be adjusted to the constrains of the physical testbed to provide a proof-of-concept implementation.
4	Platoon coordination and wireless resource management in tunnels	This scenario considers the platoon management coordination control and communications when travelling inside a tunnel. This represents a challenge of connectivity and the platoon and the network infrastructure will be designed to react and adapt to provide seamless connectivity, reliability and low latency in these challenging propagations and driving conditions.

Challenges

We can identify two main challenges in this use case:

1. The improvement of the reliability, security, and latency of all communications between the entities of the platoon architecture, i.e., the Improvement of the connectivity of the elements of the platoon to communicate with each other or with an Edge/cloud vehicular infrastructure.

2. The improvement of the platoon operation and resource management, i.e., the improvement of the capability to make an efficient resource allocation, traffic management and platoon organization in a multiple platoon environment with multiple road-side units, or base stations and multiple interfering transmissions from multiple networking entities.

To tackle these challenges, our approach will consist in:

1. Making use of MIMO tools in order to reduce interference inside the platoon and towards other platoons;

2. Implementation of an OSS system capable of processing platoon data to dynamically adapt network infrastructures accordingly, via 5G network slicing, where end-to-end networks can be segmented in an isolated manner to support different service requirements, through the usage of AI mechanisms that are able to combine data from platoons and the network infrastructure.

3. Usage of smart city sensors to complement vehicle sensors. This implies using analytics applications deployed near the sensors so that all data can be processed and sent to vehicles in very short time scales, i.e., near real-time.

4. Design of a vehicular edge and cloud infrastructure that can make use of AI algorithms to improve platoon formation, traffic management, and optimize route selection in urban scenarios.

The considered use case is characterized by the following main objectives:

1. To demonstrate the contribution of AI to vehicular platooning applications, considering two levels of AI that must be coordinated in future V2X applications:

   a. The improvement of wireless connectivity in terms of reliability, latency and security/safety for vehicle platoon and in general V2X applications.

b. The autonomous operation/control of hundreds of platoons at the city level under smart autonomous transportation systems. This involves coordination of platoon maneuver, formation, authentication, authorization.

2. To take advantage of improved 5G tools specifically suited for vehicle platoon communications, enhancing not only connectivity but fusing the decisions of the autonomous vehicles with the radio resource allocation and PHY layer adaption via an AI framework. This is driven from the need for analysing latest 5G developments for supporting V2X communications in platoon communications:

   a. The evaluation at the system level of 5G and legacy vehicle platoon communication with hundreds of platoons and relay nodes interacting with fixed and aerial infrastructure.

   b. Interference models between multiple platoons and other entities need to be considered for 5G resource allocation.

3. To integrate V2X edge computing and cloud applications considering demanding latency and capacity constraints; by addressing reliable V2X and 5G communications in platoon scenarios, it will be possible to enable real-time critical communications that will reduce risks in future autonomous or semiautonomous industrial infrastructure.

4. To validate novel proposed mechanisms for authentication, tracking, control, interference rejection, beamforming, multi-packet reception, precoding, link adaptation, energy efficiency, cloud/edge/fog application orchestration, management, service delivery, traffic prediction, etc.

5. To develop an industrial-grade secure, safe and reliable solution that can cope with cyberattacks and difficult network conditions, focused on providing standard secure V2X stack and addressing some PHY wireless attacks like signal jamming.

6. To be able to simulate, in a computational environment, the behaviour of a platoon network.

Benefits and results

Aligned with the objectives for this particular use case, the main outcome will be a common cross-layer management system for a platoon network that combines the benefits of multiple other standards, such as the ISO, ITU, and IEEE reference IoT architecture standards in a single solution, with the following functionalities:

- Device functionalities
  - Antenna features (massive MIMO & beamforming)
  - Non-Orthogonal Multiple Access.
  - Sensors.
- Network functionalities
  - Smart routing.
  - Anomality detection.
  - Scheduling.
- Service, security and virtualization functionalities.
  - Encryption & network security.
  - Service resource orchestration.
- Cloud functionalities
  - Edge URLLC.
  - Traffic management.

Partners involved

Capgemini

- Telco OSS and 5G RAN simulator.

isep Instituto Superior de Engenharia do Porto

- AI algorithms for wireless resource management, interference detection and obstacle prediction.
- Trustworthiness metrics in reference architecture.
- Spatial authentication and interference reduction.
- MIMO and wireless MAC-PHY implementation.
- Real time scheduling and ultra-low latency intra-platoon communications.

MARMARA UNIVERSITY

- Large scale emulator with digital twin entities.
- Realistic testing and scenario generation based on real vehicle trace analysis.

NXP

- 802.11p based wireless communication prototype.

TU Delft
Delft University of Technology

- Multiple node hardware prototype.
- AI algorithms for sensor and RF data.

VORTEX CoLab

- Validation framework for platoon behaviour.
- Security threat analysis.

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

Generic use case description

This use case aims to demonstrate the ability of artificial intelligence algorithms to improve the reliability of an emerging type of application called wireless avionics intra-communications (WAICs). With the synergy of AI and wireless transmission, this new technology aims to replace, substitute or help the redundancy of internal aeronautics wireline infrastructure, with major benefits such as more flexible aircraft design, lighter aircraft, fuel efficiency, improved operational range and higher payload capacity. The ultimate objective is to introduce highly reliable wireless link sin the operation of aircraft thereby achieving the concept of fly by wireless.

Challenges

The challenges of this use case is to increase the reliability of wireless technologies to behave almost like a wireline pipeline with controlled or minimum errors. The technology WAICs will interact with the internal real time network of the aircraft. The use of artificial intelligence aims to fill the gap and create a wireless layer with controlled and real time behaviour that matches the needs of critical subsystems in major aircraft. The main obstacles to achieve this are not only fading, shadowing, turbulence, time variability, jamming interference, but also high level security aspects and attacks such as man in the middle, spoofing, etc.

Main objectives of the use case

The use case objectives are focused on overall improvement and development of WAICs by:

- ♦ Improvement of reliability of WAIC to the same or similar level as the wired safety critical avionic networks of commercial aircraft.

- Introduction of adaptive transmission to WAIC by means of artificial intelligence (AI) using spatial diversity and other signal processing algorithms for WAIC to reduce impact of potential interference, avoid jamming, increase spectral efficiency and support low latency.

- Prediction of channel conditions in WAIC. The AI will aim to predict channel conditions of an aircraft during different moments of a mission, including turbulent conditions and detecting changing patterns according to the type of aircraft and the movement of passengers inside the cabin.

- Increase of Technology Readiness Level of WAICs by using a prototype demonstration in a representative scenario inside an aircraft.

- Improvement of connectivity in an aircraft by employment of reconfigurable IoT antennas.

- Increase explainability of AI decisions in the context of WAICs.

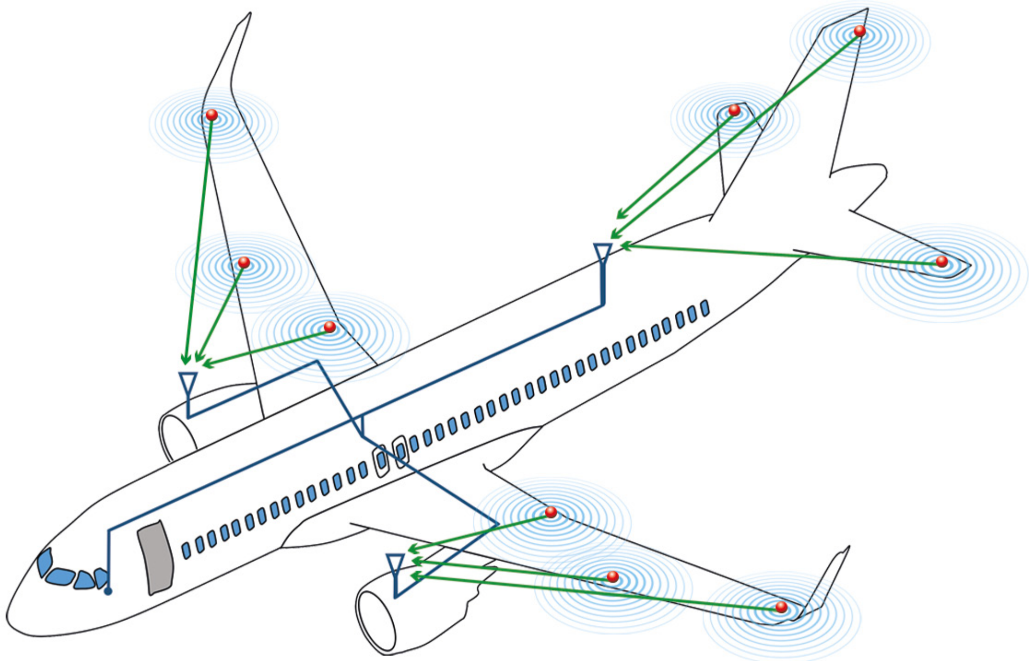


Figure 2.1

Benefits and results

The main benefit of the results of this use case is to help improve reliability, trustworthiness and operability in secure and safe manner.

The use case will attempt to expose the mechanisms and tools needed to make WAICs an efficient and successful technology.

The results also aim to show to the different stakeholder and trust in the performance of this technology to reduce expenses dramatically in the aeronautics industry.

Partners involved

- CISTER / ISEP - Portugal

CISTER
Research Center in
Real-Time & Embedded
Computing Systems

- GUT - Poland

GDAŃSK UNIVERSITY
OF TECHNOLOGY

- TU Delft - Netherlands

TUDelft
Delft University of Technology

- NXP-NL - Netherlands

NXP

Wireless security testing environment for smart IoT

Generic use case description

Smart, connected electronic systems become more and more part of many aspects in our life. IOT systems join, adapt, collaborate, and interact in scenarios in mobility, logistics, assisted living, and many more. In some circumstances, human safety directly dependents on IoT systems. A modern car is composed of 100+ electronic control units, many of which use wireless communication: Intelligent Transportation Systems (ITS) deploys IEEE 802.11p radios or alternatively cellular communication for vehicle-to-vehicle (V2V) or vehicle -to-Infrastructure (V2I) for information exchange, generalized as vehicle-to-anything (V2X). In-car systems communicate via Bluetooth and WLAN with passenger's mobile devices. RFID is used to integrate sensors monitoring the tire pressure etc. Additional systems are available to provide emergency services (eCall) or take care of software updates for vehicle's control units over the air (OTA). This has tremendously improved our comfort, safety, and driving efficiency. But on the other hand, it provides more than enough opportunities (also called "attack surface") for malign actors ("hackers"). Cyber resiliency is therefore a major goal in design and verification/validation.

In this use case, partners will build a novel system-level test bed, to verifying cyber-resilience of smart IOT systems in a car.

Challenges

Vehicles need to be tested under real-life conditions, while still being in the controlled environment of an automotive test bed. For such 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, trying to detect any un-acceptable behaviour caused by the attacks. Finally, it is important to highly automate cybersecurity testing, in order to drive down costs and time needed.

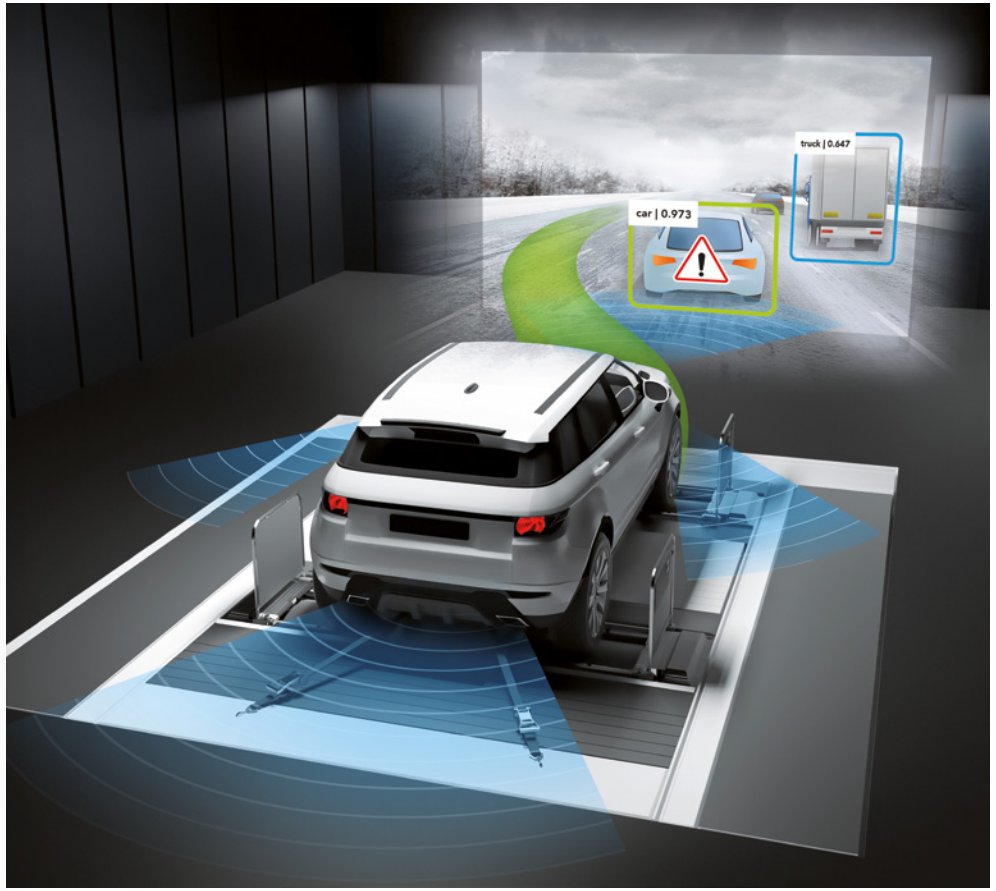


Figure 3.1

Main objectives of the use case

The vision of this use case is to develop and validate a testing environment which is able to simulate current and future wireless communication scenarios in the automotive domain. Therefore we aim to:

- enable system-level cybersecurity testing of vehicles,
- provide appropriate simulation environments (enabling tests of vehicles in realistic multi-vehicle scenarios, e.g. V2V),
- automate test case generation (attack vectors),
- simulate communication technologies used in automotive domain (IEEE802.11p ITS-G5, BT/BLE, Wi-Fi),
- mMonitor and classify system behaviour (test oracle),
- automate the whole cybersecurity testing process.

Benefits and results

Today, cybersecurity testing is a tedious, costly process: a group of experts ("white-hat hackers") try to find vulnerabilities within a defined time span ("pen testing").

In this use case, a highly automated 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.

As a result, OEMs and operators are able to find hidden vulnerabilities before market release of vehicles, therefore raising quality and cyber-resilience significantly.

Partners involved

This use case is led by

- AVL • Austria - in collaboration with
- CISC • Austria
- GUT • Poland
- HALTIAN • Finland
- ISEP • Spain
- JKU • Austria
- KAITOTEK • Finland
- KTH • Sweden
- LCM • Austria
- MarUn • Turkey
- NXP • Netherlands, NXP • Austria
- SAL • Austria
- VORTEX • Portugal

Intelligent wireless systems for smart port cross-domain application

Generic use case description

The use case is set in maritime domain, being more specific in port environment with its closest surrounding such as vessels and yachts. The main area of operation and possible deployment of components is Port of Gdansk. The Gdansk port is a major international transportation hub situated in the central part of the southern Baltic coast, which ranks among Europe's fastest growing regions. According to the strategy of European Union the Port of Gdansk plays a significant role as a key link in the Trans-European Transport Corridor No. 1 connecting the Nordic countries with Southern and Eastern Europe.

In addition to that, one of the scenarios is to be deployed and presented in Cetraro harbour in Italy. Such an approach, where the solutions are validated and tested in real, harsh industry environment is one of the key priorities of the use case. The use case is to be demonstrated through four dedicated scenarios:

Figure 4.1

Scenario 1 – V2X Communication in Smart Environment

The main objective of this scenario is to support port authorities in daily operations through secure and safe solutions for wireless communication. Main focus of this scenario is secure communication between different types of vehicles (e.g. cars, trucks, trains) and infrastructure, together with object tracking and monitoring. It is a cause of majority of problems and challenges addressed within this UC so different technical solutions that improve the wireless communication security and connectivity, with strong AI support are planned to be deployed within this scenario.

Scenario 2 – Port surveillance and monitoring with (semi)autonomous vessel operations

This scenario will focus on two main issues – first: development of an intelligent active RFID tags for objects monitoring and inventory check and dedicated algorithms as well as utilization of LiDAR and radar technologies to increase overall safety and security on small/average yacht vessels; second: improvement of monitoring of port infrastructure and inspection from the seaside. Two separated demonstrator locations are planned with different scope – one in Poland (or location where demo vessels will be available) and the second in Italy.

Scenario 3 – AI-enhanced situational awareness solutions

In this scenario situational awareness and human flow/object management in port area will be considered with regard to safety issues. Infrastructure monitoring & inspection – IoT systems for monitoring the actual situation within the facility (e.g. buildings, roads, harbour etc.), objects positioning, access control management and reliable and efficient notification distribution mechanism for supporting pedestrian safety within the facility (especially in case of emergency situation) are planned to be covered by this scenario.

Figure 4.2

Scenario 4 – Port Maintenance Management

Ports usually employ CMMS (Computerised Maintenance Management System) onsite to manage the maintenance activities associated with their critical capital equipment and sub-systems. In this scenario, connection of port crane equipment SCADA systems with a CMMS will be considered, with a view of establishing a secure network connection (considering IEC 62443) between all devices. Equipment operational and sensor data streams will be evaluated and optimal database architecture established including Edge, Network and Cloud storage options. Edge and Cloud based AI algorithms will be developed for diagnostics, monitoring and predictive maintenance techniques. Where appropriate, digital twin technologies may be developed to enhance the performance of the AI algorithms. As a consequence of this integration and application of AI, the maintenance of critical equipment in the port (and thus operational uptime and productivity) can be improved.

Challenges

The main challenge of this use case is to develop means for efficient testing of any wireless IoT system with regard to its type, configuration, usage context and without significant time efforts. For this reason, the holistic approach where all communication link layers and measurable dependencies between them will be considered. The possibility of reliable simulation of physical signals as well as protocols and applications are required. A specialist SDR platforms with dedicated software to provide reconfigurable physical layer will be required to generate communication and interfering signals as well as for communication channel emulation.

Main objectives of the use case

The main goals of the UC are:

- Providing reliable and cost-effective technology solutions to support the port operations, safety and security management.
- Focusing on the secure wireless communication components for industrial environments with increased resilience for cyberattacks.
- Development of reliable localization-based services.

- Providing interoperable solutions aligned with existing integration platforms e.g. FiWARE.
- Demonstration of the developed technologies within real operation environment.
- Increasing self-awareness and safety/security level on board of maritime vessels.

Benefits and results

The main benefits and results are defined as follows:

- Infrastructure monitoring & inspection - IoT systems for monitoring the actual situation within the facility (e.g. buildings, roads, harbour etc.).
- Vehicles tracking & monitoring - tracking the vehicles within the facility and monitoring the driver behaviour.
- Driver assistance - providing additional information about the current situation within infrastructure (e.g. navigation, traffic, speed limits etc.).
- V2X (Vehicle to X) wireless communication - secure communication between different types of vehicles (e.g. cars, trucks, trains) and infrastructure.
- Intelligent logistic - supporting IoT solutions for Logistics process optimization (e.g. on demand localization, virtual zones management).
- Logistic efficiency – managing the goods at the port with the Terminal Operation System, coordinating Cargo operators with port facilities and external inputs.
- Improved interfaces – connectivity among all the maritime and rail systems from the devices and functionality perspective.
- Vessel positioning and information – the Vessel Traffic System allows a real time control of vessel location and its attached documentations for the Port Authorities.
- Objects positioning - systems that provide precise information about current position of people, assets, vehicles and cargo within industrial, harsh environment.

- Gathering precise data about progress of rescue operations (e.g. presence of individuals at the evacuation meeting points).
- Efficient software tools for management of access control rules of objects (people, vehicles, cargos) with respect to defined internal areas of port.
- Increase the secure communication level by introducing machine learning for interferences (e.g. jamming) detection, identification and mitigation.
- Improve wireless communication connectivity by applying dedicated algorithms for smart antennas operation in case of V2X communication and wireless sensor networks.
- Increase localization accuracy by introducing machine learning for incoming signal direction estimation or high-level data fusion.
- Vessel/yacht crew monitoring.
- Inventory management on yacht/vessels.
- Increasing self-awareness of vessels through utilization of radar technologies.
- Improved monitoring and maintenance management of the critical port infrastructure (container cranes).
- Improved cyber security for the connectivity between the port operations and the critical infrastructure.

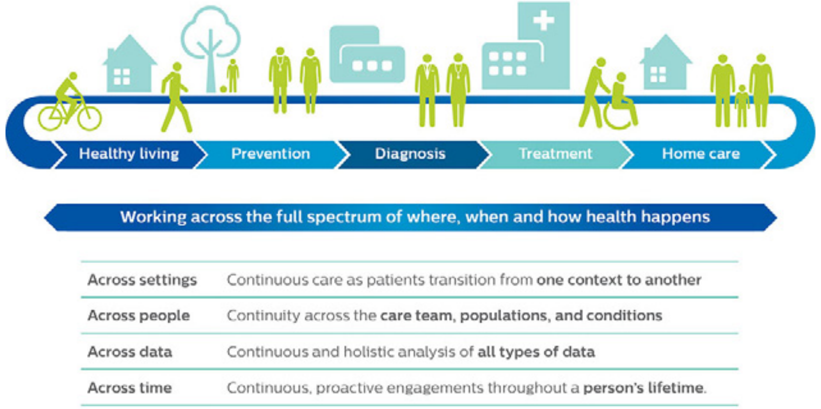
Partners involved

- CISC • Austria
- MarUn • Turkey
- LDO-SDI • Italy
- CINI-UNICAL • Italy
- ISS RFID • Poland
- GUT • Poland
- PAVOTEK • Turkey
- WAPICE • Finland
- LCC • Ireland
- JKU • Austria
- VEMCO • Poland
- KAI • Finland
- NXP AT • Austria, NXP NL • Netherlands
- UCC • Ireland
- LCM • Austria

Smart and adaptive connected solutions across health continuum

Generic use case description

The use case 5.5 aims to improve the operational efficiency in continuous care delivery using novel AI/ML and IoT solutions, thereby alleviating non-clinical burdens on the clinical team members. UC 5.5 envisions that by accurately predicting complexity and risk profile of a patient in an early stage of the clinical workflow, we could predict the need for hospital resources and provide operational insights that are interpretable and actionable by clinicians. This will enable clinicians to focus more on clinical tasks which will improve efficiency in care delivery, reduce medical errors and patient's waiting times, and save healthcare costs.


Healthy living
Prevention
Diagnosis
Treatment
Home care
Working across the full spectrum of where, when and how health happens

Across settings	Continuous care as patients transition from **one context to another**
Across people	Continuity across the **care team, populations, and conditions**
Across data	Continuous and holistic analysis of **all types of data**
Across time	Continuous, proactive engagements throughout a **person's lifetime.**

Figure 5.1

Challenges

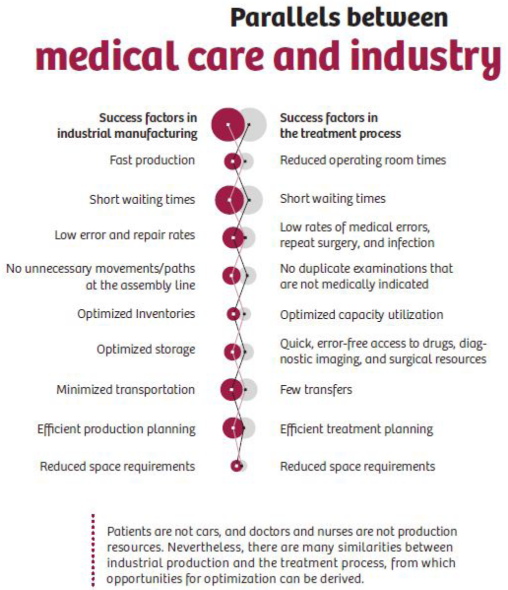
The challenge in the healthcare environment is enabling IoT solution to continuously monitor and record the usually isolated data sources distributed among multiple standalone systems. This IoT enabled connectivity will assist in deriving actionable insights based on largely distributed healthcare data. New data generated by IoT sensors is useful when combined with existing historical data in hospital information systems. Although there are several efforts in standardizing data interface using formats such as HL7/FHIR, the healthcare industry is still lacking standardized adoption of IoT. To this end, added value of AI/IoT in use case 5.5 can be summarized as follows:

- AI: Intelligent analysis of real-time patient data and historical patient data to derive actionable operational insights,
- AI: Accurate prediction of operational demands in a treatment process,
- AI: Assist in operational decision made by intelligent processing of big data,
- IoT: Enable federation of information systems and data sources which are normally isolated,
- IoT: Optimization of wireless communication in a harsh network environment,

Figure 5.2

Main objectives of the use case

- Derive actionable insights using explainable AI from various data sources for operational efficiency in healthcare;
- Assist clinical team members in operational decision making with actionable insights;
- Improve operational workflow in a hospital environment based on insights obtained from various data sources;
- Reduce operational burden in hospital environment;
- Improve care delivery while reducing costs of the non-clinical operational activities in healthcare environment;
- Enable secure connectivity and a privacy-aware point of convergence to a variety of isolated clinical and non-clinical data sources;
- Enable intelligent processing of data either in the device, the edge or the cloud.



Parallels between
medical care and industry

Success factors in industrial manufacturing	Success factors in the treatment process
Fast production	Reduced operating room times
Short waiting times	Short waiting times
Low error and repair rates	Low rates of medical errors, repeat surgery, and infection
No unnecessary movements/paths at the assembly line	No duplicate examinations that are not medically indicated
Optimized Inventories	Optimized capacity utilization
Optimized storage	Quick, error-free access to drugs, diagnostic imaging, and surgical resources
Minimized transportation	Few transfers
Efficient production planning	Efficient treatment planning
Reduced space requirements	Reduced space requirements

Patients are not cars, and doctors and nurses are not production resources. Nevertheless, there are many similarities between industrial production and the treatment process, from which opportunities for optimization can be derived.

Figure 5.3

Benefits and results

- The proposed work in the project will contribute to strengthening the industrial competitiveness, growth, and sustainability of companies by driving and validating AI based open connectivity and edge computing standards through the creation of advanced telehealth solutions based on these standards, leading to an eco-system for telehealth solutions that many companies can use and contribute to.
- Integration of various telehealth solutions by enabling smart AI connectivity and computational framework will reduce the cost of medical materials by 40% spent per patient in their health monitoring.
- Telehealth and remote patient monitoring will prevent the waste of precious time of medical experts by 30%.
- Control stations that can remotely support operation theatres, intensive care units will be enabled using the technologies created from InSecTT. This will create around 30 new job per control centre per large hospital, amounting to 120,000 health-tech jobs all over Europe.

Figure 5.4

Partners involved

List all Partners involved in the use case

- JSI • Slovenia
- NXP • Netherlands
- NXP • Austria
- Philips • Netherlands
- TU Delft • Netherlands
- UT • Netherlands
- VTT • Finland

Location awareness for improved outcomes and efficient care delivery in healthcare

Generic use case description

The primary use case for „Location awareness for improved outcomes and efficient care delivery in HealthCare" is about Emergency Logistics Services (ELSE) in mass casualty incidents (MCIs). Efficient handling of MCIs involves triage, treatment and transport of multiple casualties in catastrophic local events such as major traffic incidents, earthquakes, explosions, plane crashes and mass shootings. Based on triage, injured casualties need to be transported in the right order, with the right transport to the right most nearby hospital.

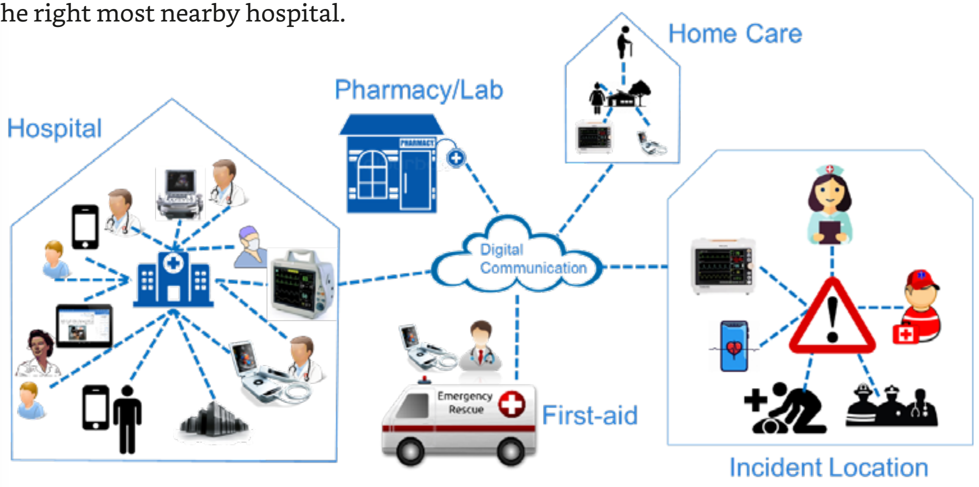


Figure 6.1

A secondary use case is about localization of valuable assets for medical facilities. Finding urgently required equipment causes delays and annoyance in the hospital workflow and the loss of equipment costs the healthcare industry millions each year. Location tags attached to valuable equipment may help to track their location and retrieve it when needed.

Both use-cases addresses both indoor and outdoor localization and may (re)use similar building blocks.

Challenges

Main challenges to be tackled in this use case is people and asset localization both indoor and outdoor, including situations where network infrastructure is not available. In addition, privacy aspects need to be carefully considered when tracking people locations. AI and ML may be applied to indoor fingerprinting, localization as well transport optimization based on priority (triage) and hospital capability/capacity.

Main objectives of the use case

Key objectives of the use case are:

- Enable seamless tracking of clinical and non-clinical assets to improve healthcare workflows both indoor and outdoor.
- Providing intelligent processing of indoor location applications and communication characteristics to enable real-time and safety-critical healthcare applications.
- Developing a secure, safe and reliable localization/logistics enterprise solution that can cope with cyberattacks and difficult network conditions.
- Providing measures to increase trust for user acceptance and make AI/ML explainable.
- Developing a Mass Casualty Incident (MCI) solution using Internet of Things technologies, i.e. wireless devices with energy — and processing-constraints, in heterogeneous and possibly hostile/harsh environments.
- Combine technologies and align reporting interfaces for outdoor and indoor positioning, for example Wi-Fi, BLE, RFID, UWB, GPS and camera-based.
- Providing re-usable solutions across the healthcare domain for people and asset tracking.

Benefits and results

Currently deployed solutions for MCI handling are based on paper forms. In this use case a digital solution will be developed that should result in an earlier and better overview of casualties involved and allow for more efficient logistics handling in MCI events. Such a solution may save lives and reduce cost of operation. A digital MCI solution may also allow for managing logistics in non-local events such as a pandemic outbreak.

Although commercial asset tracking solutions for hospitals are already available, new asset tracking solutions based on technologies investigated in this use-case, may contribute to reduced cost of operation and a broader range of applications.

List all Partners involved in this use case in alphabetical order:

- GUT • Poland
- JSI • Slovenia
- NXP • Netherlands
- NXP • Austria
- Philips • Netherlands
- TU Delft • Netherlands
- UT • Netherlands
- WAPICE • Finland

Intelligent transportation for smart citites

Generic use case description

Smart Cities are born with the objective of creating economically, socially and environmentally sustainable cities; they also represent the only solution to contain and reduce the alarming environmental and socio-economic repercussions that urbanization will cause on our planet.

Pollution in large cities, ecological awareness and overcrowding make it necessary to optimize means of transport to live in cities that are more comfortable and respectful of the environment, opting for public transport, prepared for new ways of people transportation and optimizing traffic and making cities more liveable moving to a smart transportation.

Smart transportation is one of the main ways Smart Cities are improving the daily lives of citizens and sustainability with the use of Information Systems, future connected cars and advanced traffic management systems.

The use case 5.7 focuses on the development of intelligent systems towards smart transportation, connecting rail-road domains, through a smart management system that intends to correctly manage the multimodal traffic jams in cross-domain (rail/road) areas and establish rail directives in an intelligent, secure, safe, and efficient way.

The Intelligent Rail-Road Shared Areas Management (IR2SAM) solution, that will be developed in this use case, aims to be able to broadcast relevant information to different types of vehicles and the infrastructure in a rail-road shared area in a trustable and smart way. In order to increase the efficiency of both, rail and automotive domain, and the interaction between them, IR2SAM combines information reported from each domain to actuate and solve specific traffic situations in an optimized manner.

The solution provided will enhance the management of rail-road areas making use of Edge-based AI mechanisms, increasing both the intelligence and the efficiency in the decision making. The traffic jams in these areas will be managed in a more effective way, giving the priority to different actors depending on the traffic situation of each city zone.

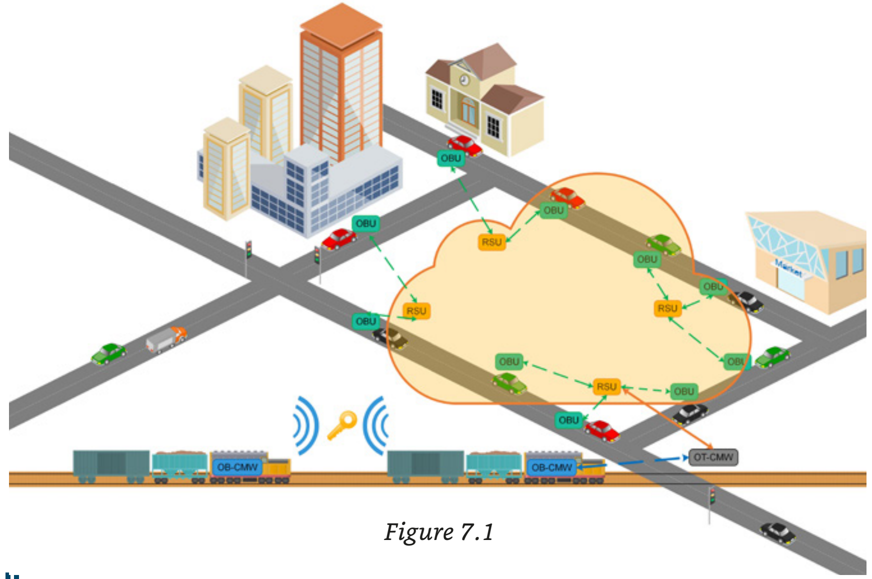


Figure 7.1

Challenges

One of the main challenges of the use case is to enhance the management of cross-domain areas making use of edge-based artificial intelligence mechanisms, which allows to efficiently manage traffic in shared areas. Another key challenge is to increase the communication between all involved actors in the defined area for considering as much data as possible before assigning priorities to a specific actor in an intelligent way that improves the effectiveness on the rail and road domain since it provides a greatest efficiency in the decisions.

Main objectives of the use case

The main objectives related to this use case are:

- Increment the safety in shared areas as level crossings by provididng intelligence to the trustable decision making as well as increasing the communication between the actors involved.
- Provide intelligent to the decision making use of Artificial Intelligent mechanisms.
- Enhance management of the cross-domains areas managing multimodal jams and establishing priorities.

- Develop a safe and secure Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V) communication technology allowing to select the best channel for the wireless communication between the actors involved.
- Minimize CAPEX/OPEX costs making use of wireless communications and introducing automation.
- Improve reliability, safety and security of the systems applying safety and secure rules and directives for the reliable communication between the urban stakeholders involved just as providing the specification for the safety and security requirements necessary for the use of distributed AI mechanisms.

Benefits and results

In consonance with the objectives defined for this use case, the main result provided is a decision making system that is able to effectively manage rail and road domains and establish priorities in an intelligent and efficient way making use of Artificial Intelligent (AI) mechanisms.

The main benefits provided by this use case are listed below:

- Improve the the citizen mobility, comfort, and accessibility to every kind of rolling stock transportation system.
- Reduces the number of injures and human losses increasing the safety and security in the railway lines as well as the reliable communication between the rail and road domain.
- Increase the 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.
- Minimizes costs of Vehicle-to-Infrastructure and Infrastructure-to-Vehicle communications due to the replacement of traditional wired solution with wireless technologies.
- Efficiently manages of the rail-road areas making use of artificial intelligent.

Partners involved

- Indra · Spain
- CEA · France
- Klas Telecom · Ireland
- STM · France
- JIG · Spain
- UPM · Spain
- MUN · Spain
- MTU · Ireland

Intelligent automation services for smart transportation

Generic use case description

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

To enhance the current railway domain, the use case 5.8 develops an automation system able to provide capable of send movement directives to the moving train for a future full train automation. By decentralizing the control of decisions making use of artificial intelligent it is possible to provide an optimal control of the composition, also forecasting the signalling systems devices along the railway track, by connecting all to all. Specifically, this system will make the movement directives considering both the position, velocity and acceleration of the train and the information of the Cloud infrastructure.

Additionally, the developments identified for this use case pretends to enhance the virtual coupling solution that was carried out in the previous project SCOTT. This solution allows to manage and control multiple platoon compositions via remote control from only one of them. Although this system solves the problems related to creating the physical composition, the limitation for long traction, the capacity and other issues need to be tackled. Specifically those related to improve the way in which the speed changes occur once the trains are coupled, as they are currently rather abrupt. These movements can affect passengers' comfort as well as cargo conditions in freight lines.

For this reason, the use case 5.8 also develops a system to refine the movement train directives to the train, adapting to the specific rolling stock capabilities via the use of AI mechanisms. These are intended to adjust through current and historical data the output parameters needed to determine the speed changes processes, accomplishing the movement order and assuring comfort as well as safe and secure conditions of passengers and cargo.

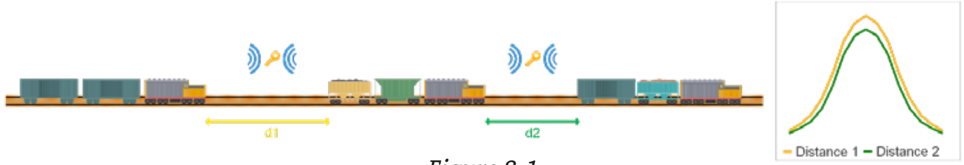


Figure 8.1

Challenges

One of the main challenges of this use case is to increase the grade of automation for the rail operation as well as the infrastructure implementing safety and security capabilities.

Another crucial challenge is to improve the deployment of virtual coupling maneuver during the trip making the speed changes processes more comfortable for the passengers and safer for the cargo.

Main objectives of the use case

The main objectives related to this use case are:

- Increase the efficiency of the rail infrastructure and the On-Board systems including the automation of the coupling and uncoupling maneuvers along the tracks, via Artificial Intelligence as well as smoothing these processes and making them comfortable for the rail users.
- The progressive conversion of conventional lines into ATO lines providing intelligence to the railway traffic processes connecting all to all and increasing the grade of automation of rail operation and infrastructure.
- Improve the flexibility of the system introducing the automation of the CCS and distributed solutions to efficiently manage the exchange of information.
- Acquire major capacity and improve the timetable adherence for a more efficient traffic management minimizing unexpected train stops as well as reducing the distance between trains.
- Improve the reliability, safety and security of the system applying safety and secure rules as well as directives for the reliable communication between the infrastructure and the trains and providing the specification for the safety and security requirements necessary for the use of distributed AI mechanisms.

- Develop a safe and secure Vehicle-to-Anything (V2X) communication technology allowing to select the best channel for the wireless communication between the actors involved.

Benefits and results

According to the objectives defined for this use case, the main results provided are two collaborative systems, the Smart Rail Automation System (SRAS) and the Smart Adaptation Movement Control (SAMC). On the one hand, the Smart Rail Automation System develops a rail automation system able to provide capabilities to control the train in an automatic way in all emergencies or degraded situations. On the other hand, the Smart Adaptation Movement Control deploys an artificial intelligent module to control in a smooth manner the speed variations during the virtual coupling process.

The main benefits provided by this use case are listed below:

- Major flexibility and improves the timetable adherence to a more efficient traffic management.
- Enhances the citizen comfort and accessibility to every kind of rolling stock transportation system
- Improves the flexibility of the current systems by connecting all to all by means of an automated and distributed system.
- Provides auto control capacity with a safe, secure and trustable system.
- Decentralizes the control of decisions making use of artificial intelligence.

Partners involved

- Indra • Spain
- CEA • France
- STM • France
- UPM • Spain
- MUN • Spain

Cybersecurity in manufacturing

Generic use case description

The emergence of Industry 4.0 enabled, the systems operated in manufacturing such as robots, PLC's or other devices that both directly controls or supports the production in factories, to be connected to higher layers of factory networks and even to the internet to access the data of process in production. The high number of the interconnection of devices, provided by both wired and wireless communication infrastructure within factory network and with the outside world, thus generates a severe vulnerability from either intentional cyberattacks from external sources or unintentional disruptions caused by the devices utilized in manufacturing sites themselves. This vulnerability ultimately leads to a decrease in profitability of the company with hindrances in continuous production and it may even cost human lives in critical processes that require industrial safety precautions. The main purpose of the "Cybersecurity in Manufacturing" use case is to develop a reliable, secure, and safe communication layer for both wired and wireless network infrastructure for the manufacturing domain.

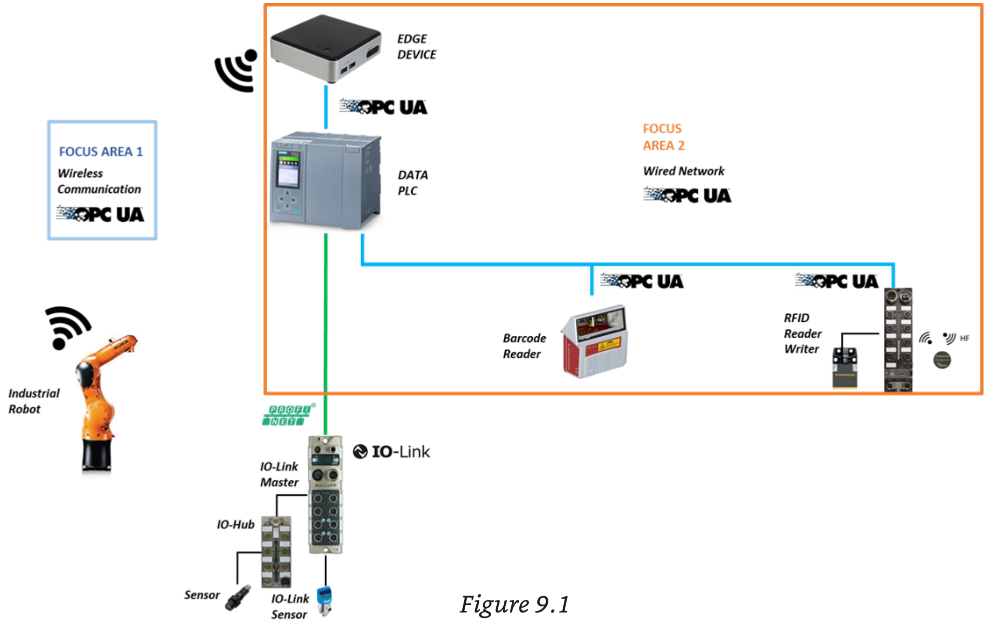


Figure 9.1

Challenges

The main challenge of this use case is to develop a system that detects the cyberattacks via AI/ML supported anomaly detection in a manufacturing environment, takes measures to minimize or end the attack effect according to attack type. Another challenge of this use case is the applicability of the developed system in the manufacturing environment without challenging the continuity of the productivity of industrial processes and hindering the effectiveness and speed of industrial communication within manufacturing networks.

Figure 9.2 Atölye 4.0, Arçelik Advanced Robotics Lab.

Main objectives of the use case

The main objectives set for this use case are:

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

- Develop AI-based wireless network jamming detection and identification algorithm for wireless OPC-UA communication

- Develop anomaly detection routines supported by AI for detecting cyber-attack attempts within wired OPC-UA networks and securing devices in the network.

- Improve wired OPC-UA communication security with a certification-based authentication mechanism in a network of IoT devices, edge devices, and industrial equipment interconnected via OPC-UA network in manufacturing plants.

- Increase awareness of the impacts of cyberattacks in manufacturing sites and present methodologies for achieving a secure and reliable communication infrastructure for the automation network layer in the manufacturing domain.

Benefits and results

Per the objectives defined for this use case, the main output will be a network layer that maintains and improves the security and reliability of industrial networks in manufacturing sites. The main benefits granted by this use case are as follows:

- Maintaining continuity of production activities in the event of cyberattacks,

- Increasing the use of wireless communication technologies in the industrial environment,

- Prevent workforce safety vulnerabilities that may be caused by cyberattacks in manufacturing sites,

- Promoting the utilization of more networked equipment in the manufacturing domain with enhanced cybersecurity measures.

Partners involved

- Arcelik • Turkey

- MarUn • Turkey

- NuRD • Turkey

Robust resources management for construction of large infrastructure

Generic use case description

The use case "Robust Resources Management for Construction of Large Infrastructures" aims to leverage the potential of Artificial Intelligence of Things (AIoT) for increasing the productivity and improving the safety of the construction sector, focusing on construction projects for the development of large civil infrastructures (e.g. construction of tunnels, highways, railways, etc.).

Figure 10.1

This goal will be achieved by enabling seamless tracking and monitoring of machinery, workers, and other assets within the construction site area. Through the advanced processing of the data collected, it will be possible to automate tracking of project construction activities and project progress measurement, to ensure the continuity of the operation of the construction machinery through the optimization of maintenance tasks, and to monitor and manage safety and security related risks and incidents within the construction site.

Challenges

The construction sector has traditionally lagged behind other industry domains in the adoption of innovative digital technologies. This has led to a stagnation of productivity compared to the sectors that have already undergone more profound transformations, by taking full advantage of the latest technological developments in the fields of connectivity, artificial intelligence, robotics, data science, etc.

One of the reasons for this slower adoption is the challenging environment where these technologies shall be deployed. Unlike other industry sectors that carry out their operations in fairly fixed and structured factories/facilities, the construction sector is based on the execution of projects in varied locations, during a limited period of time, and the layout of the working environment evolves constantly as the project progresses.

Furthermore, the construction environment (both in indoor and outdoor spaces) frequently presents harsh conditions for the deployment of ICT infrastructure and electronic devices in general, as well as for reliable wireless communications.

Another barrier to consider is the frequently low qualification of construction workers, which makes it difficult to deploy digital technologies that may require their direct intervention. Thus, the integration of IoT-based tracking and monitoring solutions combined with AI/ML techniques is crucial in order to enable automated data capture and analysis on site, minimizing the inputs requested to workers.

Figure 10.2

Main objectives of the use case

1. Deployment of a reliable and cost-effective IoT-based solution for tracking and monitoring of machinery, workers and other assets, both in indoor and outdoor spaces.

2. Integration of the IoT-based solution with legacy machinery and equipment from different vendors, with different levels of instrumentation and communication capabilities.

3. Minimization of IoT solution intrusiveness, in order to increase acceptance and lower deployment costs.

4. AI/ML based processing of data collected for automated identification and measurement / quantification of construction activities.

5. Matching of detected construction activities with project schedule in order to

provide up-to-date real progress of the project, and support early detection of delays and deviations.

6. Automated identification / management of safety and security related risks and incidents, based on the location and interaction of workers and machinery combined with environmental parameters monitoring.

7. Correlation of machinery maintenance and operation patterns in order to anticipate the need of replacing spare parts and thus reducing the number of unscheduled stops of machinery.

Benefits and results

The automated identification and measurement of project construction activities and the subsequent tracking of project progress will allow early detection of delays and execution risks, allowing a faster reaction in such situations.

This will lead to an increased productivity, by reducing the inspection efforts of project managers, supervisors, etc., as they will spend less time on the collection and treatment of data from the construction site, and will be able to focus on efficient decision-making processes.

Data collected from the machinery will also support the optimization of maintenance strategies, which will result in a reduction of unscheduled stops of machinery, thus reducing the cost overruns caused by this type of incidents.

Furthermore, the data collected will allow automated calculation of Key Performance Indicators (KPIs) of construction projects. The KPIs collected from already completed projects will help to estimate more accurately the cost and duration of construction tasks in new tenders or in other future similar projects.

Lastly, safety and security managers will be provided with a reliable solution for detecting potential risks and for managing critical incidents, e.g. to support evacuation of a tunnel in case of emergency.

Partners involved

- ACCIONA • Spain

Smart airport

Generic use case description

In the airport various kind of facilities and resources are used to achieve various tasks and operations. This use case will address the use of AI-enhanced secure and reliable communication technologies to enhance the security, safety, reliability in the airport operations. Moreover, the use of AI-integrated wireless technologies for localization and asset management will improve the service quality at airport operations and passenger experience.

Challenges

Figure 11.1

Airport is one complex system where various types of entities and resources are collocated to achieve various tasks. However, all services and operations are time and mission critical which require security, reliability and safety at high level. Services for the passengers (and their visitors) and the airport operations (inside the terminals, within apron and docking area) require smart infrastructure with accurate information on time. Wireless connectivity is the only technology that provide mobility to all (passengers, visitors, airline staff, employees, vehicles e.g. planes, trucks, carriers, buses) within the whole facilities plant including terminals, runways, aprons, docks, offices, industrial sites, public transportation inbound/outbound.

Main objectives of the use case

The use case specific goals are to:

- Develop a solution capable of providing integrated planning & inspection of events in real-time to prevent & quickly react to potential delays and execution risks.
- Increase the productivity using advanced IoT and AI, that alleviate the inspection efforts of managers and on-site players.
- Based on the data gathered, provide advanced quality analysis & management based on KPIs and BI reports.
- Increase transparency and seamless collaboration among involved players using fully adopted wireless technologies.
- Analyse images and videos of the works with the aim of identifying safety problems and reckless behaviour.
- Improve the analysis platform's ability to collect data from sensors, analyse them and provide real-time solutions, as well as to cut costs, prioritise preventive maintenance and avoid downtime due to bottlenecks or disorganisation problems (e.g. delays in the arrival of materials).

Figure 11.2

Benefits and results

Airport is a complex system with various infrastructures (terminals, runways, aprons, offices, industrial sites, public transportation hubs), various type of entities and assets (passengers, visitors, airlines staff, airport employees, planes, supply vehicles, cars, trucks and special machinery), performing different activities and tasks, which also span a large operational area. Moreover, most of the operations requires real-time communication. Interaction of these various types of entities and the management of all assets operations introduces challenges which requires enhancements primarily in the following topics:

- Securing wireless communication (resilient to interferences and cyberattacks) for all wireless technologies within the airport facilities plant e.g. Vehicles (V2X communications), airplanes, drones, all mobile assets and the infrastructure.
- Providing reliable communication in harsh environment.
- In-door navigation, Objects/assets localization, tracking and management.
- Driver assistance to the vehicle operators and the drivers by providing additional information.
- Communication between various types of vehicles (buses, trucks, supply vehicles, trucks and special machinery) and infrastructure with the use of V2X communications.
- Enabling the use of (semi)autonomous platforms e.g. drones, vehicles, mobile platforms in order to increase situational awareness.
- Design and implementation of tracking algorithms for dangerous goods (e.g. with integrated substance sensors and video tracking), with path prediction for efficient situation containment (e.g., predicting where the substance is going and alerting security personnel).
- Securing the communication at high level by introducing machine learning.
- Mitigating adverse effects of interference.
- Detecting, identifying, and mitigating the jamming.
- Enhancing the connectivity and coverage with the use of AI-based approaches for more resilient communication.

Partners involved

- GUT - Poland
- CISC - Austria
- VIF - Austria
- KAI - Finland
- PAVOTEK - Turkey
- MarUn - Turkey

Driver monitoring and distraction detection using AI

Generic use case description

Distracted driving is known to be one of the leading causes of vehicle accidents. Thus, this use case called "Driver Monitoring and Distraction Detection Using AI" develops technical innovations to detect driver distraction. Thereby, it includes a proof-of-concept implementation of a technical framework for driver distraction monitoring and detection that focuses on driver distraction (e.g. detect phone usage) using AI to assesses distractions in a comprehensive manner. When evaluating and giving feedback to the driver, we attach great importance to making it understandable for the driver.

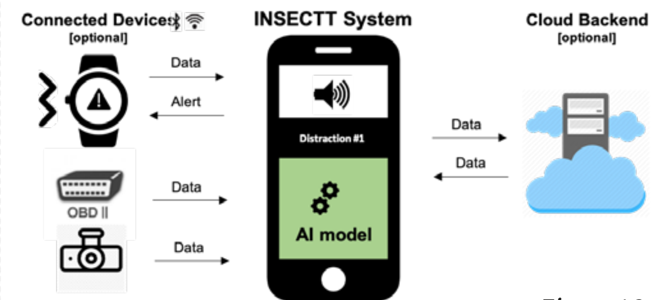


Figure 12.1

By addressing distracting events from a driver actively (to not only inform about general distractive behaviour) the overarching goal is to change driver behaviour and to avoid risks connected to driver distraction.

Challenges

In automotive, the driving force to many technological advances is the avoidance of road accidents, while distracted driving is one of the leading causes of vehicle accidents. The main causes of driver distraction are tasks performed by drivers that are not related to driving, such as using the vehicle's multimedia interface, texting on their smartphone, or looking at their passengers while talking with them. The detection of such tasks utilizing sensor data is crucial for driver monitoring systems.

As modern vehicles have become computers on wheels equipped with a plethora of sensors, distraction detection systems can integrate the data generated by vehicles during operation and infer certain types of distraction. However, distraction detection systems can also be based on additional hardware and software that is used in vehicles, such as smartphones. The adoption and use of smartphones while driving is significantly high, but at the same time smartphones are equipped with sensors, the computing power of smartphones has increased significantly, and modern smartphones allow the deployment of machine learning approaches to the benefit of distracted driving.

The use case targets the following **technical challenges**:

- Using real-time data from a safety-critical everyday activity and performing computations for time-critical operations (alerts/warnings) at the device edge.
- Processing data using AI in an automated manner, by using AI models to classify/ identify possible distracted behaviours.
- Providing a secure, safe and reliable solution.
- Placing the driver in the centre of the application design to increase trustworthiness and user acceptance by explaining the AI result properly.

Main objectives of the use case

The main objective of the use case is to **increase road safety** by contributing actively to the minimisation of driver inattention and distraction. In particular, this use case aims to:

- Collect and analyse driver needs w.r.t. driver inattention and distraction.
- Model driver's inattention and distraction using AI.
- Develop a concept for a 'driver inattention and distraction application' to alert drivers in an appropriate situation with detected inattention / distraction events.
- Develop a proof-of-concept implementation including the detection of at least one driver distraction event (e.g. smartphone usage) using AI.
- Explore and develop a proper way of data processing and sensor data accumulation in different architectures (e.g. offline on the device edge or/and online in the cloud).

- Develop a proof-of-concept dashboard showing the driver distraction events within a given distraction dataset.

Benefits and results

The smartphone is to serve in the approach as the central element, because it brings several advantages:

- Commodity hardware is used, which is usually "always online", so no additional hardware costs occur.
- It is already widespread in the population, thus it scales in a practical way.
- Driving behaviour and distraction can be induced from the smartphone sensors.
- Enables the possibility to detect interactions with the smartphone, which constitute a major distraction while driving.
- It is possible to combine the smartphone with other devices (e.g. SmartWatch, OBD logger or smart glasses).
- It can be extended and used across other industrial domains (i.e., rail and aeronautics).

Partners involved

- RISE • Sweden
- VIF • Austria
- Tieto SE • Sweden

Secure industrial communication system

Generic use case description

Industrial control systems are increasingly being connected to the external world (e.g., the Internet) via different communication mediums, which make them more vulnerable to cyber-attacks. The main idea in this use case (UC) is to design and evaluate intrusion detection techniques to be integrated into an industrial digital twin, thereby being able to detect attacks, and also classify the type of attacks detected. The outcome can assist industrial control systems with detecting and classifying cyber-attacks before they cause damage to the system or environment. This will be beneficial in selecting the proper mitigation method for each type of attack.

Cybersecurity Frameworks typically include five functions: Identify, Protect, Detect, Respond, and Recover. Figure 1 shows three of these functions.

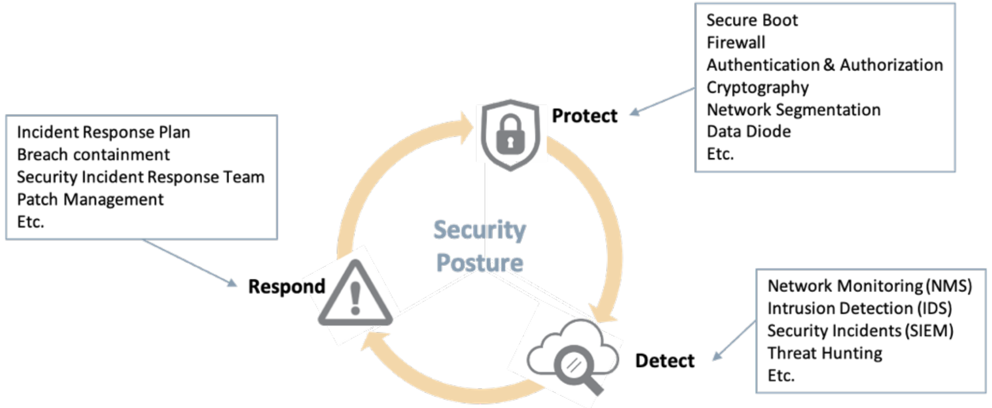


Figure 13.1. Cybersecurity Framework's Three Functions

The work in this UC includes:

1. Validation of changes and ensurement that ey will not affect the operation of industrial systems. These changes will mostly likely be software updates and changes.

2. Validate the new setup? Devising how to use the digital twin (virtual copy of the action-production system) to validate the new setup?

3. Differentiation of intrusions from a bad configuration or functionality.

4. Proposing an IDS for industrial systems.

5. Considering similarities between predictive maintenance and security. For both purposes the data needs to be collected and monitored. The data traffic from vantage points will be aggregated to be sent to the central office or (public or private) cloud over a Virtual Private Network (VPN) connection.

6. Correlation of security and physical (maintenance) alerts in order to detect intrusions.

Assumptions:

1. We assume that data is not encrypted, at least not at the edge, and that data will be encrypted before transmission to the central office.

2. We assume both wired and wireless communication between industrial machines and to the cloud. Figure 2 shows a typical industrial network setup, including control network, central office, firewall, and the network, which is typically wired, but it can also include wireless equipped devices with connection to the cloud. Considering a heterogeneous communication system including both wired and wireless communication technologies we will add more threats and vulnerabilities to the scenarios.

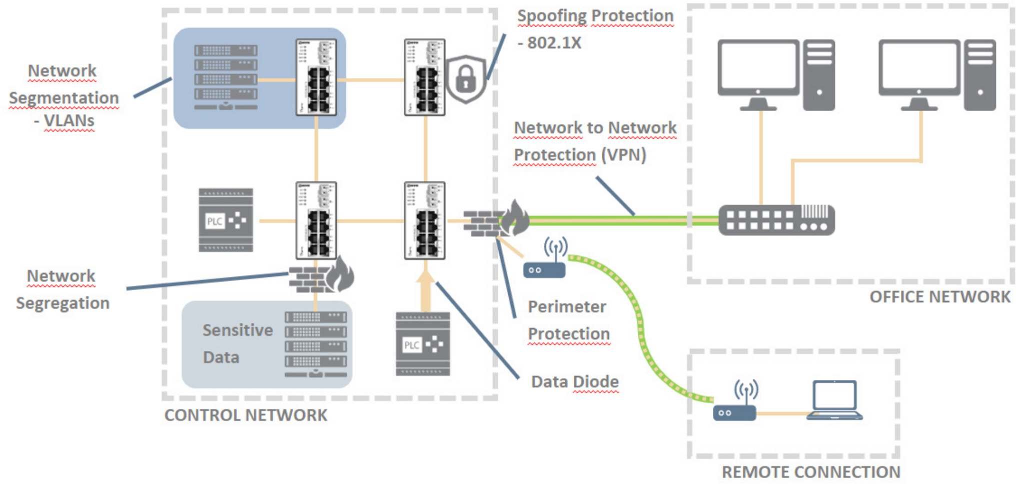


Figure 13.2. Typical industrial setup

Challenges

We can identify the following main challenges in the context of this use case:

1. Industrial systems typically have long-lived networking hardware infrastructures. The cyber security attacks have a dynamically evolving landscape. Most of the mitigation mechanisms are enabled though the networking software level as well as configuration updates, which themselves can open up new vulnerabilities. Efficient and effective methods for intrusion detection and deployment of appropriate mitigations is a key challenge in industrial systems.

2. Even though the AI and ML based approaches for intrusion detection mechanisms seem promising in the above context, the computational/communication overheads needed for their functioning may not be acceptable in time critical applications. Moreover, transferring collected data from industrial systems to a central location (e.g., cloud) to be analysed has two main issues, latency and privacy. Hence, we need to develop efficient and distributed algorithms with less resource availability at the edge to satisfy the above requirements.

Main objectives of the use case

The main objectives of this UC are as follows:

1. To investigate different Intrusion Detection Systems (IDS), including both Artificial Intelligence (AI) and non-AI based algorithms.

2. To investigate different AI and machine learning models and algorithms that can be run at the edge (considering the limited power and storage available) and cloud respectively for intrusion detection in industrial control systems.

3. To design a novel intrusion detection algorithm that does not need a specification of the system's correct behavior in the design stage.

4. To demonstrate how the novel intrusion detection algorithm works in the provided digital twin of Industrial Control Systems (ICS).

5. To propose an approach to diagnose the type of a detected attack by building an attack classification model to evaluate the capability of the proposed anomaly and attack detection algorithms through simulation studies.

Benefits and results

With industrial control systems being more connected with the Internet, ICS can make full use of the universal protocols, software and hardware resources on the Internet, to achieve remote process monitoring and wide information exchange. Despite of all benefits that connecting ICS to the internet will bring, the shift from isolated environments to open environments exposes ICS to a broad scope of malicious cyber-attacks. Disruption of ICS could have a considerable negative impact on public safety or cause significant economic losses. Therefore, it is important and urgent to develop effective technologies for identifying malicious attacks against ICS.

IDS, a necessary complement to traditional firewall solutions, provide an effective way to detect malicious attacks against ICS. IDS can identify malicious activities violating security policies of ICS. In addition, they can provide evidences to inform the system administrator to make proper reactions to cyber-attacks. Developing effective intrusion detection technologies plays an important role in protecting the security of ICS.

Partners involved

WESTERMO designs and manufactures data communications products for mission-critical systems in physically demanding environments. The products are used both in social infrastructure, such as transport, water and energy supplies, as well as in process industries, such as mining and petrochemical. The realisation that the needs of the industry are different from those of corporate IT creates growth in the requirement for industrial grade data communication. The industrial operating environments are tough and the impact of failure in the field can lead to business threatening situations demanding that products have a lifetime in excess of 10 years. The company is growing rapidly and currently has over 200 employees and global sales in excess of €50m. All development and production take place in Sweden at the company's facilities in Stora Sundby and Västerås. Westermo's main tasks in iTRUST4.0 is as an expert on industrial networking and handling of related cybersecurity issues, as well as a provider of an industrial communication use case and a simulation environment for the company's industrial communication systems.

RISE is an independent, state-owned research institute, which offers unique expertise and over 100 testbeds and demonstration environments for future-proof technologies, products and services. With over 2,700 employees we engage in and support all types of innovation processes. The Digital Systems division offers expertise throughout the chain for a digital, innovation-driven society – hardware, software, business development and industry knowledge in a range of strategic areas. The division offers cutting-edge expertise in areas such as sensor systems, automation, printed electronics, AI and data science, cyber security, visualisation, interaction design, fibre optics, sustainable transport and circular business models.

TIETO SWEDEN AB aims to become customers' first choice for business renewal as the leading Nordic software and services company.

In a rapidly changing world, every bit of information can be used to provide new value. Tieto aims to capture the significant opportunities of the data-driven world and turn them into lifelong value for people, business and society. Having a strong role in the ecosystems, we use our software and services capabilities to create tools and services that simplify everyday life of millions of people; to help our customers renew their businesses by capturing the opportunities of modernization, digitalization and innovation and to foster new opportunities based on openness, co-innovation and ecosystems.

Building on a strong Nordic heritage, Tieto combines global capabilities with local presence. Headquartered in Espoo, Finland, Tieto has around 24,000 experts in over to 20 countries. Turnover is approximately €3 billion. Tieto's shares are listed on NASDAQ in Helsinki and Stockholm.

Mälardalen University (MDH) is a young and modern university focusing on applied research and education in close cooperation with industry. The project work will be conducted as part of the embedded systems (ES) research environment at MDH. The ES research environment is the largest at MDH, where it is recognized as a center of excellence. ES has a successful track record of co- production with industry and is a holder of many national and international research projects, including ECSEL (nine ARTEMIS/ECSEL projects, currently coordinating one), other FP7 and Horizon 2020 projects and ITEA3 projects. ES consists of six cooperating research directions: (1) Dependable systems, (2) Real-time systems, (3) Robotics and avionics, (4) Sensor systems and health, (5) Software engineering, and (6) Verification and validation. MDH is Member of: BDVA (Big Data Value Association), ARTEMIS-IA, A.SPIRE, EFFRA, UIIN, European Network on High Performance and Embedded Architecture and Compilation (HiPEAC).

Secure and resilient collaborative manufacturing environments

Generic use case description

Use case 5.14 on Secure and resilient collaborative manufacturing systems focuses mainly on cybersecurity challenges related to the emerging characteristics of dynamic and modularized manufacturing systems, which is a part of the Industry 4.0 evolution. In particular, the use case looks at vertical controller-to-controller interactions in a modular automation system with the aim of developing and adapting technical solutions for use-control and anomaly detection in such a system lacking “base-line” behaviour.

Challenges

One important characteristic relating to cybersecurity of future manufacturing systems is their dynamic and flexible nature. The systems are expected to adapt to changing manufacturing needs over time, including adding and removing processing modules. As the system composition and behaviour changes over time, no base-line is defined. This causes several challenges related to cybersecurity:

- The access control policies have to adapt to the system composition to allow for actions in line with the current system composition and running workflows.

- If using mechanisms for intrusion/anomaly detection, the ruleset has to adapt to changing behaviour and system composition to avoid false positives.

Handling access control policies can be a time-consuming task, and for a system with dynamically changing characteristics, it could prove extremely difficult. This is one of the main challenges that will be addressed in this use case.

Traditional methods for anomaly detection are reliant on a well-defined base-line which can be used to record the expected system behaviour. In dynamic collaborative manufacturing systems, there is a need to find solutions for anomaly detection that are similarly adaptive. The increasing inclusions of secure technologies for network communication, such as TLS and secure OPC UA will also challenge some of the traditional methods for anomaly detection algorithms using stateful data inspection. Developing methods for anomaly detection useful in such scenarios is the second main challenge being addressed in this use case.

Main objectives of the use case

The main objective of this use case is to develop and evaluate architectural mechanisms and methods that provide higher confidence regarding the security and safety of collaborative manufacturing environments, which are highly critical and cannot afford any risks to its high-cost machinery as well as the production processes.

The use case should demonstrate an innovative and extendable method for manufacturing environments, which allows dynamic integration and collaboration of manufacturing units/elements which are both secure and seamless.

Furthermore, a prototype will be built with a secure digital infrastructure and method capable to protect factories of future (FoF) against cybersecurity threats, as well as to demonstrate and evaluate it in representative industrial settings. The prototype will demonstrate results related to the presented challenges, e.g., solutions for a scalable enforcement architecture, and methods for dynamic access control rule inference, useful in collaborative manufacturing systems.

Benefits and results

The outcome from the use case is expected to be in the form of technical solutions for fine-grained efficient and scalable access control to be used in collaborative, dynamic manufacturing systems. Especially enforcement architectures in relation to OCP UA will be evaluated. Methods for adaptable access control policy formulation will be developed. Put together, this will allow for fine-grained access control policies following the dynamic system behaviour with minimal management effort.

The benefit for end users will be an increased visibility and reduced manoeuvrability for many classes of attacks, including insider attacks. This will increase the security of manufacturing systems, and decrease the management effort for sustaining access control rules close to the least-privilege principle.

Partners involved

- ABB - Sweden
- MDH • Sweden
- RISE • Sweden
- CEA • France

Intelligent safety and security of public transport in urban environment

Generic use case description

Public transportation is one of the key factors for a sustainable, secure and efficient urban mobility. Artificial Intelligence (AI), edge computing and IoT are crucial technologies capable to provide unprecedented opportunities to improve the domain of public transportation, in terms of quality of service, safety and security of the transportation system, productivity of transportation vital assets and return of investment of technologies.

In this use case the public transport bus is considered as a Safety Critical System, composed of the vehicle itself and the technological infrastructure with which it is equipped. As the bus moves in an urban environment, often highly crowded, its intrinsic malfunction or breakage, or something induced by external events, can sometimes be very critical for the safety of the people on board or located nearby the bus. The proposed distributed system is a smart solution to improve on board safety and security during the bus trip, focusing on the definition of innovative sensing & processing solutions to monitor the external environment, the internal passengers' area and the vehicle conditions.

The use case will use innovative technologies and develop solutions which will be demonstrated through the following three scenarios:

Scenario		Problem Statement	How the problem is planned to be solved
1	**AI for Internal and External Bus Safety and Security**	Safety and security are of primary concern for any public transport system. Passengers expect transportation to be safe.	UC15 Scenario 1A will increase the level of safety and security of a public bus as events like fights/brawls can be detected early and alarms can be raised for a rapid intervention eg. by police force. UC15 Scenario 2A will detect potholes on the road during the trip. Potholes occurrence and repair have an impact for bus passengers (eg. elderly people on the bus might lose their balance and fall), for road users with respect to traffic safety, reduced speed, traffic congestion, etc. and for public transport authorities as bad roads increase vehicle maintenance costs. Potholes can appear suddenly and anytime, so having a constant, online detection is crucial.

Scenario		Problem Statement	How the problem is planned to be solved
2	**On-board Data Acquisition and Predictive Maintenance**	Public transport disruption can occur due malfunctions and breakdowns of vehicles	UC15 will develop algorithms for Predictive Maintenance so that public transport authorities can achieve a much lower down-time and costs, improve safety, prevent service interruptions and critical mechanical failure on the road, while promoting passenger satisfaction and public safety.
3	**Heterogeneous sensing technologies for bus safety**	Overcrowded buses decrease passengers' degree of comfort and can constitute a health risk (eg. during pandemics).	UC15 will use on-board intelligent devices to automatically identify specific patterns of the air quality inside the bus and to provide an accurate estimation of the number of passengers. The correlation of the patterns with the passenger count will allow to generate automatic alert messages when a critical situation occurs.

The above scenarios deployment will take place in Modena, in the MASA area and demonstrated on a bus made available by SETA.

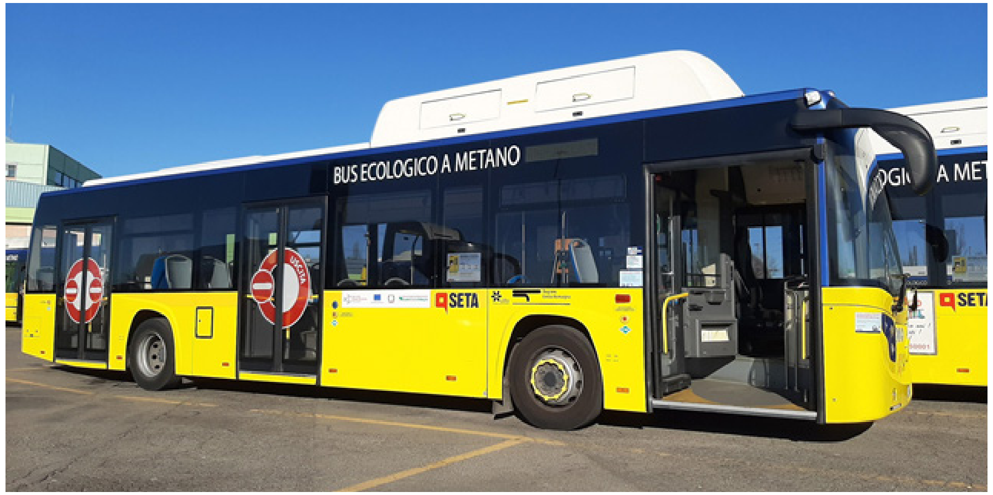


Figure 15.1

Challenges

The capability to a) directly analyse the data collected from the environment on the edge, b) take decisions on the edge (EdgeAI) and c) constantly monitor both vehicle fleet and passengers, enable the creation of end-to-end solutions, which are fundamental to manage complex and multistakeholder-based applications (such as smart mobility).

The successful adoption of AI, edge computing and IoT is not just a technical matter but requires also a good understanding of the relationships between the collected data, the transportation system characteristics, the conditions on-board and the events that are taking place on the vehicle (overcrowding, act of burglary, violence, etc.).

The partners involved in the use case cover almost entirely the public transportation value chain based on AI/IoT, ensuring that both technical and application-specific knowledge base and expertise are available. Moreover, the coverage of the value chain and the availability of an end to end (E2E) solution could provide a strategic advantage for transport authorities to capture and address the necessities of future transportation systems, improving the quality of service, t he safety and security of the transportation system, the productivity of their vital assets and the return of investment in technologies.

Use case UC15 addresses such challenges, focusing on the safety and security of public transportation to:

- Enhance passenger safety during the trip,
- Improve the reliability of the vehicle (bus),
- Monitor passenger flow and the on-board environment.

Main objectives of the use case

UC15 is characterized by the following main objectives:

- Demonstrate how smart sensors correlation and fusion in a mobile environment can improve the safety and security condition of people travelling on the bus, by enabling multi-sensor decision making, environmental perception and abnormal situations detection and how edge computing and IoT technologies allow distributed decision making.

- Provide efficient monitoring with autonomous data collection capabilities on the edge (the on-board embedded devices on the bus) and IoT-based remote monitoring.

- Detect anomalies w.r.t. the "normal" events occurring during the bus trip (eg. fights/brawls), based on video streams together with the detection of safety critical audio events in noisy conditions and possibly monitoring anomalous noises from mechanical components.

- Improve both passenger comfort during the bus trip and road safety, via detection and segmentation of road potholes.

- Reduce bus fleet down-time and costs, improve safety, prevent service interruptions and critical mechanical failure on the road via predictive maintenance.

- Comply with GDPR, Regulation (EU) 2016/679 w.r.t. personal data processed and collected during the implementation and the operational phase of the UC.

Benefits and results

The use case covers the value chain, starting from CPS (Cyber Physical Systems) Manufacturers to the End users. Each stakeholder has a specific role in the business case and obtains many benefits from being part of the value chain. CPS Manufacturers are the on-board technology providers, and they represent the main technology enabler for the business case, which is an opportunity for the CPS manufacturers to enter a new market or consolidate their presence in the transport sector.

System Integrators are responsible to set up the end to end solution, that enables data collection, analysis and cloud — based services provisioning, upgrading the functionalities offered to Public Transport Operators (government agencies and/or private companies):

- Center application, **real-time monitoring** – improved remote management of all the vehicles that make up a company fleet. For each of them the user can consult live streams and send commands to the cameras (zoom on details, tilt).

- Automatic alarm generation able to automatically detect the main **„dangerous"** behaviour on the bus.

- Integration with the AVM (**Automatic Vehicle Monitoring**) system, to compare information from the present system with data on the public transport service (routes, drivers, shifts, etc.).

End users are the Public Transport Operators: they will have a direct positive impact due to the increased safety and security conditions, and the overall quality of service perceived by the passengers. The cloud solution introduces new business models when selling these services, allowing the reduction of costs and opening new opportunities for the stakeholders and for third parties. CPS manufacturers, system integrators and the end users will greatly benefit from remote control functionality, especially if, with reference to a limited set of manoeuvres, these will be applicable:

- on existing vehicles of various manufacturers,

- or, if possible, independently from the vehicle manufacturers, promoting standardization of basic remote control for safety critical conditions.

Partners involved

LEONARDO is a global player in the high-tech sectors and a major operator worldwide in the Aerospace, Defence and Security sectors.
Based on the dual application of technologies, Leonardo designs and creates products, systems, services and integrated solutions both for the defense sector and for public and private customers of the civil sector, both in Italy and abroad.

LEONARDO
CYBER SECURITY

EUROTECH Group is an international company that operates in the areas of research, development and commercialization of solutions for the CPSs, Internet of Things (IoT), machine-to-machine and cloud computing.
The company is based in Italy and located mainly in Europe, Japan and USA, with an important presence in several markets: industrial, aerospace and defence, transportation and logistics, medical, security and scientific research.

EUROTECH

CINI is a consortium of 41 public Italian universities, today one of the most significant point of reference for the national academic research activities in the fields of Computer Engineering, Computer Science, and Information Technologies.
Established in 1989, CINI is under the supervision of the Italian Ministry for University and Research.

SETA – Società Emiliana Trasporti Autofiloviari S.p.A. is a company that manages road Local Public Transport (LPT) in the provincial territories of Modena, Reggio Emilia, and Piacenza. SETA manages the whole LPT service of the three provincial basins, organizing all its aspects: urban and suburban bus transport, vehicle maintenance, the sale of travel tickets, ticket offices management and services for users (information, complaints, etc.).

Airport security – structured and unstructured people flow in airports

Generic use case description

Airports play a vital role in today's age and are regarded as critical facilities as such. Security and safety are the pillar on which customer trust is built and constitute the foundation for the development of air transportation, while actively contributing to the passenger number growth and the global recovery of this market vastly damaged by COVID-19 pandemics. Indeed, the air transport sector exposed us to a high risk, contributing to the virus diffusion, but is one of the market that is paying the saltiest price. A successful security screening is adamant to prevent and eliminate many potential threats while reassuring the travellers of their safety, affecting efficiency as little as possible and still continuing to offer the best experience and quality to passengers and airlines alike. New technologies, with greater monitoring, detection and tracking capacities, are key to address these challenges.

This UC aims at improving airports safety and security by applying multi-biometrics approaches, video analytics – where a huge amount of video streams are jointly taken into account – and heterogeneous sensing technologies. The envisaged dual biometric screening offers a very high degree of accuracy while enabling instant people identification, removing the need for physical documents and credentials verification at checkpoints and promoting a paperless and swift journey. The adoption of heterogeneous sensing technologies, installed at strategic positions in the airport public spaces, enables the identification of anomalous and potentially hazardous situations for the passengers and for the airport. Automatic detection of overcrowded situations and passengers screening at the security control area (for fever and social distancing) are further functionalities offered by the proposed system to support security operators and improve passenger safety. After the identification of these anomalous situations and after the generation of an alert, the system enables security operators to monitor the people inside a suspected area to track and isolate specific subject(s) generating the anomalous situation.

The UC will use innovative technologies and develop solutions which will be demonstrated through the following three scenarios:

Scenario		Problem Statement	How the problem is planned to be solved
1	**Enrolment and gate crossing on-the move**	Traditional recognition processes to access to the different airport areas are not always efficient and/or reliable.	UC16 Scenario 1 proposes an AI solution based on multi--biometrics recognition from face and hand vein patterns. We shall show that the solution is efficient, reliable and secure by means of a pair of gates, an enrolment gate and an access gate to simulate the flow of passengers within the airport.
2	**On-board Data Acquisition and Predictive Maintenance**	Monitoring vast and crowded areas such as terminals of an airport is a challenging task.	UC16 Scenario 2 will demonstrate an AI-based monitoring system with specific services such as people counting and social distancing monitoring which will make use of visual and audio data. Environmental sensors with an embedded AI-based system for the detection of hazardous substances within the airport area shall also be demonstrated.
3	**Anomaly Tracking**	Tracking the evolution of an anomalous situation.	UC16 Scenario 3 will demonstrate an AI algorithm for anomaly tracking: triggered by an alert send by the network of environmental sensors, cameras will track the movements of travellers which were initially inside a certain radius about the location where the hazardous substance has been spotted, and will communicate to security operators for a quick and efficient response.

Challenges

As we are dealing with a critical infrastructure, efficiency of the proposed system is of vital importance. AI and ML algorithms are ubiquitous in our proposal which focuses on recognition algorithms and anomaly detection. In particular algorithms for (multi-) biometrics recognition provide a very high level of accuracy in people identification; implementing the technology and testing its efficiency will be an important step in the development of smart enrolment and crossing gates. From the point of view of Anomaly Detection and Tracking the applications to check the respect of social distancing, the detection of overcrowded situations etc. have become a major issue during the pandemic. This UC addresses the problem with an AI based system which will allow a quick response from control and security operators. The detection of hazardous substances on the other hand is extremely important; accuracy and reliability of the solution here is vital in order to avoid false alarms and to make the technology deployable in this critical context. Finally, Anomaly Tracking is a functionality of great interest for control and security operators and is also a challenging from the point of view of the design of the algorithm as well as from the point of view of the cooperation of different sensor networks.

Main objectives of the use case

- Developing low-latency AI-supported processing techniques able to improve the accuracy of environmental surveillance and the effectiveness of identification and containment of hazardous situations.
- Connecting together multiple sensors through an IoT infrastructure, creating a distributed intelligence where the use of AI-based algorithms will be capable to improve the information flows inside the system.
- Providing a scalable monitoring system, in terms of technologies and costs, where “scalable” refers to the ability to monitor any area – from the typical airport large areas to those of small dimensions.
- Monitoring the airport environment in an unobtrusive way, in near real-time via autonomous data collection distributed on the edge (the airport) and collected/managed through an IoT secure infrastructure.
- Offering prompt and reactive containment of hazardous situations, enabled by a hierarchical data processing which relies on local decisions at IoT node level (for immediate reaction), at edge level (based on data fusion in local contexts), at cloud level (for holistic overview).
- Performing biometric recognition on-the-move, in a modality comfortable for the users; performing thermal screening by a validated, non-invasive method; providing a multi-sensor surveillance systems and innovative sensors with reduced impact on people.

- Extracting hidden and useful knowledge embedded within audio sequences to support an efficient decision making process that can contribute to the safety in the airport.

- Making events collection easily available via real-time monitoring.

Benefits and results

Critical infrastructures such as Airports are required to be compliant with rigorous standards for security and safety and at the same time they provide services for and are visited by a large number of passengers. In particular, technologies to be deployed in airports should both take into account the security and safety aspects and the quality of service perceived by the passengers. The UC16 addresses these issues in its different Scenarios through the demonstration of several components which have been summarized in the table above.

The partners involved in the UC ensure that both technical and application-specific knowledge base and expertise are available. Each stakeholder has a specific role in the business case and obtains benefits from being part of the value chain.

Partners involved

LEONARDO is a global player in the high-tech sectors and a major operator worldwide in the Aerospace, Defence and Security sectors.

Based on the dual application of technologies, Leonardo designs and creates products, systems, services and integrated solutions both for the defense sector and for public and private customers of the civil sector, both in Italy and abroad.

EUROTECH Group is an international company that operates in the areas of research, development and commercialization of solutions for the CPSs, Internet of Things (IoT), machine-to-machine and cloud computing.

The company is based in Italy and located mainly in Europe, Japan and USA, with an important presence in several markets: industrial, aerospace and defence, transportation and logistics, medical, security and scientific research.

CINI is a consortium of 41 public Italian universities, today one of the most significant point of reference for the national academic research activities in the fields of Computer Engineering, Computer Science, and Information Technologies.

Established in 1989, CINI is under the supervision of the Italian Ministry for University and Research.

ADP – Aeroporti di Puglia S.p.A. is a company whose primary purpose is the licensed management of Apulia's airports. The corporate purpose includes management of both aviation and non-aviation services, from the management of central infrastructure to security services, sub-concessions etc.

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.

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