Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
UNICO I+D
GOBIERNO DE ESPAÑA

SUCCESS-6G: DEVISE

WP2 Deliverable E5

Use case description, service requirements, and key performance indicators

Project Title:	SUCCESS-6G-DEVISE
Title of Deliverable:	Use case description, service requirements, and key performance indicators
Status-Version:	v1.1
Delivery Date:	31/10/2023
Contributors:	Carmen Vicente, Javier Santaella (Cellnex), Charalampos Kalalas, Ricard Vilalta, Raul Muñoz, Roshan Sedar, Pavol Mulinka, Miquel Payaro, Adriano Pastore, Jesus Gomez (CTTC), Joan Ramon Balasch, Miguel Fornell, Francisco Paredes (IDNEO), Jose Cunha, Guillermo Candela (Optare) Angelos Antonopoulos, Maria Serrano (Nearby Computing)
Lead editor:	Cellnex
Reviewers:	Charalampos Kalalas (CTTC)
Keywords:	use cases; user stories; innovations' description; service level requirements; key performance indicators; facilities

Document revision history

Version	Date	Description of change
v0.1	31/05/23	Table of Contents (ToC) and initial content added
v0.2	06/06/23	First content added related to the user stories and general use case description
v0.3	16/06/23	Modification of ToC to include SUCCESS-6G innovations' descriptions. Additional content was added to user stories' descriptions.
v0.4	30/06/23	Information gathered from workshops was added to use case and user stories sections, and content on innovation and facilities was added.
v0.5	14/07/23	Content added
v0.6	28/07/23	Content added; reformulation of innovations and facilities
v0.7	04/08/23	Content added; updates on service level requirements section
v0.8	25/08/23	Content added; overall quality check; additions of references; updates on figures
v1.0	31/08/23	Final version, upload to the website
v1.1	31/10/23	Updates to Section 6, upload to the website

Acknowledgment

The research conducted by SUCCESS-6G - TSI-063000-2021-39/40/41 receives funding from the Ministerio de Asuntos Económicos y Transformación Digital and the European Union-NextGenerationEU under the framework of the "Plan de Recuperación, Transformación y Resiliencia" and the "Mecanismo de Recuperación y Resiliencia".

[1] http://creativecommons.org/licenses/by-nc-nd/3.0/deed.en_US

Executive Summary

The key research objectives underpinning SUCCESS-6G-DEVISE reside on the design of a secure framework that builds on the extracted knowledge from vehicular streams to offer: i) *real-time vehicle condition monitoring and fault provisioning*, and ii) *over-the-air vehicular software updates in an autonomous manner*.

This deliverable establishes the initial technical foundations on top of which the SUCCESS-6G-DEVISE solutions will be developed. This includes, on the one hand, the elaboration of the SUCCESS-6G vehicular use cases that will be targeted by DEVISE, and, subsequently, the initial set of innovations that will be developed by project partners to address the technical challenges associated with these use cases. For each use case, a user story has been defined, providing a high-level description of the scenarios targeted by SUCCESS-6G-DEVISE. Each user story describes the overall scenario and services to be supported, the involved actors and their roles, the flow of events that form the services, relevant pre-conditions, requirements or constraints, and other information. In addition, a brief description of the lab and real-environment facilities available to the consortium is given, which will be leveraged and extended within the context of the project to develop and showcase the SUCCESS-6G-DEVISE technical innovations and demonstrations. Finally, an initial set of service level requirements and key performance indicators are defined for each use case.

The deliverable is structured in the following sections:

- Introduction.
- Use Case 1 “Vehicular condition monitoring and fault provisioning” and User Story description.
- Use Case 2 “Automated software updates for vehicles” and User Story description.
- SUCCESS-6G-DEVISE innovations.
- Use case facilities.
- Key performance indicators.
- Conclusions.

Table of Contents

List of Figures

List of Tables

1 Introduction

Modern vehicles are progressively transforming into sophisticated computing units able to gather, process, and exchange information with each other and with relevant entities. Equipped with on-board units, vehicles are able to perform sensor data interactions with neighbouring vehicles, roadside units (RSUs) and cloud applications, over wireless connectivity. SUCCESS-6G-DEVISE will bring several novelties for emerging vehicular services in 5G-enabled networks. To showcase these contributions, two use cases have been selected and will be thoroughly studied in the context of the project.

In order to provide a common framework for the work to be conducted in SUCCESS-6G-DEVISE, the following approach has been adopted, inspired by the methodology proposed by 5GAA to describe scenarios in the automotive domain, with the necessary adaptations required to capture the specific characteristics of the SUCCESS-6G scenarios. In that sense, two levels of description have been defined: *use case* and *user story*. The use cases provide the overarching scenarios for the coordinated SUCCESS-6G project, focusing respectively on ***vehicular condition monitoring and fault provisioning*** and ***automated software updates for vehicles***. For each use case, a user story has been defined, corresponding to the DEVISE subproject of SUCCESS-6G. Each user story describes the overall scenario and service to be supported, the involved actors and their roles, the flow of events that form the service, relevant pre-conditions, requirements/constraints, and other information.

With these elements in place, a list of SUCCESS-6G-DEVISE innovations has been identified, capturing the key technical challenges that will be addressed in the context of the project, and bringing added value to the defined user stories. These innovations will be the starting point for the technical contributions to be developed within WP3-5 and will be validated within the aforementioned WPs, as well as through SUCCESS-6G-DEVISE proof-of-concept demonstrations to be specified within WP4-5. To this end, use case facilities and key performance indicators are specified in Sections 5 and 6 respectively.

2 Use case 1: Vehicular condition monitoring and fault provisioning

2.1 General description and overall objectives

Vehicle manufacturers are expected to highly benefit from AI-based predictive maintenance services to implement automatic condition monitoring in on-board vehicular equipment. In this context, data-driven mechanisms analysing historical data and real-time information from vehicles are essential to identify irregular functional conditions/patterns in monitoring information, leading to predictive maintenance tailored to the needs of each individual piece of equipment. In turn, the detection of anomalies reduces unplanned downtime and costs, by quickly providing an estimate about when the equipment is expected to fail.

C-V2X technology and infrastructure enable vehicles to exchange real-time data related to their operating conditions, performance, and maintenance needs with infrastructure and service providers. Furthermore, C-V2X secure connectivity could enable service providers to remotely access a vehicle's onboard diagnostics and troubleshoot issues without physically being present saving time and costs associated with traditional on-site inspections. Of particular importance are the AI-empowered visualization tools and customized dashboards, which support tailored queries and provide a wide range of charting capabilities, e.g., trajectory graphs and trend maps, for analysing and presenting the monitoring information to interested stakeholders.

Figure 1: Implementation phases for a vehicular predictive maintenance service

As illustrated in Figure 1, the implementation **phases** for a vehicular predictive maintenance service comprise: i) identification of the critical assets in a vehicle, ii) acquisition of monitoring information, iii) data fusion and transmission, iv) establishment of a database for storage of historical data, v) analysis of failure modes and failure predictions and vi) decision-making. Maintenance is then only performed when data analytics indicate that performance has degraded, or a failure is likely to occur.

Modern vehicles' electrical and electronic systems are managed by various electronic control units (ECUs) which use the Controller Area Network (CAN) bus to exchange real-time information, including:

- Engine parameters such as load, coolant temperature, throttle position, and mass air flow (MAF).
- Vehicle speed.
- Transmission data such as gear position, shift requests, torque converter lockup status, and transmission temperature.
- ABS and stability control data on wheel speed, brake pressure, and yaw rate.
- Instrument cluster data such as speed, fuel level, warning lights, and other vehicle-related information to display to the driver.
- Climate control such as HVAC (Heating, Ventilation, and Air Conditioning).

Specific information available on the CAN bus can vary depending on the vehicle's make, model, and original equipment manufacturers (OEM). Most part of this data can be sampled through the On-Board Diagnostics (OBD) port by constant polling.

The overall **objectives** of this use case can be summarized as follows:

- Real-time condition monitoring of vehicular assets.
- Identification and classification of abnormal system behaviour.
- Minimization of the number of unexpected breakdowns.

- Safety improvement.
- Vehicular equipment's lifespan can be optimized to its fullest.
- Reduction of operational costs by performing maintenance only when necessary.
- Maximization of production hours.
- Maintenance costs are streamlined through reduced equipment, inventory costs and labour.

The key **stakeholders** involved in the use case are:

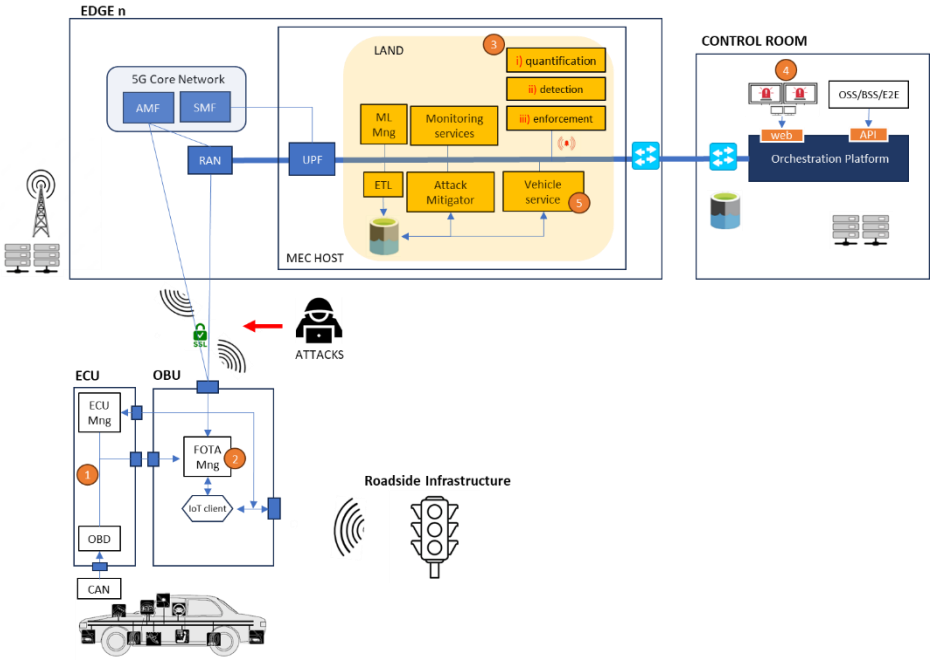
- The ***Mobile Network Operator (MNO)***, providing wireless connectivity between the vehicle, the edge monitoring infrastructure, and the remote maintenance center. The MNO is interested in optimizing the network operation by enhancing its energy efficiency and coverage, while offering novel services to accommodate more users.
- The ***edge infrastructure provider***, offering and managing computational resources at the edge and supporting real-time services as well as virtualized network functions and AI-empowered algorithms for advanced computational tasks.
- The ***maintenance team,*** entitled with the remote supervision of the vehicular condition indicators and health status.
- The ***equipment provider,*** providing in-vehicle monitoring infrastructure, such as hardware components and sensor devices, to be deployed in the vehicle for condition supervision purposes.
- The ***software developers***, devising and applying data-processing modules for the aggregated measurement streams to determine the condition of vehicular equipment and predict when maintenance actions should be performed.
- The ***cloud providers*** can optionally be involved, offering additional computational resources to host the service.

Note that, without loss of generality, some stakeholders may assume multiple roles or, equally, some roles may be assumed by multiple stakeholders. For instance, the MNO could also be the owner of the edge infrastructure, or an equipment provider may act as responsible for the vehicle maintenance or outsource it to a third party.

2.2 User story: Vehicular condition monitoring with security guarantees

This section contains the user story defined in the context of the SUCCESS-6G-DEVISE subproject for the first use case. We provide the details in the following table.

User story name	*Vehicular condition monitoring with security guarantees*
Subproject	DEVISE
User story description	A C-V2X infrastructure provides coverage to the connected vehicle throughout its trajectory for monitoring purposes. Wireless transmission of in-vehicle monitoring data is susceptible to various security threats which may destabilize system operation, degrade network performance, and potentially lead to incorrect decision-making regarding the vehicle condition status. At the same time, the pervasive integration of data-driven techniques expands the attack surface, giving rise to finely targeted, stealthier, and scalable attacks targeting both phases (training, inference) of ML techniques. The mitigation of such threats becomes imperative for the correct estimation of vehicle condition. Condition monitoring data used for subsequent predictive diagnostics should be properly secured such that they do not contain falsified information, while abnormal traffic should be detected and isolated in its entirety. In this context, appropriate security countermeasures are expected to accurately detect

	malicious content in the transmitted information and ensure the semantic correctness of the aggregated data for trustworthy decision-making.
Illustration	The following diagram illustrates the flow of the main events taking place in the user story:  *Figure 2: Use Case 1 - User Story diagram*
Main event flow	1. Data is captured from the OBD port where ECU information from sensors installed in the vehicle is available. 2. Transmission to the edge monitoring infrastructure takes place with the aid of a vehicular OBU which fuses aggregated information from various sensors and a C-V2X roadside infrastructure comprising mobile radio stations and/or road-side units (RSU). 3. Measurement streams are aggregated and processed at the edge monitoring units. Aggregated information can be directly or indirectly used for downstream tasks: i) quantification of the impact of threat vectors injecting falsified information in supervisory data; ii) detection of injected false data with the aid of AI/ML techniques to ensure trustworthy connectivity; iii) enforcement of security policies and development of defensive measures towards secure condition monitoring by empowering a fully new breed of autonomic cyber-capabilities, e.g., self-protection, self-healing, which increase resiliency to attacks. 4. Based on the knowledge extracted and with the help of appropriate visualization tools and platforms, instructive and actionable insights are derived by the maintenance team towards an enhanced end-to-end performance, e.g., flag whether a fault has occurred and diagnose its type in event-detection operations. The selection of appropriate security countermeasures for trustworthy decision-making is also performed. 5. Appropriate actions, e.g., alerts, modification of sensor reporting frequency, are communicated back to the vehicle as a response to the automated supervision of measurement flows. Attack/threat mitigation strategies should have minimum impact on the underlying communication.
Alternative	Trustworthiness may also be preserved by instantiating virtual security

event flow	functions. Automation of security services with zero-touch workflows and self-managing capabilities may also be considered.
Actors	Automaker/OEM, OBU, roadside C-V2X and edge infrastructure operator, MEC platform, MNO, service provider, maintenance team.
Vehicle role	Vehicle is equipped with monitoring sensors which acquire status information related to various vehicular operations. The vehicle communicates monitoring information and other data to the infrastructure and receives information from the edge infrastructure.
Infrastructure role (including edge, cloud, and communications infrastructure)	• Communication infrastructure provides C-V2X connectivity between the vehicle, the roadside infrastructure, the edge platform and other involved connected actors (e.g., maintenance centre). • Edge monitoring infrastructure aims at storing, processing, analysing, and responding to data close to the acquisition points, enabling dramatically faster processing times and localized decision-making.
Service provider	• Agile decision-making and automated response for adaptation to a dynamic V2X threat landscape will be supported. • Service provides an Intrusion Detection System (IDS) for attack detection. • Service provides an attack mitigation system at the edge, ensuring low latency responses.
Other actors' roles	• MEC Orchestrator provides lifecycle management functionalities of the vehicular condition monitoring services into the edge infrastructure. • The MNO provides the wireless connectivity necessary for data transmission from the OBUs to the monitoring infrastructure. • The maintenance team offers situational awareness and appropriate supervisor actions for informed decision-making, e.g., about when vehicular maintenance should be performed.
Pre-conditions	• Availability of a scalable and reliable underlying communication system capable of supporting vehicular data transmission towards computing units, being them edge- or cloud-based (if needed, to perform computationally heavy tasks). • Attack patterns and malicious behaviour should be adequately characterized as part of the considered scenario.
Post-conditions	• Predictive diagnostics allow for instructive and actionable insights to be derived towards enhanced end-to-end performance, e.g., flag whether a fault has happened or is about to happen and diagnose its type in event-detection operations. • Automatically learn attack patterns and signatures from experience and generalize to future unseen V2X threats. • Secure service provisioning for condition monitoring of vehicles in untrusted environments.
Information requirements	• Information (e.g., event log data) pertaining to the condition of vehicular components. Such information originates from captured sensor data and/or equipment status reports. • Network data pertaining to edge servers and L3/L4 related data.
Constraints/	Part of information available on the CAN bus is proprietary data and exclusively

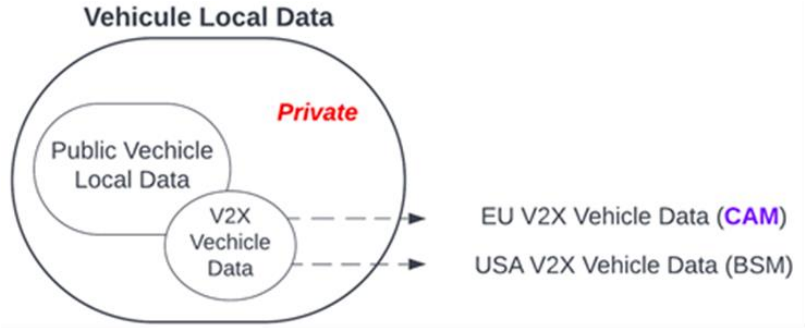
Presumptions	accessible to the car manufacturer and its licensed partners. The following diagram illustrates how data is distributed within the vehicle, differentiating between the public and private domains.  *Figure 3: Use Case 1 - Vehicle data domains* Vehicular assets/conditions to be monitored should have a high failure occurrence ratio. However, the accessibility to such information may be a constraint. As data is collected through the OBD connector which is connected to the CAN bus through a gateway, this device introduces a delay in the data acquisition which can range between 5ms and 50ms. Therefore, the response time of the gateway will condition the frequency at which the information is uploaded to the database. Approximately, it is expected that every 800/1.200 ms the database will be updated with a data packet containing multiple sensor values. When vehicle moves along the road, it can use roaming functions to connect to different MNO networks and keep the connectivity services. In SUCCESS-6G project roaming will not be considered, as the vehicle will remain always inside the same MNO network.
Geographic scope	ParcMotor Circuit will be used for testing the use case providing a continuous 5G coverage.

Table 1: Description of user story for use case 1.

3 Use case 2: Automated software updates for vehicles

3.1 General description and overall objectives

Over-the-air software updates are delivered remotely from a cloud-based server, through a cellular connection, to the connected vehicle with the aim of providing new features and updates to the vehicle's software systems. Such software updates may include changes to any software that controls the vehicle's physical parts or electronic signal processing system. In practice, the updates often tend to apply more to user interfaces like infotainment screens and navigation (i.e., vehicle maps). The update procedure, when performed over-the-air, enables a vehicle's performance and features to be continuously up-to-date and improved. The integration of advanced data analytics, automated and remote service delivery eliminates the need for visiting repair/service centres, while technological advancements in these updates give vehicle manufacturers the freedom to constantly "freshen up" finished products remotely. C-V2X technology plays a crucial role for the update process, enabling efficient, scalable and seamless wireless communication between vehicles and software management platforms.

Figure 4: Implementation phases for the automated software updates.

Figure 4 illustrates the implementation phases for this use case.

The overall **objectives** of this use case can be summarized as follows:

- Safer and more entertaining driving experience.
- Hardware and software components maintained and updated regularly during a vehicle's lifespan, implying a slower rate of depreciation.
- Prevention of cyberattacks targeting outdated software.
- Compliance to new rules and standards.
- Lower repair costs and elimination of labour charges.
- Lower warranty costs for manufacturers and lower downtime for customers

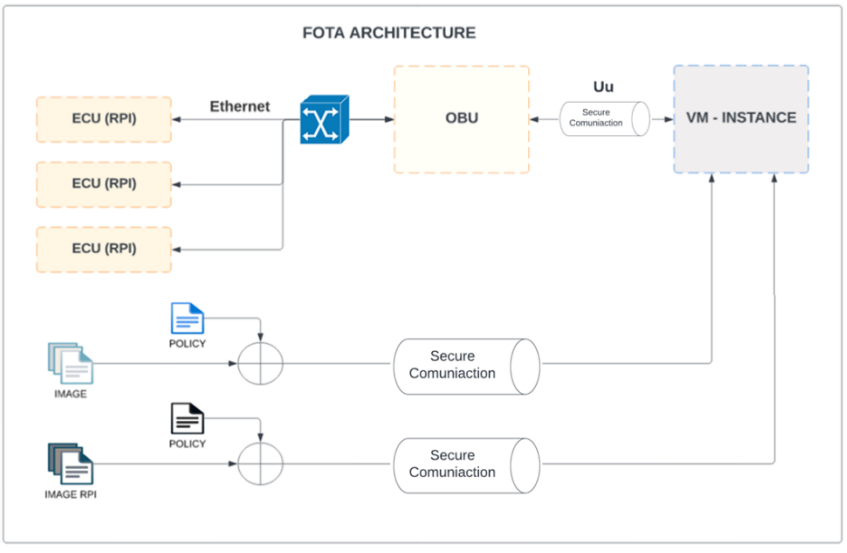
The key **stakeholders** involved in the use case are:

- The ***Mobile Network Operator (MNO)***, providing wireless connectivity between the vehicle, the edge computing infrastructure, and the vehicular software management system. The MNO is interested in optimizing the network operation by enhancing its energy efficiency and coverage, while offering novel services to accommodate more users.
- The ***edge infrastructure provider***, offering and managing computational resources at the edge and supporting real-time services as well as virtualized network functions and AI-empowered algorithms for advanced computational tasks.
- The ***equipment provider,*** providing in-vehicle embedded devices, e.g., hardware components and sensor devices, that can be remotely reconfigured and updated.
- The ***vehicular software management system,*** operated by the equipment provider or vehicle manufacturer, is responsible for issuing periodically new software updates.
- The ***software developers***, devising and applying data-processing modules for automated update of vehicular components' software.
- The ***cloud providers*** can optionally be involved, offering additional computational resources to host the service.

Note that, without loss of generality, some stakeholders may assume multiple roles or, equally, some roles may be assumed by multiple stakeholders. For instance, the MNO could also be the owner of the edge infrastructure, or an equipment provider may also be responsible for the operation of the vehicular software management system or outsource it to a third party.

3.2 User story: Over-the-air vehicular software updates with security guarantees

This section contains the user story defined in the context of the SUCCESS-6G-DEVISE subproject for the second use case. We provide the details in the following table.

User story name	*Over-the-air vehicular software updates with security guarantees*
Subproject	DEVISE
User story description	Over-the-air software updates deliver critical information to on-board vehicular devices. As vehicles introduce new functionalities (such as advanced driver-assist features like self-parking) and the number of connected vehicles keeps growing, automakers need to handle the regular software updates required in a secure and trustworthy way. Thus, the integration of intelligent security enforcement solutions, and effective prediction/mitigation of security threats are deemed essential for the secure operation of over-the-air update service and to preserve trustworthiness. Additionally, by instantiating virtual security functions and by exploiting secure edge provisioning empowered by AI-driven capabilities, the threat risk for software updates can be further minimized.
Illustration	The following diagram illustrates the flow of the main events taking place in the user story:  *Figure 5: Use Case 2 - User Story diagram*

Main event flow	1. The vehicular software management system issues a new software update. 2. The update is uploaded to the cloud where it is queued, downloaded, and verified by the target device over a cellular connection. 3. Once verified, the system typically triggers an alert that prompts the vehicle owner to approve or decline the update. 4. After confirming approval, the software package is delivered, and the update is installed in the vehicle. Security enhancements are implemented to guarantee a high grade of security in over-the-air update service and prevent malicious actions, e.g., unauthorized access, during vehicular software updates. 5. After installation, diagnostic information is sent back to the vehicular software management system as feedback. Measurable outputs in terms of trust for networking components involved in security service-level agreements for software updates are provided.
Alternative event flow	Secure lifecycle service management for software updates will ensure that the introduced software capabilities advance the level of security of vehicles and reduce any potential malfunction problems derived from insufficient system trustworthiness.
Actors	Automaker/ECU, OBU, roadside C-V2X and edge infrastructure operator, MEC platform, MNO, service provider, vehicular software management system.
Vehicle role	Vehicle is equipped with embedded devices and hardware components that support remote software updates and configurability of their functionalities.
Infrastructure role (including edge, cloud and communications infrastructure)	• Communication infrastructure provides C-V2X connectivity between the vehicle, the roadside infrastructure, the edge platform and other involved connected actors (e.g., software management system). • Edge infrastructure hosts storing and processing services for the updates providing faster processing times, reduced backhaul bandwidth consumption and localized decision-making
Service provider	• The vehicular software management system makes usage of monitoring protocols for verifying the state of software updates and generate decision actions for the edge-specific orchestrator. It is also responsible for the configuration, management and quality control of the updates. It further defines the update requirements and ensures updates are executed safely and will not affect the safety or certification of vehicles. Finally, it ensures compliance with the existing regulations for the delivery of software updates.
Other actors' roles	• MEC Orchestrator provides lifecycle management functionalities of the software updates and application services into the edge infrastructure. • The MNO provides bidirectional wireless connectivity necessary for the download of the updates and any other message exchange related to the verification of the downloaded content.
Pre-conditions	• Availability of a scalable and reliable underlying communication system capable of supporting vehicular data transmission towards

	computing units, being them edge- or cloud-based (if needed, to perform computationally heavy tasks). • Over-the-air software update platform needs to be compatible with the operating systems and the remotely connected in-vehicle network, to update vehicle software and features in the field while collecting real-time operational data.
Post-conditions	• Ensure that vehicular software updates are performed with minimized threat risk and prevent that the edge server is compromised or eavesdropped by attackers. • Efficient infrastructure/service data mining and on-boarding of containerized AI blocks for secure zero-touch orchestration. • Ensure secure over-the-air connectivity with backend servers at network edge, by preventing unauthorized access to vehicular software updates for the preservation of trustworthiness. • Secure lifecycle service management for vehicular software updates.
Information requirements	Information (e.g., event log data) pertaining to the condition of vehicular components, including vehicle location. Such information originates from captured sensor data and/or equipment status reports. Network data pertaining to edge servers and L0/L3/L4 related data.
Constraints/ Presumptions	Security threats will be defined at a later stage in order to provide the definition of the security service level agreement. Vehicle will remain always connected to the same MNO network. Thus, roaming functions will not be used in the project to keep the communication services.
Geographic scope	ParcMotor Circuit will be used for testing the use case providing a continuous 5G coverage area including two radio stations in order to test connectivity robustness while cell handover.

Table 2: Description of user story for use case 2

4 SUCCESS-6G-DEVISE innovations

This section covers the different technological innovations that will be explored within the SUCCESS-6G-DEVISE subproject for use case 1 and 2. The innovations will be developed and validated during the subproject lifetime within the corresponding WP scope and showcased if successfully implemented and tested in the final demos.

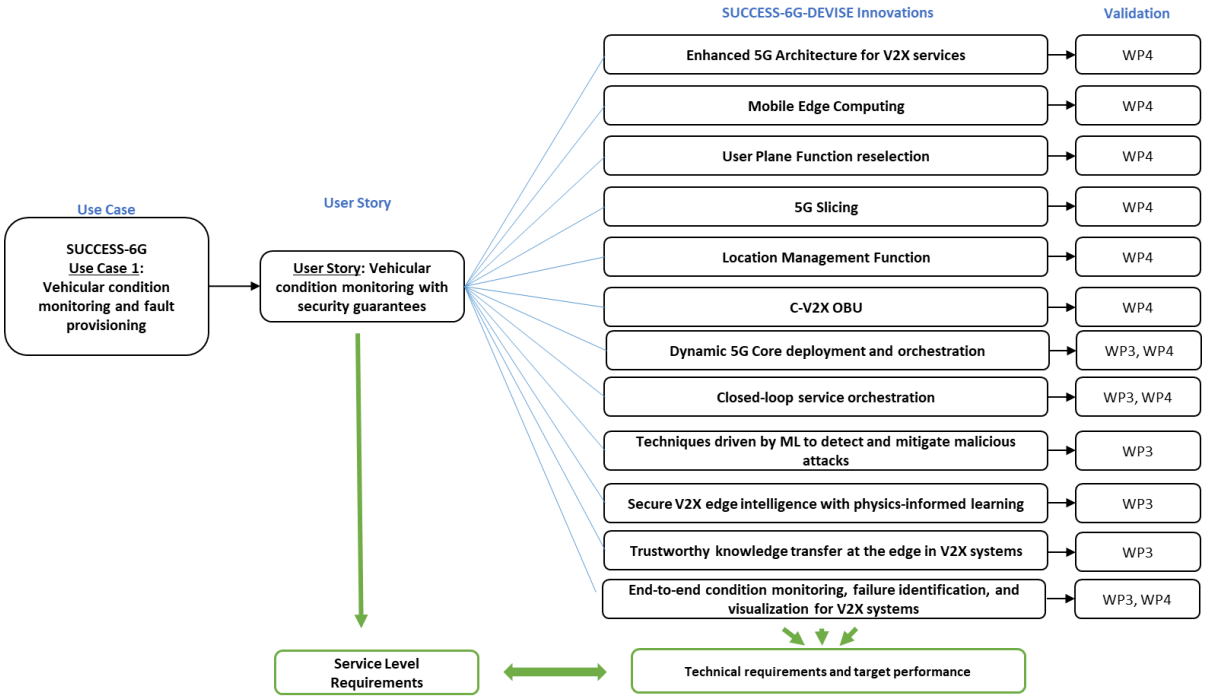


Figure 6: Use case 1, relevant user story and mapping of technical contributions.

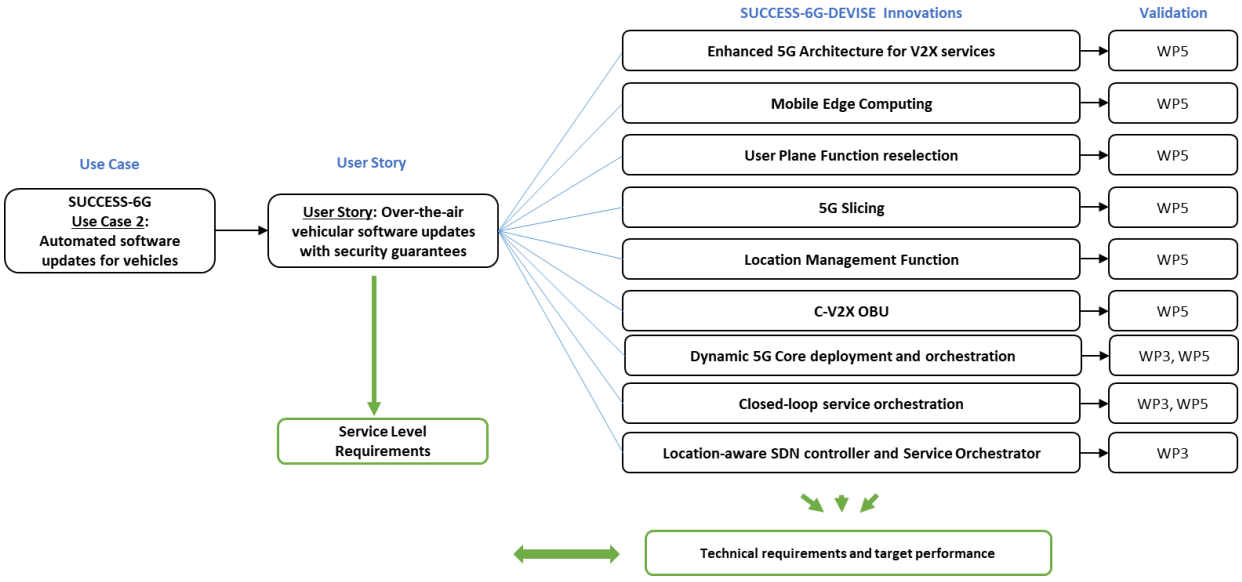


Figure 7: Use case 2, relevant user story and mapping of technical contributions.

The identified SUCCESS-6G-DEVISE innovations and their mapping to user stories and WPs are illustrated in Figure 6 and Figure 7 for use case 1 and use case 2, respectively.

4.1 Innovations that apply to both Use Cases

4.1.1 5G Architecture enhancements to support V2X services

ETSI TS 123 287[2] is a technical specification defined by the European Telecommunications Standards Institute (ETSI). The main objective of ETSI TS 123 287 is to standardize the "Application Layer (AP) for V2X (Vehicle-to-Everything) communication systems."

5G System to be deployed in SUCCESS-6G-DEVISE project will follow main enhancements for 5G systems to support V2X services specified in ETSI TS 123 287. These architectural improvements focus on vehicular communication and enable the efficient delivery of V2X services over PC5 and Uu reference points.

One of the key improvements at the Uu reference point is the support for 5G Core (5GC) network integration. Project's 5G Core solution ensures seamless connectivity and communication between V2X devices and the 5G network which includes roaming and non-roaming scenarios, inter-PLMN, Application Function (AF) based services and service-based interfaces. This integration enables the delivery of advanced V2X services, such as real-time traffic information, vehicle platooning, and enhanced road safety features.

4.1.2 Mobile Edge Computing

Mobile Edge Computing is the concept of implementing more of the communications handling at the Edge of the network, closer to the cellular radio coverage. This is in contrast to previous centralised core network architectures which bring user traffic to a central point in the network before processing can take place.

Two models of Edge Computing are supported by the Raemis[3] platform that compose the Core of the network. The basic model is pure MEC data plane offload. This model has been promoted by the ETSI MEC working group and an overview of the Raemis support for this model is provided in the next section.

Nevertheless, the MEC data plane offload model is not an effective approach in providing resilience and survivability to the network Edge. To address this requirement, which is key for critical communications use cases, the Raemis platform provides the distributed Edge Core model which provides fully resilient service at the network edge in addition to the data plane offload capabilities.

[2] https://www.etsi.org/deliver/etsi_ts/123200_123299/123287/17.06.00_60/ts_123287v170600p.pdf

[3] https://www.druidsoftware.com/raemis-cellular-network-technology/

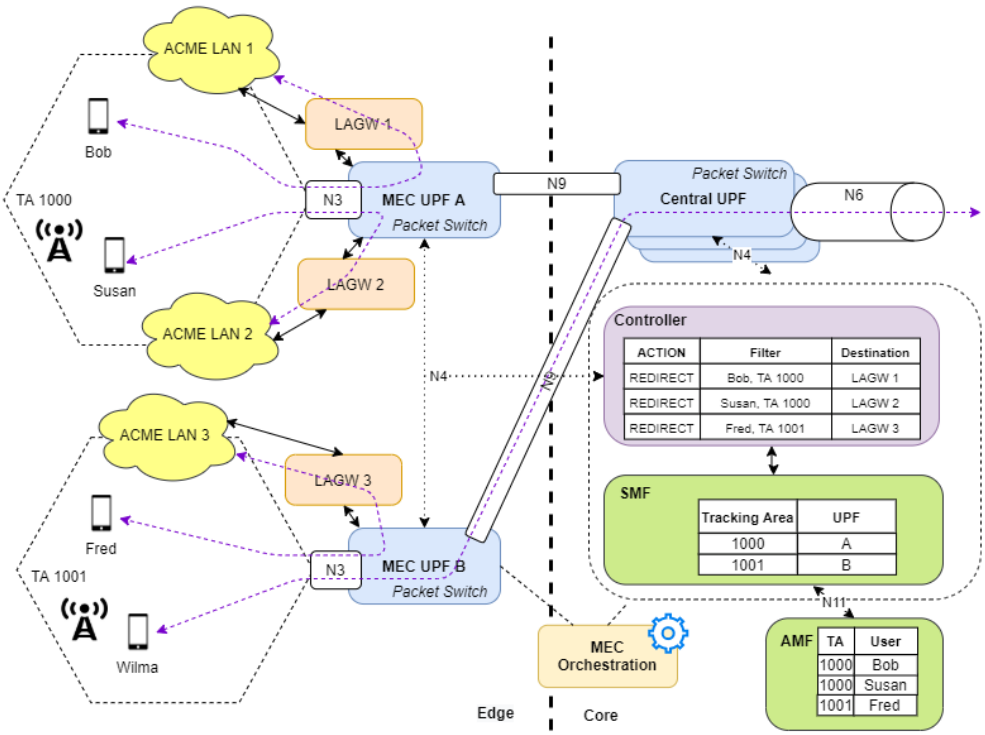


Figure 8: The Raemis Enterprise Slice

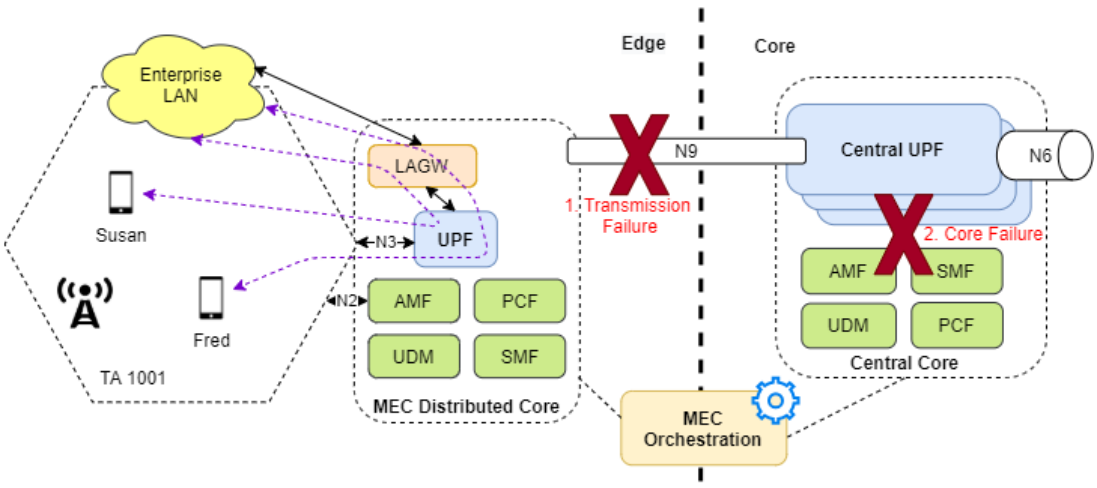


Figure 9: MEC Distributed Resilient Core

The distributed core model of delivering MEC services has the added advantage of being capable of delivering completely autonomous local service. This is particularly important for use cases requiring some form of critical services. The Edge core configuration is implemented as MEC slices by the orchestration function.

4.1.3 User Plane Function reselection

Distributed UPF (User Plane Function) refers to the deployment of the 5G core network UPF functionality in a distributed manner within a network architecture. Distributed UPF allows for the distribution of user data processing tasks across multiple instances of the UPF function deployed at different locations. Improving the overall efficiency of data processing by minimizing the distance data needs to travel, reducing latency, and optimizing resource utilization.

UPF reselection refers to changing a UE's UPF(s) seamlessly based on the current location. It can be used to continuously provide the optimal data path for UEs on the move for systems/applications relying on low-latency communication and/or MEC offload.

3GPP has defined Session and Service Continuity Modes (SSC) Modes 1, 2 and 3 for changing anchor UPF. SSC mode 3 enables seamless reselection of UPF anchor however it is optional for UEs to support and has a signalling overhead.

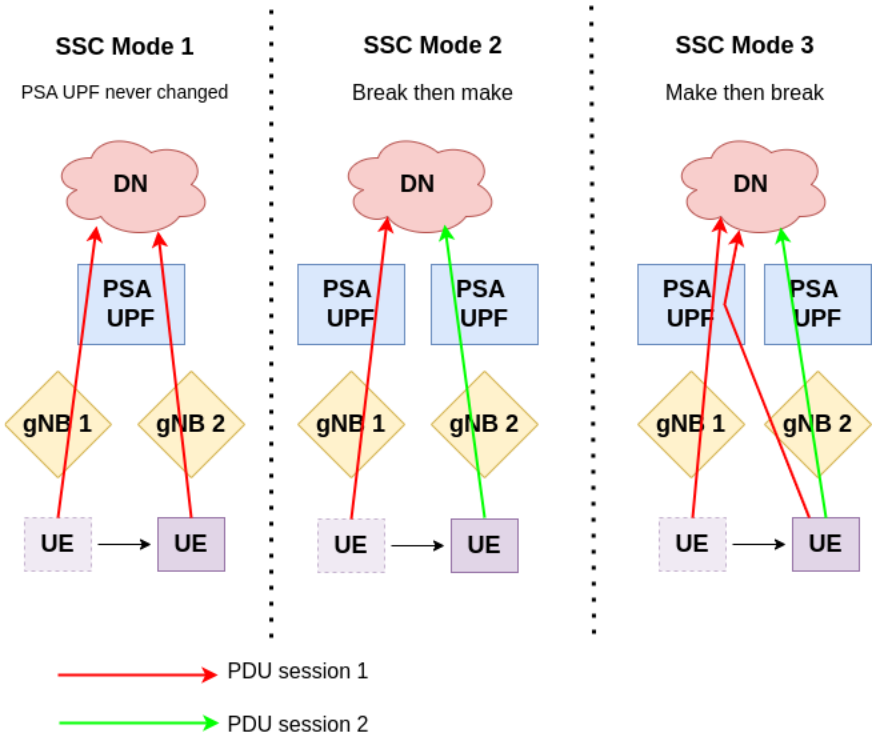


Figure 10: 3GPP UPF reselection modes

Raemis provides a solution for seamless UPF reselection without relying on UE's support for SSC mode 3. The solution relies on UE IP address allocation being handled by a central SMF or DHCP server and UE IP address is routable on N6 interface of all UPFs. This way, UE moves from gNB 1 to gNB 2 while sending uplink data with zero interruption in data stream.

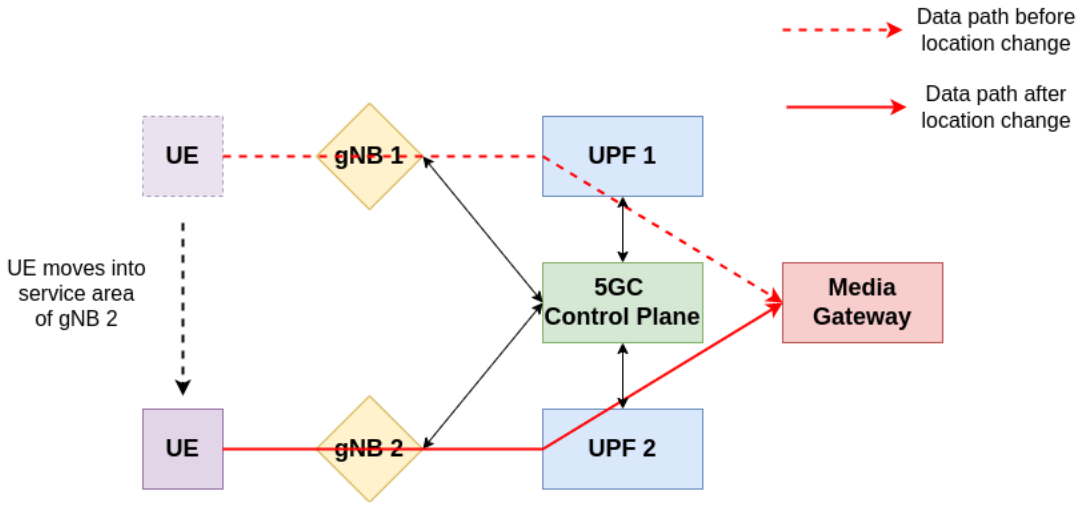


Figure 11: Raemis UPF reselection

4.1.4 5G Slicing

5G slicing refers to a key architectural feature in 5G networks that allows the creation of multiple virtual, independent, and logically isolated networks, known as “slices,” within a single physical 5G infrastructure. Each slice can be customized to cater to specific service requirements, use cases, or customer needs, while sharing the same underlying 5G infrastructure efficiently.

Raemis administrator can create multiple Packet Data Networks (PDNs). PDN logical network can be associated with an enterprise VLAN (or the physical network port on the server or a VM) to provide Security & Traffic Separation, Load Balancing, and Configurable QoS.

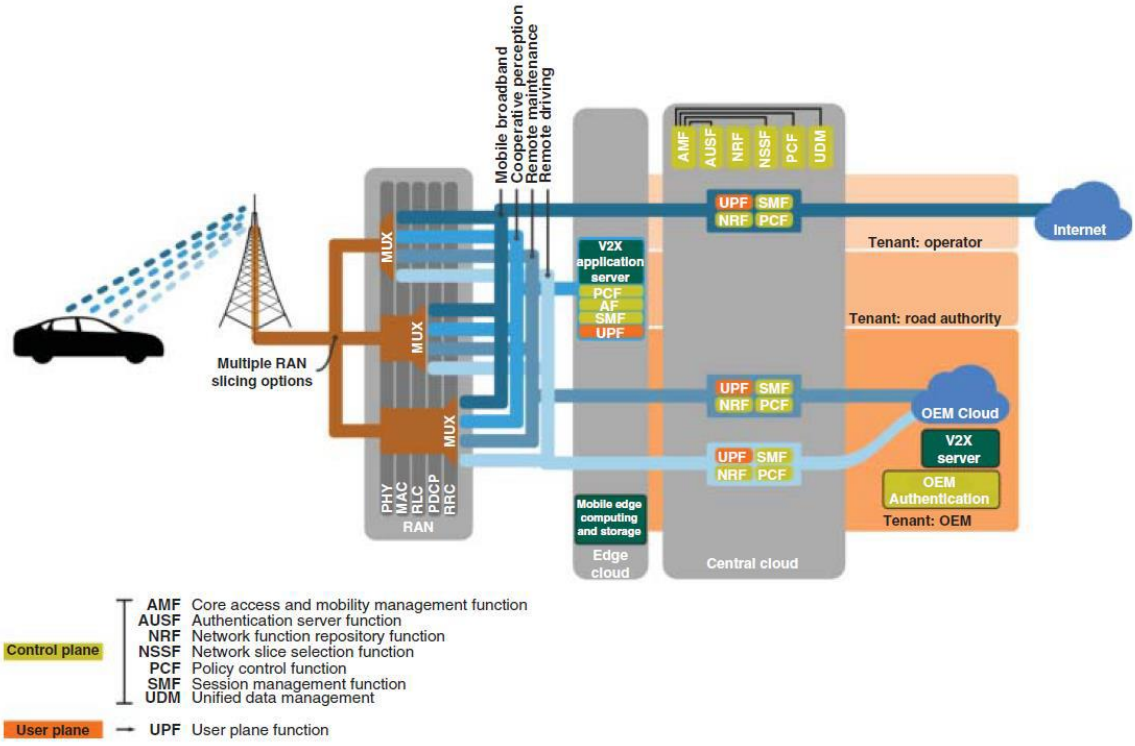


Figure 12: 5G Slicing flow of functions[4]

4.1.5 Location Management Function

Location Management Function (LMF) is a crucial component in 5G networks, responsible for managing location-related functionalities and services for mobile devices. Its main role is to track and handle the mobility of user equipment (UE) as they move within the cellular network.

[4] M Fallgren et al, “Cellular V2X for Connected Automated Driving”, 2021

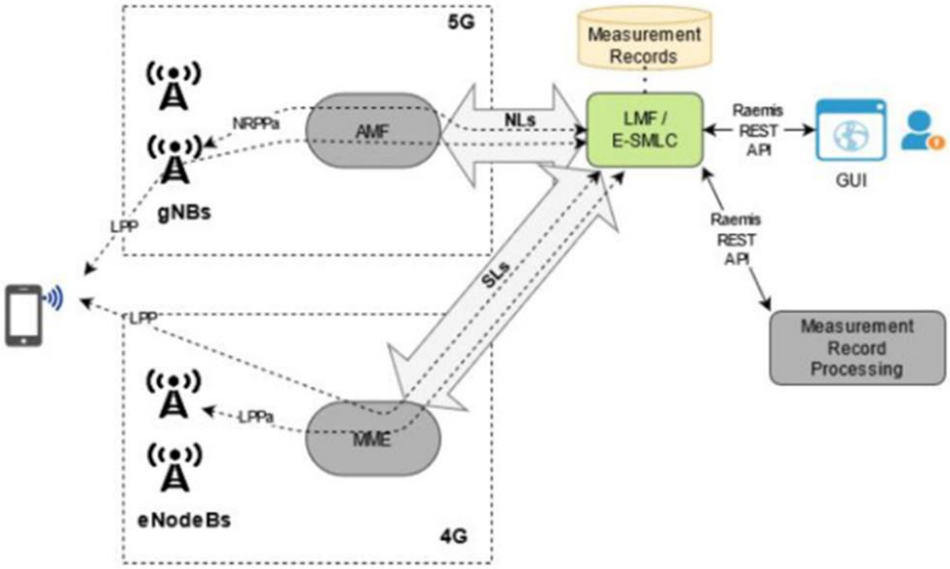


Figure 9: Location Management Function (LMF)

Main benefits include:

- Accurate Positioning: ensures that connected vehicles can accurately determine their geographical location and share this information with other vehicles and infrastructure. High precision positioning is critical for advanced driver assistance systems (ADAS), cooperative mobility applications, Autonomous Driving, Emergency Services and Traffic Management and Optimization.
- Contextual Information Sharing: With precise location data, safety applications like collision avoidance, blind-spot warnings, and intersection assistance can be enabled. Vehicles can exchange real-time position updates to help prevent accidents and ensure safe driving practices.
- Smart Navigation: The LMF allows for intelligent route planning and dynamic rerouting based on real-time traffic conditions. Connected vehicles can receive updated navigation instructions to avoid traffic jams, accidents, or road construction, leading to more efficient and stress-free journeys.

4.1.6 C-V2X OBU

The hardware platform designed to meet the requirements of SUCCESS-6G-DEVISE use cases is primarily based on two latest generation modules specifically designed to address the latest advancements in C-V2X systems within the 5G NR environment. This OBU is one of the first Automotive Grade Compliant devices with 5G NR Sub-6 GHz capabilities, supporting both Stand Alone (SA) and Non-Stand Alone (NSA) modes.

The OBU is specifically designed for C-V2X vehicle communications, such as advanced driving safety, autonomous driving, Intelligent Transportation Systems (ITS), and Advanced Driver Assistance Systems (ADAS). Apart from that, it also provides critical security functions in C-V2X through its ARM processors, ECDSA cryptographic module for message verification, and HSM module for message signing. This way, the AP provides all the necessary elements for executing a C-V2X Stack, a C-V2X messaging software that manages, among other functions, the verification of received messages and secure signing of sent messages.

Thanks to this, the vehicle will be connected to the infrastructure, providing a low-latency channel to transmit the vehicle's data, ensuring a secure connection that guarantees the integrity and encryption of the data, as well as its robustness and efficiency. This innovation will be associated to all user stories.

4.1.7 Dynamic 5G Core deployment and orchestration

The 5G Core may be deployed manually, or through the orchestrator. In SUCCESS-6G-DEVISE, the 5G core will be deployed as a service through NearbyOne, as part of the orchestrator's onboarded application in its Marketplace. Figure 14 shows the NearbyOne Marketplace in the environment that has been created for SUCCESS-6G-DEVISE subproject. It is expected that the different 5G core elements (e.g., 5G core as a service, distributed UPF, etc.) will be onboarded in NearbyOne and appear as blocks in that section.

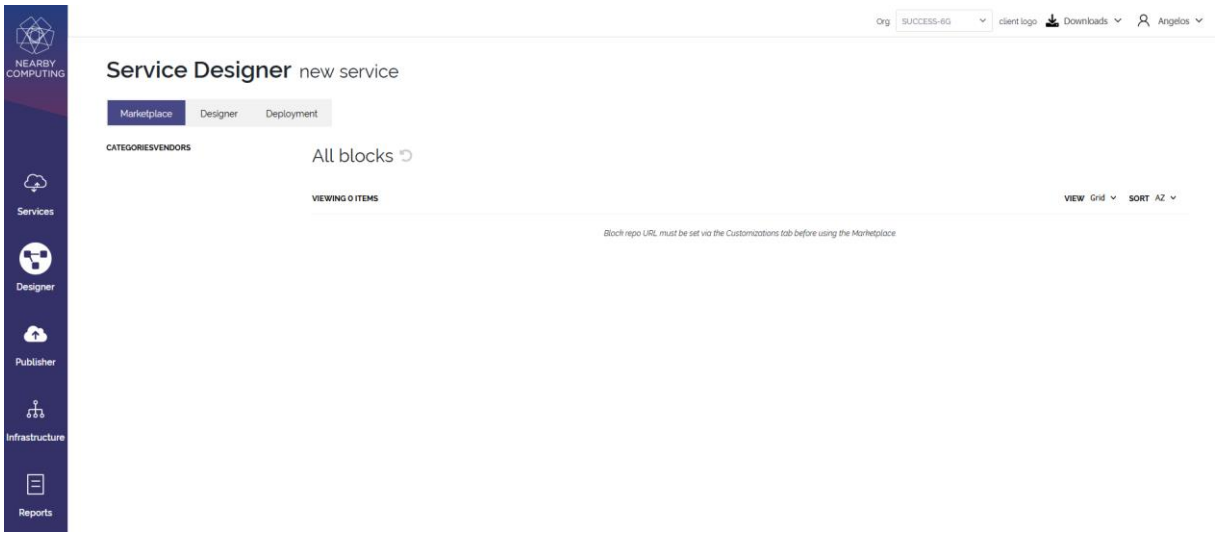


Figure 10: NearbyOne Marketplace for SUCCESS-6G-DEVISE project

In particular, the orchestrator has the ability to onboard the network functions provided by the network operator that are needed to enable access to the workloads to be deployed. 5G Core software components will be packaged into Nearby Blocks and will be onboarded on the platform. The conversion is made by encapsulating logic and code for the different application-specific functionalities and is created according to the defined policies. Nearby Blocks describe how to deploy the 5G Core, including several aspects such as:

- Rendering 5G Core configurations
- 5G Core placement across the registered clusters
- Number of Instances to be deployed.

The process of definition and packaging of the different components that are part of a certain block and the actual action of uploading the block into the NearbyOne platform is known as Block Onboarding. This setup enables the deployment of the 5G Core in any infrastructure that is orchestrated by NearbyOne, as well as the deployment of the distributed UPF in a different location (e.g., at the edge closer to the user).

4.1.8 Closed-loop service orchestration

SUCCESS-6G-DEVISE foresees a closed-loop orchestration framework for automotive scenarios. Closed-loop orchestration is an advanced and dynamic process that involves a seamless integration of data collection (through monitoring), an analytics engine running AI algorithms, a decision engine, a

broker, and an automated orchestrator. This comprehensive framework operates in a continuous feedback loop, continually analyzing, adapting, and automating actions based on real-time insights.

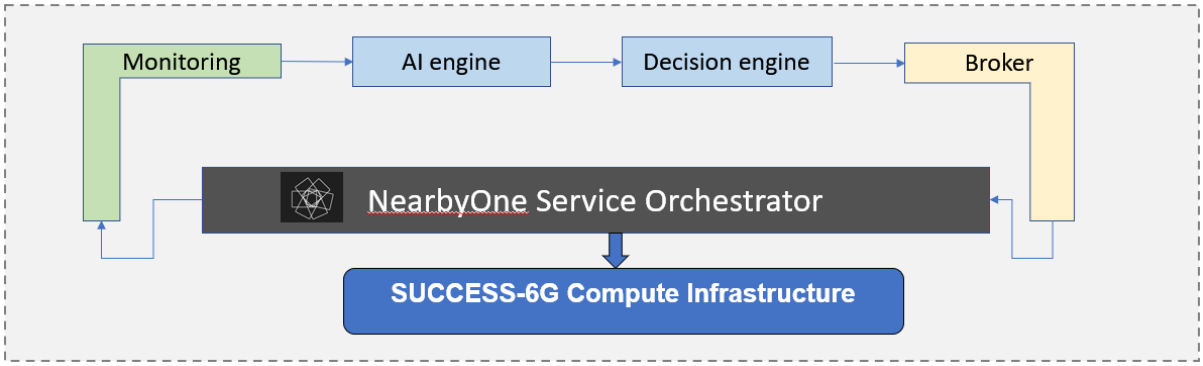


Figure 11: Closed-loop service orchestration in SUCCESS-6G-DEVISE project.

The above closed-loop process in the context of SUCCESS-6G-DEVISE is depicted in Figure 15. The foundation of closed-loop orchestration lies in the data collection phase, where diverse data types are acquired from various sources. This data includes network-related metrics, application-specific information, location-based data, and other relevant parameters, forming a rich and varied dataset to drive subsequent stages.

Once the data is collected, it undergoes rigorous analysis and processing in the analytics engine, leveraging powerful AI algorithms such as ML models, deep learning neural networks, anomaly detection, and predictive analytics. These algorithms derive valuable insights, detect patterns, predict trends, and identify potential issues or opportunities within the system.

The decision engine is the intelligence center of the closed-loop orchestration. It integrates the outputs and insights from the analytics engine, making informed judgments and decisions. These decisions involve fine-tuning system parameters, dynamically adjusting configurations, or triggering automated actions in response to changing conditions and data inputs.

The broker acts as an intermediate actor between the decision engine and the orchestrator. It receives the decisions from the decision engine and processes and translates them into actionable instructions for the orchestrator. The broker plays a crucial role in decoupling the decision-making process from the orchestration process, enabling more flexibility and adaptability in the overall system architecture.

The orchestrator is responsible for implementing the instructions received from the broker. It automates actions such as scaling up or down resources, dynamically reconfiguring the system, allocating resources efficiently, and initiating service migrations to optimize the system based on the decisions.

In SUCCESS-6G-DEVISE, the closed-loop orchestration process will ensure a self-regulating, adaptive, and efficient system that can respond in real-time to fluctuations in demand, changing environments, and evolving needs. By enabling automated decision-making and proactive system management, closed-loop orchestration will ensure optimal performance and is expected to enhance the user experience across various domains and applications.

4.2 Innovations that apply only to Use Case 1

4.2.1 Techniques driven by ML to detect and mitigate malicious attacks

Related to the user story of use case 2 and mapped to WP3 activities, the following innovation is proposed:

- Develop intrusion detection mechanisms and data encryption schemes to protect confidential monitoring information from external threats.
- Develop security assets for automated monitoring of the state of the vehicles and guarantee the confidentiality and integrity of V2X interactions in unreliable V2X environments by means of techniques based on AI/ML to detect/mitigate malicious activity.

4.2.2 Secure V2X edge intelligence with physics-informed learning

Recent advancements in deep learning have revolutionized the way security attacks against V2X systems are detected and mitigated. By leveraging their ability to learn high-level features from data in an incremental manner, deep learning techniques have been pervasively used in cyber-threat detection due to their improved accuracy compared to conventional machine learning. The rapid emergence of deep learning is also dictated by the fact that classical learning-based classification and intrusion detection methods often become inadequate to handle large data volumes induced by the high number of connected vehicles in V2X systems [5]. However, deep neural networks trained from natural or synthesized datasets could encounter challenges concerning stability, reliability, and security, e.g., out-of-distribution problem, and adversarial examples [6]. In addition, deep learning techniques may not work well when unforeseen changes in vehicular scenarios, caused by either naturally drifting traffic mobility patterns or non-anticipated variability in malicious behaviour of attackers, take place.

In this context, integrating physical knowledge in deep learning models can dictate the model to follow the underlying governing laws and guarantee the preciseness. Thus, a promising direction towards enhancing the security of vehicular edge against adversarial attacks, is to exploit the underlying physics of traffic in the learning process, with consistency checks against fundamental physical laws dictated by traffic flow theory. The incorporation of domain knowledge (e.g., traffic density, kinematics laws of motion and vehicle mobility, spatiotemporal correlations) in training would improve model robustness by reducing uncertainty in decision-making, while overcoming the incomplete measurement streams owing to edge deployment limitations. By steering the learning process towards identifying physically consistent or plausible solutions, the detection of highly sophisticated attacks would be possible. However, a major challenge towards integrating the underlying traffic dynamics to control the learning phases in distributed setups lies in devising strategies that increase model robustness to adversarial perturbations without sacrificing its performance (e.g., accuracy), and with no elevated computational cost.

The aforementioned innovation applies to the user story of use case 1 and it is mapped to WP3 activities.

4.2.3 Trustworthy knowledge transfer at the edge in V2X systems

The efficiency and effectiveness of collaborative learning mechanisms highly depend on the available vehicular data, which may not be the same at various edge entities and levels. Across the edge monitoring infrastructure, road-side units can acquire mobility data from neighbouring entities which reside within their communication range. However, such information might be insufficient for detecting accurately events or proactively situations along the vehicular trajectory [5]. Given the delay-sensitive nature of such scenarios, inference methods should be agile enough to perform detection and/or incident response in real-time. This cogently justifies the use of distributed and decentralized

models for rapid event detection with localized training. However, distributed learning solutions may be vulnerable to adversarial attacks. For instance, a malicious edge node may manipulate the local model updates or inject mislabelled training data to compromise the global model. Other adversarial manipulations (e.g., carefully crafted malicious samples altering the data distribution) are also possible.

In such untrusted mobility environments, trustworthy information exchange across the edge monitoring infrastructure (i.e., access points or road-side units) needs to be guaranteed by properly designed knowledge-transfer algorithms. Considering a collaborative transfer learning setup, target edge nodes should progressively learn to select beneficial knowledge for their task (i.e., event detection) only from a selected set of source nodes. At the same time, negative transfer from source nodes subject to adversarial manipulations should be minimized, while such malicious nodes need to be isolated from the transfer learning process. Trustworthy knowledge exchange will consider scenarios of known events and projected situations (i.e., unseen for the target node) as well as partial observability of the environment by the different edge nodes.

The aforementioned innovation applies to the user story of use case 1 and it is mapped to WP3 activities.

4.2.4 End-to-end condition monitoring, failure identification, and visualization for V2X systems

In SUCCESS-6G-DEVISE, an open-source monitoring software solution for V2X predictive diagnostics is expected to be developed. This modular and containerized end-to-end solution will provide actionable insights for the real-time performance of vehicular condition monitoring with the aid of user-friendly customized dashboards. In particular, the key building blocks of the solution will be: i) Generator, a Python script sending rows from the vehicular dataset to a collector using the HTTP POST method, imitating the communication between sensors and the fusion center; ii) Collector, a RESTful application program interface implemented in Python Flask web framework used to authenticate connecting clients and validate received data; iii) Storage, a module including databases and applications for data storage (database and queue) and visualization; iv) Models, a module representing a trained model currently used for classification of events; v) Model builders, a framework for tracking of the model experiments. The solution will also employ highly customized dashboards for knowledge extraction, which support tailored queries and provide a wide range of charting capabilities (e.g., trajectory graphs and trend maps) for analysing and presenting vehicular monitoring information [7] [8]. The solution is currently implemented in Docker containers and will be publicly available on GitHub.

The aforementioned innovation applies to the user story of use case 1 and it is mapped to WP3 and WP4 activities.

4.3 Innovation that applies only to Use Case 2

4.3.1 Location-aware SDN controller and Service Orchestrator

The Location-Aware Software-Defined Networking (SDN) Controller and Service Orchestrator is an innovative solution designed to revolutionize network management and service provisioning in modern data centers and communication infrastructures. This cutting-edge technology seamlessly integrates software-defined networking with intelligent service orchestration capabilities, creating a highly efficient and dynamic network environment.

Some of its key features to be exploited in SUCCESS-6G-DEVISE are:

- Software-Defined Networking (SDN) Integration: The solution incorporates an advanced SDN controller that centralizes the network control plane, enabling administrators to dynamically

manage and configure network resources, policies, and services through a unified, programmable interface.

- Real-Time Location Awareness: One of the defining features of this innovation is its ability to harness real-time location data. By integrating with location-aware devices and sensors, the SDN controller can identify the physical location of connected network devices, end-users, or IoT devices with remarkable precision.
- Geographically Optimized Routing: Leveraging the location information, the SDN controller and service orchestrator can make intelligent routing decisions based on the physical proximity of network elements. This allows for efficient data transmission, reduced latency, and improved overall network performance.
- Dynamic Service Orchestration: The service orchestrator component of this innovation can dynamically provision and manage services based on location and network conditions. It enables automatic scaling of resources, load balancing, and failover mechanisms to ensure optimal service delivery.
- Context-Aware Service Deployment: With location-awareness and real-time data, the SDN controller can intelligently deploy services or allocate resources according to the specific needs of users or devices in different locations. This level of context-awareness enhances the overall user experience and resource utilization.
- Enhanced Network Security: Location-based access control and security policies can be enforced, allowing the SDN controller to detect and respond to potential security threats in a timely manner. Unauthorized access attempts or anomalies in device behaviour can trigger immediate actions to safeguard the network.
- Analytics and Insights: The location-aware SDN controller and service orchestrator also come equipped with powerful analytics tools that provide valuable insights into network performance, user behaviour, and resource utilization. These insights can be leveraged to optimize network design and resource allocation over time.

5 Use case facilities

For the implementation and the validation of SUCCESS-6G-DEVISE innovative solutions, a number of facilities and assets available to the project partners will be employed. A summary of the key use case assets will be described next, whereas a more detailed specification of the use case infrastructure and experimental setups will be produced as the project progresses, and within the scope of WP3, WP4 and WP5 outputs.

5.1 Facilities for both Use Cases

5.1.1 CELLNEX Mobility Lab

The CELLNEX Mobility Lab, located at the Circuit Parcmotor Castellolí near Barcelona (Spain), is a pioneering and innovative test space for the development of ITS technological solutions associated with 5G, sustainable mobility and autonomous vehicles. The circuit has been equipped with C-V2X, 5G and Edge Computing technologies and a private wireless network with coverage throughout the venue.

Furthermore, the Mobility Lab provides a GPS reference station that provides positioning measurements with errors under 5 centimetres, that is mandatory to address driving safety services.

Thus, the CELLNEX Mobility Lab supports the development of future mobility services and infrastructures through the assessment of different trials and Proofs of Concept in a well-controlled field scenario, prior to the deployment on the final mobility scenarios. Smart Connectivity offered in the Mobility Lab makes possible vehicle-to-vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N) and Vehicle-to-People (V2P) communications, setting the scene for future mobility services for vehicles, cities, roads and motorways.

The CELLNEX Mobility Lab is based on green infrastructures, that operate under the premise of efficient energy management and environmental sustainability, since most of them are self-sustainable sites that use eolic and/or solar energy. Besides, future road deployments will follow same premises, as most of the roads are located in isolated areas with few possibilities to connect to the grid power.

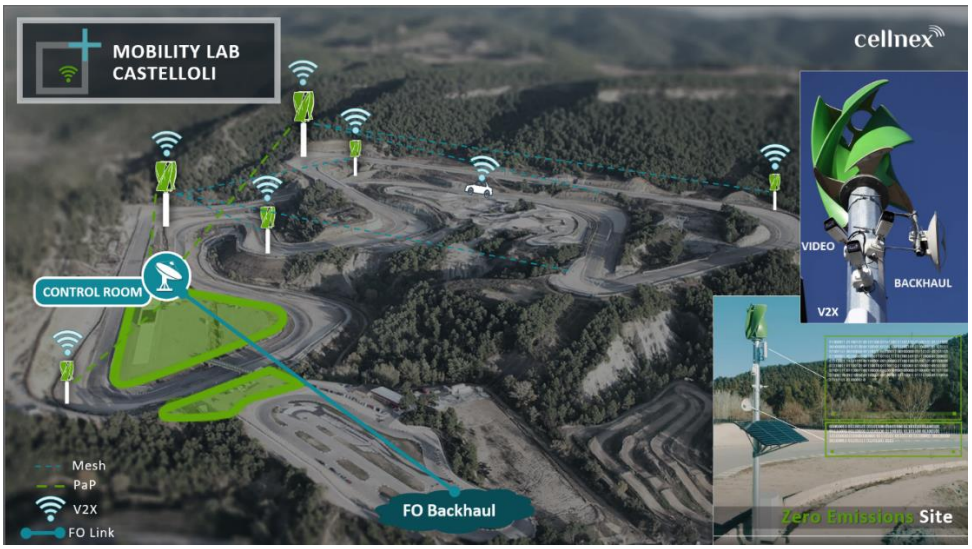


Figure 12: CELLNEX Mobility Lab (Castelloli)

Regarding communication infrastructures, the Cellnex Mobility Lab in Castelloli has a 5G private network which is composed by a 5G SA Core (Druid solution) and several 5G New Radios (Sunwave solution).

All the infrastructure deployed in the Cellnex Mobility Lab in Castelloli is supervised and monitored

from the Cellnex NOC (Network Operation Center), assuring the SLA and an efficient response time to resolve any incident that affects the Mobility Lab reliability.

Main parts of the Connectivity Infrastructure available in the Cellnex Mobility Lab are the "Core" Infrastructure located at the Control Room, and the "Edge" infrastructure located in different site nodes to cover all the circuit.

Thus, the Mobility Lab is composed by:

- 1 Grid Site, connected to the power supply
- 1 Hibrid Node, connected to the power supply and eolic/solar energy
- 7 Green Nodes (Zero Emissions Site), only connected to eolic/solar energy

The Green Sites are linked in a mesh network using mmW Radio Links at 60GHz that offer a bit rate of 1,2Gbps and grant a good performance in terms of capacity and reliability for the access network.

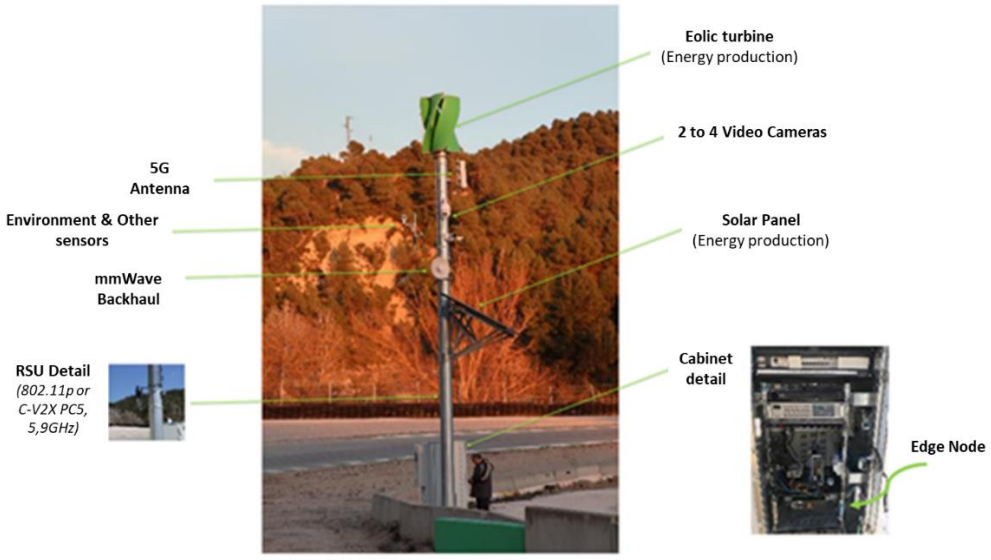


Figure 13: Cellnex Mobiliy Lab - Green Nodes

Green Nodes are self-sustainable, and all the consumed energy is produced by their solar panels and wind turbines. Advanced algorithms for energy management and dashboards for monitoring the energy consumption of each device connected to the node (cameras, UI, servers, etc) are also implemented to enhance the management of this kind of sites. Besides, thanks to the IoT sensors, is possible to monitor environmental and atmospheric parameters, and forecast future conditions using AI tools and the information gathered by the sensors network. If the AI system predicts that the weather conditions aren't good enough to support the energy load of the green node, then the main services are transferred to the Grid Site or the Hybrid one until the energy performance of the Green node can support again all the workload. Thus, the efficient edge infrastructure ensures the continuity of essential services that are provided in the Mobility Lab.

The **Grid Site** and the **Hybrid** one are connected to the power supply system. In addition, these nodes are also connected to the FO network.

The Hybrid node works with eolic & solar energy, which also has an energy storage system to save the surplus energy from the renewable energy sources. Besides, it is complemented with grid power supply in case the energy demand can't be supplied by the green or the stored energy, enhancing the reliability of the site communications infrastructure.

The Grid Site has also a mini-datacenter at its base, that hosts several servers submerged in liquid. This special datacenter can manage services and applications that migrate from the Green Sites to safe energy.

Operation and restrictions

In order to deploy the Use Cases, Cellnex will manage the access to the Mobility Lab and its ICT infrastructure.

The ICT infrastructure could be accessible either locally from the Cellnex Control Room in the Mobility Lab, or in remote by using a VPN connection. Cellnex will coordinate the dates for experiments, since there could be other trials or projects running in the Cellnex Mobility Lab.

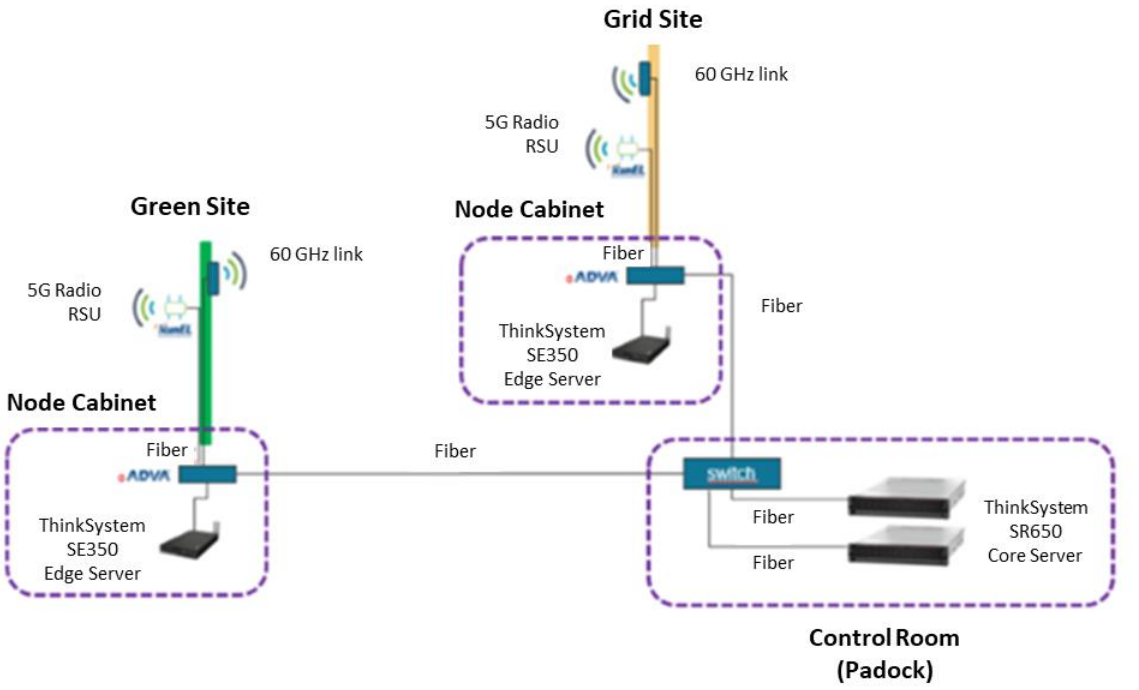


Figure 14: Cellnex Mobility Lab - ICT Architecture

- **Control Room – ICT Infrastructure:**
  The ICT infrastructure hosted in the Control Room is composed by 2 servers, Lenovo ThinkSystem SR650. One server contains the 5G Core SA (Druid solution) and the other contains the MANO (that is the NearByOne solution of Nearby Computing discussed in Section 4).
  The Lenovo ThinkSystem SR650 server provides support for data analytics, hybrid cloud, hyperconverged infrastructure, video surveillance, high performance computing and much more.
  Intel® Optane™ DC Persistent Memory delivers a new, flexible tier of memory designed specifically for data center workloads that offer an unprecedented combination of high capacity, affordability, and persistence. This technology will have a significant impact on real-world data center operations: reduction of restart times from minutes down to seconds, 1.2x virtual machine density, dramatically improved data replication with 14x lower latency and 14x higher IOPS, and greater security for persistent data built into hardware.

- **Node Cabinet – ICT Infrastructure:**
  Each node cabinet hosts one Edge Server, Lenovo ThinkSystem SE350, that will contain the services of the Use Case. These services will run over dockers and containers, that are orchestrated by the NearByOne Edge Orchestrator solution of Nearby Computing, as discussed in Section 4.

Besides, if it is needed to use the racetrack, Cellnex will also manage the required access to run the experiments.

5.1.2 5G Stand Alone mobile network

The 5G Stand Alone mobile network is based on a Raemis™ Druid SW solution, which is a 3GPP compliant 5G core, RestAPI and additional functionality. The Core Solution is complemented with a Sunwave RAN solution for the 5G-NR side.

5G SA Core Solution

The Raemis™ technology platform implements all the 3GPP 5G components and features. It includes a private network with private subscribers, private cell network, mobility Xn handover, unknown subscriber rejection, idle mode cell reselection, UE attachment/implicit detach/re-attach and VoNR calls/data service.

The Raemis™ Druid solution is radio agnostic, simple to use, easy to integrate and easy to scale up & down. It also exposes a powerful RESTful API that enables application developers to build on top of Raemis ™ or integrate external applications with the Raemis ™ platform.

Raemis™ 5G platform supports distributed architectures which can be deployed in cloud native environments with central management of multiple edge sites. The solution is designed to enable advanced demonstration of 5G SA early features, allowing to define, assess and prepare innovative 5G solutions before launching new communication services to the market.

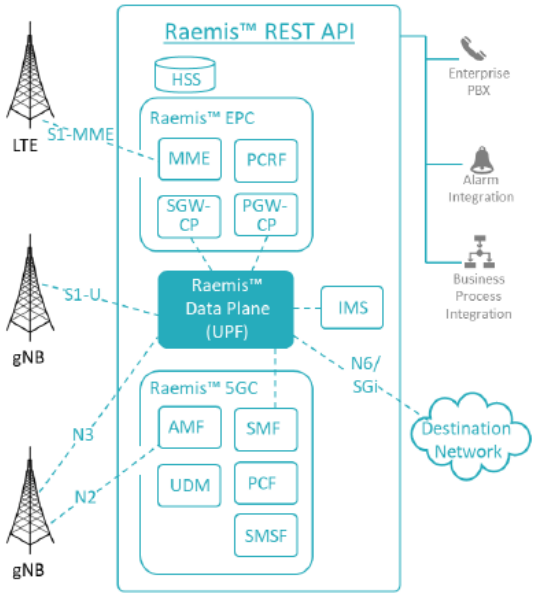


Figure 15: Raemis™ Druid Core Solution - 5G SA Network

Main features of the 5G SA solution are:

- Private Core Network Dashboard
- Enhanced integration with “enterprise LANs”, allowing Enterprise Slicing functionalities
- 5G-SA capabilities and 5G URLLC features
- Location Management Function (LMF)
- 5G Radio Network Slicing: Configuration of Radio QoS and Radio Congestion Control per

network

- Real-time System Monitoring
- 5G-LAN (non-IP) communication between 5G end devices
- Group Management and Network Management
- PBX Integration
- Cells Management with ACS Integration System Management
- Alarm Monitoring, Troubleshooting and Emergency Call
- User Equipment IP address assignment using DHCP
- Up to 20 subscribers (with 20 SIM cards)

The Raemis™ solution supports Security and Traffic separation, Load Balancing and Configurable QoS. The administrator tool can create multiple Packet Data Networks over the same infrastructure. Each PDN logical network can be associated with an enterprise VLAN, setting different performance service parameters for everyone.

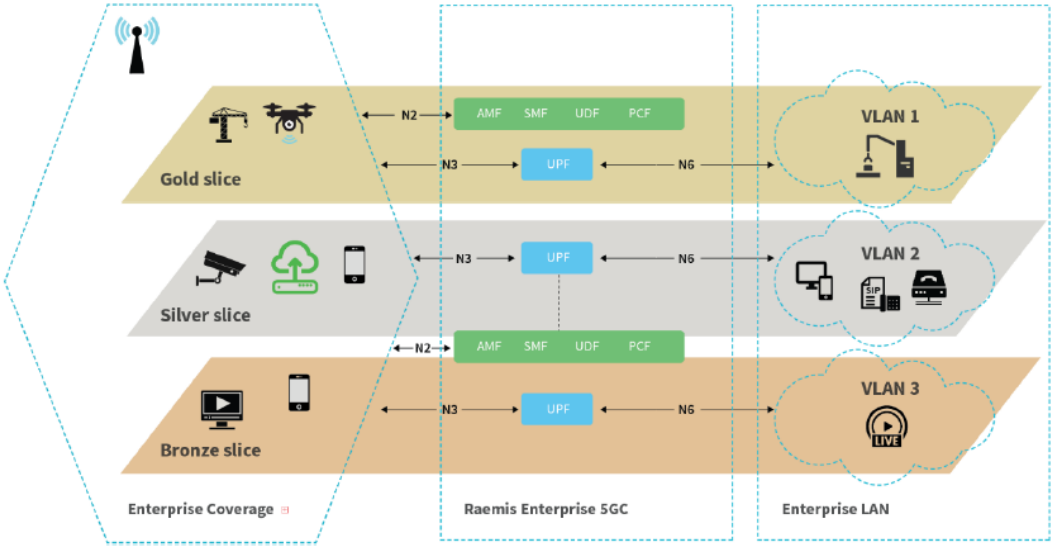


Figure 16: Network Slicing

PDNs enable the following functions:

- Security and Traffic Separation: users can be organised in logical groups and assigned to the PDN that best suited to support the group needs.
- Load balancing: for performance reasons and to avoid traffic bottlenecks, different PDNs can be used to spread the network traffic load across the different “enterprise VLANs”.
- QoS allocation: It is possible to create PDNs that provide different QoS levels on the 3GPP network and easily control user access to those PDNs.

The Dashboard panel provides a comprehensive summary of the overall status of the system. It is the main area for monitoring user activity and system resources. The information updates every five seconds by default. The Dashboard panel has four sections that provide information about:

- User Status.
- Cells Status.
- Network Status.
- Miscellaneous Information.

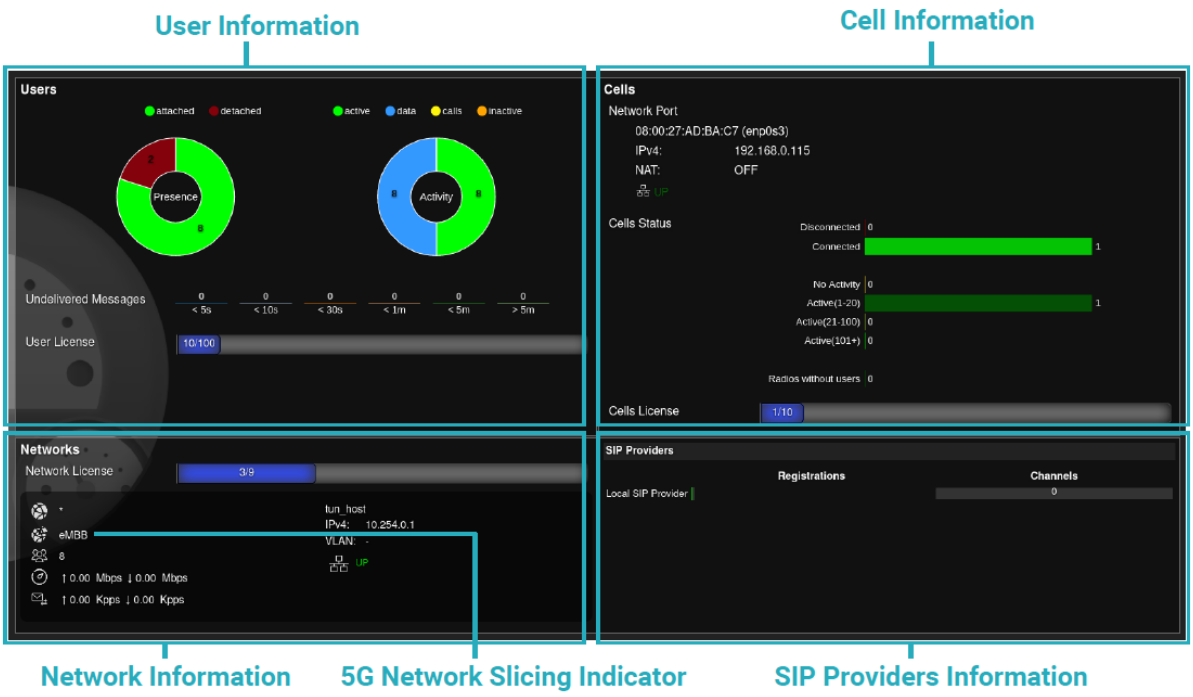


Figure 17: Dashboard panel.

For 5G systems, there is very little difference from 4G systems. 5G subscribers are accounted for in the Users area and 5G cells are accounted for in the Cells area. In addition, there is a 5G Network Slicing indicator in the Network Information area.

The Cells area of the Dashboard provides a summary view of more detailed information presented in the Cells panel.

The availability of service depends on the network connection from Raemis to the radios and whether the radios are operational. The Cells area identifies which network interface services the radios. In simple terms, the IP address of the Mobility Management Engine (MME) configured in the radios must match the IP address of the network device shown in this panel.

If the network is UP, the cell status shows the number of eNodeB devices connected.

The Radios without Users indicator can highlight possible issues with the radios. For example, a radio with no users, may indicate:

- A normal situation because the system does not expect users in the area at a particular time of day.
- An under-used radio device providing coverage in an area that is not frequently used.
- An issue with a radio that is not transmitting or that UEs cannot see.

5G-NR solution

The Cellnex Mobililty Lab in Castelloli has a Sunwave solution for the 5G-NR side, with distributed BBU and RRU.

The **BBU nCELL-T5000** is used to realize 5G NR base station processing unit, centrally control and manage the entire base station system, realize direct access and data interaction with 5G core network, realize NGAP, XnAP interface, and realize 5G NR access network protocol stack function, RRC, PDCP, SDAP, RLC, MAC and PHY protocol layer functions, baseband processing functions.

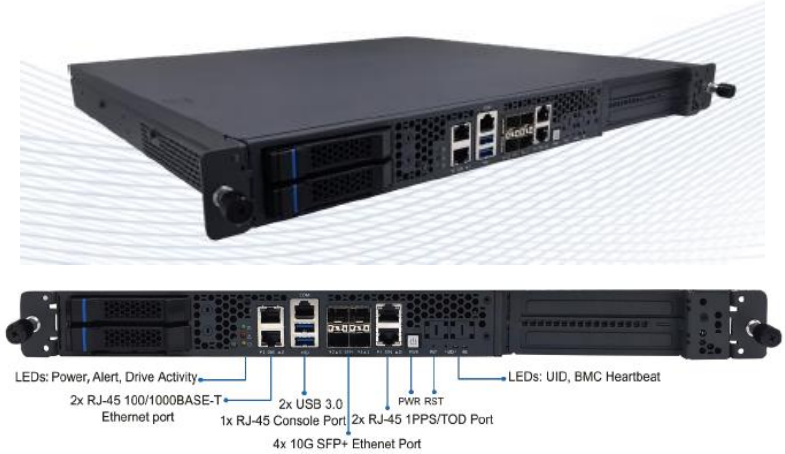


Figure 18: 5G-NR Sunwave BBU - nCELL-T5000

Main functional features are:

- Standard 3GPP Rel.15
- Server platform Xeon D-2177NT Processor
- Maximum number of cells: 4
- Maximum number of carriers: 1
- Carrier bandwidth: 100 MHz
- Subcarrier spacing: 30KHz
- Number of active users: up to 400 users
- Downlink peak rate: 1,5 Gbps
- Uplink peak rate: 260Mbps
- Max number of data streams: 4 DL / 2 UL
- Number of concurrently scheduled users: 4 users / slot
- Duplex mode: TDD, FDD
- BS spatial layers: 4
- UE spatial layers: 2
- Fronthaul bandwidth: 10G

The BBU unit is complemented with a FGAF Acceleration Card that uses Xilinx's Zynq Ultra Scale+ MPSOC and Kintex Ultra Scale+ FPGA to realize the functions of baseband processing acceleration and data forwarding, and meets the application requirements of high bandwidth, low latency and multi-cell deployment required by the 5G BBU system. Very high integration and ease of use. This card is a single-slot, full-height half-length (FHHL) card, using PCIeGen3x16 interface (supports bifurcation into two sets of Gen3x8 interfaces) to connect to the system, and externally supports 4 SFP+ optical ports. The card is equipped with a high-precision clock source and clock phase-lock circuit, supports external 1588V2 and GPS input, and can provide stable clock synchronization services to the next-level network node through the SFP+ fronthaul interface.

The **RRU RU4370** is a digital transport platform supporting cellular technologies on fibre optic cable using the CPRI protocol. The power amplifier technology adopts DPD (Digital Pre-Distortion), allowing for a significant improvement in power consumption compared with analogue technology.

Figure 19: 5G-NR Sunwave RRU - RU4370

Main features of this component are:

- 5G NR compliant
- Supports 4T4R digital radios
- Up to 5W (37dBm) Output Power and up to 100MHz IBW
- Supports cascading
- Supports Sub-6GHz TDD and External Alarm
- Digital bandwidth per channel (DL & UL): 20/40/50/60/80/100 MHz
- Band Frequency: 3500 MHz (UL & DL Freq: 3800-4100)
- 3GPP band: N77
- Complies with 3GPP TS36.106, 3GPP TS25.106

5.1.3 Mobile Edge Computing infrastructure

Main components of the Mobile Edge Computing infrastructure are the Lenovo ThinkSystem SE350 Edge Servers, located at every Cabinet node.

These servers will manage the dockerized services and containers of the Use Case, which are orchestrated by the NearByOne Edge Orchestrator solution of NearbyComputing, as discussed in Section 4.

The Service Docker will provide the V2X services of each use case, and the Core Docker will manage the different containers for the network communication services like VDU, vCU-CP, vCU-UP, etc.

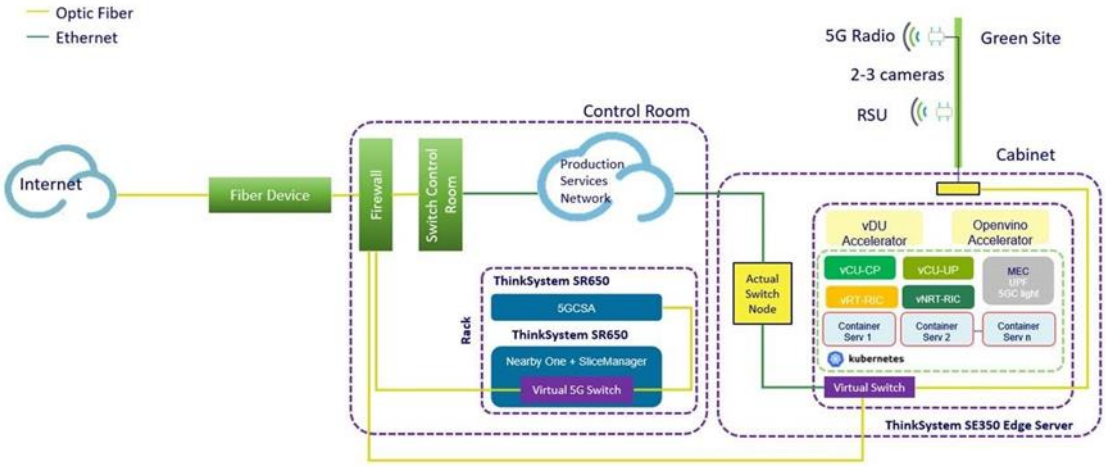


Figure 20: Cellnex Mobility Lab - ICT Infrastructure

The ThinkSystem SE350 is an Intel® Xeon® D processor-based server, with a 1U height, half width and short depth case that can go anywhere. Mount it on a wall, stack it on a shelf or install it in a rack. This rugged Edge server can handle anything from 0-55°C as well as full performance in high dust and vibration environments.

The ThinkSystem SE350 is designed and built with the unique requirements for Edge servers in mind, it is versatile enough to stretch the limitations of server locations, providing a variety of connectivity and security options and easily managed with Lenovo XClarity Controller. The ThinkSystem SE350 is a rugged compact-sized Edge solution with a focus on smart connectivity, business security, and manageability for the harsh environment.

5.1.4 MEC orchestrator and MEC platform

The MEC Orchestration is based on NearbyOne, an orchestration solution developed by Nearby Computing. NearbyOne provides a zero-touch orchestration framework for lifecycle management of application and edge resources. This includes the use of AI algorithms with the objective of providing closed-loop autonomy and zero-touch reconfiguration at all layers of the edge infrastructure. The MEC platform is a cloud-native platform (e.g., a Kubernetes cluster) to host network functions and MEC applications or V2X services.

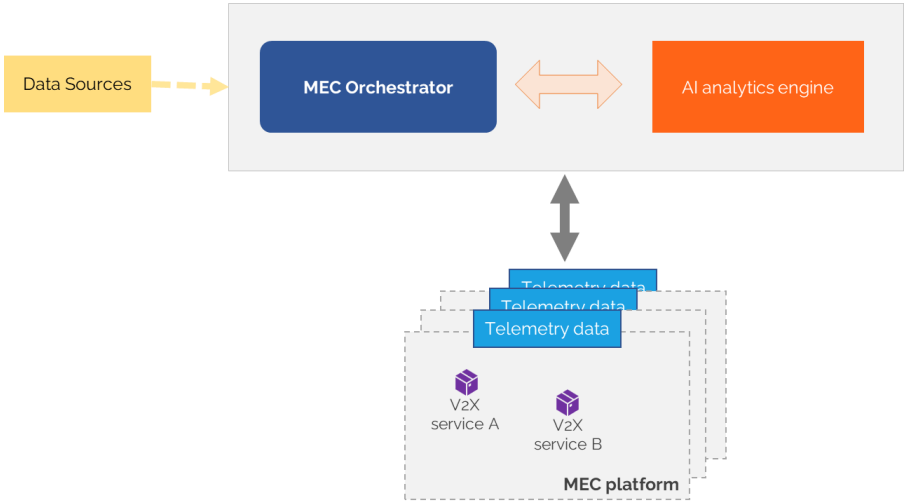


Figure 21: MEC orchestrator and MEC platform.

The main elements considered in this layer are shown in Figure 25 and detailed below:

- The **MEC orchestrator**, guided by the AI/optimization analytics, executes decisions pertaining to application placement or migration within the edge infrastructure.
- The **AI analytics engine** module analyses the collected telemetry data (and/or any other source of relevant data) and provide decisions or suggestions to the orchestrator.
- The **MEC platform(s)** (edge nodes), are the geographically distributed computing resources, where the applications are deployed. As an example, each edge node can consist of a Kubernetes cluster.
- The **data sources** are the custom target QoS/QoE objectives of the AI analytics engine and the MEC orchestrator.
- The **telemetry data**, including various live metrics of interest from the platform and applications, which may encompass factors such as energy availability, latency, or end-user location, among others.
- The **V2X services** are the end-user orchestrated MEC applications (vehicular condition monitoring services).

5.1.5 C-V2X infrastructure

Main components of the C-V2X infrastructure deployed in the Cellnex Mobility Lab in Castelloli are the RSU (Road Side Units) devices, based on the Lacroix Neavia V2I Stations or similar.

Figure 22: C-V2X RSU

Neavia v2i Station is the V2X solution for connected roads and autonomous vehicle applications. Neavia v2i station operates on 5.8 / 5.9GHz bands according to US or European standards (WAVE 1609 / EN 302 571). The unit is designed to ensure permanent and rugged use along the roads, while ensuring technological scalability. A wide range of interfaces is available to communicate with sensors for advanced vehicle perception and existing traffic lights. The embedded software includes a Web HMI and API, as well as all application/communication stacks required to communicate with the vehicles and the traffic management centres. It is compliant with C-ITS corridors, providing 802.11p DSRC and C-V2X PC5 communication.

5.1.6 C-V2X OBU

The C-V2X OBU based on two latest generation modules specifically designed to address the latest advancements in C-V2X systems within the 5G NR environment, specifically Release 15.

The first module is a Network Access Device (NAD), specifically the Quectel AG550. This module is one of the first Automotive Grade Compliant modules with 5G NR Sub-6 GHz capabilities, supporting both Stand Alone (SA) and Non-Stand Alone (NSA) modes. Adopting 3GPP Release 15 technology, the module supports a maximum download speed of 2.4 Gbps and an upload speed of 550 Mbps (in NSA mode). It is compatible with previous 3GPP releases, including 4G LTE-A. It supports C-V2X PC5 for direct vehicle-to-infrastructure communications.

The second main module is the Application Processor (AP), which has a high-speed connection to the NAD. It is the Quectel AG215 module, an automotive-grade AP specifically designed for C-V2X vehicle communications.

Regarding the GNSS module which is embedded within the NAD AG550. This GNSS module is capable of processing signals from GPS, GLONASS, BEIDou, Galileo, and QZSS constellations. It operates in the L1/L2/L5 frequency bands. Additionally, the modem ensures compatibility with previous technologies such as GSM, UMTS, and LTE-A.

The main characteristics of the OBU (Vmax) which will be deployed in the vehicles are:

- NAD (Network Access Device) module 5G NR (New Radio) 3GPP Release 15
  - C-V2X Sidelink (PC5 Mode 4) features
  - Frequency Range 1 (FR1)
  - Uplink and Downlink greater than 500 Mbps
  - Degree of automotive
- AP (Application Processor) C-V2X module + Hardware Security Module (HSM)
  - 1.4 GHz Dual-Core Cortex-A53
  - LPDDR2 512 MByte
  - Flash 512 MByte (available 190MB) for SO
  - External flash eMMC 8GByte as expansion capacity
  - Signing of C-V2X messages to be sent using an associated HSM
  - Internal HSM to the AP module (ECDSA) up to 2500TPS through CPU
  - External HSM to the AP module
- GNSS positioning receiver
  - Multi-constellation and multiband.
  - Update rate greater than or equal to 10 Hz.
  - Supported input and/or output formats: NMEA1803, RTCM2, RTCM3, or equivalent.
  - RTK and Dead Reckoning functionalities
- Power management and intrusion detection microcontroller
  - Low power consumption
  - Active during system "sleep" mode
  - With backup battery
  - Firmware erasure system in case of intrusion
- CAN and Ethernet communication ports for communication with other vehicle systems
- Critical communication lines on the printed circuit board
  - Identification and routing of critical lines on internal layers
  - Identification of access points and definition of elimination or contingency procedures in case of commercial hardware versions.
- Mechanical characteristics:
  - 166 x 101 mm (without connectors and fixing points).
  - Sealing grade: IP52
  - Thermal strategy: Conductions through metallic bracket and air convection

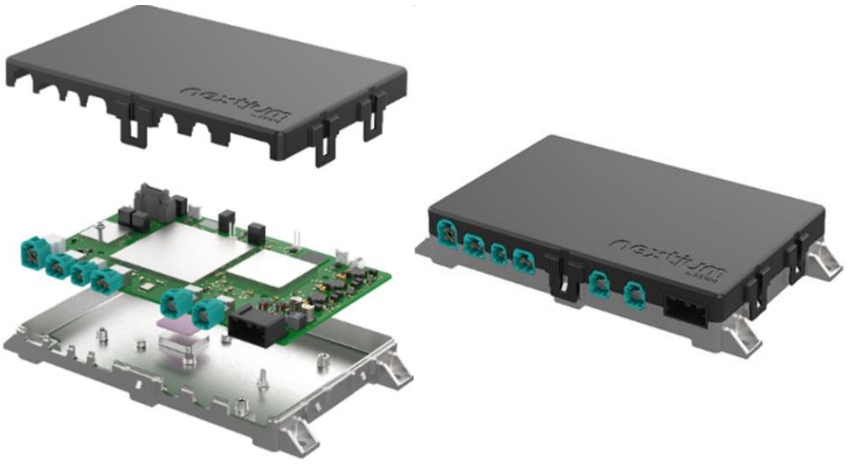


Figure 23: C-V2X OBU for a vehicular predictive maintenance service.

5.2 Facilities for Use Case 1

5.2.1 SUPERCOM platform

The Sustainable and High-Performance Computing (SUPERCOM) platform[5] is owned and maintained by the Sustainable Artificial Intelligence (SAI) research unit at CTTC and comprises central, edge and on-device computing engines, SUPERCOM is controlled via ad hoc-designed software for multiple data-processing and mining tools, spanning from real data collection and generation, data cleaning, pre-processing and visualization to model building, results analysis, and informed decision-making. The different innovations developed in the context of SUCCESS-6G-DEVISE.

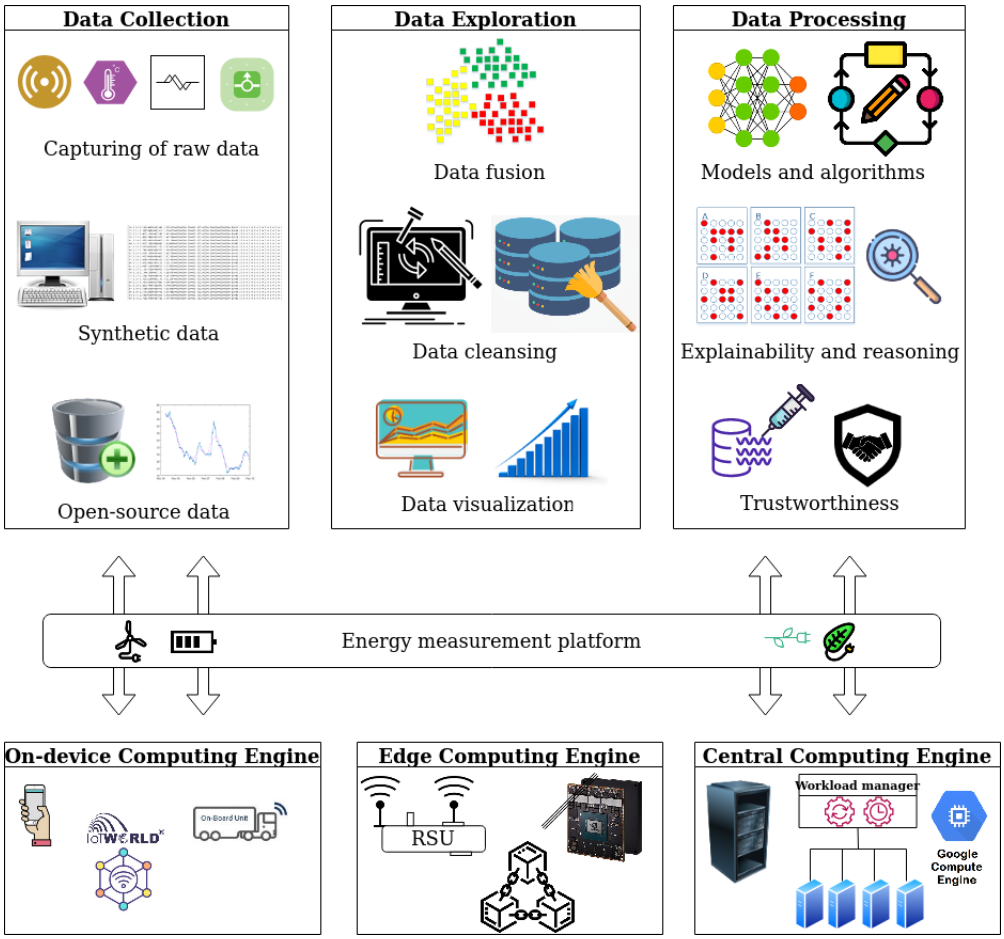


Figure 24: Building blocks of SUPERCOM platform.

Figure 28 demonstrates the key building blocks of SUPERCOM.

5.3 Facilities for Use Case 2

5.3.1 ADRENALINE Testbed

The ADRENALINE testbed® is an open and disaggregated SDN/NFV-enabled packet/optical transport network and edge/cloud computing infrastructure for Beyond 5G, 6G and IoT/V2X services. It embraces several network segments such as access, metro, and core. The key elements include (1)

[5] https:// supercom.cttc.es/

SDN-enabled partially disaggregated optical network. It is composed of: i) 1 photonic (flexi-grid DWDM) mesh network (PMN) with 4 nodes (2 ROADMs & 2 OXCs) and 5 bidirectional DWDM amplified optical links up to 150 km (overall 600 km of optical fibre); ii) a Spatial Division Multiplexing (SDM) domain formed by 2 Spatial Cross Connect devices (SXCs) connected by a 19-core 25Km multi core fibre (MCF); iii) a pair of packet optical nodes with optical pluggable transponders providing aggregated 400G data rates for transporting traffic flows between the access and the core network segments; iv) heterogeneous access network technologies are connected to the metro infrastructure such as IP Cell Site Gateways (CSGs) equipped with Edge DC capacities, a Passive Optical Network (PON) tree formed by disaggregated Optical Network Terminals (ONTs) offering connectivity to several Customer Premises Equipment (CPEs), and a pool of (OpenFlow-based) packet switches domain deployed on COTS and using Open vSwitch (OvS) for the network connectivity needed by several Edge/Core DC nodes; v) optical metro nodes are also connected to programmable SDN-enabled Sliceable Bandwidth Variable Transponders (S-BVTs) to transmit multiple flows at variable data rate/reach up to 1 Tb/s.

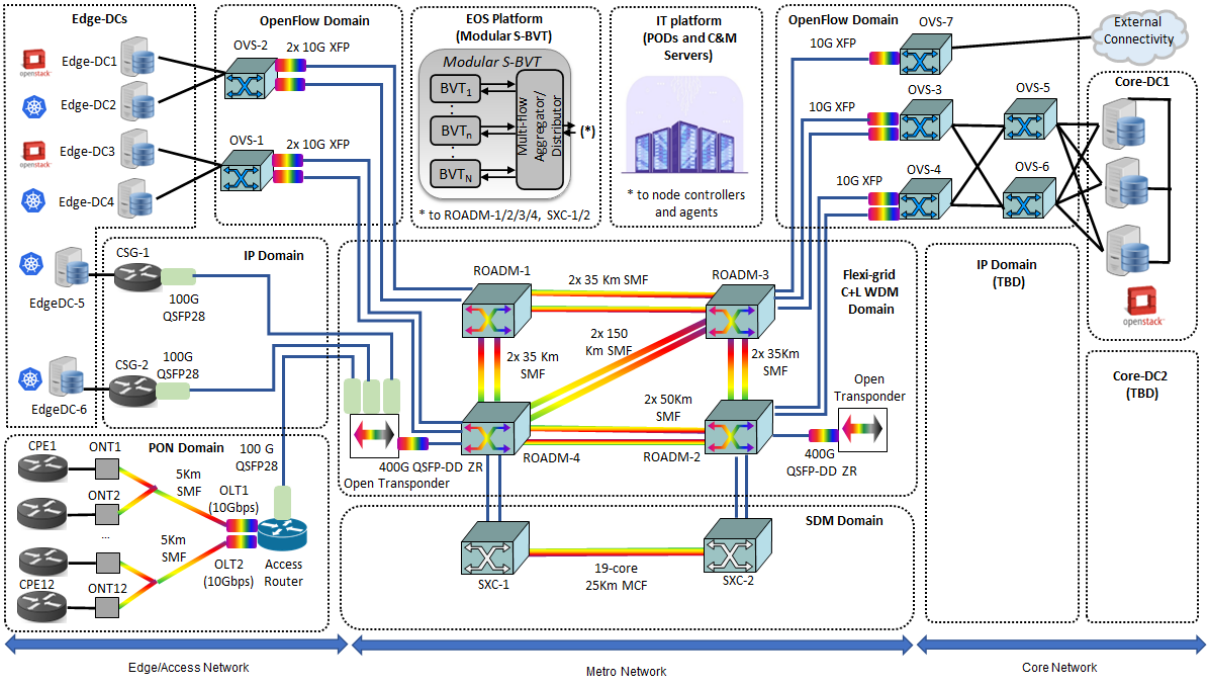


Figure 25: CTTC Adrenaline Testbed

The different domains access (i.e., PON, IP CSGs, OpenFlow) and metro (i.e., Flexi-grid DWDM and SDM) are managed by dedicated orchestrators/controllers (e.g., Optical Line System SDN controller or OpenDayLight) to automatically handle the connectivity services entailing the de-/allocation of heterogeneous network resources (i.e., packet and optical devices). Those domain-specific controllers and orchestrators are coordinated hierarchically by implementing the ETSI TeraFlowSDN controller. The TeraFlowSDN controller exposes a NorthBound Interface to allow an external system (e.g., NFV service platform) to request network connectivity services. This NFV service platform orchestrates the transport (optical/packet) and computing (edge/cloud) resources: i) Multi-VIM (virtualized infrastructure managers) combining OpenStack and K8s controllers for virtual machines and containers; ii) TeraFlowSDN controller for end-to-end connectivity among virtual machines, containers, and end-points. The NFV service platform is also in charge of managing the life-cycle of NFV network services and network slices: i) an NFV network service is composed of chained VNFs or cloud-native network functions (CNFs) deployed on VM and/or containers; ii) a network slice is composed of one or several concatenated NFV network services that deploy a set of VNFs and/or CNFs.

6 Key performance indicators

For the implementation of the SUCCESS-6G-DEVISE innovations, the project defines specific key performance indicators (KPIs). The considered use cases revolve around real-time monitoring of vehicles and software updates for vehicles. To ensure the successful realization of these use cases with the deployment of a 5G SA private network at Circuit ParcMotor with two 5G radios, the KPIs are defined towards achieving a high-quality 5G network and comprehensive 5G coverage. This involves guaranteeing reliable and stable connectivity throughout the designated area.

Additionally, the applications running on the edge of the network need to meet high-performance standards. This includes low latency, high bandwidth, and seamless data transfer to support the real-time monitoring and software updates. Such requirements emphasize the need for a robust and efficient 5G infrastructure that can deliver reliable connectivity and support the demanding applications running on the network's edge.

6.1 User story: Vehicular condition monitoring with security guarantees

KPI	Definition	Unit	Relevant SUCCESS-6G enabler
Number and frequency of failures	Number and occurrence of the anomalies in the vehicular equipment operation.	Absolute number	-End-to-end condition monitoring, failure identification, and visualization for V2X systems -Data analytics for informed decision-making regarding the vehicles condition status -C-V2X OBU
Remaining useful lifetime (RUL)	The time duration a monitored component is likely to operate before it requires repair or replacement. By taking RUL into account, maintenance can be scheduled, operating efficiency can be optimized, and unplanned downtime can be avoided.	Time	End-to-end condition monitoring, failure identification, and visualization for V2X systems
Downtime	Defined as the time duration during which the vehicular component's working conditions are affected by a failure which results in a faulty operation.	Time	-End-to-end condition monitoring, failure identification, and visualization for V2X systems -C-V2X OBU
Maintenance response time	Defined as the time elapsed from the detection of the failure until the equipment works properly again.	Time	End-to-end condition monitoring, failure identification, and visualization for V2X systems

Reliability	The reliability rate for C-V2X message delivery is typically 99%, ensuring that critical messages are successfully transmitted.	%	C-V2X OBU
Unauthorized access	The OBU should implement robust security measures to ensure secure communication and protect against unauthorized access.	%	C-V2X OBU
Accuracy	Accuracy is defined as the ratio of all correct predictions (i.e., true positives and true negatives) to the total number of considered input samples.	%	- Trustworthy knowledge transfer at the edge in V2X systems - Secure V2X edge intelligence with physics-informed learning
Precision	Precision is defined as the ratio of true positives to the number of true positives plus the number of false positives.	%	- Trustworthy knowledge transfer at the edge in V2X systems - Secure V2X edge intelligence with physics-informed learning
Recall	Recall is defined as the ratio of true positives to the number of true positives plus the number of false negatives.	%	- Trustworthy knowledge transfer at the edge in V2X systems - Secure V2X edge intelligence with physics-informed learning
F1-score	F1-score is defined as the harmonic mean between precision and recall metrics.	%	- Trustworthy knowledge transfer at the edge in V2X systems - Secure V2X edge intelligence with physics-informed learning
Mean Time to Detect (MTTD)	MTTD is defined as the average time elapsed between the time the security incident takes place and its discovery by the applied detection algorithm	Milliseconds/ seconds	Trustworthy knowledge transfer at the edge in V2X systems
Mean Time to Resolve (MTTR)	MTTR is defined as the average time elapsed between the time the security incident is detected and the enforcement of the mitigation action.	Milliseconds/ seconds	Trustworthy knowledge transfer at the edge in V2X systems

Table 3: KPIs for user story of use case 1.

6.2 User story: Over-the-air vehicular software updates with security guarantees

KPI	Definition	Unit	Relevant SUCCESS-6G enabler
Update Success Rate	This KPI measures the percentage of vehicles that successfully receive and apply the over-the-air software updates while maintaining security guarantees. It reflects the reliability and effectiveness of the update process in delivering secure updates.	%	-Location-aware SDN controller and Service Orchestrator -C-V2X OBU
Security Vulnerabilities Discovered	This metric tracks the number of security vulnerabilities discovered in the software updates. A low number indicates a robust and secure update process.	# incidents	-Location-aware SDN controller and Service Orchestrator -C-V2X OBU
Update Completion Time	This KPI tracks the average time taken for a vehicle to download and apply the software update securely. A shorter completion time indicates a more efficient and timely update process.	seconds	-Location-aware SDN controller and Service Orchestrator -C-V2X OBU
Secure Communication Rate	This metric evaluates the percentage of secure communications established during the update process. It ensures that updates are delivered securely between the update server and the vehicles.	%	-Location-aware SDN controller and Service Orchestrator -C-V2X OBU
Integrity Verification Success Rate	This KPI measures the percentage of vehicles that successfully verify the integrity of the received update before installation. High integrity verification success indicates that updates have not been tampered with during transit.	%	-Location-aware SDN controller and Service Orchestrator -C-V2X OBU
Authentication Success Rate	This metric tracks the percentage of vehicles that successfully authenticate the source of the software update. It ensures that updates are received only from trusted sources.	%	-Location-aware SDN controller and Service Orchestrator -C-V2X OBU
Security Incident Response Time	This KPI measures the time taken to respond to and address any security incidents or breaches that may occur during or after the update process. A prompt response minimizes potential risks and	seconds	Location-aware SDN controller and Service Orchestrator

	damages.		

Table 4: KPIs for user story of use case 2.

6.3 5G network relevant KPIs

The KPIs that affect a network can vary depending on the context and specific objectives of the network. However, the following tables summarize some common KPIs that are relevant for evaluating the performance and efficiency of a network regarding the defined use cases.

- KPIs can be extracted from the core:

KPI	**Category**	**Definition**	**Unit**
Number of seconds this system has been running	SYSTEM STATUS	raemis_kpi_raemis	Hours, minutes, seconds
max_attached users permitted	SYSTEM STATUS	raemis_kpi_raemis	Number
Max attached radios permitted	SYSTEM STATUS	raemis_kpi_raemis	Number
Number of attached Radios	RADIOS	raemis_kpi_ran	Number
Number of active radios (more than 1 user attached)	RADIOS	raemis_kpi_ran	Number
number of paging failures – Since the last poll	RADIOS	raemis_kpi_ran	Number
Number of attached Users	USERS	raemis_kpi_subscribers	Number
Number of Active Users (not idle mode)	USERS	raemis_kpi_subscribers	Number
average CPU usage for PS	CPU USAGE	raemis_kpi_system_dp_load	%
Current UL bits per second on S1-U/N3	TROUGHPUT	raemis_kpi_dp_throughput	Mbps
Current DL bits per second on S1-U/N3	TROUGHPUT	raemis_kpi_dp_throughput	Mbps
Current UL bits per second on Sgi/N6	TROUGHPUT	raemis_kpi_dp_throughput	Mbps
Current DL bits per second on Sgi/N6	TROUGHPUT	raemis_kpi_dp_throughput	Mbps
Control Plane Latency	LATENCY	raemis_kpi_monitor	ms
User Plane Latency	LATENCY	raemis_kpi_monitor	ms
Event Latency	LATENCY	raemis_kpi_monitor	ms

Table 5: Network KPIs that can be extracted from the core.

- KPIs can be extracted from the final user (e2e):

KPI	Definition	Unit	Expected performance range
Uptime	Measures the amount of time the network is available and functioning properly. High uptime is an indicator of a stable and reliable network.	%	
Latency	The time it takes for a data packet to travel from its source to its destination. Low latency is crucial for ensuring fast and smooth communication on the network.	ms	Node 8 min/avg/max [20-35ms] [25-40ms] [40-65ms] Node 1 min/avg/max [9-20ms] [10-30ms] [50-65ms]
Bandwidth	Measures the amount of data that can be transmitted through the network in a given period of time. Adequate bandwidth is essential for supporting traffic load and avoiding bottlenecks.	Hz	Max 100Mhz
DL (downlink) throughput **- Very good radio conditions** **- Good radio conditions** **- Medium radio conditions**	Indicates the speed at which data can be downloaded across the network. High throughput is important for efficient communication and a smooth user experience.	Mbps	Node 8 [60Mbps-80Mbps] Node 1 [300Mbps-400Mbps]
UL (uplink) throughput **- Very good radio conditions** **- Good radio conditions** **- Medium radio conditions**	Indicates the speed at which data can be sent across the network. High throughput is important for efficient communication and a smooth user experience.	Mbps	Node 8 [5Mbps-8Mbps] Node 1 [140Mbps-150Mbps]
Reliability	Measures the likelihood that the network operates without errors or interruptions. A reliable network minimizes downtime and ensures constant connectivity.	%	
Communication	Communication range is the maximum distance	Meters/	

range	between a transmitter and its intended receiver allowing communication with a targeted packet size, latency, and reliability, and for a given effective transmit power and receiver sensitivity.	Kilometres	
RSRQ	Reference Signal Received Quality: Quality considering also RSSI and the number of used Resource Blocks (N) RSRQ = (N * RSRP) / RSSI measured over the same bandwidth. RSRQ is a C/I type of measurement, and it indicates the quality of the received reference signal. The RSRQ measurement provides additional information when RSRP is not sufficient to make a reliable handover or cell reselection decision.	dB	
RSRP	Reference Signal Received Power: RSRP is a RSSI type of measurement, as follows there are some definitions of it and some details as well. It is the power of the LTE Reference Signals spread over the full bandwidth and narrowband. A minimum of -20 dB SINR (of the S-Synch channel) is needed to detect RSRP/RSRQ	dB	
SNR	Compares the level of a desired signal to the level of background noise	dB	
Signal Strength	Signal strength	dB	

Table 6: Network KPIs that can be extracted from the final user (e2e)

7 Conclusions

This deliverable focuses on the elaboration of the vehicular use cases that will be targeted by SUCCESS-6G-DEVISE project and presents the initial set of innovations that will be developed by project partners to address the technical challenges associated with these use cases. Each SUCCESS-6G-DEVISE use case has been elaborated around a user story, which describes, among others, the involved actors, their roles, main event flows and service requirements.

The SUCCESS-6G-DEVISE technical innovations focus on various beyond-5G advancements and cover diverse aspects of the use cases, including enhancements to the 5G architecture to support V2X services. Notably, the key role of AI is highlighted in several technical assets to be developed by partners. Data-driven intelligence will be leveraged to improve multiple aspects of the system performance. In addition, MEC is expected to play a crucial role in providing infrastructure and orchestrating MEC platforms. For the implementation and validation of the SUCCESS-6G-DEVISE innovative solutions in the context of the use cases, the project partners will make use of both real-environment and lab facilities, depending on the envisioned technology readiness level for each innovation. Finally, an initial set of service level requirements and key performance indicators have been defined for each user story.

8 References

[1] C. Kalalas and J. Alonso-Zarate, “Sensor data reconstruction in industrial environments with cellular connectivity,” in 2020 IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (IEEE PIMRC ’20), August 2020.

[2] L. Li, J. McCann, N. S. Pollard, and C. Faloutsos, “Dynammo: Mining and summarization of coevolving sequences with missing values,” in Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ser. KDD ’09. New York, NY, USA: Association for Computing Machinery, 2009, p. 507–516. [Online]. Available: https://doi.org/10.1145/1557019.1557078

[3] N. Srebro and T. Jaakkola, “Weighted low-rank approximations,” in Proceedings of the Twentieth International Conference on International Conference on Machine Learning, ser. ICML’03. AAAI Press, 2003, p. 720–727.

[4] S. L. Brunton and J. N. Kutz, Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control. Cambridge University Press, 2019.

[5] R. Sedar, C. Kalalas, F. Vázquez-Gallego, L. Alonso and J. Alonso-Zarate, "A Comprehensive Survey of V2X Cybersecurity Mechanisms and Future Research Paths," in IEEE Open Journal of the Communications Society, vol. 4, pp. 325-391, January 2023, doi: 10.1109/OJCOMS.2023.3239115.

[6] R. Sedar, C. Kalalas, F. Vazquez-Gallego, J. Alonso-Zarate, “Reinforcement Learning Based Misbehaviour Detection in Vehicular Networks," in Proc. of IEEE International Conference on Communications 2022 (IEEE ICC ’22), Seoul, South Korea, May 2022.

[7] P. Mulinka, C. Kalalas, M. Dzaferagic, I. Macaluso, D. Gutierrez-Rojas, P. Nardelli, and N. Marchetti, “Information Processing and Data Visualization in Networked Industrial Systems," in Proc. of IEEE International Symposium on Personal, Indoor and Mobile Radio Communications 2021 (IEEE PIMRC ’21), virtual conference, September 2021.

[8] P. Mulinka, S. Sahoo, C. Kalalas, P. Nardelli, “Optimizing a Digital Twin for Fault Diagnosis in Grid Connected Inverters - A Bayesian Approach", in Proc. of IEEE Energy Conversion Congress and Exposition 2022 (IEEE ECCE ’22), Detroit, Michigan, USA, October 2022.

[end of document]