Reflections and findings from the WI VRU-DEMO experience and lessons learned

5GAA Automotive Association
Technical Report

CONTACT INFORMATION:
Executive Manager – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:
5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

VERSION:	0.1
DATE OF PUBLICATION:	24 April 2024
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes/No
DATE OF APPROVAL BY 5GAA BOARD:	22 July 2024

Contents

Introduction

The Work Item (WI) VRU-DEMO was developed following two previous 5GAA WIs on the topic of Vulnerable Road Users (VRUs). The aim of this WI was to build on previous work in 5GAA on the topic of VRUs and focus on co-existence and interoperability between different companies' solutions. Previous showcases and demonstrations have shown the functionality and safety benefits of VRU protection solutions, whereas the objective of VRU-DEMO is to show how these solutions are able to interact with each other.

1 Scope

The present document has been conceived to produce a Technical Report (TR) on the WI VRU-DEMO. Starting with the discussions on the System Architecture, the TR explains the intricated process of putting the different system components (e.g., application servers, intra-MEC connectivity, interchange functionality, etc.) together and developing interfaces for a matching user experience. The process of selecting the right use cases is described in its entirety.

The TR aims to comprehensively document the key aspects and outcomes of the VRU-DEMO WI, a breakthrough initiative conducted in cooperation between 5GAA member companies. The VRU-DEMO project primarily focuses on showcasing the interoperability of various network-based VRU protection services and applications, thereby contributing to the advancement and implementation of C-V2X for safety-enhancing scenarios. The TR starts with a section dedicated to the System Architecture by delineating the comprehensive version that was employed for the real-life demonstrations that took place at M-City, University of Michigan, USA. It provides an in-depth analysis of the technical framework, including hardware, software, and network components, which facilitated the seamless integration and functioning of network-based VRU protection services and applications. Next, the report outlines the rigorous process involved in the selection of use cases. It elucidates the criteria used for use case prioritisation, detailing the rationale behind the chosen scenarios that effectively demonstrate the capabilities and interoperability of network-based VRU protection services and applications. An essential aspect of the TR is the detailed analysis of the measured performance and Key Performance Indicators (KPIs) using evaluation instruments during both the trial phase and the live showcases. The chapter sheds light on the specific metrics used to evaluate the efficiency, reliability, and effectiveness of the network-based VRU protection services and applications, thereby providing valuable insights into the project's evaluation results.

The TR includes a comprehensive section dedicated to discussing the key lessons learned during the implementation of the VRU-DEMO project. It emphasises the challenges encountered, the strategies adopted to overcome them, and the valuable insights gained throughout the project lifecycle, thus providing crucial recommendations and best practices for similar future endeavours. The segment on the message type standardisation offers a detailed exploration of the considerations and recommendations for standardising message types for VRU protection. It emphasises the importance of establishing uniform protocols and message formats to ensure seamless communication and interoperability among different VRU protection services and applications, fostering a cohesive and efficient operational environment.

Through this comprehensive delineation of the project's key components and outcomes, the TR aims to offer an insightful and informative resource for industry professionals, researchers, and stakeholders invested in the evolution and advancement of C-V2X technology and its implications for network-based VRU protection services and applications.

2 References

[1]	5GAA, (2020) White Paper: Vulnerable Road User Protection. Retrieved from: https://5gaa.org/content/uploads/2020/08/5GAA_XW3200034_White_Paper_Vulnerable-Road-User-Protection.pdf
[2]	5GAA, (2023) Technical Report: Accelerate the understanding and adoption of VRU protection services enabled by C-V2X. Retrieved from: https://5gaa.org/content/uploads/2023/02/5gaa-p-220057-accelerate-the-understanding-and-adoption-of-vru-protection-services-enabled-by-c-v2x.pdf
[3]	SAE,(2023) J2735: V2X Communications Message Set Dictionary
[4]	SAE,(2023) J3224: V2X Sensor-Sharing for Cooperative & Automated Driving

3 Definitions, Abbreviations and Participating Companies

3.1 Definitions

For the purposes of the present document, the following definitions apply:

Alert: Information requiring the increased attention of the driver or in-vehicle assistance systems giving time for an adaptation of speed, change of lane, or even re-route.

Awareness: Information to the driver anticipating an area of interest along the route.

Intervention: Actuation of the active safety systems leading to a notable change of speed or direction. This may avoid an impact at the last moment or reduce the gravity of an impact.

Safety-critical: Situations that demand immediate action to prevent accidents or collisions. In these scenarios, the driver's response time is critical, and the vehicle may also autonomously take evasive or corrective actions (e.g., sudden lane change, or unexpected pedestrian crossing the road).

Safety-enhancing: Situations involving the provision of additional information and situational awareness to the driver, in order to improve their driving decisions and overall road safety. This information allows drivers to make informed choices on traffic safety.

Warning: Information to the driver or in-vehicle assistance systems requiring a rapid change of vehicle dynamics such as speed or lane change.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AS	Application Server
API	Application Programming Interface
BSM	Basic Safety Message
CSP	Communication Service Provider
C-V2X	Cellular Vehicle-to-Everything
DL	Downlink Latency

E2E	End-to-End
GW	Gateway
GW RSU	Gateway RSU
I2N	Infrastructure-to-Network
IPX	Internetwork Packet Exchange
IOO	Infrastructure Owner/Operator
ITS	Intelligent Transportation System
MEC	Multi-access Edge Computing
MNO	Mobile Network Operator
MSO	Multi Service Operator
MQTT	Message Queuing Telemetry Transport
NTP	Network Time Protocol
OBU	On-Board Unit
PC5	Direct Communication
PKI	Public Key Infrastructure
PSM	Personal Safety Message
RF	Radio Freuqncy
RO	Road Operator
RSU	Road-Side Unit
SAE	Society of Automotive Engineers
SDSM	Sensor Data Sharing Message
SP	Service Provider
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TIM	Traveller Information Message
V2X	Vehicle-to-Everything
V2N2X	Vehicle-to-Network-to-Everything
VRU	Vulnerable Road Users, defined as: a non-motorist with a Fatality Analysis Reporting System (FARS) person attribute code for pedestrian, bicyclist, other cyclist, and person on personal conveyance or an injured person that is, or is equivalent to, a pedestrian or pedal-cyclist as defined in the ANSI D16.1-2007. (See 23 U.S.C. 148(a)(15) and 23 CFR 490.205). VRU may include people walking, biking, or rolling. VRUs can also include a highway worker on foot in a work-zone, given they are considered a pedestrian and it does not include a motorcyclist Source.
VRU-DEMO system	The setup used in the VRU-DEMO Work Item and subsequently used during the 5GAA Detroit demonstration in October 2023
UI	User Interface
Uu	Network-based Communication
UL	Uplink Latency
UX	User Experience
WI	Work Item

3.3 Participating Companies:

Digital Twin Provider#1: Anritsu

Digital Twin Provider#2: Keysight

MEC Platform Provider#1: Verizon

MEC Platform Provider#2: T-Mobile

Service Provider#1: LGE

Service Provider#2: Commsignia

Connectivity Provider#1: Verizon

Connectivity Provider#2: T-Mobile

Inter-change Provider: Commsignia

IOO Application Service Provider: Commsignia

4 System Architecture

In this section, the comprehensive system architecture of the VRU-DEMO system is presented by comprising various components and interfaces that contributed to its functionality. The system architecture in the VRU-DEMO trial followed the principles of a previous MEC4Auto WI [1] (reference). One of the main objectives of the VRU-DEMO was to reflect all relevant complexities when using a Vehicle-to-Network-to-Everything (V2N2X) data-sharing architecture in conjunction with the operation of V2X applications on a Multi-access Edge Computing (MEC). The primary reason for using the MEC as a computing environment was the sensitivity of the VRU use cases regarding latency between V2X sender (vehicle, VRU, traffic infrastructure) and V2X receiver (vehicle, VRU).

The following are the relevant complexities related to a MEC operation:

- V2X mobile users (vehicles, VRUs, special purpose vehicles, e.g., emergency vehicles) are subscribed to different mobile network operators if they are using public mobile networks for data transmission;
- MEC is operated in different operational setups, dependent on the decisions and strategies of the respective Mobile Network Operator (MNO);
- V2X mobile users use different Service Providers to receive V2X data and to provide a V2X service. This is organised by a service subscription between the user and the Service Provider. Service Providers can be the car OEM or a Service Provider which specifically provides the V2X service or in conjunction with other services (e.g. navigation, traffic jam notifications, speed camera alerts etc.);
- Traffic infrastructure sending and receiving data is connected by an IOO/Road Operator, either by fixed or mobile networks.

[1] https://5gaa.org/moving-toward-federated-mec-demos-trials/

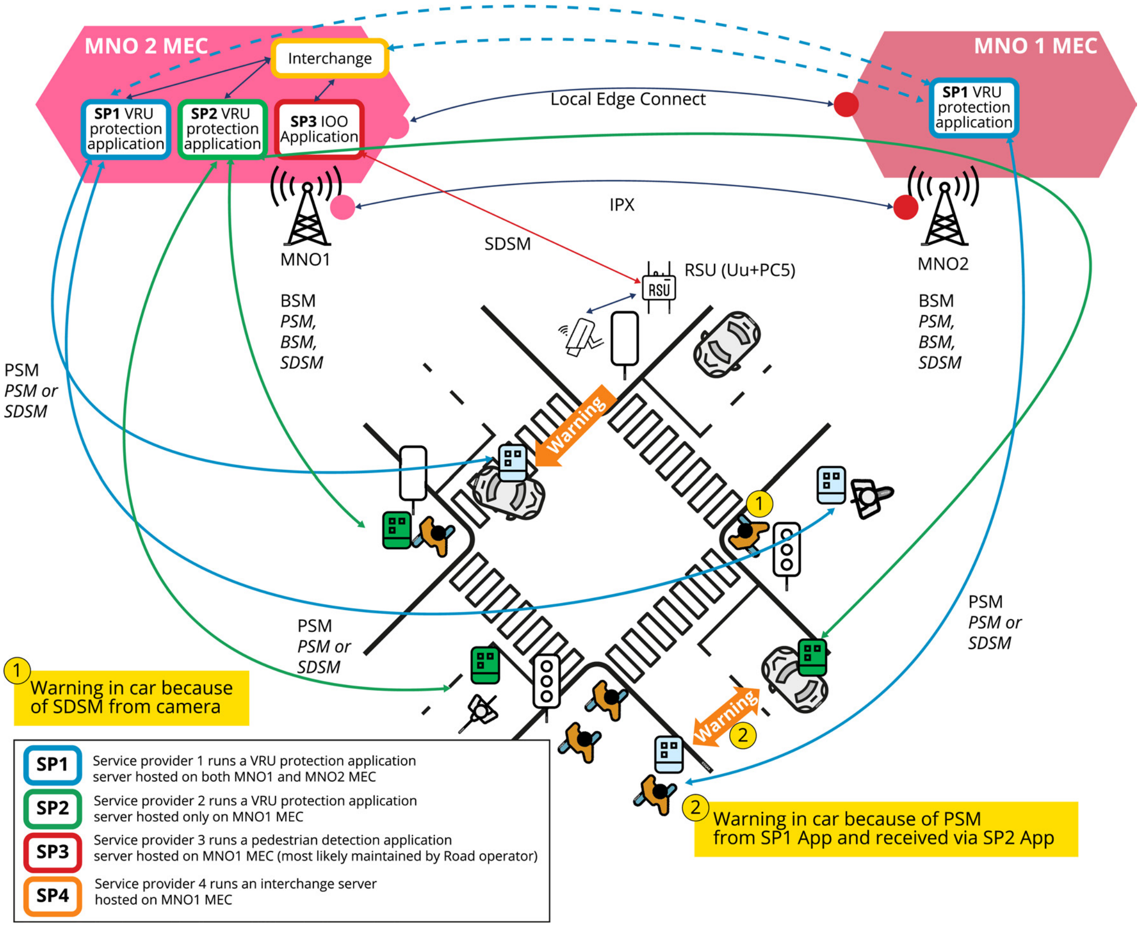


Figure 1: General System Setup

- The setup of the VRU-DEMO system is shown in Figure 1: Two Mobile Network Operators participated in the VRU-DEMO: MNO#1 and MNO#2.
  - MEC of MNO#1 was operated on *AWS Wavelength* attached to a MNO#1 MSO located in Detroit, MI. AWS Wavelength enables developers to build ultra-low latency applications. Wavelength deploys standard AWS compute and storage services to the edge of Communications Service Providers' (CSP) 5G networks.
  - MEC of MNO#2 was operated in *AWS Local Zones*, which are smaller versions of AWS Regions designed to provide low-latency access to AWS services in a Multitenant/Public Cloud setup. AWS Local Zone offers infrastructure deployment that brings services closer to large populations, industries, and IT centres. MNO#2 has chosen the Chicago Local Zone for the demo, as it was one of the closest available options for the Detroit demo.
- A local edge connect link based on internet connection was established to directly route all traffic between the MECs. In parallel, a standard Internetwork Packet Exchange (IPX) connection was used to route network traffic from user devices to the service in case the user is subscribed to a

service not operated in the respective MEC (see Figure 2).

- Two V2X Service Providers, SP#1 and SP#2, operated their applications in the MEC. Two different setups were used: a dual operation of the V2X application in both MECs (chosen by SP#1), and a single-mode operation only in one MEC (chosen by SP#2). The local edge connect link was used to route all data traffic between the applications operating in a dual mode.
- One road operator service application provided by SP#2 is able to provide V2X messages from a traffic infrastructure (camera: SDSMs).
- Two major classes of VRU alert applications were demonstrated: a) in-vehicle alerts generated by the camera in the form of SDSMs, and b) in-vehicle alerts in the form of PSMs from the VRUs. These alerts are sent by either application/Service Provider#1, or application/Service Provider#2, dependent on the service subscription.
- The following alerts were demonstrated to notify the driver about 'road works' and 'emergency vehicle behind' scenarios:
  a) Road Work Alert: The driver is alerted when the vehicle is approaching a work zone and a Traveller Information Message (TIM) with work zone information is received by the vehicle.
  b) Police Car Behind: The driver is alerted when the vehicle receives BSM message with emergency vehicle alert.
- To demonstrate efficient data distribution and sharing between the various data/Service Providers, an interchange service provided by SP#2 was integrated. Both Service Providers and the IOO data provider (also provided by SP#2) were interconnected via the interchange service.

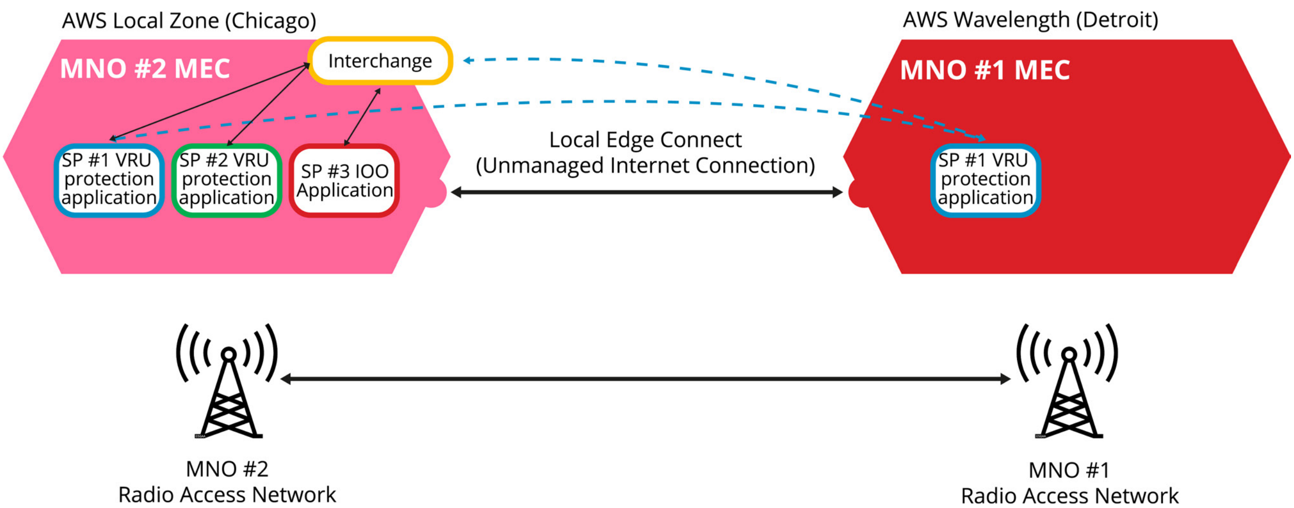


Figure 2: Local Edge Connect and Mobile Network Operator Interconnect

The Inter-server Bridges shown in Figure 3 were deployed by SP#1, a protocol-specific setup to establish Inter MNO-MEC connection. The Service Bridge uses the Message

Queuing Telemetry Transport (MQTT) protocol to initiate a Transmission Control Protocol (TCP) session from AWS Wavelength (MNO#1 MEC) towards the AWS Local Zone (MNO#2 MEC) to establish bi-directional communication so that services running on both operator's MECs can be synchronised.

Figure 3 shows an integrated view of VRU-DEMO MEC application components and interfaces.

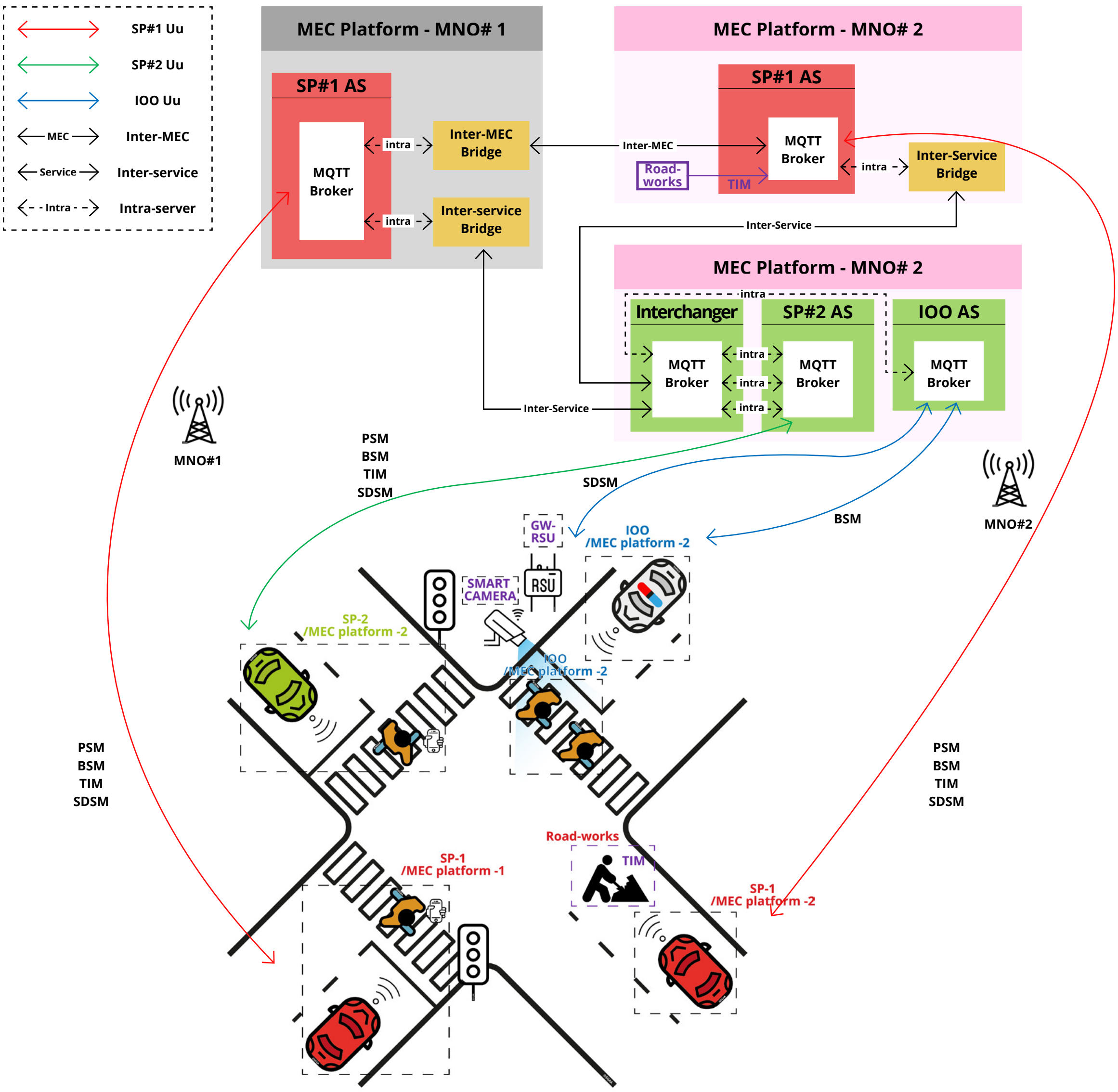


Figure 3: System Architecture of VRU-DEMO System

The System Architecture of the VRU-DEMO system includes the following key elements:

- Consistent User Experience between different VRU Protection Service Providers via Standard ITS Messages (SAE J2735[3], J3224[4]).
- Standard Message Compatibility between different Service Providers: The system ensures smooth compatibility of ITS standard messages between

two Service Providers, allowing seamless data communication even across different Service Provider applications, as well across different MEC Platforms belonging to different Mobile Network Operators.

- Interconnected MEC Deployment between different MEC Platforms: It facilitates connectivity between distinct MEC Platforms, enabling low-latency operation and scalability of VRU protection services and applications.
- Scalability Enhancer and Data Collector, Interchange: An important component in the VRU-DEMO system, enhancing system scalability and flexibility. It connects IOOs and ASs, enabling seamless data exchange.
- Backend Architecture connecting ASs using MQTT Protocol: The VRU-DEMO system establishes a Backend Architecture that seamlessly connects application servers supporting data exchange and communication.

4.1 Interfaces

In this section, a more detailed description of the interfaces and their use in the VRU-DEMO system is provided:

- MEC Access Interface#1 – Hosting SP#1 Applications: The SP#1 Uu interface serves as a connection point for the Service Provider#1 Application using the MQTT Protocol with both MEC Platforms. Through this interface, the MQTT Clients can publish messages to the MQTT broker in response to road events. Also, the MQTT Clients are able to subscribe to receive messages from MEC Platforms via the MQTT Broker.
- MEC Access Interface#2 – Hosting SP#2 Applications: The SP#2 Uu interface serves as a connection point for the SP#2 Application using the MQTT Protocol with MEC Platform#2. Through this interface, the MQTT clients can publish messages to the MQTT Broker in response to road events. Also, the MQTT Clients are able to subscribe to receive messages from MEC Platforms via the MQTT Broker.
- MEC Access Interface#3 – Hosting IOO Apps Inter-MEC Interface: It connects app servers of the same Service Provider over an unmanaged network, enabling data exchange between different platform-hosted app servers.
- Inter-Service Interface: It enables service interoperability between different service entities by connecting with the interchange over unmanaged network.
- Intra-Server Interface: It refers to an interface that connects and enables different interactions between various components or modules within a single MEC Platform. The Intra-Server Interface connects Inter-Bridges and the MQTT brokers, which are compatible with the existing MQTT protocol interaction.
- Interchange Configuration:
  - Messaging protocol: The MQTTv5 protocol was utilised to send V2X

messages between clients and their corresponding SP Application Servers, as well as between Application Servers and the Interchange. To guarantee security and give choices for authentication and authorisation, self-signed certificates were used to allow additional Secure Socket Layer (SSL) security (certificates from a Public Key Infrastructure, PKI, should be used for a non-demo implementation).

4.2 Components

In this section, a more detailed description of the components and their use in the VRU-DEMO system is provided:

- MEC Platform Providers : MEC Platform#1 was AWS Wavelength Zone (MNO 1) and MEC Platform#2 was AWS Local Zone (MNO 2).
- Road Users: These included VRUs equipped with SP applications installed on smartphones and vehicles equipped with SP applications installed on smartphones or Onboard Units (OBU). These shared location and status updates based on standard ITS messages via the SP applications, which are connected to the MEC Platforms. This component performs a role in the VRU-DEMO system by supporting seamless and safe interactions among road users.
- VRU App (VRU End-User App): An application installed on a handheld device (e.g., smartphone) that functions as a software component which transmits and receives V2X messages when linked to the SP AS. This component could employ a type of visual interface to provide the user with information about other entities. It is capable of receiving notifications and alerts to inform the user of impending occurrences, such as potentially hazardous circumstances. Standard Personal Safety Messages (PSM) were broadcast by the implemented apps using network communication.
- Road Works: This component referred to a simulated construction/ maintenance site on a road that potentially impacts road usage and safety. The road works produced TIMs and transmitted the safety messages to the SPs.
- On-Board Unit: It is located in a vehicle, which has the ability to transmit and receive V2X messages over the SP AS, as well as directly between other OBUs. It may receive alerts and messages from the SP AS in addition to implementing safety applications. This component can have a visual interface that notifies the driver of impending alerts and notifications. Using the 5G Uu interface, the OBUs utilised in the demonstration exchanged standard BSMs with an SP AS.
- Connectivity Gateway (GW) RSU: It is equipment that supports the connectivity between Application Servers and the smart roadside infrastructure e.g., collecting information from smart sensors/cameras, and forward the extracted data feed from these to the IOO AS residing in the cloud or MEC. During the demonstration, a GW RSU was used to implement

the Connectivity Gateway functionality and uplink data via Infrastructure-to-Network (I2N) to the IOO AS to further distribute ITS messages via the interchange function, or directly to the SPs.

- Smart Camera: It produces SDSMs and is connected to the RSU to transmit SDSM data to IOO AS.
- SP AS: As described above, in the VRU-DEMO system two SPs provided VRU safety services, SP#1 and SP#2. There are two main objectives of the SP (V2X) AS. First, it sends and receives V2X messages to and from subscribers within the same domain, which might include either customers of the same SP or users of other SPs. Second, depending on pre-configured circumstances and data encoded in the V2X messages, the SP AS can implement logic that digests the traffic of V2X messages and generates alerts/notifications to subscribing entities (e.g., vehicles, smartphone applications). These V2X communications may originate from an IOO AS, another SP AS, or any other V2X-capable entity (such as a car or pedestrian using an app). Either MEC-based or cloud-based SP ASs are possible.
- IOO AS: Serves as the system's entry point to the IOO's data sources. A V2X AS or Interchange receives raw or processed perception data from various types of sensors, such as traffic cameras, which are connected to the IOO AS. The IOO AS then applies logic to generate the appropriate V2X messages depending on pre-configured circumstances and parameters. Either MEC-based or cloud-based IOO ASs are possible. Based on the smart camera feed, the RSU sent SDSMs to the implemented IOO AS. Via the Interchange, the received SDSMs were sent to further SP AS instances. The IOO AS received data from smart traffic infrastructure, in this case smart camera, to provide ITS data to other road users.
- MQTT Broker: It facilitates communication between road users, such as vehicles and VRUs, by managing message queues and topic subscription.
- MQTT Client: Implemented in service applications used by road users.
- Interchange (information-sharing entity): The Interchange is a component that enables the compatibility between different Service Providers who are early adopters of V2X AS technology. It transfers V2X communications across several V2X AS instances, effectively acting as a message hub. The Service Providers running these instances might be the same or different. Additional functionality that the Service Providers use, such as message translation/conversion between various message formats and encodings, may be implemented by the Interchange. It was possible to access the implemented Interchange entity over the MQTT Protocol.
- Inter-MEC Bridge: The Inter-MEC Bridge is a component deployed to connect different MEC Platforms hosting app servers of the same Service Provider. Compliant with the MQTT Protocol interaction, this bridge enables the connection of MQTT Brokers across different MEC Platforms through symmetric MQTT clients. The inter-MEC bridge is designed to establish TCP sessions between MQTT Brokers, enabling them to perform 'Publish and Subscribe' operations for real-time data exchange and MEC interoperability.

- Inter-service Bridge: A component deployed to connect app servers (SP#2, IOO) of different service entities through the Interchange. Compliant with the MQTT Protocol interaction, this bridge enables the connection of MQTT Brokers across different MEC Platforms through symmetric MQTT Clients. The Inter-service Bridge is designed to establish TCP sessions between MQTT Brokers enabling them to perform 'Publish and Subscribe' operations for real-time data exchange and service interoperability.

5 Use Case Selection

5.1 Explanation of Rationale Behind Use Case Prioritisation

For this demo, the use cases were selected based on the criteria for which mutual presence awareness already significantly enhances traffic safety. Mutual presence awareness can be achieved with awareness notifications which have the intention to raise and guide driver awareness towards a potentially dangerous situation, leaving enough time to assess the situation and react accordingly in a safe way. These notifications do not have the intention to trigger a strong and immediate driver reaction.

Among the participants of VRU DEMO, there was a consensus that mutual presence awareness can be realised through both cellular communication (Uu) and direct communication technologies like PC5. Therefore, the choice of the use cases with a focus on Uu-enabled ‘safety-enhancing’ notifications fits well with the other focus of the demo, which was to demonstrate the interoperability of Uu-based approaches of different MNOs and Service Providers.

As shown below, Figure 4 summarises different kinds of notifications (to the driver) in the different phases prior to a potential collision. As a reference, the definitions of the different kind of notifications are added.

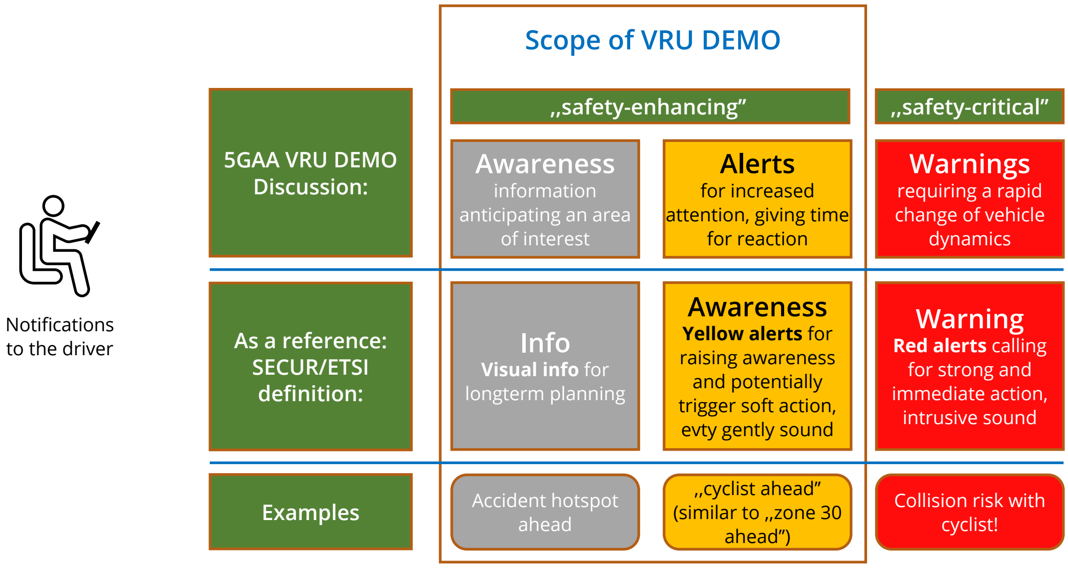


Figure 4: Different Driver Notifications and Definitions.

Note: The figure describes different kinds of driver notifications prior to a potential collision, with definitions used in the VRU-DEMO WI, and in the scope of this TR (topmost row). As a reference, it also contains the definitions used in SECUR/ETSI (center row).

5.2 Overview of VRU-DEMO Scenarios

In this section, an overview of VRU-DEMO Scenarios is provided, including the overall scenario that was demonstrated during the project. The VRU-DEMO involved the demonstration vehicles operating Uu-based Application, each subscribed to different MNOs and seamlessly connected to the AS hosted on the MEC platforms provided by respective MNOs. The Service Providers operating the Uu-based Application, along with MNOs managing the MEC Platform, validated the commercial viability of VRU protection services and demonstrated interoperability through VRU-DEMO. This validation extended to Inter-MEC and Inter-Service interactions, showcasing the potential for seamless integration and functionality.

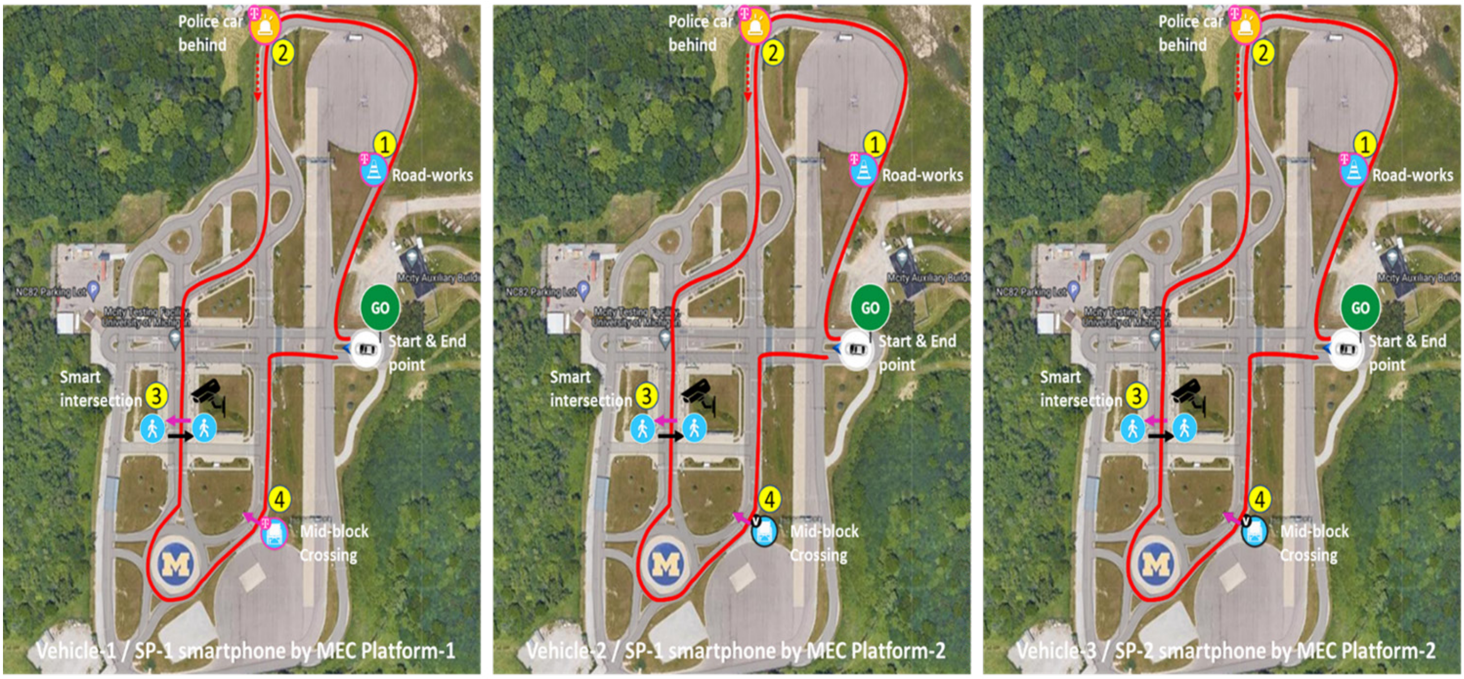


Figure 5: VRU-DEMO Event Loops

Note: Figure 5 illustrates the combinations between three vehicles and respective MNOs operating Uu Application.

- Vehicle#1 – SP 1 / Uu Application / MEC Platform#1 network
- Vehicle#2 – SP 1 / Uu Application / MEC Platform#2 network
- Vehicle#3 – SP 2 / Uu Application / MEC Platform#2 network

The primary objective of the design for each loop is to enable interoperability and interfacing between two MEC Platforms, allowing seamless communication between the two operators' services, regardless of the MEC Platform from which SAE messages are received. Additionally, the various events were selected to demonstrate the scalability and efficiency of Interchange through a range of communication sequence scenarios. The events within each loop have been arranged as follows:

Table 1: Set-up of Events by Demonstration Vehicle Loop

Number of vehicle (Loop)	Event 1, Actors (Which MEC Platform is coming from)	Event 2, Actors (Which MEC Platform is coming from)	Event 3, Actors (Which MEC Platform is coming from)	Event 4, Actors (Which MEC Platform is coming from)
Vehicle#1	Road-works / Worksite (MEC Platform#2)	Police Car behind / Police Car (MEC Platform#2)	Smart intersection / Two Pedestrians (MEC Platform#1,#2)	Mid-block Crossing / Wheelchair User (MEC Platform#2) See note
Vehicle#2	Road-works / Work-site (MEC Platform#2)	Police Car behind / Police Car (MEC Platform#2)	Smart intersection / Two Pedestrians (MEC Platform#1,#2)	Mid-block Crossing / Wheelchair User (MEC Platform#1) See note
Vehicle#3	Road-works / Worksite (MEC Platform#2)	Police Car behind / Police Car (MEC Platform#2)	Smart intersection / Two Pedestrians (MEC Platform#1,#2)	Mid-block Crossing / Wheelchair User (MEC Platform#1)
NOTE: The use cases are events related to E2E KPI measurements. The average latency in reaching MQTT Clients of VRU deployed on a different MEC Platform from MQTT Clients of vehicle was measured. For detailed information, please refer to Section 6.				

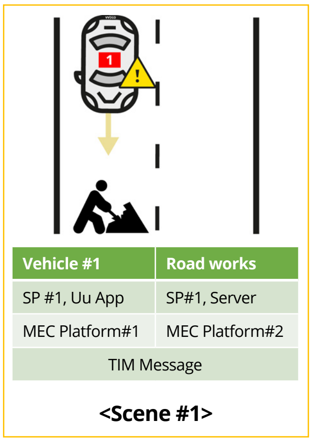
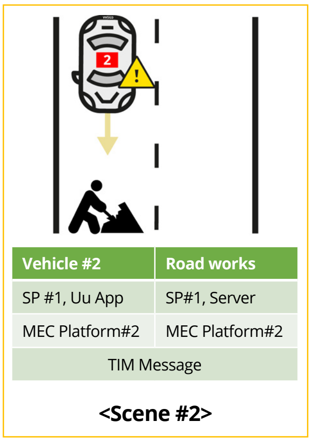
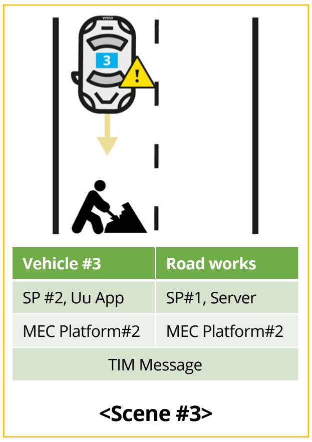
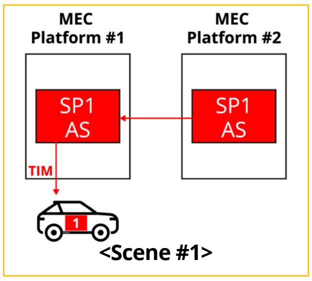
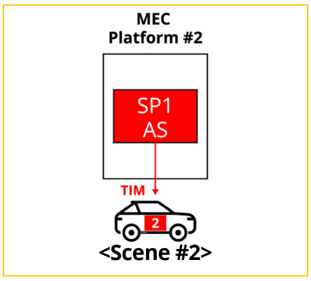
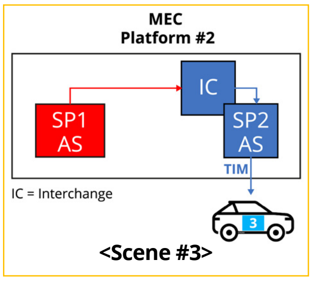
The storylines of Vehicle#1 and Vehicle#2 are designed to demonstrate Inter-MEC interactions between identical application providers deployed on different MEC Platforms. On the other hand, the storyline of Vehicle#3 is designed to prove Inter-Service interactions between different application providers deployed on different MEC Platforms.

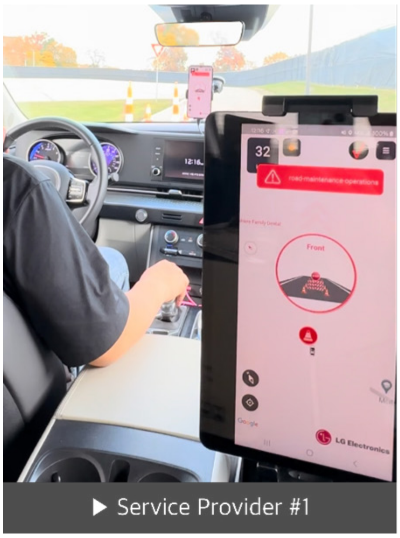
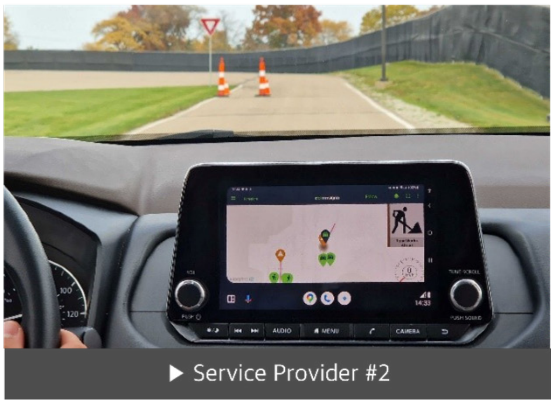
- Vehicle#1, SP1 app, which is being operated by MEC Platform#1, receives and processes SAE messages from the Infrastructure Owner Operator server linked to Interchange, as well as SAE messages from VRU app, which is being operated by MEC Platform#2.
- Vehicle#2, SP1 app, which is being operated by MEC Platform#2, receives and processes SAE messages from the Infrastructure Owner Operator server linked to Interchange, as well as SAE messages from VRU app, which is being operated by MEC Platform#1.
- Vehicle#3, SP2 app, which is being operated by MEC Platform#2, receives and processes SAE messages from the Infrastructure Owner Operator server linked to Interchange, as well as SAE messages from VRU app, which is being operated by MEC Platform#2.

Each vehicle and VRU application executes algorithms based on event-triggering information and provides appropriate alerts to drivers and pedestrians through user interfaces.

5.3 Use Case Descriptions

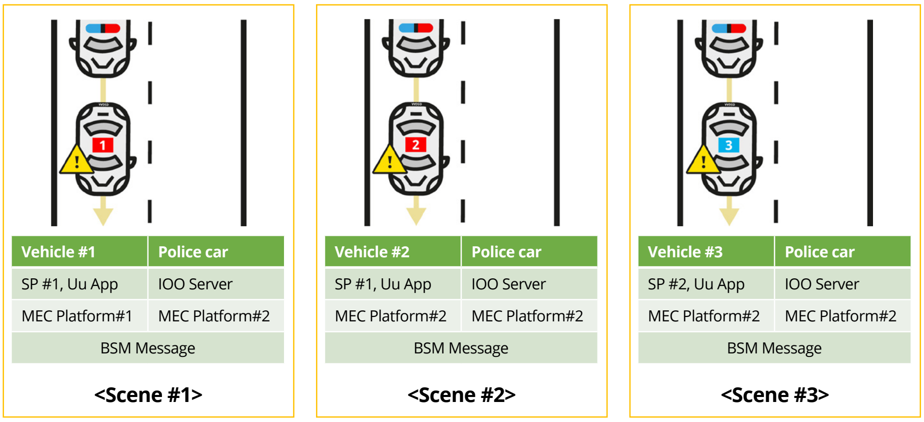
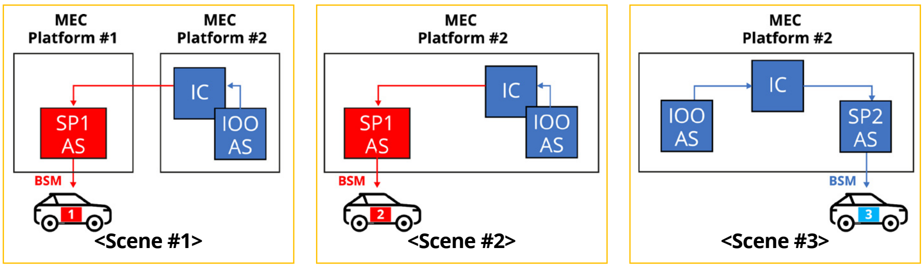
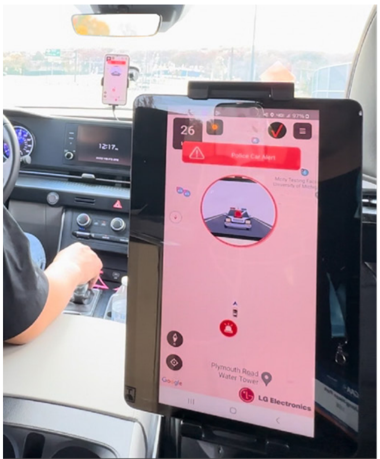
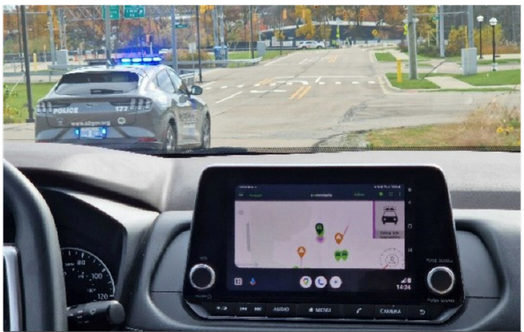
5.3.1 Road Works

Use case name	Road Works		
Basic description	In this scenario, road works are in progress, with a roadwork sign placed on the road. TIMs about road works are transmitted via Uu. The vehicles receive them, thus identifying the presence of road workers. In response to the alert, the driver temporarily reduces speed and changes route to bypass the work site.		
SAE message type	Traveller Information Message (TIM)		
Triggering condition	The vehicle is approaching a road work zone		
Scene and actor, Where the message originates			
Dataflow			

Illustrations	 
Scene description	<Scene#1> At the work site, a roadwork sign is placed on the road. SP#1 AS (MEC Platform#2) initiates the TIM transmission to SP#1 AS (MEC Platform#1) and subsequently relays these messages to Vehicle#1 (SP#1 AS, MEC Platform#1). As Vehicle#1 approaches the work site, the driver of the vehicle confirms the alert displayed on the UI/UX and recognises the roadwork sign. In response to the alert, the driver temporarily reduces speed and diverts from its original route to bypass the work site. Once the detour is complete, the vehicle resumes its regular route. <Scene#2> At the work site, with a roadwork sign placed on the road. SP1 AS (MEC Platform#2) initiates the TIM transmission to SP#1 AS (MEC Platform#2) and subsequently relays these messages to Vehicle#2 (SP#1 AS, MEC Platform#2). As Vehicle#2 approaches the road work zone, the driver of the vehicle confirms the alert displayed on the UI/UX and recognises the roadwork sign. In response to the alert, the vehicle temporarily reduces its speed and diverts from its original route to bypass the work zone. Once the detour is complete, the vehicle resumes its regular route. <Scene#3> At the work site, a road work sign is placed on the road. SP#1 AS (MEC Platform#2) initiates the TIM transmission to the Interchange of MEC Platform#2. The messages are transmitted from SP#1 AS(MEC Platform#2) to the Interchange and relayed to (SP#2 AS, MEC Platform#2), Vehicle#3. As Vehicle#3 approaches the work zone, the driver of the vehicle confirms the alert displayed on the UI/UX and recognises the roadwork sign. In response to the alert, the driver temporarily reduces speed and diverts from the original route to bypass the work site. Once the detour is complete, the vehicle resumes its regular route.

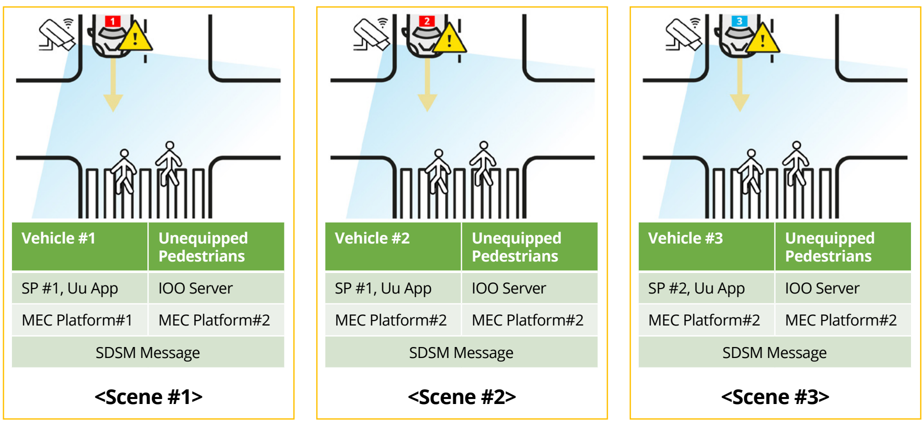
5.3.2 Emergency Vehicle - Police Car Approaching

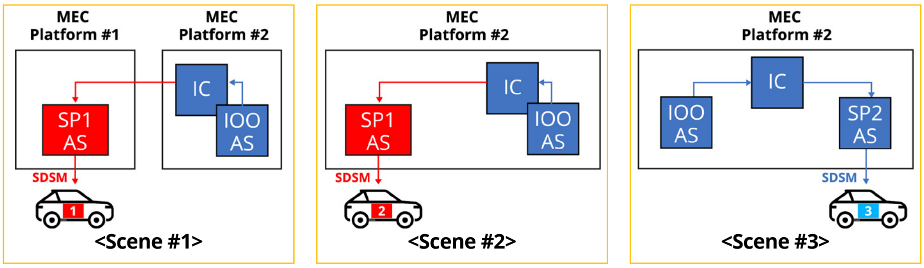
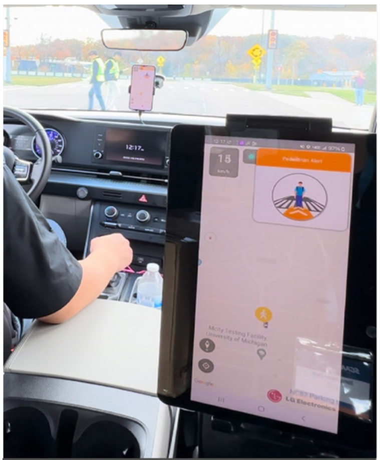
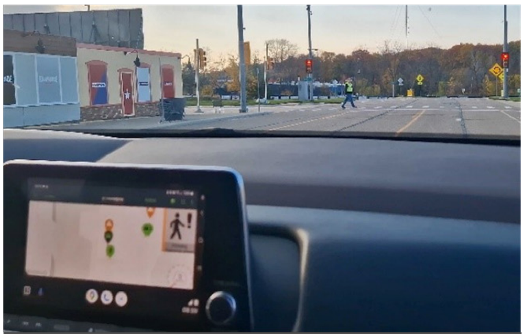
Use case name	Emergency Vehicle – Police Car Approaching
Basic description	As vehicles are driving on the road, the drivers receive notifications that an emergency vehicle (Police Car) is approaching from behind. In response to the alert, the drivers create a safe distance by pulling over. The Police Car overtakes the vehicles, and once it has passed, the vehicles resume their normal driving sequence.
SAE message type	Basic Safety Message (BSM)

Triggering conditions	Approach distance between Police Car and vehicles Heading direction of Police Car
Scene and actor Where the message originates	
Dataflow	
Illustration (photo)	 ▶ Service Provider #1  ▶ Service Provider #2

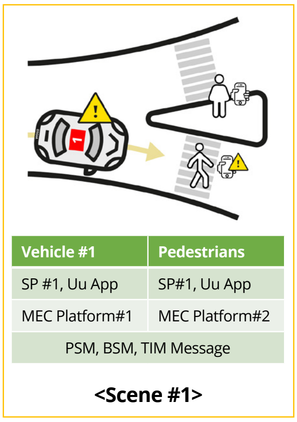
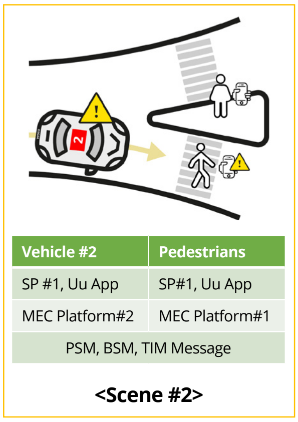
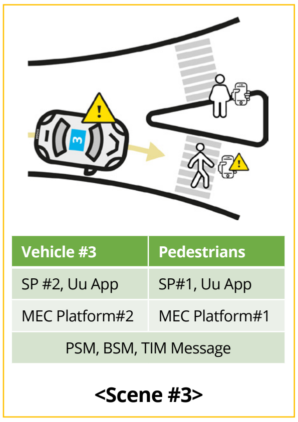
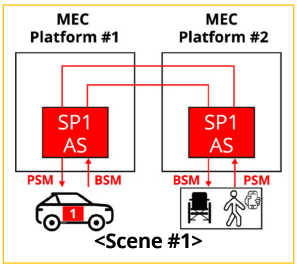
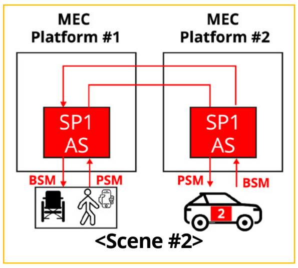
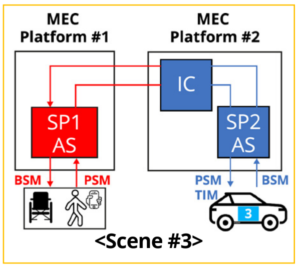
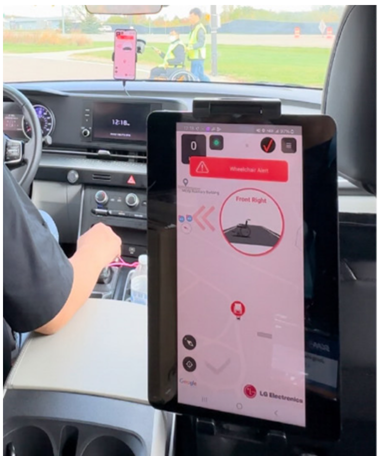
Scene description	<Scene#1> Vehicle#1 is driving on the road. The Police Car starts driving due to an emergency and transmits BSMs to an IOO AS, which in turn transmits the messages to the Interchange. BSMs are transmitted from the IOO server to the Interchange and relayed to SP#1 AS (MEC Platform#1) and Vehicle#1. As the Police Car approaches Vehicle#1, the driver of Vehicle#1 confirms the alert displayed on the UI/UX and recognises the emergency vehicle alert. In response to the alert, the drivers create a safe distance by pulling over. Once the Police Car has passed, the vehicles resume their driving sequence. <Scene#2> Vehicle#2 is driving on the road. The Police Car starts driving due to an emergency and transmits BSMs to the IOO App Server who then transmits them to the Interchange. BSMs are transmitted from IOO server to the Interchange and relayed to SP1 AS (MEC Platform#2), Vehicle#2. As the Police Car approaches Vehicle#2, the driver of Vehicle#2 confirms the alert displayed on the UI/UX and recognises the emergency vehicle alert. In response to the alert, the drivers create a safe distance by pulling over. Once the Police Car has passed, the vehicles resume their driving sequence. <Scene#3> Vehicle#3 is driving on the road. The Police Car starts driving due to an emergency and transmits BSMs to the IOO AS, which transmits them to the Interchange. BSMs are transmitted from IOO server to the Interchange and relayed to SP#2 AS (MEC Platform#2), Vehicle#3. As Police Car approaches Vehicle#3, the driver of Vehicle#3 confirms the alert displayed on the UI/UX and recognises the emergency vehicle alert. In response to the alert, the drivers create a safe distance by pulling over. Once the Police Car has passed, the vehicles resume their driving sequence.

5.3.3 Smart Intersection

Use case name	Smart Intersection
Basic description	Unequipped pedestrians enter an intersection where a smart camera and RSU are installed. The smart camera and GW RSU are interconnected. The smart camera detects the unequipped pedestrians, and the GW RSU connected to the smart camera transmits messages to the IOO server via Uu. The vehicle's app receives the messages and displays the unequipped pedestrians. The driver of the vehicle recognises the presence of the unequipped pedestrians on the UI/UX and slows down in advance until it comes to a complete stop.
SAE message type	Sensor Data Sharing Message (SDSM)
Triggering condition	Approach distance between pedestrians and vehicles
Scene and actor, Where the message originates	

Dataflow	
Illustration(photo)	 ▶ Service Provider #1  ▶ Service Provider #2
Scene description	<Scene#1> Unequipped pedestrians enter and prepare to cross a smart intersection with a smart camera and GW RSU installed. The smart camera detects unequipped pedestrians, and the RSU connected to smart camera transmits SDSMs to the IOO AS. The messages are transmitted from the IOO server to the Interchange and relayed to SP#1 AS (MEC Platform#1), Vehicle#1. Vehicle#1 receives SDSMs and displays the unequipped pedestrians. Vehicle#1 approaches the smart intersection. The driver of Vehicle#1 receives an alert and recognises the presence of the unequipped pedestrians on UI/UX and slows down in advance before coming to a stop. Once the unequipped pedestrians have finished crossing, the vehicle resumes its driving. <Scene#2> Unequipped pedestrians enter and prepare to cross a smart intersection with a smart camera and GW RSU installed. The smart camera detects unequipped pedestrians, and the RSU connected to smart camera transmits SDSMs to the IOO AS. The messages are transmitted from the IOO server to the Interchange and relayed to SP#1 AS (MEC Platform#2), Vehicle#2. Vehicle#2 receives the SDSMs and displays the unequipped pedestrians. Vehicle#2 approaches the smart intersection. The driver of Vehicle#2 receives an alert and recognises the presence of the unequipped pedestrians on UI/UX and slows down in advance before coming to a stop. Once the unequipped pedestrians have finished crossing, the vehicle resumes its driving. <Scene#3> Unequipped pedestrians enter and prepare to cross a smart intersection with a smart camera and GW RSU installed. The smart camera detects unequipped pedestrians, and the RSU connected to smart camera transmits SDSMs to the IOO AS. The messages are transmitted from the IOO server to the Interchange and relayed to SP#2 AS (MEC Platform#2), Vehicle#3. Vehicle#3 receives SDSM messages and displays the unequipped pedestrians. Vehicle#3 approaches the smart intersection. The driver of Vehicle#3 receives an alert and recognizes the presence of the unequipped pedestrians on UI/UX and slows down in advance, and comes to stop. Once the unequipped pedestrians have finished the way, the vehicle resumes its driving.

5.3.4 Mid-block Crossing

Use case name	Mid-block Crossing
Basic description	Pedestrians and wheelchair users are on the mid-block and, transmit PSM messages via SP application, indicating their intention to cross the mid-block. Vehicles approach the mid-block zone. The driver recognises the presence of the pedestrians and wheelchair users on the UI/UX and slows down in advance before coming to a stop. Once the pedestrians and wheelchair users have finished passing, the vehicle resumes its driving.
SAE message type	Personal Safety Message (PSM), Traveller Information Message (TIM), Basic Safety Message (BSM)
Triggering condition	Approach distance between pedestrians and vehicles
Scene and actor, Where the message originates	  
Dataflow	  
Illustration (photo)	 ▶ Service Provider #1  ▶ Service Provider #2

Scene description	<Scene#1> A pedestrian and wheelchair user (SP#1 App, MEC Platform#2) enter the mid-block. They transmit PSM messages through the application indicating their intent to cross the mid-block. These PSMs are transmitted from their applications to Vehicle#1. The messages are relayed from SP#1 AS (MEC Platform#2) to SP#1 AS (MEC Platform#1) through Inter-MEC interface. The driver of Vehicle#1 receives an alert and recognises the presence of the pedestrian and wheelchair user on the UI/UX and slows down in advance before coming to a stop. Simultaneously, Vehicle#1 transmits BSMs to the pedestrians and wheelchair users. These messages are relayed from SP#1 AS (MEC Platform#1) to SP#1 AS (MEC Platform#2) through the inter-MEC interface. The pedestrians and wheelchair users become aware of the approaching Vehicle#1 through the UI/UX of the application that received BSMs. <Scene#2> A pedestrian and wheelchair user (SP#1 App, MEC Platform#1) enter the mid-block. They transmit PSMs through the application indicating their intent to cross the mid-block. These messages are transmitted from their applications to Vehicle#2. The PSMs are relayed from SP1 AS (MEC Platform#1) to SP#1 AS (MEC Platform#2) through Inter-MEC interface. The driver of Vehicle#2 receives an alert and recognises the presence of the pedestrian and wheelchair user on the UI/UX and slows down in advance before coming to a stop. Simultaneously, Vehicle#2 transmits BSMs to the pedestrians and wheelchair users. These messages are relayed from SP#1 AS (MEC Platform#1) to SP1 AS (MEC Platform#2) through the inter-MEC interface. The pedestrians and wheelchair users become aware of the approaching Vehicle#2 through the UI/UX of the application that received BSMs. <Scene#3> A pedestrian and wheelchair user (SP#1 App, MEC Platform#1) enter the mid-block. They transmit PSMs through the application indicating their intent to cross the mid-block. These messages are transmitted from their applications to Vehicle#3. PSMs are transmitted from SP#1 AS (MEC Platform#1) to the Interchange and relayed to SP#2 AS (MEC Platform#2). The driver of Vehicle#3 receives an alert and recognises the presence of the pedestrian and wheelchair user on the UI/UX and slows down in advance before coming to a stop. Simultaneously, Vehicle#3 transmits BSM messages to the pedestrians and wheelchair users. These BSMs are transmitted from SP#2 AS (MEC Platform#2) to the Interchange and relayed to SP#1 AS (MEC Platform#1). The pedestrians and wheelchair users become aware of the approaching Vehicle#3 through the UI/UX of the application that received BSMs. SP#2 AS defines the mid-block zone through TIMs, and when pedestrians and wheelchair users enter the predefined mid-block zone, their mid-block crossing request messages become valid and are transmitted to vehicles.

6 Testing and Performance

6.1 Digital Twin

Many of the VRU-DEMO system service scenarios were recreated using Digital Twin Provider#1 and Digital Twin Provider#2. From an automotive perspective, a digital twin could be a full or partial representation of the actual physical environment, infrastructure, vehicles, fusion data, human actors, and test tools in a virtual digital environment.

From a test tools perspective in the VRU interoperability evaluation, it was a combination of virtual and physical equipment. Test and measurement digital twins are used to simulate tests, experiments, or scenarios that would otherwise be conducted using physical equipment and environment. This digital representation can model the performance, characteristics, and functionalities of real-world devices or instruments allowing engineers to virtually validate designs, configurations, or measurements before deploying or utilising actual hardware.

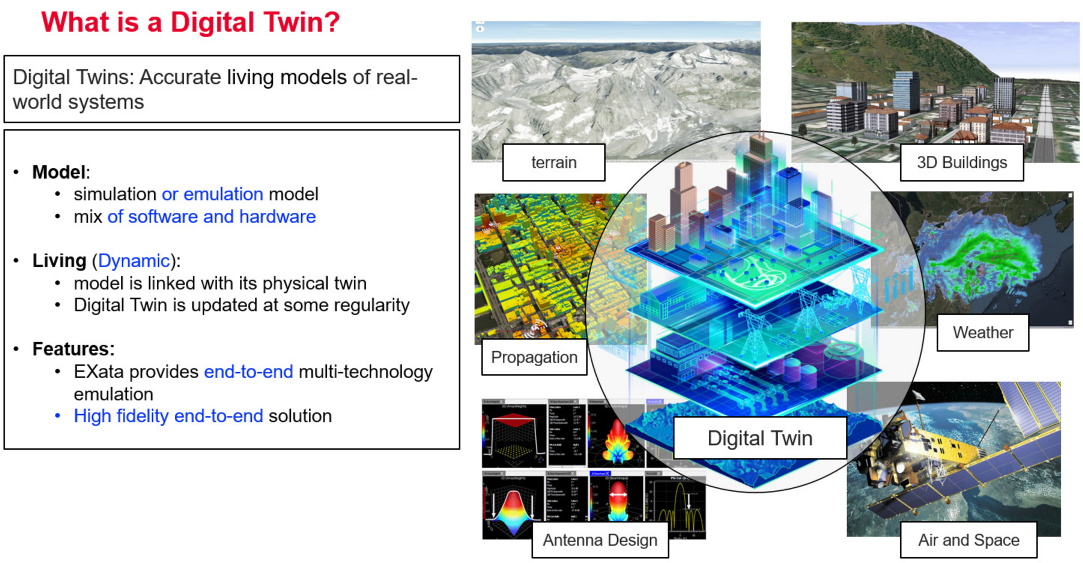


Figure 6: Visual Representation of a Digital Twin

6.1.1 Evaluation Instruments

6.1.1.1 Digital Twin Provider#1

Digital Twin Provider#1 participated in the VRU-DEMO by deploying two different setups of digital twins. The first setup is a digital twin of a network performance tester (MT1000A) that could reside on any site hosting the application server running on the MEC Platform. This setup, as shown in the figure below, is capable of measuring different transport layer KPIs using a combination of a physical network performance tester at one of the testing endpoints and a digital twin representation of the tester (MEC hosted) on AWS Wavelength as the other endpoint. The packet size, frame rate, data rate, transport protocol are configured to measure E2E Packet Service Performance (1-Way UL/DL/Simultaneous and 2-Way UL/DL/Simultaneous with different intensities of Traffic Loading). Below is a diagram showing the combination of Digital Twin Provider#1's physical network communication tester installed on AWS Wavelength in Detroit and the physical unit connected to a wireless modem device in the vehicle.

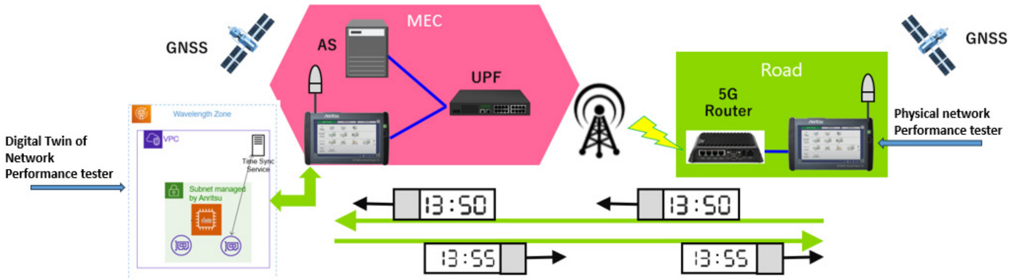


Figure 7: First Setup of Digital Twin Provider#1 Network Performance Tester

The digital twin of the network performance tester was configured and instantiated on AWS Detroit: us-east-1-wl1-dtw-wlz-1, where the Application Server is hosted on the MEC. The physical network performance tester was placed in the vehicle connected to a 4G/5G router that provides the Uu interface. The vehicle was driven to follow the actual route with a user profile created on the network performance tester to replicate the use cases as in the table below.

Table 2: Digital Twin Provider#1's Network Performance Tester Configuration

Family	Vulnerable Road User (VRU)
Device involved	MEC-AWS-Wavelength Smartphone Vehicle MT1000 Network Perf Tester Network Perf Tester Twin on AWS
Message interval (ms)	50
Message frequency (pps)	20
Ethernet Frame Size (Bytes)	254 Byte (Exc. UDP header) 300 Byte (Inc. Eth/IPv4/UDP header)
Message Transport	UDP
Traffic Generation Direction	Bidirectional
Measured Latency	1-way, DL, UL, Round trip
Max MTU (bytes)	< 1414
Test Duration (min)	7
Data Samples Created (points)	420

Background Data Rate (kbps)	8
Network Capability	n77
Time Synchronisation	GPS at Network Perf Tester in Vehicle NTP Server at Digital Twin of Network Perf Tester on AWS Wavelength

- Different KPIs, as mentioned in Section 6.1.2, were measured and an M-City track heat map was generated, as shown in Section 6.1.3. A Radio Frequency (RF) heatmap was also generated by driving on the route and capturing the RF KPI using Handheld RF Spectrum Analyser MS2090A.
- A digital twin of the in-field demonstration to simulate the M-City environment, including drive route, human actors, ITS messages, RF environment, physical environment, sensor realistic data, infrastructure, devices and vehicles. The digital twin follows the drive routes and alerts are sent and received from the same location, as in a real scenario. The figure below shows the setup that was used to create a digital twin of the demonstration.

Figure 8: Second Set-up of Digital Twin Provider#1 VRU-DEMO Digital Twin

Once the baseline digital twin has been created, varying sensor fusion data (Camera, Lidar, Radar, Ultrasonic, V2X), varying RF conditions (inter/intra Radio Access Technology (RAT) handovers, cell outage, cell acquisition, RF congestions, etc.) and varying transport conditions (network congestion, delays, different QoS treatments) could be introduced to evaluate the overall performance of the UE and network ITS messages being sent and received. Testing using a digital twin setup with simulated vehicles, sensor realistic data, and simulated virtual environment offers repeatability, scalability, and regression analysis in a safe and cost-effective manner for issues that are difficult and expensive to duplicate in the real network.

6.1.1.2 Digital Twin Provider#2

Digital Twin Provider#2 contributed to the VRU-DEMO showcase by providing a Digital Twin of M-City, which combined the VRU-DEMO scenarios (AV1025A WaveBEE Creator and AV1021A WaveBEE Touch) as well as a physics-based model of the RF environment (SN100EXBA EXata).

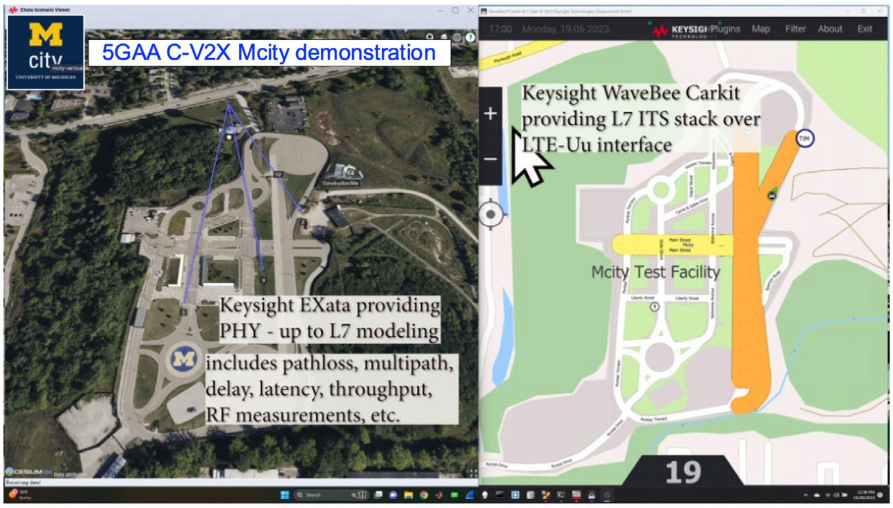


Figure 9: Digital Twin Provider#2 Demo Display

This unique combination enables researchers to recreate the VRU-DEMO scenarios (e.g., Emergency Vehicle Behind, Mid-Block Crossing, etc.) and then layer on top of varying levels of RF impairments to see if and when system performance is compromised. KPIs such as Rx Power, latency, throughput, and multipath interference can be predicted via the modelling engine. The models can be enhanced if real RF measurements are taken and the data is fed back into the internal channel model.

Figure 10 illustrates the calculated RSRP profile for the ego vehicle as it travels around the track (varying distance from the Uu interface of the Base Station).

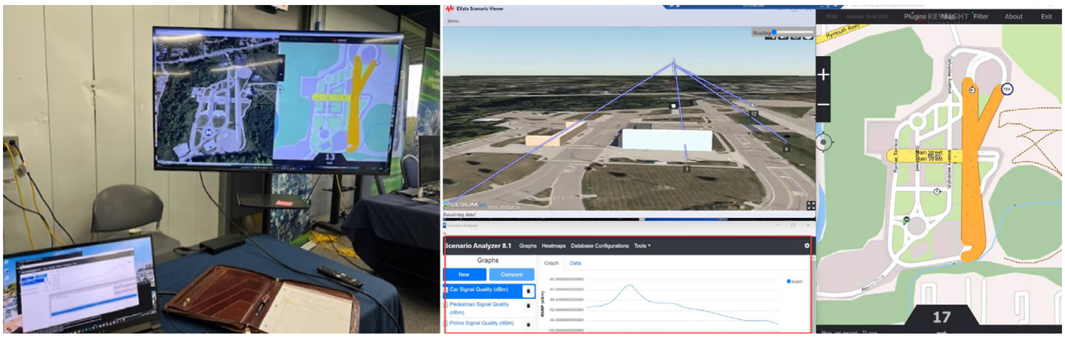


Figure 10: Digital Twin Provider#2 Digital Twin with predicted Ego Vehicle Rx Power (RSRP)

6.1.2 Key Performance Indicators

The following Key Performance Indicators are measured every second using Digital Twin Provider#1's Network Performance Digital Twin.

Table 3: KPIs from First Set-up of Digital Twin Provider#1

Min Latency
Max Latency
Average Latency
Min Jitter
Max Jitter
Average Jitter
Frame Loss Rate
Throughput
Physical Cell Identifiers (PCI)
Received Signal Reference Power (RSRP)

6.1.3 Evaluation Results

6.1.3.1 Digital Twin Provider#1 Results

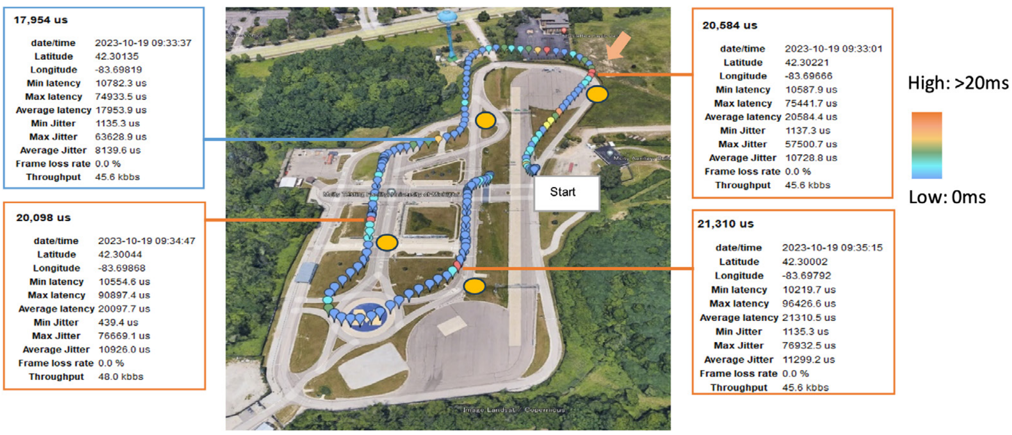


Figure 11: Network Transport KPI Heat Map

Figure 12: RF Signal Physical Cell Identifier (PCI) Heat Map

As can be seen in the transport KPI heatmap (Figure 11), the round-trip average latency between the Device Under Test (DUT) in the vehicle and AS on the MEC server was around 20ms. However, there were points where the maximum latency increased to over 95ms, even in light background traffic loading. The RSRP measured throughout the test was between -50dBm and -85dBm. The RF signal PCI heatmap in Figure 12 above shows the PCI plotted. The same colour points correspond to the same PCI as seen by the UE (in-vehicle) and colour change corresponds to a change in the PCI. Based on this heat map, there were areas where PCIs were switching, and these align close to areas where the measured maximum latency was significantly higher than the measured average latency. This suggests the device was going through intra- or inter-base station handovers, while some of the packets may be getting queued. Hence, introducing an additional instantaneous max latency of 95ms, even though the average latency numbers were lower, at around 20ms.

Test Profile
- Small Frame Size, Slow Data Rate
- With modest background data
- UL/DL/RT simultaneous measurement

Data Stream	Frame Size (byte)	Data Rate (bps)
For Round Trip	300	50 k
For Uplink/Downlink	300	50 k

Measurement Direction	Latency (us)			
	Avg.	P50	P90	CDF(99%)
Round Trip	16,096	16,007	18,040	21,217
Downlink	12,451	12,351	13,039	14,055
Uplink	4,487	4,453	6,240	8,362

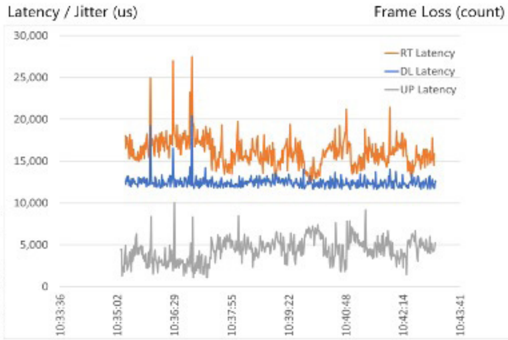


Figure 13: Statistical Analysis Network KPI

As shown in the above analysis, latency was measured independently in UpLink (UL), DownLink(DL), and Round Trip(RT), and categorised accordingly as average latency, latency of 50% of the packets sent, latency for 90% of the packets sent, and latency for 99% of the packets sent. Overall, the round trip latency between the devices and the MEC server was 21ms for 99% of the packets. This latency could increase if the background traffic was increased to show congestion, however, for the purpose of the demonstration the traffic was kept at a minimum. Another unusual feature was that the UL latency was lower than the DL latency; after investigation, it was concluded that since each packet is time stamped from the source (GPS at the DUT in vehicle) and MEC server (NTP clock), there was an offset in the accuracy of the NTP server providing the reference to MEC server. It is possible that the NTP server has higher stratum, hence exhibiting significant drift from stratum 0.

6.1.3.2 Digital Twin Provider#2 Results

Performance Indicators from Digital Twin Provider#2 can be seen in the figures below – these indicators are calculated in real time by the Physics Engine and passed on to a SQL Database. They can be accessed and formatted in tabular form as per the figure below.

RowId	Timestamp	SenderID	ReceiverID	ChannelIndex	Pathloss	TxGain	RxGain	PropDelay	Distance	TerrainLoss	RainPathloss
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	0.150338408	1	2	0	95.3675	0.0	-55.0	1.209e-06	362.603582010725	NULL	NULL
2	0.795232814	1	2	0	95.2939	0.0	-55.0	1.198e-06	359.544673591956	NULL	NULL
3	3.794952814	1	2	0	94.9617	0.0	-55.0	1.154e-06	346.050137563616	NULL	NULL
4	6.794932814	1	2	0	94.643	0.0	-55.0	1.112e-06	333.586409827128	NULL	NULL
5	10.175439542	1	2	0	94.306	0.0	-55.0	1.07e-06	320.88879546847	NULL	NULL
6	20.219452201	1	2	0	93.5287	0.0	-55.0	9.78e-07	293.421557947691	NULL	NULL

RowId	Timestamp	NodeId	MessageId	SenderAddress	ReceiverAddress	PacketSize	EventType	InterfaceIndex	MessageSeqNum	Overhead
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	0.053704719	2	N2S0	169.0.0.4	255.255.255.255	36	NetworkReceiveFromUpper	0	0	
2	0.053704719	2	N2S0	169.0.0.4	255.255.255.255	56	NetworkSendToLower	0	0	
3	0.149668408	1	N1S0	169.0.0.1	255.255.255.255	36	NetworkReceiveFromUpper	0	0	
4	0.149668408	1	N1S0	169.0.0.1	255.255.255.255	56	NetworkSendToLower	0	0	
5	0.324682905	2	N2S1	169.0.0.4	255.255.255.255	16	NetworkReceiveFromUpper	0	1	
6	0.324682905	2	N2S1	169.0.0.4	255.255.255.255	36	NetworkSendToLower	0	1	
7	0.794842814	1	N1S1	169.0.0.1	255.255.255.255	16	NetworkReceiveFromUpper	0	1	
8	0.794842814	1	N1S1	169.0.0.1	255.255.255.255	36	NetworkSendToLower	0	1	

	RowId	Timestamp	NodeID	MessageID	PhyIndex	Size	EventType	ChannelIndex	OverheadSize	FailureType	SignalPower	Interference	PathLoss
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	0.054049719	2	N2S0	0	84	PhyReceiveFromUpper	0	0	NULL	15.0	NULL	NULL
2	2	0.054049719	2	N2S0	0	128	PhySendSignal	0	192	NULL	15.0	NULL	NULL
3	3	0.054054719	1	N2S0	-1	128	PhyDrop	0	NULL	Signal below Propagation Limit	NULL	NULL	95.382289238
4	4	0.150333408	1	N1S0	0	84	PhyReceiveFromUpper	0	0	NULL	15.0	NULL	NULL
5	5	0.150333408	1	N1S0	0	128	PhySendSignal	0	192	NULL	15.0	NULL	NULL
6	6	0.150339617	2	N1S0	0	128	PhyDrop	0	NULL	Signal below Rx Threshold	NULL	-100.970077403	95.36752457
7	7	0.324887905	2	N2S1	0	64	PhyReceiveFromUpper	0	0	NULL	15.0	NULL	NULL
8	8	0.324887905	2	N2S1	0	108	PhySendSignal	0	192	NULL	15.0	NULL	NULL
9	9	0.324892905	1	N2S1	-1	108	PhyDrop	0	NULL	Signal below Propagation Limit	NULL	NULL	95.352775375
10	10	0.795227814	1	N1S1	0	64	PhyReceiveFromUpper	0	0	NULL	15.0	NULL	NULL
11	11	0.795227814	1	N1S1	0	108	PhySendSignal	0	192	NULL	15.0	NULL	NULL
12	12	0.795234012	2	N1S1	0	108	PhyDrop	0	NULL	Signal below Rx Threshold	NULL	-100.970077403	95.293939957

Figure 14: Real-Time M-City Performance Indicators from Digital Twin Provider#2

In addition to tabular formatted performance indicators, it is possible to display them graphically, such as the RSRP of the ego vehicle as per Figure 15.

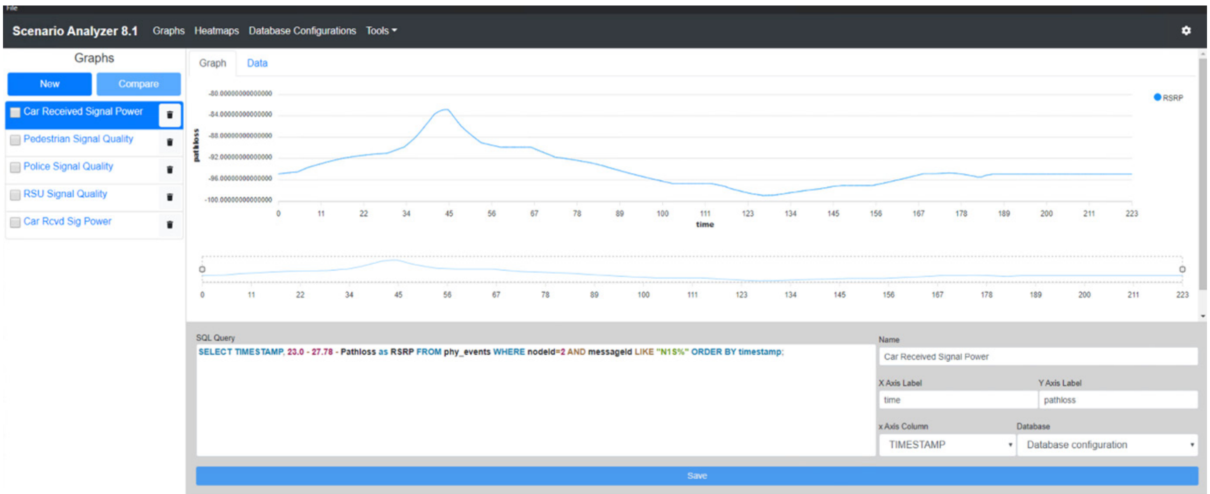


Figure 15: Ego Vehicle RSRP Driving Round M-City Test Track

The next step in the test cycle would be to connect instruments, such as Base Station Emulator and Channel Emulator to real hardware, in order to test how it performs for each use case and in the real world, giving early indications of performance before the costly phase of deployment and installation. A rich set of parameters are available from Digital Twin Provider#2, via the integrated SQL Database, which are calculated in real time – a few examples include Pathloss, Propagation Delay, Timestamped Events, Power, and Interference.

6.2 MEC Interoperability Measurements from SP Perspective

6.2.1 Measurement Configurations

Table 4: End to End latency measurement configurations

Parameters	**Values**	**Descriptions**
Measurement duration	5 min	Inter MEC Scenario, end-to-end Latency Measurement Duration
Data samples	300	Extracting data samples once a second
Estimation field name	@secMark	BSM, @secMark
Message size (BSM)	40 byte	BSM size
Message interval	100ms	Transmission interval
Backend resources	AWS MEC resource	MEC Platform#1 – AWS Wavelength Zone MEC Platform#2 – AWS Local Zone
Delivery protocol stack	TCP/ IP / MQTT	MQTT broker(SW, Version 5) / client model-based interoperability interface implementation
Time synchronisation	NTP time server	All MQTT clients are synchronized with NTP time
Network capability	5G C-band(n77)	C-band capable devices

- The measurement duration of 5 minutes was selected to assess the latency time of applications deployed on different MEC Platforms during the specific time frame.
- Data samples were extracted at a rate of once per second, resulting in a total of 300 samples collected during the measurement duration. This sampling allows for a granular analysis of latency.
- The estimation field name used for these measurements was @secMark, corresponding to the BSM timestamp value defined in SAE J2735.
- The message size was approximately 40 bytes.
- The message interval, representing the time interval between successive message transmissions from MQTT Clients, was set at 100ms.
- The Inter-MEC Bridge refers to a software module that establishes a Subscribe/Publish connection based on an existing MQTT Client to support backward compatibility of up-to-date MQTT Brokers installed on different MEC resources.

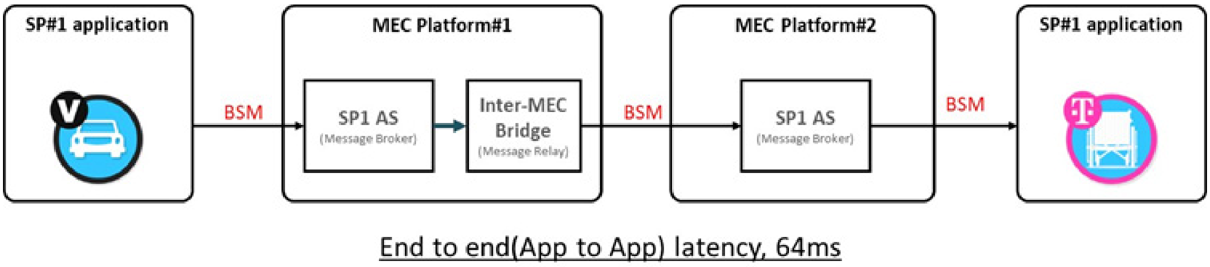


Figure 16: End-to-end Interface between Applications Deployed on Different MEC Platforms

Figure 16 represents the end-to-end (E2E) interface between applications deployed on different MEC Platforms. The SP#1 (Vehicle#1) application in the left box deployed on MEC Platform#1 is interconnected with SP#1 (Wheelchair User) application in the right box deployed on MEC Platform#2 via Inter-MEC Bridge.

Starting from the left side of the figure, as soon as SP#1 application (Vehicle#1) begins driving for VRU-DEMO events, it starts continuously transmitting BSMs to SP#1 AS on Platform#1. These messages are then relayed to SP#1 AS on MEC Platform#2 through Inter-MEC Bridge. SP#1 AS on Platform#2, upon receiving the BSM, transmits it to the SP#1 Application (Wheelchair User). The E2E latency value was measured by comparing the @secMark timestamp value of the BSM transmitted by SP#1 application (Vehicle#1) with the @secMark timestamp value of the BSM received by SP#1 application (Wheelchair User).

6.2.2 Measurement KPIs

As mentioned in Section 5, KPIs were measured through MEC interfacing and interoperability events involving SP1 ASs deployed on two different MEC Platforms. The measurement environment facilitated seamless communication of SAE messages across interconnected SP1 ASs, and the KPI measured was the E2E latency across the same SPs Cross-MEC Platform.

To conduct end-to-end latency measurements between applications using different MEC Platforms, it is crucial that the reference time of all interconnected MQTT Clients is synchronised (i.e., synchronisation of message generation and reception at the MQTT Client level with the reference time enables precise KPI measurements). For the accurate measurement of KPIs during this demonstration, SP1 established a dedicated NTP time server. The NTP server was used to synchronise all MQTT Clients, ensuring precisely aligned timekeeping across the network.

KPI measurements were conducted during Event 4 (Mid-Block Crossing) in a Cross-MEC Platform environment, specifically focusing on data exchange between Vehicle#1 and Wheelchair User. During Vehicle#1's operation (SP1 App, MEC Platform#1), the message exchange (BSM) was monitored as it travelled from Vehicle#1 to Wheelchair User (SP1 app, MEC Platform#2) through the Inter-MEC Interface. Specifically, the key metric under measurement was the message delivery latency between two applications. The latency values were measured by comparing the transmission timestamp of the BSM from Vehicle#1 with the reception timestamp of the BSM by the Wheelchair User.

6.2.3 Evaluation Results

After collecting network latency sample data, the analysis results indicate the following:

Data Analysis	Value
Average	63.90
Standard Deviation	23.51
Median	59

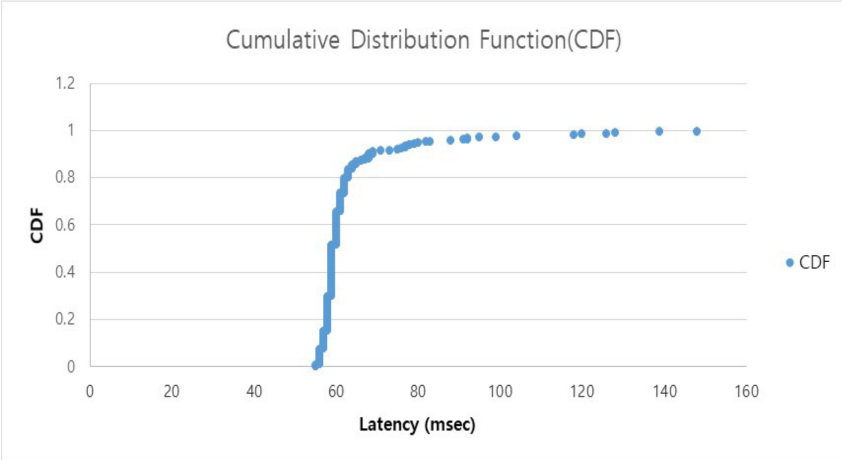


Figure 17: Data Analysis and CDF Result from the Sample Data

- Figure 17 represents E2E average latency values lower than the message generation interval of 100ms, providing evidence of the successful establishment of a low-latency Inter-MEC deployment. This demonstrates the smooth interoperability among infrastructure operators and Service Providers in the V2N communication, particularly in the context of Inter-MEC Platform.
- The standard deviation, measuring at 23.51ms, indicates a consistent range of network latency values.
- The Cumulative Distribution Function (CDF) graph means the majority of latency data is concentrated in the lower range. This indicates that a major portion of the data shares similar latency values, implying a consistency in network performance for most cases.

Percentiles	Value
Percentiles(25%)	58
Percentiles(75%)	62
Percentiles(80%)	63
Percentiles(90%)	69
Percentiles(95%)	82.05

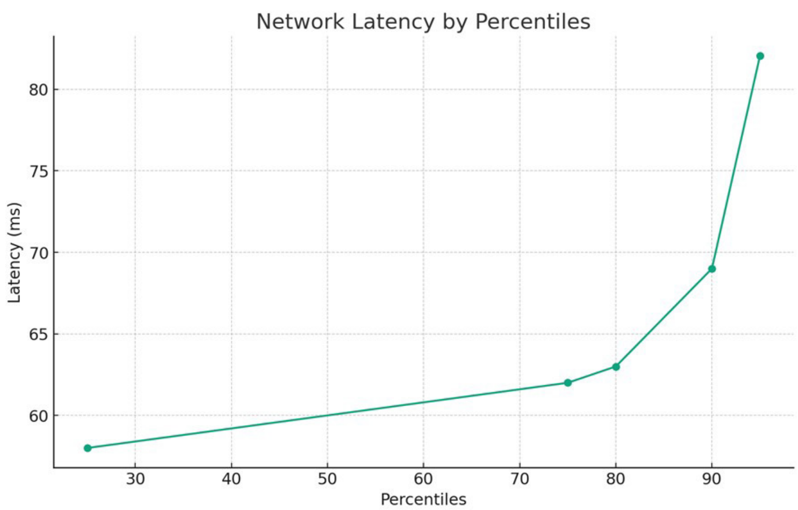


Figure 18: Percentile-based Analysis of Network Latency

The objective of analysing network latency through percentiles is to understand end-to-end network performance in interconnected MEC scenarios. These percentiles provide a granular view of the latency distribution, representing not only stable performance (as indicated by lower percentiles) but also providing insights into the latency variations.

- The analysis shows that 25% of network traffic encounters a latency of 58ms or lower, demonstrating reliable latency for most inter-MEC message traffic.
- The percentiles 75%, 80%, and 90% indicate the majority of traffic maintains acceptable performance levels.
- At the 95% percentile, it indicates potential delays for a small portion of the traffic – mainly caused by the delays in the section of unmanaged IP network that connects two MEC Platforms. However, this result also implies that latency levels are still adequate for V2X message exchanges between service applications hosted on different network platforms.

6.3 Conclusions

Digital Twin Provider#1: Network Performance Tester Digital Twin

- Measured key parameters of network performance including one-way UL/DL/roundtrip latency, jitter, throughput, packet loss and plotted latency heatmap of the entire VRU-demo route.
- Observed low latency in the condition of Small Frame Size, Slow Data Rate and modest background Data.
- Observed KPIs, such as latency and jitter, can be significantly changed in areas where there are handovers or the background data stream rate is changed.
- Differences in the accuracy of reference timing at both measurement end points can skew the measurements when Uplink and Downlink latency (one-way) is measured separately. This issue will be camouflaged if roundtrip measurements are done. Hence, it is important to measure one-way latency because traffic loading in a network is asymmetric. It was observed that UL was lower than UL. This was probably due to the fact that the test equipment connected to the UE was using GPS signal (stratum 0) as its timing source and the MEC server's timing source was based on an NTP clock, which had much higher drift in this scenario and thus lower accuracy than a GPS source.
- Latency is not only dependent on the distance from the MEC location but also on congestion, routing, and network topology.

Digital Twin Provider#2: Conclusions on Digital Twins

- Performance parameters can be presented in real time allowing for accurate prediction of system performance before the expense of hiring test tracks, vehicles, etc.
- Given the situation facing companies such as Cruise who had one of the licences for automated taxi service in San Francisco, and subsequently had it revoked, getting accurate physics-based KPIs – such as congestion, latency, carrier interoperability and throughput – would have given early indications of possible problems.
- Predictions of latency, power and overall time for vehicles to perform a loop around M-City were very close to actual.

Service Providers: Conclusion (Service Provider's Perspective)

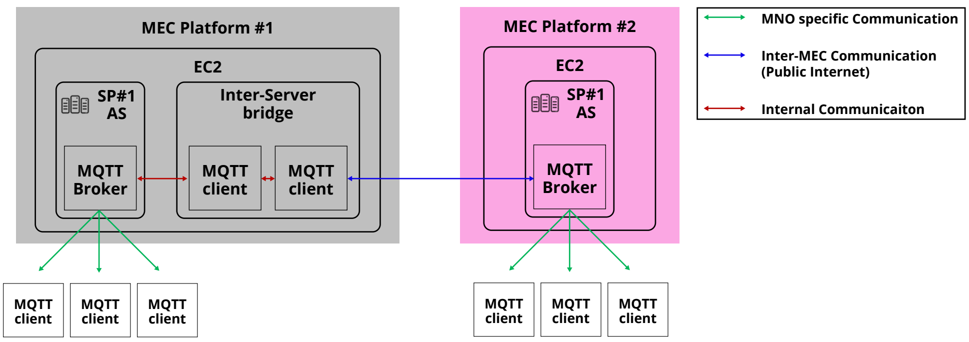
- The comprehensive analysis of end-to-end network latency in interconnected MEC scenarios within the VRU-DEMO system demonstrates an adequate performance across different MEC Platforms.
- The majority of network traffic maintains acceptable latency levels, with only a minor fraction experiencing higher delays, primarily due to the unmanaged IP network section in the inter-server interface.
- These findings indicate the successful integration and reliable performance of V2X message exchanges, illustrating the potential of interconnected MEC Platforms in enhancing V2N communication efficiency.

7 Lessons Learned

In this section, the experiences and insights gained during the VRU-DEMO WI, and the related deployment examples are reflected upon. Throughout the VRU-DEMO system, the project team encountered interoperability issues, identifying optimal solutions to resolve them. The purpose of this section is to share these experiences and the key take-aways, by providing a comprehensive view of the VRU-DEMO project's deployment, including considerations for future standardisation activities.

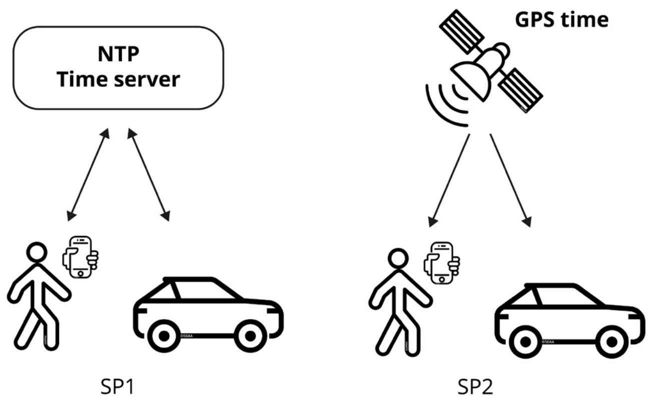
7.1 Development Challenges and Lessons Learned

7.1.1 Establishment of Inter-Server Connectivity

Challenge	Establishment of Inter-Server Connectivity
Goal	This project aims to implement seamless interfacing between two App servers, both utilising the MQTT Protocol and communicating over an agreed topic(="5GAA"): one operating on MEC Platform#1 and the other on MEC Platform#2.
Issues	a. One issue arises from the inherent design of the MQTT Protocol, which assumes MQTT Clients typically connect to a single broker and 'Publish/Subscribe' to messages through that broker. b. This challenge arises from the absence of defined standards for creating an IP-based MQTT standard inter-server interface between different server platforms, with no existing reference guidelines tailored to connecting MQTT Brokers.
Development requirements	a. Establish communication that is compatible with the existing Protocol Publish/ Subscribe intervals and an MQTT standard-compliant software version. b. To reduce latency, the process of packet encapsulation and decapsulation should be minimised, and unnecessary redundancy should be eliminated. c. An unintended data-looping issue that could potentially arise in this interconnected setup and an agreed topic should also be resolved.
Diagram	

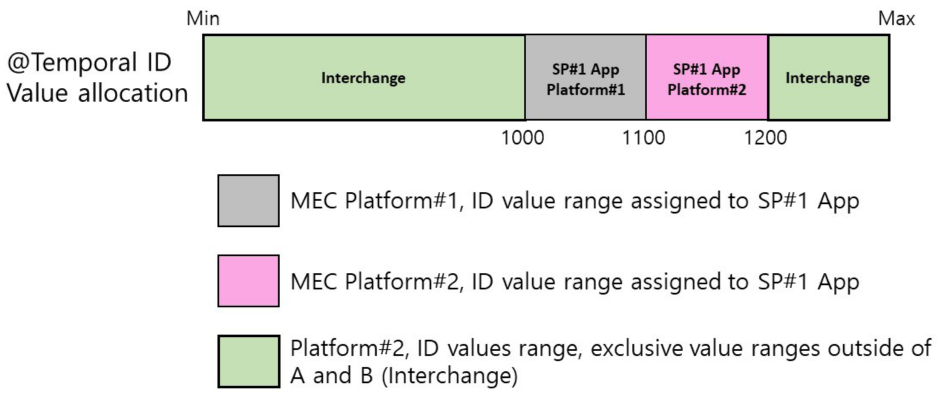
Solution	a. To maintain the communication model of the existing MQTT Protocol and enable connectivity between the brokers of each server platform's AS, a bridge module is implemented for connecting sessions of independently operating MQTT brokers. b. This Inter-Server Bridge builds an inter-server interface compatible with the MQTT Protocol and comprising symmetric MQTT Clients capable of Publish/Subscribe operations in each MQTT Broker. c. Issues that occurred in the interconnected setup environment were resolved on the App server (e.g., data-looping issue through filtering).
Considerations for standardisation	a. Technical guidelines can be developed for Inter-Server connectivity. These guidelines should provide recommended practices and design principles for connecting MQTT Brokers across different server platforms. b. Consideration points with the guideline can be discussed: existing protocol compatibility, practical profiles for interoperability, common declarative configurations, APIs.

7.1.2 Time Synchronisation Issue

Challenge	Time Synchronisation Issue – NTP Time and GPS Time
Goal	Ensure that all Apps support proper execution of use cases by providing synchronisation of message timestamps under the Inter-Server system.
Issues	a. SP#1 Apps are synchronised using NTP reference time obtained from an NTP server, while SP#2 Apps are synchronised using GNSS/GPS time obtained from an OBU. b. Smartphone Apps usually rely on NTP time, as GPS time from the OS (Android, iOS) often proves inaccurate, mainly because smartphone manufacturers face the challenge of fitting many components into a tight space. Different manufacturers use different solutions (antenna configuration, GNSS chip), potentially leading to time variations between devices. Consequently, SP#1 Apps use the NTP server's reference time for synchronisation. c. Even though GNSS/GPS systems provide accuracy in the range of microseconds, using NTP smartphones may achieve better time synchronisation overall in some network-based applications (e.g., between multiple clients and a server). Nevertheless, standard V2X messages were adopted for outdoor ad-hoc scenarios where GNSS/GPS time is a suitable solution for synchronisation. Therefore, standard V2X services and message formats require a GNSS/GPS-based timestamp as it is commonly available for the communicating entities, and it ensures backward compatibility with existing systems. d. Conversion is needed between NTP(UTC) time and GNSS/GPS time, which usually must be handled on the application level (e.g., leap seconds).
Development requirements	Timestamp values referenced by SP#1 apps and SP#2 apps shall be synchronised.
Diagram	
Solution	a. A temporary solution for time synchronisation was implemented by manually adjusting the timestamp value of the SP Apps.

Considerations for standardisation	a. A generalised issue and common understanding: ensuring a common understanding among relevant entities and addressing potential issues in practical scenarios is necessary. b. The technical guidelines have been mentioned as follows: ▶ Revise the GNSS/GPS accuracy of smartphones in outdoor scenarios (since the demonstrated V2N/V2X use cases involving VRUs are outdoor based) and determine if the quality is adequate for a stable performance of the VRU protection services. ▶ Revise the role of NTP and GNSS/GPS time in the SP ASs. For example, NTP may be more reliable for session management of the clients and monitoring network performance indicators, whereas GNSS/GPS can be used for the standardised V2X messages. ▶ For another example, methods to apply GNSS/GPS in V2X standardised messages can include acquiring GNSS/GPS time from the infrastructure or ITS systems and adjusting it in the backend as a reference time.

7.1.3 Identifying the Service Entity from which Messages Are Generated

Challenge	Identifying the Service Entity from which Messages Are Generated
Goal	In a network environment where different service entities are interconnected, Apps should be able to identify the source (e.g., name of the Service Provider) of received messages and monitor reception quality of those messages in the message layer.
Issues	a. Clients were unable to identify the source service entity of the messages. b. Standard messages lacked information necessary to confirm the Service Entity from which messages are generated.
Development requirements	a. To solve the interoperability issue, it is necessary to identify the Service Entity that generated the messages. b. Ensure compliance with standard message formats and compatibility to support interoperability. c. The origin of messages at the message layer should be verifiable and displayed in the user interface, i.e., the purpose of VRU-DEMO validation.
Diagram	
Solution	a. For the demonstration, a temporary solution was implemented by dividing the Temporal ID value of V2X messages into three allocated ranges. b. Clients were able to identify the source entity of the received messages and monitor their quality by checking the Temporal ID value range. But Service Entities of messages coming from the Interchange could not be identified.
Considerations for standardisation	a. Exploring the relevance and viability of the issue: discussing potential challenges when implementing this as an actual service becomes necessary. b. Exploring optimal solution: referring to C-Roads 'IP-based Interface profile' document, defining MQTT-based solutions.

7.2 Observations and Recommendations for Future Work

The primary goal of the VRU-DEMO Work Item was to establish interoperability deployment and implement inter-working operation between the brokers of application servers installed across Multi-MNO MEC Platforms. Technical observations from the lessons learned are indicative of the need for common guidelines to accommodate delivery protocols and data exchange methods operated by Service Entities, and to consider specific policies and configurations for cloud venders. Therefore, for actual deployment, it is necessary to have standardised interfaces that enable inter-working across applications and servers that are managed by different parties. It is also important to ensure that such interfaces can fulfil the requirements of the target services (e.g., in terms of latency, reliability) while minimising data traffic for reasonable operational cost, as well as supporting scalable operations to embrace a large number of service users. This standard-based approach will encourage various stakeholders to join the V2N2X ecosystem, thereby contributing to the enhancement of VRU safety.

The cross-MNO MEC interconnect architecture worked well enough to meet the requirements of the demonstrated use cases, and further optimisation is possible if required. Standardisation of MEC/cloud interfaces is required for mass deployment. Also, standardisation and adoption of network and MEC APIs will be beneficial for the MEC application developers (work in progress in Camara/5GFF, ETSI MEC etc.).

Discrepancies in reference timing accuracy between NTP and GPS at both measurement endpoints can introduce errors when measuring one-way latency for uplink and downlink separately, potentially skewing the results. This issue will be camouflaged if roundtrip measurements are done. Hence, it is important to measure one-way latency because traffic loading in a network is asymmetric. It was observed that Uplink Latency was lower than Downlink. This was probably due to the fact that the test equipment connected to the UE was using GPS signal (stratum 0) as its timing source and the MEC server's timing source was based on an NTP clock, which had much higher drift in this scenario and lower accuracy than the GPS source. More investigation needs to be done on how the delta between two different reference timing sources can be accurately measured using test equipment and automatically compensated. Moreover, utilising advanced simulation tools such as a Digital Twin enables accurate planning to be done before the actual physical test scenarios are carried out – saving time and costs. Predictions of the RF environment can provide insights into what performance might be expected and can give early indications of possible sources of interference or line-of-sight issues. Estimates of latency provide further insights which can be augmented by real-world measurements using appropriate equipment.

5GAA is a multi-industry association to develop, test and promote communications solutions, initiate their standardisation and accelerate their commercial availability and global market penetration to address societal need. For more information such as a complete mission statement and a list of members please see https://5gaa.org

5GAA Automotive Association