Mobile Edge Computing Use Cases, Initial Test Specifications and Evaluation Methodology Review

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:	2.0
DATE OF PUBLICATION:	15 July 2025
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	3 April 2025

Contents

Introduction

This second edition of Technical Report (TR) provides an updated set of Use Case requirements, and a new evaluation methodology review for deployment potential using Mobile Edge Computing (MEC) infra-structure. The work is based on Use Cases (UC) and requirements developed by 5G Automotive Association's Work Group 1 (WG1) and other organisations, such as the European Telecommunications Standards Institute (ETSI) MEC [2] and China's IMT 2020 PG.*

Down-selection and analysis of UCs are outlined in this TR according to different objectives and criteria, including the technology's feasibility and demonstrated capabilities, its evaluated performance, its proven business potential, etc. For this, a vehicle Original Equipment Manufacturer (OEM) perspective on UCs is featured because the end application is consumed on the vehicle side. Additional requirements, such as end-to-end (E2E) security schemes, should also be considered.

The newly introduced evaluation methodology presented in this TR is examined through discussion of examples and best practices. The aim of this approach is to help OEM's better evaluate how/when to deploy vehicle features on-board, in MEC, or in a central cloud. A discussion of the relevant criteria to be considered, and the related technical or business issues for these criteria, is given to guide the reader through the evaluation methodology.

* *Thanks to collaboration agreements between 5GAA and those organisations. An extended analysis may be possible by liaising with other standards developing organisations (e.g. 3GPP and SAE), and industry groups (e.g. AECC, 5G-Americas, NGMN, etc.).*

1 Scope

Mobile Edge Computing is a key enabler of several Cellular Vehicle-to-Everything (C-V2X) applications that require ultra-low latency and high reliability. This document analyses the C-V2X Use Cases, in particular those defined by 5GAA WG1, that require the processing of large amounts of data and could benefit from the use of MEC instead of uploading the data to the cloud, which could cause additional round trip delays. The selection and evaluation of Use Cases is based on inputs from auto OEMs and their key requirements about interoperability between different Mobile Network Providers (MNPs), different vehicle OEMs and different C-V2X application providers. In addition, other criteria for down selection includes feasibility of demonstration, technology capabilities for performance evaluation and demonstration of the highest business potential. The down selected MEC Use Cases will be used as inputs to related WG MEC4AUTO Task 2, Task 3 and Task 4 activities.

In Chapter 5, a set of criteria for the analysis of Use Case relevance is described. This has been used to select a set of UCs relevant to MEC deployment and to highlight the key criteria used to evaluate the relevance for MEC. This is intended as a guide to enable readers to understand the selection process and to be able to apply a similar selection process on any other candidate Use Cases. Following this, Chapter 6 of this document then provides an analysis of a selection of Use Cases, as worked examples, to show the potential for deployment and benefits of MEC for different UCs.

In this, the second edition, the scope has been extended to provide an evaluation methodology to help analyse if/when to deploy vehicle functions on-board, in MEC, or in the central cloud. This methodology takes the Use Case requirements and characteristics from the existing Chapter 4, and provides a suggested methodology on how to evaluate the possible deployment options and the likely benefits applying to MEC. The new analysis methodology thus considers the more detailed Use Case technical requirements and corresponding capabilities of the vehicle, MEC, and available cloud services.

2 Abbreviations

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

3GPP	3rd Generation Partnership Project
AECC	Automotive Edge Computing Consortium
AI	Artificial Intelligence
API	Application Programming Interface
ATS	Abstract Test Suite
AVP	Automated Valet Parking
C-ITS	Cooperative Intelligent Transport System
C-V2X	Cellular Vehicle-to-Everything
DN	Data Network
ETSI	European Telecommunications Standards Institute
GCF	Global Certification Forum
HMI	Human-Machine Interface
HV	Host Vehicle
ICS	Implementation Conformance Statement
IMA	Intersection Movement Assist
IMT-2020	International Mobile Telecommunications-2020
I/O	Interoperability
ISV	Independent Software Vendor
IVE	In-Vehicle Entertainment
JWT	JSON Web Token
KPI	Key Performance Indicators
LV	Lead Vehicle
MEC	Mobile Edge Computing (or Multi-access Edge Computing)
NFV	Network Function Virtualisation
MNO	Mobile Network Operator
MV	Member Vehicle
NGMN	Next Generation Mobile Networks
OBD	Onboard diagnostics
OBU	Onboard Unit
OEM	Original Equipment Manufacturer
QoS	Quality of Service
RNI	Regional Network Interface
RSU	Roadside Unit
RV	Remote Vehicle
RTT	Round Trip Time
TLS	Transport Layer Security
TP	Test Purpose
SDO	Standards Developing Organisation
SLR	Service Level Requirement
uCPE	Universal Customer-Premises Equipment
UPF	User Plane Function
VIS	Vehicle Information Service

VNF	Virtual Network Functions
VR	Virtual Reality
VRU	Vulnerable Road User

3 Sources of V2X Use Cases enabled by MEC

MEC4AUTO Task 1 stakeholders reviewed the work produced in different organisations on V2X Use Cases that are enabled by MEC. For example, Task 1 reviewed 5GAA internal work, IMT-2020 3GPP, ETSI MEC, SAE, 5G-Americas, NGMN as well as AECC V2X Use Cases enabled by MEC

3.1 AECC

The Automotive Edge Computing Consortium, or AECC, is a global consortium for driving the network and computing infrastructure needs of automotive 'big data'. The AECC has published two documents – a white paper [22] on Driving Data to the Edge: The Challenge of Traffic Distribution and an AECC Use Case and Requirement Document, which has considered the following service scenarios for edge computing in the automotive domain [21]:

- Intelligent driving focused on data collection
- High-definition map for data collection, processing and delivery
- V2Cloud cruise assist advanced Use Case in high-volume data environment
- Multi-tenant systems
- Security and system security
- Mobility service

Most AECC Use Cases have a broader scope rather than being associated with a specific application. The Use Cases considered for MEC4AUTO cover most of the Use Cases defined in AECC.

3.2 IMT-2020

International Mobile Telecommunications-2020 (IMT-2020) has published a white paper on MEC for C-V2X services. It classifies MEC scenarios according to the degree of vehicle-roadside infrastructure cooperation and in-vehicle cooperation. Vehicle-roadside cooperation involves the support of intelligent roadside devices and in-vehicle cooperation requires the support of other vehicle-shared information.

The four broad categories of Use Cases considered are:

(1) Single vehicle + MEC scenario

- Local info broadcast

- Dynamic HD maps
- Onboard info enhancement
- Online onboard diagnostics (OBD)

(2) Single vehicle + roadside unit (RSU) + MEC scenario

- Dangerous driving warning
- Illegal driving warning

(3) Multi-vehicle + MEC scenario

- V2V info bridging
- Sensor sharing

(4) Multi-vehicle + RSU + MEC scenario

- Ramp merging assistant
- Intelligent cross-road
- Large-scale traffic scheduling

3.3 ETSI-MEC

ETSI-MEC has published a document that focuses on a MEC V2X information service in order to facilitate V2X interoperability in a multi-vendor, multi-network and multi-access environment [15]. It describes V2X-related information flows, required information and operations. The document also specifies the necessary application programming interface (API) with data model and data format. A Specialist Task Force (STF) at ETSI is responsible for the specifications defining the cooperative ITS vulnerable road user (VRU) service. The ETSI document defines the VRU-related requirements, as well as the functional architecture of the VRU system that will prevent collisions with other road users. In addition, it analyses the impact of Use Cases, requirements and functional architecture on existing standards, identifying which messages are needed to support the Use Cases.

4 Criteria for selection of Use Cases

Introduction

In the following chapter, a set of criteria for the analysis of Use Case relevance is described. This is intended as a guide to enable readers to understand the selection process and to be able to apply a similar selection process on any other candidate Use Cases. Following this, Chapter 6 of this document then applies these analysis criteria to a selection of Use Cases, as worked examples, to show the potential for deployment and benefits of MEC for different Use Cases. In chapter 7 of this document, there is presented a methodology and analysis criteria to further evaluate deployment options of a specific implementation of a Use Case. Chapter 7 analysis methodology takes into account the more detailed Use Case technical requirements and the corresponding capabilities of the vehicle, MEC and cloud services that may be available.

4.1 Main criteria for MEC relevance

In the following sub-sections, a set of criteria for the analysis of Use Cases is described. The main motivation is to clarify the technical relevance to MEC, i.e. why each Use Case (which has already been studied by 5GAA in WG1 [1][2]) is relevant for MEC. In other words, it should be clarified why MEC is needed for a specific Use Case, or how it provides further benefits, e.g. with respect to situations without MEC (i.e. hosted in a remote cloud). The reader should also note that criteria can be both quantitative and qualitative. While quantitative evaluation can be clear for certain key performance indicators (KPIs), qualitative evaluation on the MEC relevance should be performed by a simple ranking (e.g. high/mid/low) to give an overall assessment.

4.1.1 Interoperability in multi-stakeholder environments

One of the key requirements from auto OEMs for MEC4AUTO is to address the interoperability scenarios between two different OEMs each with its own MNO contract, as well interoperability between two MNOs where only one MNO has the MEC, or variants where two different MNOs have different MECs. The MEC4AUTO architecture (Task 2) for interoperability scenarios should ensure that MEC services should be available even in roaming conditions, by not losing the benefits of low latency and other KPIs required by these MEC services.

4.1.2 MEC performance and related KPIs

In the following, we provide a list of the main Key Performance Indicators (KPIs) and metrics to evaluate relevance to MEC.

Metric/KPI	Description	Beneficiary
End-to-end latency	The latency definition in the scope of MEC4AUTO is referring to round trip time or RTT, measured on the application level (see also [3]). Depending on the service type, the RTT might include very heterogeneous paths (e.g. simple client-server applications, or multi-client communication through server, etc.).	End-user, OEM
Bandwidth saving	A key benefit of MEC is a reduced load on the transport network [4]. This can be measured in terms of network throughput saving (i.e. user plane traffic at IP level) with respect to the usage of remote server applications.	MNO
Security and privacy	Security compliance can be potentially a complex assessment, even hard to be performed in an exhaustive manner. The same considerations can be made for privacy. A qualitative assessment of a Use Case for this metric can be performed.	All stakeholders
Energy efficiency	According to [3], energy efficiency can be defined on the user equipment side (terminals) and on the network side (infrastructure). Energy saving could be relevant in specific Use Cases for smartphones, and for certain RSU/small cell deployments.	MNO (e.g. RSU/small cell) and end-user (e.g. smartphones)
Bitrate guarantee	Besides latency, MEC can also impact the ability to provide bitrate guarantees. This is not intended for quantitative evaluation as it is a qualitative metric. Examples of such evaluations could be attributes like: 'best effort/elastic', 'guarantee required – fixed bitrate', 'guarantee required – minimal bitrate', 'maximum bitrate (no benefit for application if a higher one is provided)', 'event- triggered messages without fixed bitrate requirement', etc.	End-user

The reader should note that, for each metric/KPI described in the above, the actual performance gains provided by MEC should be compared against the Service Level Requirements (SLR) of that specific Use Case. The SLRs are provided by the studies of the WG1 [1].

NOTE: the 'beneficiary' column can also be customised depending on the specific Use Case.

4.1.3 Consumed MEC services

One of the most important benefits of edge computing is the availability and exploitation of local and context information, providing the opportunity to produce (and thus consume) edge services in close proximity to the application endpoint. This approach offers multiple advantages, ranging from improved latency end-to-end, to better management of computing capabilities (by conveniently splitting server processing among MEC and the remote cloud), to improved privacy (through local filtering and anonymisation of sensitive data).

Many APIs can be considered as consumers of edge services. As an example, a good reference is provided by edge service APIs standardised by ETSI MEC2 [5] and 3GPP3

4G [28] and 5G [29] 'exposure functions'[1,2]. These are currently the only international standards available in this space for edge computing. Other examples of APIs can also be seen thanks to the TSC Developer API sub-committee [32] in Akraino Edge Stack, which defines community APIs across various network edge stack blueprints. However, the ETSI MEC standard enables the creation of proprietary APIs which can be 'exposed' by the MEC platform [6]. As a consequence, anyone can build its own API – without the need to standardise it - and 'expose' to higher layer MEC applications through the service registry in the MEC platform [6]. These APIs[3] simply need to be designed by following the MEC service API guidelines in MEC-009 [7].

Regarding the MEC4AUTO Use Cases, each of them can be assessed in terms of impact on edge service consumption, i.e. by describing the possible need to produce (and consume) local services at the edge of the network. For example, a specific Use Case may benefit from the usage of a regional network interface (RNI) API and a location API for quality of service (QoS) predictions – refer to NESQO work item [33] – or a V2X API using vehicular information services (VIS) for addressing interoperability between multiple MNOs (see also MEC vision paper [34]). In addition, customised APIs can be envisaged, e.g. through data collection from cars, sensors, terminals, and suitable local elaboration and exposure through other edge service APIs to the server application.

4.2 Viability of demonstration

The MEC4AUTO Task 3 will cover the experimental/demo/testing activities. It will include the alignment and coordination between the different regional demos. The applications or Use Cases considered for demonstration should work in the same way in the various regions (Europe, Asia and North America). Demos might reuse platforms or solutions already employed in other companies' engagements. End-to-end security should be considered when defining/describing the demo architecture. The Use Cases are also selected according to the viability of demonstrating them following those criteria.

[1] When it comes to consuming service APIs, 3GPP performed a study, called CAPIF [27], on 'Common API Framework for 3GPP Northbound APIs'. This is a general framework allowing an API invoker to access service APIs from the PLMN domain and third-party trusted domain. Nevertheless, the framework is not specifying APIs and it is not necessarily related to the edge.

[2] The following list contains the Exposure Function APIs currently defined (or under definition) by 3GPP: 5G Core Network Exposure Function (NEF) Northbound APIs [29], [30] include Monitoring (UE location, UE loss of connectivity, UE reachability, UE roaming status, number of UEs in area), Reporting (network congestion level in area, background data transfer), QoS and charging, and Traffic Influence supporting routing to/from edge hosts. Except for the last, all are also available with 4G Evolved Packet Core (EPC) with sometimes reduced functionality. The study on eV2X related network enhancements [31] showed the evolution of the NEF Northbound interface to support QoS prediction.

[3] The following list contains the APIs currently defined (or under definition) by ETSI ISG MEC: GS MEC 012: Radio Network Information API [8], GS MEC 028: WLAN Information API [9], GS MEC 029: Fixed Access Information API [10], GS MEC 013: Location API [11], GS MEC 014: UE Identity API [12], GS MEC 015: Bandwidth Management API [13], GS MEC 016: UE Application Interface API [14], GS MEC 030: MEC V2X API [15], GS MEC 033: MEC IoT API [15].

4.3 Analysis of potential value chain and business potential

The MEC4AUTO Task 4 will evaluate and seek to understand the value creation by using MEC for the Use Cases selected in Task 1. It is important to establish a schedule guiding the market launch, including the multi-vendor, multi-network and multi-access environments, and global availability of MEC-application operations, and to adhere to the plan over the course of the action.

5 Analysis of selected Use Cases

Introduction

This chapter provides an analysis of a selection of Use Cases, as worked examples, to show the potential for deployment and benefits of MEC for different Use Cases.

5.1 Use Case 1 – 'See-through'

Based upon the user story defined in WG1 [1] describing see-through characteristics, a driver of the host vehicle (HV) that signals an intention to pass a remote vehicle (RV) using the oncoming traffic lane is given access to a video stream showing the view in front of the RV. In this Use Case, the usage of MEC is beneficial especially due the need for interoperability between the vehicles that participate in the see-through service (this is also emphasised by SLRs in 5GAA WG1 [1]). In fact, MEC solutions and the use of standardised APIs (or more generally APIs 'exposed' in a standard MEC platform) improve interoperability in terms of data exchange. A see-through application can be designed by an independent company, so that the MEC app can run on different MEC servers/systems and the multiple client app instances can run on different cars (belonging to different OEMs), possibly also attached to different network subscriptions. The exposure of edge services through 'RESTful' messages enables interoperability in multi-dimensional scenarios.

MEC-based solutions can also be beneficial for managing video-streaming communication through a MEC server, exchange of communication capabilities (including codecs, and related software updates), but also video elaboration and object recognition on the MEC side (e.g. to help the driver during an overtaking manoeuvre).

Moreover, the presence of MEC could improve the information transferred to the HV (i.e. situation awareness and knowledge gathered about cars in the surrounding area). In fact, this could be extremely critical in situations with multiple cars in the lane, when overtaking an RV could be risky. The MEC server could provide additional information about all cars in the same lane, and transfer the video stream of the first car in the lane, together with the total distance between the first car and the last one.

NOTE: from a performance point of view, multiple metrics are relevant to the quality of the video stream (data rate, latency). Nevertheless, the value of MEC-based solutions rests on the possibility to exploit more context information from the MEC server, e.g. using location API and other information related to the different vehicles in the zone. This means that MEC solutions should simply respect the SLR for video- streaming KPIs.

From a security point of view, MEC is providing a series of features able to improve security on the application layer (these features can be also valid for other Use Cases).

- The MEC-009 specification on 'Generic principles for designing APIs' [7] (applicable to all MEC reference points, including Mp1 and Mx2) defines the use of 'The OAuth 2.0 Authorisation Framework' [35] to secure a RESTful MEC service API. It is used for the RESTful APIs defined by ETSI ISG MEC. Service-producing applications defined by third parties may use other mechanisms to secure their APIs, such as stand-alone use of JSON web tokens (JWT) [17].
- MEC uses also RESTful Transport Security (HTTPs / TLS), by including relevant fields in the security Info structure (Token, KeyID). In particular, TLS uses KeyID to establish secure transport, and HTTP uses Token to establish access authorisation.
- At lower level, Security Info structure is integrated into the VNF (as typically MEC is deployed in NFV environment) and Virtual Machine (VM)/container protects NFV code. Moreover, the MEC infrastructure (mainly hosted in the MNO domain) is considered as trusted environment. This is also helping to improve service level reliability.

Business role: Who buys MEC service and receives business value from MEC?

- MNOs can exploit their network and edge cloud to offer to road operators and to Car OEMs a key point-of-presence of edge instances that can enable interoperable See-through and other high-performing services.
- Road operators and municipalities can improve the quality of life of citizens, and the safety of the population, e.g. reducing accidents, getting e.g. more funds from central governments.
- Car OEMs can integrate this service in their in-vehicle platforms increasing the added value of the vehicle and services package.
- ISVs (app vendors, virtual network function or VNF vendors, MEC vendors, MANO players) and OEMs/ODMs (e.g. Dell, HPE, server vendors and RSUs Vendors like Harman, etc.) can provide the MNOs the hardware, software components of the solution stack that constitutes the service. MNOs will monetise the service through the road operators, city governments/ municipalities who will host the service on their premises (traffic poles, street light poles, universal customer-premises equipment, or uCPE, etc.) as an add-on to the MNO infrastructure in their NGCOs or regional data centres.
- Essentially, the vehicle owners/drivers would use the service and pay for it directly/indirectly through the road operator (e.g. tolling, taxes etc.) or city authorities.
- Latency/response time KPIs are key as an in-car solution has better response time for this case vs. through an MNO service

5.2 Use Case 2 – In-Vehicle Entertainment (IVE)

Based upon the user story defined in WG1 [2], In-Vehicle Entertainment content is delivered to the passengers of a moving or stationary vehicle. This Use Case is applicable to both automated and non-automated vehicles, where in the latter the driver is restricted in the content (s)he is allowed to consume. The content may include video, gaming, virtual reality (VR), office work, online education, advertisement, etc. Contextual information can be embedded in the entertainment media depending on the location of host vehicle.

In this Use Case, MEC is highly critical for improving the quality of service (QoS) performance of the content transferred, e.g. in terms of E2E latency, data rate, etc. In fact, the presence of the MEC app in close proximity to the end-user provides a low latency environment able to improve E2E performance, with respect to a generic remote cloud solution.

MEC is also beneficial due the need for interoperability between the vehicles subscribed to IVE services. MEC solutions and the use of standardised APIs (or, more generally APIs 'exposed' in a standard MEC platform) help interoperability in terms of data exchange. An IVE application can be designed by an independent company, so that the MEC app can run on different MEC servers/systems and the multiple client app instances can run on different cars (belonging to different OEMs), possibly also attached to different network subscriptions. The exposure of edge services through RESTful messages enables the interoperability in multi-dimensional scenarios.

MEC-based solutions can also be beneficial in managing video-streaming communication through a MEC server, and for communication exchanges (including codecs, and related software updates), but also for inserting additional content based on local and contextual information. As an example, some proofs of concept on 'MEC infotainment for smart roads and city hot spots' [18] exploit the presence of MEC, not only to improve the E2E performance of the content transferred to the client app (about 30% delay gain in real- life cases, and huge savings in terms of reduced load on the transport network), but also to enhance it with customised information, possibly also based on the UE location, profile and preferences (of course, based on privacy consent to use these features).

MEC also provides a series of features able to improve security towards the application layer (these features are also valid for other Use Cases).

- The MEC-009 specification on 'Generic principles for designing APIs' [7] (applicable to all MEC reference points, including Mp1 and Mx2) defines the use of OAuth 2.0 [35] to secure a RESTful MEC service API. It is used for the RESTful APIs that are defined by ETSI ISG MEC. Service-producing applications defined by third parties may use other mechanisms to secure their APIs, such as stand-alone use of JWT [17].
- MEC also uses RESTful transport security (HTTPs/Transport Layer Security, TLS), by including relevant fields in the security information structure (token vs. ID). In particular, TLS uses KeyID to establish secure transport, and HTTP

uses tokens to authorise access.

- At lower levels, security information structure is integrated into the VNF (as typically MEC is deployed in that environment) and the VM/container protects the NFV code. Moreover, the MEC infrastructure (mainly hosted in the MNO domain) is considered a trusted environment. This also helps to improve service level reliability.

Business role: Who buys MEC service and receives business value from MEC?

- End customers may buy premium services from content providers enabled by MEC functionalities.
- MNOs and content/service providers can benefit from the introduction of MEC, to offer added/value services.
- The ISV partners the content delivery network (CDN) enablers (e.g. Qwilt, etc.) will play a role here along with the content creation and distribution companies like Netflix, Walt Disney, etc.

5.3 Use Case 3 – Intersection Movement Assist (IMA)

Based upon the user story defined in WG1 [1], in the IMA a stationary host vehicle proceeds straight from stop at an intersection. The HV is alerted if it is unsafe to proceed through the intersection, and warned of a risk of collision due to some of the following events:

- Approaching cross-traffic from the left
- Approaching cross-traffic from the right
- Oncoming traffic intending to turn left

In this Use Case, MEC is beneficial especially due the need for interoperability between the vehicles that participate in the IMA service (this is also emphasised by SLRs in 5GAA WG1 [1]). In fact, MEC solutions and the use of standardised APIs (or APIs 'exposed' in a standard MEC platform) boost interoperability in terms of data exchange, which can be done via Uu or PC5 interfaces. An IMA application can be designed by an independent company, so that the MEC app can run on different MEC servers/systems and the multiple client app instances can run on different cars (belonging to different OEMs), possibly also attached to different network subscriptions. The 'exposure' of edge services through RESTful messages enables interoperability in multi-dimensional scenarios.

MEC-based solutions can also be useful from a scalability point of view, i.e. for the management of multiple messages coming from several vehicles. In fact, according to the SLRs, this Use Case should support high vehicle density in urban situations.

Moreover, MEC can be very useful as the IMA Use Case requires the gathering of a wide set of heterogeneous information (that can be processed in the MEC server):

- Vehicle location
- Lane designations and geometry
- Intersection geometry
- Posted speed limits
- Road conditions (if available)
- Traffic stop signs
- Traffic light signal phase and timing.
- Etc.

As a consequence, the MEC app can be the perfect processing entity, able to build a model of the intersection and of the current situation. This model is common to all vehicles, and the MEC app can conveniently dispatch suitable messages to different vehicles. The resulting saving in terms of signalling (and network capacity) can be huge, especially when considering a dense network of vehicles (according to the SLRs).

In addition, the MEC server can be a solid repository for local and contextual information, which can be read/written in an interoperable way through RESTful messages (for example: information based on local traffic laws and rules controlling right of way through three-way and four-way and unsigned intersections).

MEC also provides a series of features able to improve security up to application layer (these features are also valid for other Use Cases).

- The MEC-009 specification on 'Generic principles for designing APIs' [7] (applicable to all MEC reference points, including Mp1 and Mx2) defines the use of OAuth 2.0
- [35] to secure a RESTful MEC service API. It is used for the RESTful APIs that are defined by ETSI ISG MEC. Service-producing applications defined by third parties may use other mechanisms to secure their APIs, such as standalone use of JWT [17].
- MEC uses also RESTful Transport Security (HTTPs / TLS), by including relevant fields in the security Info structure (Token, KeyID). In particular, TLS uses KeyID to establish secure transport, and HTTP uses Token to establish access authorisation.
- At lower level, Security Info structure is integrated into the VNF (as typically MEC is deployed in NFV environment) and VM/container protects NFV code. Moreover, the MEC infrastructure (mainly hosted in the MNO domain) is considered as trusted environment. This is also helping to improve service level reliability.

Business role: Who buys MEC service and receives business value from MEC?

- MNOs can exploit their network and edge cloud to offer to road operators and to OEMs a key point-of-presence of edge instances that can enable interoperable IMA and other high-performing services.
- Road operators and municipalities can improve the quality of life of citizens, and the safety of the population, e.g. reducing accidents, obtaining more funds from central governments, etc.
- Car OEMs can integrate this service in their in-vehicle platforms increasing the added value of the vehicle and services package.
- Same as Use Case 1.

5.4 Use Case 4 – Vulnerable road user (VRU)

Based upon a US Department of Transport report [19], the case 'Vehicle Going Straight' while a pedestrian is on the road is the highest frequency vehicle to pedestrian crash scenario. Further, according to the Federal Statistical Office of Germany[4], accidents involving pedestrians and cyclists account for around 30% of road traffic deaths in the country.

5.4.1 In-vehicle sensor-based approach

As mentioned in the WG1 Use Case description [1], there are many possible user stories that can be defined for the interaction between vehicle, VRU, and other external entities (e.g. RSU, cloud). In this contribution, the focus is on the particular case where the VRU is not equipped with a device (see also [20]), i.e. the VRU is not V2P-enabled and cannot directly communicate with a vehicle.

In the VRU Use Case descriptions [1], either the presence of infrastructure-based surveillance cameras or V2P-capable VRUs are assumed. The following VRU Use Case describes a complementary approach, which is slightly different to descriptions in [1].

In this VRU scenario, a HV uses its forward-facing, in-vehicle camera to send sensor data (e.g. HD video) concerning the road situation ahead to its machine-learning, enabled application counterpart in the edge cloud. This cloud-hosted application processes the received data and alerts the in-vehicle application frontend of imminent incidents, e.g. the likelihood of a pedestrian walking beside the road stepping into traffic. The vehicle may then decide on appropriate actions and/or notify the driver, e.g. via human-machine interface (HMI).

In this Use Case, MEC is essential for enabling the machine-learning-based application, as it is able to provide dedicated processing capabilities. Such MEC-hosted applications need 'service availability' as well as interoperability across the MEC platforms of different providers/operators/vendors and connected vehicles (belonging to different OEMs).

Moreover, scalability must be ensured and may only be supported with corresponding edge cloud deployments, for example, to cope with a varying number of service users in densely populated areas.

[4] https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/_inhalt.html#sprg249316

Further, the 'local' nature of interaction between edge cloud and vehicle relieves mobile networks of having to provide additional backhaul user data transmissions to centralised cloud entities. Here, video data is locally processed by the edge cloud and does not need to be transferred to a central cloud or data centre for AI processing.

Thus, significant savings in terms of network backhaul traffic and capacity could be achieved.

The vehicle's video data is solely used for analysing the VRU movements and is relevant during service usage (e.g. vehicle usage time). However, as requirements for tracing the decision-making of automated vehicles may appear, there could be a legal/regulatory requirement imposed on the service provider for storing video data feeds for a certain amount of time (e.g. 24 hours)

For enhanced privacy, data may only be locally hosted and deleted after the (legally/regulatorily required) minimum storage time expires. If the legal framework permits, data may be pseudonymised, aggregated, and analysed by central entities for enabling additional services.

The Use Case scope appears to be limited to a one-to-one relationship between the vehicle and 'local' edge cloud, which also informs business analyses comparing the return on investment in on- versus off-board processing. However, the Use Case can easily be extended in the direction of 'collective perception' and 'situational awareness', creating added value for other traffic participants.

Business role: Who buys MEC service and receives business value from MEC?

- MEC HW/SW vendors can provide the relevant components.
- MNO can receive value from application hosting as well as service and communication provisioning, savings in terms of network backhaul traffic and capacity, centralised resources are used more efficiently.
- OEMs can integrate this AI-based service in their in-vehicle platforms increasing the added value of the vehicle and services package.
- Road operators and municipalities can improve the quality of life of citizens and the safety of the population, e.g. reducing the number of accidents.

5.4.2 Infrastructure sensor-based approach

Based upon the WG1 Use Case description [1], there are many possible user stories that can be defined for the interaction between vehicle, VRU, and other external entities (e.g. RSU, MEC). Here, the presence of infrastructure-based sensors (e.g. surveillance cameras) is assumed. Regarding the interaction and communication between the VRU and the external (vehicle, roadside, or network) systems, there are different possibilities (according to [20]):

- VRU is not equipped with a device
- VRU has a device that can only transmit/broadcast data, e.g. a cooperative

intelligent transport system (C-ITS) transmitter attached to a backpack or the safety vest of a road worker

- VRU has a device that only receives (broadcasted) data
- VRU has a device that possesses both transmitting and receiving functionalities

The mobile VRU device can be either stand-alone (e.g. a smartphone), a device integrated in the VRU vehicle (bicycle, motorcycle), or a tethered/connected device (sensors in the vehicle, communication using smartphone, attached via cable or connected via Bluetooth/Wi-Fi).

In this VRU Use Case, an application hosted in the local MEC platform uses the attached infrastructure-based sensors (e.g. surveillance cameras, wireless detection mechanisms) for monitoring and analysing VRU movements (e.g. at crossings). In the event a VRU is predicted to step out onto the road or cross an intersection, the MEC application alerts approaching vehicles that are likely to coincide with the VRU's trajectory.

Awareness notifications are either directly shared with drivers (e.g. notification via HMI) or the vehicles' C-ITS Onboard Unit (OBU) actively monitors VRUs equipped with a corresponding device.

Here, MEC is essential for analysing possible trajectories, predicting potential collisions using infrastructure-based sensor inputs, and alerting approaching vehicles. Sophisticated, AI-based object detection algorithms may require dedicated hardware capabilities for real-time analysis of video streams. Such MEC-hosted applications have clear 'service availability' needs as well as interoperability across connected vehicles (belonging to different OEMs) and MEC platforms of different providers/operators/vendors, as well as potentially connected VRU devices.

Moreover, scalability must be ensured and may only be supported by corresponding edge cloud deployments, for example, to cope with a varying number of service users in densely populated areas.

Further, the 'local' nature of interaction between edge cloud and local traffic participants relieves mobile networks of the burden of having to provide additional backhaul user data transmissions to centralised cloud entities. Here, video data is locally processed by the edge cloud and does not need to be transferred to a central cloud or data centre for AI processing. Thus, significant savings in terms of network backhaul traffic and capacity could be achieved.

The MEC application solely uses the obtained sensor data for analysing the VRU movements and is only relevant for the local service provisioning as well as during service activity (e.g. when VRUs are present). However, as requirements for tracing the decision making of automated vehicles may appear, there could be a legal/regulatory requirement imposed on the service provider for storing video data feeds for a certain amount of time (e.g. 24 hours).

For enhanced privacy, data may only be locally hosted and deleted after the (legally/regulatorily required) minimum storage time expires. If the legal framework permits, data may be pseudonymised, aggregated, and analysed by central entities for enabling additional services.

The presence of a 'local' MEC with access to infrastructure-based sensors (e.g. surveillance cameras, wireless detection mechanisms) as well as communication capabilities extends the Use Case towards 'collective perception' and 'situational awareness', creating added value for other traffic participants.

Business role: Who buys MEC service and receives business value from MEC?

- MEC HW/SW vendors can provide the relevant components.
- MNO can receive value from hosting applications as well as providing services and communications, savings in terms of network backhaul traffic and capacity, centralised resources are used more efficiently.
- Road operators and municipalities can improve the quality of life of citizens, and the safety of the population, e.g. reducing the number of accidents.
- Vehicle owners without in-built VRU protection can improve the vehicle's feature set (based on V2X messages) and receive discounts on their vehicle insurance. Car owners could pay for the service via a corresponding service platform.
- Municipalities could enforce via regulation that only VRU protection- capable vehicles can enter certain areas.
- Municipalities could offer 'data as a service' to insurance companies (according to local privacy laws).

5.5 Use Case 5 – Vehicle Platooning

Vehicles platooning allows vehicles to drive closer than normal in a coordinated manner as a group. Forming such close coordinated vehicular groups or 'platoons' enhances safety and efficiency by reducing the influence of unanticipated driving behaviour and speed variations, which ultimately increases traffic flow and reduces fuel consumption and CO2 emissions.

In this Use Case, the lead vehicle (LV) receives information from the member vehicles (MVs) through the following basic event flow [1]:

- The LV receives information about the road and weather conditions, if available, as well as traffic conditions according to the route that the platoon follows.
- The LV receives information about the status of the MVs (e.g. speed, location).
- Based on the information collected, the LV decides the behaviour and configuration of the platoon (e.g. inter-vehicle distance guidance, speed,

location, direction and intentions such as acceleration, etc.).

- The MVs receive configuration information about the platoon from the LV (e.g. trajectory, speed and acceleration intention).
- The MVs receive speed, position and indications of intent, such as braking and accelerating, of the preceding MV.
- Based on the information assembled and considering its own dynamics and parameters (e.g. tyre pressure), the MV determines an appropriate driving behaviour (e.g. accelerate, brake, maintain speed and distance with front vehicle).

MEC nodes are actively discussed in the literature for the high-density platooning Use Case [36], [37] and the cooperative lane-change scenario [38].

MEC can be used for timely platoon-control information, such as identification of the LV and vehicles in the adjacencies of the MVs, which is then used by them to communicate with other MVs of the same platoon. This identification may be based on global traffic information, weather conditions, etc.

MEC can also be helpful for collecting the status information of one or multiple platoons and low-latency dissemination of this information to the platoon members. The status information may be, for example, the position or speed of the platoon MVs or LV. The MEC can help the LV in its platoon-formation decisions. MEC also helps with platoon en route in advance QoS notifications, where the QoS change along the path of the platoon is calculated at the MEC node and notified to the platoon LV. The LV or the MEC decide whether and how to inform MVs when the platoon reaches an area affected by a QoS notification.

MEC can support platoon reconfiguration based on QoS estimation and/or notification. The platoon reconfiguration includes changes such as MV speed, inter-MV distance, membership (i.e. adjacency list/neighbouring vehicles) or a different LV. MEC can also support in-advance QoS notification to the platoon in order to further improve its performance en route.

The latency of the communication between the MEC node and platoon members is critical for most of the aforementioned uses of MEC in high-density platooning.

Business role: Who buys MEC service and receives business value from MEC?

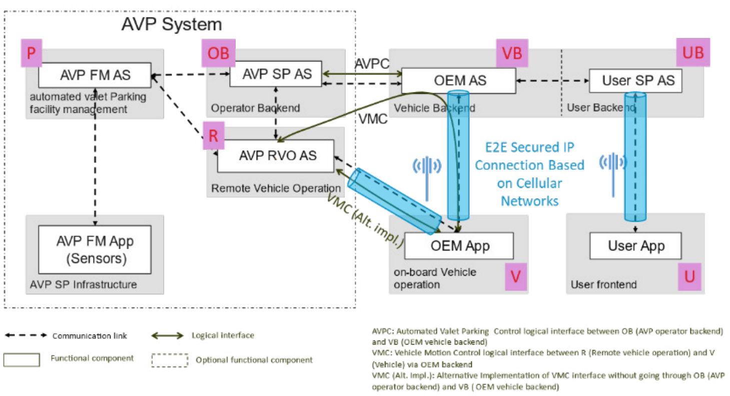
- MEC vendors: Use Case can be enabled by many platforms.
- MNO: more business opportunities, reuse of edge cloud infrastructure.
- OEM: performance: Use Case requires low E2E latency.
- OEM: business: enable edge-hosted applications with low-cost in-vehicle frontend
- Road operator/insurance companies/society (incentives, regulations).
- Platooning service provider: lower telecom costs, increase safety.

5.6 Use Case 6 – Automated Valet Parking (AVP)

Partially or full automated vehicles can be operated by Automated Valet Parking systems that operate these vehicles unoccupied from the drop off area where the driver and passengers have left the vehicle to a parking destination, and also return the vehicles to a pickup area upon the user's request to retrieve the vehicle. Automated Valet Parking (AVP) can include different types of services and functionalities to allow a parking service also to vehicles with an AD level lower than level 4, i.e. the AVPS will perform level 4 automated driving on the vehicles to be parked.

Image below shows the main entities involved in the AVP communications system. In particular, the cellular communications links are highlighted in blue.

MEC node is of relevance to host the 'AVP system' when providing the Vehicle Motion Control (VMC) function. This function requires low latency and high reliability due to it carrying directly the commands to control the motion of the remote driverless vehicle. The AVP System is expected to be implemented locally/regionally to the actual parking facility, and so MEC provides a suitable local/regional access for the function. If the VMC is routed through OEM AS, then MEC provides a suitable local/regional entity for the related OEM AS functions to ensure that latency and QoS requirements can be met.



5GAA App. Layer System Architecture	ISO 23374-1 System Architecture
AVP Service Provider Application Server (AVP SP AS)	Operator Backend (OB)
AVP Remote Vehicle Operation Application Server (AVP RVO AS)	Remote vehicle operation (R)
OEM Application Server (OEM AS)	Vehicle Backend (VB)
OEM Application (OEM App)	on-board Vehicle operation (V)
User Service Provider Application Server (User SP AS)	User Backend (UB)
User Application (User App)	User frontend (U)
AVP Facility Management Application Server (AVP FM AS)	automated valet Parking facility management (P)
AVP Facility Management Application (AVP FM App)	
Interchange Function (IF) (Information broker for service discovery and scalability in real deployment with multiple OEMs and AVP SPs.)	(The Interchange Function is out scope of the ISO standard.)

Figure 5.1 AVP Functional Architecture Entities

Business Role: who buys MEC service and receives Business value from MEC?

- Detailed description in AVP Use Case Description (5GAA T-210023).
- OEM AS and AVP SP AS locating in MEC, for efficient support of logical interface for geographically static garage locations. MEC provides suitable

environment to ensure SLR's (e.g. latency and reliability) for Vehicle Motion Control (VMC) service, connecting between vehicle and RVO AS.

- AVP system operator (parking garage owner/operator) is able to provide stable and reliable service by utilising MEC. This can then be monetised by offering high reliability parking service to vehicle owners.

6 MEC performance evaluation for Use Case deployment

Introduction

This chapter presents a methodology framework and analysis criteria to further evaluate deployment options of a specific implementation of an automotive function applied to a Use Case. This framework takes into account more detailed Use Case technical requirements, and the corresponding capabilities of the vehicle, MEC and cloud services that may be available. The framework is first described in Section 7.2, and then evaluation details are described in Section 7.3. Lastly, in Section 7.4, a set of worked examples are provided, to enable the reader to better understand the proposed evaluation methodology.

6.1 Framework for evaluation of deployment options

The use of cloud technologies and MEC offer great opportunities for flexible deployment of new, advanced or additional functionalities in vehicles. However, the performance impact and related benefits of these technologies to automotive functions in real implementation/deployment settings is not yet sufficiently understood by OEMs. Therefore, to facilitate an assessment by automotive stakeholders of why MEC benefits a specific function, a technical evaluation methodology for MEC performance and impact in the specific automotive context is needed.

A proper discussion on the performance evaluation of MEC technologies for automotive Use Cases should consider the following topics:

- Whether OEMs are observing new developments in computing, internet services, and communication technologies, and their intentions to apply these technologies in the development of future services and products that may require a high level of computational power and large amounts of data.
- How stakeholders will deal with increasing digital/computational complexity in the sector and particular on the deployment side (on-board). This needs to be properly addressed during the whole life cycle of a vehicle (spanning more than 10 years). A clear vision on these issues would reduce costs and increase the quality of experience for customers engaging with new automotive services and functions.
- Appreciating the advantages and additional computational capabilities of technologies deployed on a central cloud and/or edge cloud computing. These solutions also offer a high degree of flexibility and scalability for various vehicle types across the whole life cycle. This advantage is complemented by several operational and maintenance tools allowing an OEM and its

customers to manage, update, and tailor the customer experience.

- Recognising how ongoing enhancements in cellular communication technologies, such as 5G and beyond, reduce and often help to close the communication gap between server entities and vehicles. This development supports high volumes of sensor data, with lower latencies on the radio link, and it offers efficient maintenance options due to features such as software-defined networking, network slicing, enhanced security mechanisms, etc. all performed at the core network level. Thanks to its distributed nature, using the cloud also improves other service aspects, such as energy efficiency and power saving.
- Taking all of these advantages together, technical advances and better availability of cloud and MEC technologies means complex processing can be moved away from (or outside) the vehicle, enabling new and/or improved functionalities and helping to solve related OEM issues.

In practice, several critical aspects must be understood before the rollout of such services and functionalities. These aspects could be, for example, high-level requirements related to MEC and cloud deployment for V2X such as:

- Fulfilment of communication-based functional requirements such as e.g. latency and data rate.
- Fulfilment of automotive requirements such as high mobility and reliability but also availability of the services.
- Software and hardware architecture development, operation, and maintenance.

As a first step, OEMs need to evaluate which service/(sub-)function can be implemented under which conditions and cost (as related to complexity, latency, mobility, reliability, availability, etc.) in vehicles, in MEC (e.g. at UPF, as an application function AF in the MNO core network, and at MNO aggregation points), and in cloud. The goal of this evaluation would be a basic understanding of the feasibility, as shown in Figure 7.2-1, and related to deployment options indicated in Figure 7.2-2. In more detail, Figure 7.2-1 shows the fundamental trade-off between performance (i.e. KPI values against SLR limits) and deployment options (i.e. processing in-vehicle, processing in MEC, processing in the remote cloud). The trade-off also includes a certain cost optimisation, since MEC deployment closer to devices (with better performance) typically implies the deployment of more edge nodes (possibly increasing CAPEX and OPEX), while at the extreme right-side of the figure fewer remote sites imply fewer deployment costs (therefore without the benefits of the edge).

This work aims at delivering a helpful and simple understanding of the links and fundamental trade-offs between function type and complexity/performance related to the processing location in the system.

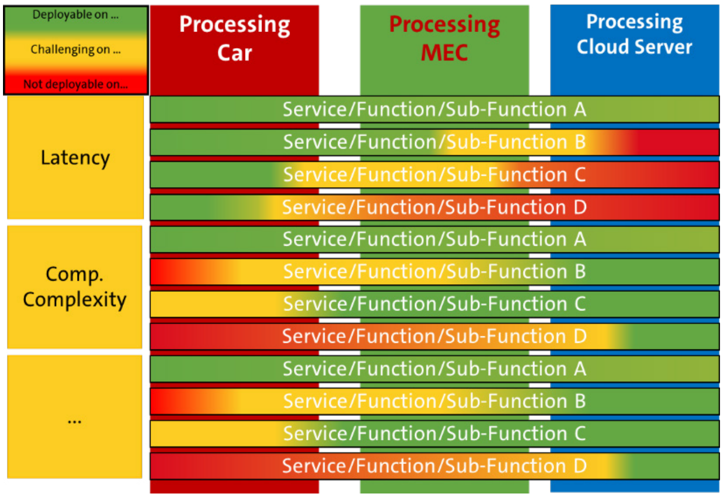


Figure 7.2-1: Proposed evaluation scheme for a full or partial service deployment (trade-off between KPIs and processing options in-vehicle, MEC, or remote cloud); a partial service realisation/example is indicated by a main function or a sub-function of a service on the shown deployment options

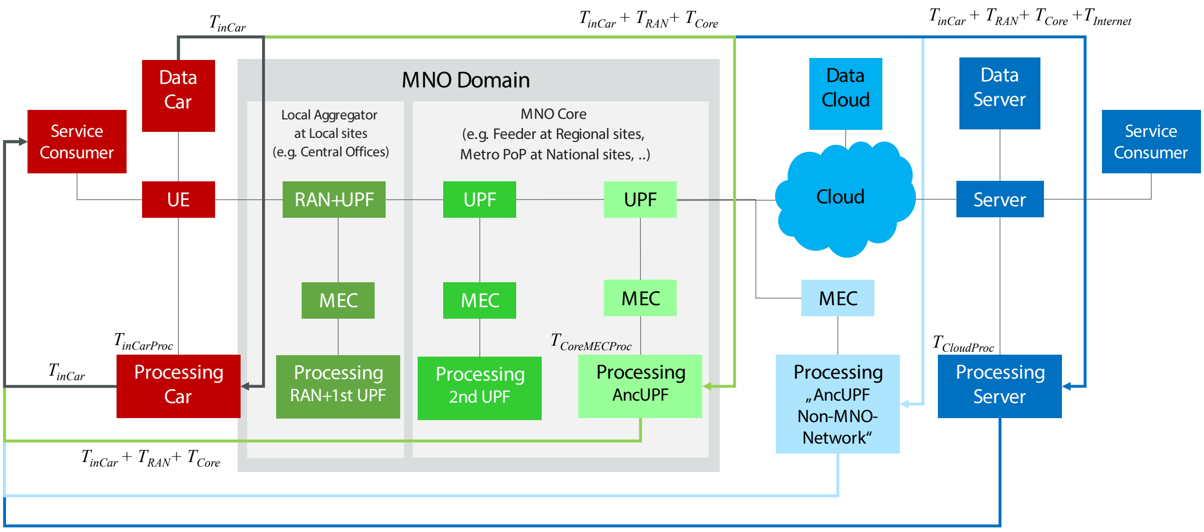


Figure 7.2-2: Simplified overview of several alternative MEC deployment options

In the context of this evaluation methodology, several questions are posed to clarify (from the OEM perspective) on how and why the usage of MEC or cloud can deliver the promised benefits:

- Which SLR limits are resulting from a given deployment system architecture?
- Which gaps or issues are to be resolved to enable MEC or/and the cloud-based deployment of services?
- Which tools/methodology are appropriate for making this evaluation?

The objective of this MEC performance evaluation methodology is thus to provide – for a reasonable number of Use Cases relevant for MEC – a method of better assessing their suitability against relevant KPIs and related SLR values. This is achieved by comparing different deployments (from device to MEC to cloud implementations).

6.2 Criteria related to evaluation options when considering whether to deploy in MEC

As a working assumption, for an accurate and credible MEC-performance assessment, the relevant evaluation criteria need to be evaluated on a case-by-case basis. Depending on the specific Use Case, each evaluation criterion can have a different weighting relevant to the MEC deployment assessment in that particular Use Case. Moreover, the entire assessment should include a clear definition and explanation why a certain criterion is relevant for evaluation in that specific Use Case.

The main evaluation criteria are based on MEC4Auto TR evaluation criteria (Chapter 5 of this document) and additional criteria relevant for Use Case evaluation. Not all of the criteria are relevant for all MEC Use Cases, and they should be evaluated for relevance on a case-by-case basis:

6.2.1 List of evaluation criteria

(1) Computing load (CPU, GPU, resources, etc.) in the vehicle.

a. The computing load increases depending on the number and type of applications/functions. This demand is determined in several dimensions:

- the number of functions concurrently executed,
- the complexity of the functions (from simple process management to multi-dimensional detection and optimisation operations such as xD-filtering and ML/AI), and
- the data processing requirements (very low latency, high throughput, etc.), which are the most decisive aspects.

b. The computing load analysis should focus on the most relevant and decisive parts of a service/application/function/operation. The selection of these parts should result from a review of 5GAA Use Cases, where performance requirements can be seen.

(2) MEC and central cloud operational capacities (such as available CPU and memory resources), including data pre-processing possibilities in MEC, and how to reduce data transmission costs in the backhaul for OEMs (i.e. utilising network process backend expertise, such as cache, compression, routing, and other operational aspects) to achieve the required service KPIs such as capacity/redundancy.

(3) Demand for data transmission (up-/downlink) between vehicle/UE and MEC, and consumption of radio resources by MNOs.

a. Data transmission volume mainly relates to data rate, uplink and downlink combined with the service usage period/duration.

b. Data transmission is impacted by the functional split of the OEM service (or ITS-related automotive services, in general), which in turn depends on the expected communication system and MEC/cloud capabilities. This interdependency has to be continuously evaluated as OEMs gradually increase the MEC/cloud involvement in their services.

(4) Demand for latency or the ability to achieve lower latency is one of the justifications for MEC-operated applications compared to a central cloud. The type of latency involved – i.e. peak/average latency or latency variation (jitter) – is linked to the 'reliability' of the communication/service where, for example, it may be specified that '99.5% of messages are delivered within 100mS', and it is normally expressed as 'end-to-end' latency. So this should include both the processing and transport time that it takes the telecom network to deliver data packets between sender and receiver. The processing time is therefore very much dependent on the processor type and load used, and the transport time is dependent on the routing architecture and distance that the data travels.

(5) Orchestration and maintenance of the function.

a. Orchestration consists of the initialisation of the function in a particular location (e.g. in a MEC or cloud), and requires a management system to ensure the function is set up well with correct parameters. The orchestration function will also close down the function if not required in a specific location. There is normally a specified time required initialise and set up a function, and so the ability to conduct this orchestration within the time period required (i.e. when it is being used) is an important aspect. Maintenance consists of several aspects, such as monitoring, controlling and updating a function. It also includes scalability and flexibility aspects of a service deployment, for both new and deployed vehicles.

(6) Function can use multiple data sources (e.g. from various C-ITS UEs/devices) in real time.

a. Usage of multiple data sources potentially improves a service, or enables new service deployments. However, it also increases the challenges at the network communications level (data transmission, security/privacy, and data processing).

b. The number of data sources, as well as the amount of data, depend on the type of service and deployment in a given region, thus making it a rather UC/deployment/location-specific criteria.

c. When multiple sources are being used (or expected as such) interoperability between users, systems, and data types needs to be evaluated and confirmed. This includes the interoperability of data types and message formats at the data-processing and function level.

(7) MEC interoperability is a key aspect when the serving MNO network is not hosting or directly connected to the MEC; the MNO network and MEC need to be interoperable to provide the expected low latency connection. Also, any sub-function in the vehicle needs to be fully interoperable with the MEC host environment – ensuring that the MEC sub-function has same behaviour regardless of the host MEC environment.

(8) For each function, the combination of MEC/cloud reliability and availability is important, and often requires significant effort in terms of communication system deployment and management.

a. The availability is determined by several dimensions: location area (e.g. cities), time (e.g. public transport schedule), network load due to an event (e.g. sporting event), etc.

b. The reliability is linked to latency (topic (4) above), as it requires that packets of data can be delivered within a given upper bound of time latency, and with a certain probability (e.g. 99.5% of packets are delivered within 100mS upper bound). The remaining 0.5% of packets may be delayed longer than 100mS, or may be dropped by the network, but this is not specified in terms of functional 'reliability'.

c. Within these 'requirements' the MEC/cloud as well as the network should provide the required (communication) services with a minimum level of availability and reliability needed by the function.

(9) Data privacy, the processing of personal data locally and anonymisation of data are vital issues. When deploying a function into MEC or the cloud due care must be taken to protect data privacy and respect relevant regulations and laws. The MEC or cloud environment should be able to provide the required level of data privacy and protection, or the data should be suitably anonymised before submitting to MEC or the cloud. It should also be clearly identified where in the process the data privacy is verified (e.g. during construction of the function, during orchestration into a specific MEC/cloud, during use/transaction process, etc). This may vary depending on UC, type of data, geographical/regional requirement, etc.

(10) Specific security demands may be relevant to certain Use Cases. Similar to the data privacy topic (8), when deploying a function into MEC/cloud due care must be given to meet data security requirements. The MEC or cloud environment should be able to provide the required level of data security and protection, or the data should be suitably encrypted before submitting to MEC/cloud. It should also be clearly identified where in the process the security credentials are verified (e.g. during construction of the function, during orchestration into a specific MEC/cloud, during use/transaction process, etc). Again, this may vary depending on UC, type of data, geographical/regional requirement, etc. Security requirements may also exist for the orchestration and automation functions associated with MEC/cloud, and the evaluation should ensure that these requirements can be met within the deployment option.

(11) Energy efficiency is an important consideration in relation to MEC/cloud developments.

a. Energy efficiency in automotive context differs from conventional handheld device usage and design considerations. One of the main aspects is the accessibility in special areas such as underground parking situations (Reference to CE/LP NWI proposal [1]).

b. More recently, with the move towards Battery Electric Vehicles (BEV) and Autonomous Driving functions (ADAS), the use of high-performance 'compute' resources within the car can consume significant amounts of available energy in the vehicle. So it is also an option to offload intensive compute tasks to the cloud or MEC in certain situations, and thus reduce the use of vehicle power resources. This requires a trade-off between energy resources required to transmit to/from the cloud/MEC versus the energy resources required for the compute workload of the vehicle. This evaluation can also be combined with point (6) and the use of multiple data sources, as compute functions in a central location (cloud or MEC) may also provide a better result/outcome thanks to the use of a wider cross-section of source data.

Table 7.3-1. Simplified table view for the proposed evaluation criteria.

Criteria	Description of needs	Related KPI or values	Use Case relevance	Comments
CPU demand UE (vehicle, other)				
Cloud operation capacities				
Data rate transmission (bandwidth up/ downlink)				
E2E latency				
Orchestration and maintenance				
Various data sources				
MEC interoperability				
Availability				
Privacy				
Security				
Energy efficiency				

6.2.2 Overview of potentially relevant aspects for the evaluation for a potential implementation

The following table provides Use Case examples, criteria and related aspects for consideration:

Table 7.3-2 Relevant aspects to use case evaluation criteria.

Availability **[refer to point (8) in text above]**	**Data sources** **[refer to point (6) in text above]**	**Orchestration and maintenance** **(refer to point 5 in text above)**	**Data transmission** **[refer to point (3) in text above]**	**CPU demand** **[refer to point (1) in text above]**
Areas	Broadcast	Functional safety aspects	Data Amount	Complexity
Cities			High Data Single Source	Operation Per Sec
Urban	Multicast		High Data Multiple Source	Specific Function
Highways				Object Recognition
Specific Traffic Areas	Unicast	Scalability	Data Traffic Pattern	Image Processing
Time				Multi-Dim Filtering
Day-Time	Server		Service Type	Machine Learning
Event-Time			Stream	Security
Duration	Reception Situation		Event High Data	Data Amount
Situation			Event Low Data	Sensor Data (Video, RADAR, LiDAR, etc.)
Number of Vehicles			Low Latency	Massive Object Data
Number of Total Service Requests			High Latency	
Number of Expected Requests				Type of Operation
				Calculation
Roaming				Perception
Cross-Border				Decision
				Steering
Guaranteed Link/ Service Quality				
Functional Safety				Non-Computational Power Consumption

An alternative and more detailed presentation of three of the key criteria ('availability', 'data transmission', and 'CPU demand') is visualised in Figure 7.3-1.

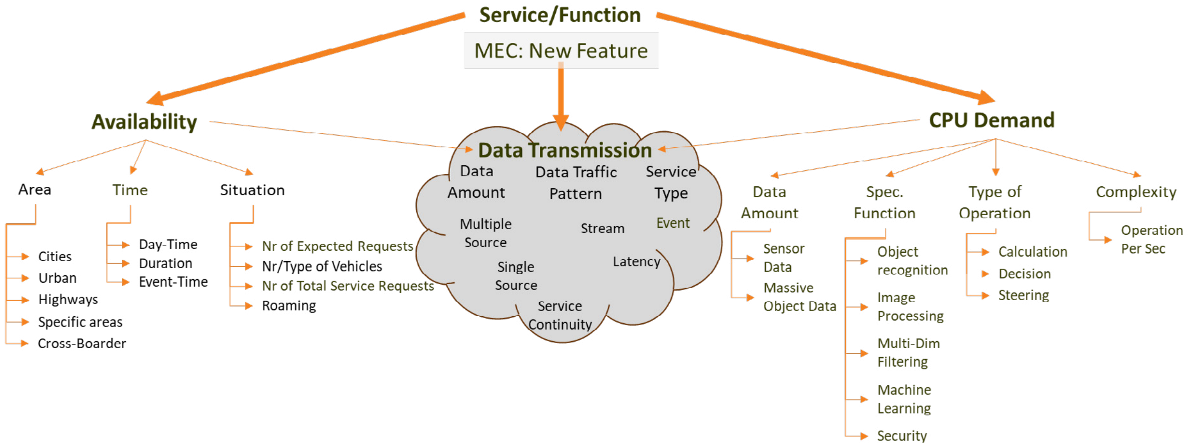


Figure 7.3-1: Expanded visualisation of three key evaluation criteria

6.3 Evaluation process and framework

As discussed in Section 6.2, vehicle manufacturers have increasingly opportunities to deploy similar or extended services/applications and functions either as in-vehicle, MEC, and/or central cloud implementations. These main three service/function design options are illustrated in Figure 7.4-1. The overall evaluation process is recommended to focus on these three reference design options, while important variations can be listed for further analysis and evaluation if required.

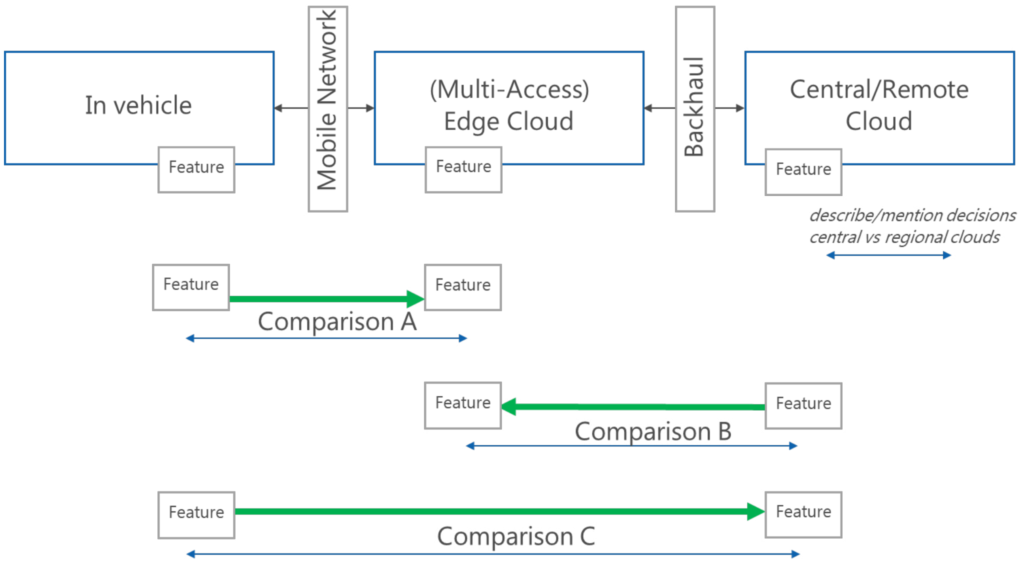
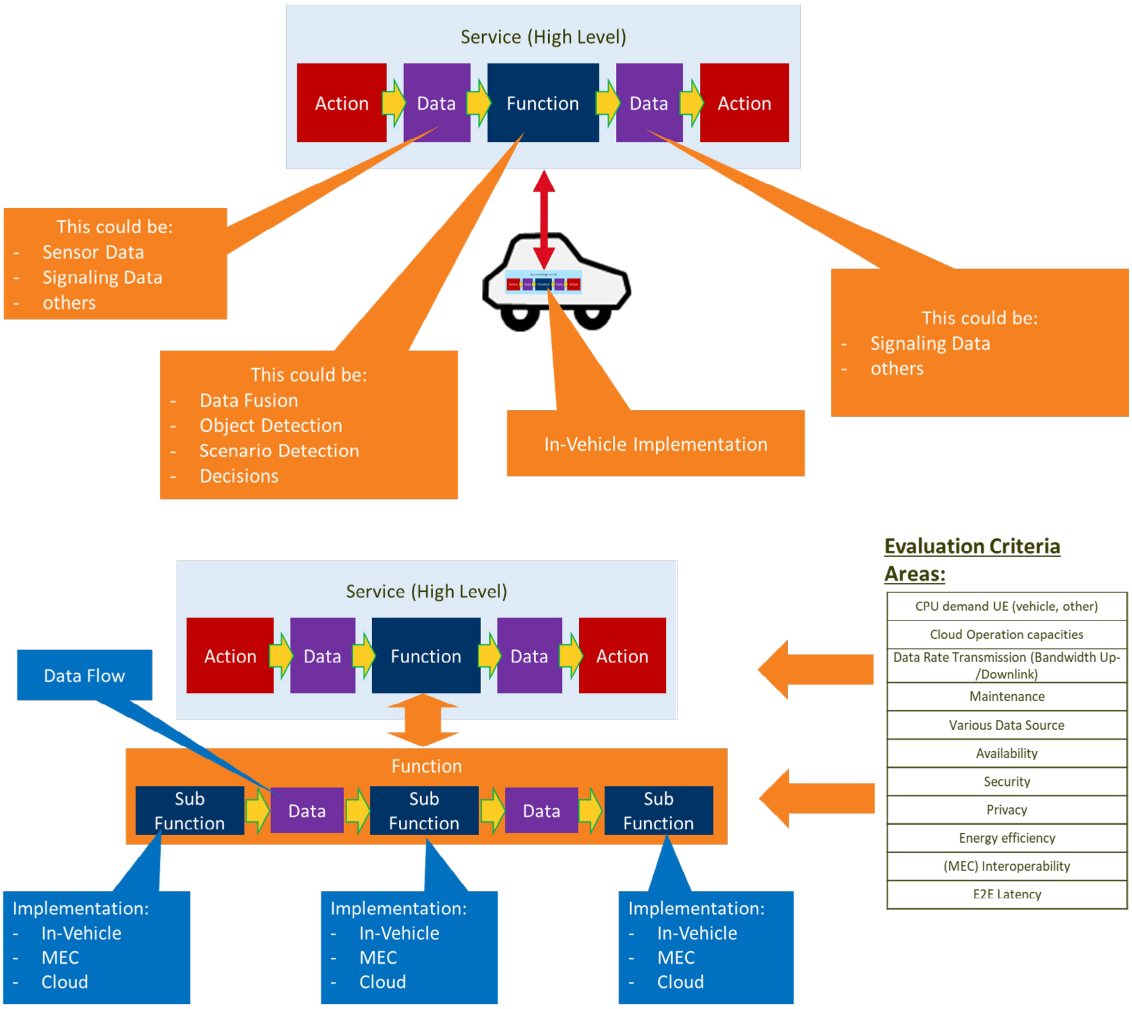


Figure 7.4-1: Terminology and methodology

These three design options lead to the three comparisons shown (A, B, and C) in terms of where the feature (also known as the (sub) function) can be located. The corresponding evaluation, based on the criteria identified in Section 7.3, should deliver the required answers to compare these deployment options.

When evaluating a function and to compare the deployment options, the function itself should be clearly defined. As shown in Figure 7.4-2, the automotive function may itself be broken down into a number of sub-functions. The evaluation may then also be made at different levels, applying the evaluation criteria at either 'function level' or 'sub-function level', and using the corresponding data flow requirements.



- Objective is to define the threshold for implementation of function partially or even fully outside the vehicle.

Figure 7.4-2: Breaking down a service or function

6.3.1 Explaining the basic idea of an evaluation methodology

As a working assumption, for an accurate and credible MEC deployment assessment, the relevance of each evaluation criterion needs to be assessed on a case-by-case basis. Depending on the specific Use Case, each evaluation criterion can have different weighting according to the overall MEC deployment assessment in that particular Use Case. Moreover, the entire assessment should include a clear definition and explanation why a certain criterion is relevant for evaluation in that specific Use Case.

The main evaluation criteria presented in Section 7.3 are based on the initial MEC4Auto TR evaluation criteria (Chapter 5 of this document), and additional criteria identified as relevant for Use Case evaluation. Not all of the criteria are relevant for all MEC Use Cases, and they should be selected for relevance on a case-by-case basis.

After establishing the weighting and relevance of the proposed evaluation criteria, this methodology can be used to determine the key points and deciding factors for the 'comparison A', 'comparison B', and 'comparison C' previously presented. This comparison, made for each of the chosen evaluation criteria, will then indicate the opportunity and possibility to deploy the (sub)function into vehicle/edge/central cloud.

6.3.2 Evaluation of a general structure of a service

Based upon the evaluation criteria presented in the following table, the evaluation methodology has been created.

Table 7.4-1: Evaluation criteria informing the proposed methodology

Criteria	Description
A) Various Data Source	Which sources should/can be used: In-vehicle, several vehicles, cloud sources
B) CPU Demand UE (vehicle, other)	Which main functions are used to provide a service at the required QoS level? What is the amount of data produced/ consumed by the function?
C) Data Rate Transmission (Bandwidth Up-/ Downlink)	Which data rate for which function/sub-function?
D) E2E Latency	Which latency for which function/sub-function?
E) Availability	Which area at which time requires which MEC/cloud service QoS?
F) Cloud Operation Capacities	Which main functions are used to provide a service at the required QoS level?
G) (MEC) Interoperability	How to handle the interoperability aspects?
H) Energy Efficiency	What is the impact on energy consumption (both '*in-vehicle*' and '*in-cloud*')?
I) Maintenance	How to handle the maintenance aspects?
J) Privacy	Which privacy issues need to be handled?
K) Security	Which security issues need to be handled?

The process of this evaluation methodology should consist of:

- Breakdown of the selected function into sub-function level blocks relevant for edge/cloud deployment.
- Selection of evaluation criteria relevant to the Use Case.

- Weighting of the selected evaluation criteria.
- Description of the key issues and factors affecting the selected criteria.
- Four-quadrant analysis of the selected criteria to indicate quick wins and further investigation areas.

Following on from this evaluation, an OEM can then have a clear indication of remaining issues to be investigated, and key points determining the feasibility of deploying the function in or on the vehicle/edge/cloud.

Additionally, the final results are recommended to be presented in a simple and clear four-quadrant graph, as shown in Figure 7.4-3. In this example, the Data Rate Transmission criteria (which corresponds to a certain cost of using the MNO network) is evaluated against the CPU Demand in the vehicle. This four-quadrant graph quickly identifies the following:

- Top Left (high network costs, low benefit in CPU demand), keep the function in the vehicle as cost-benefit does not appear when using cloud/MEC for this function.
- Top right (high network costs, but high benefit in CPU load), shows the feasibility of using cloud/MEC for the function, but needs careful evaluation of the business case.
- Bottom left (low network costs, low benefit to CPU load), shows that it is worth investigating other business drivers for this function, as only the cost-benefit to CPU load may be marginal or not attractive.
- Bottom right (low network costs, high benefit to CPU load), shows that this is a 'quick win' as the evaluation indicates that benefits may be had at an effective cost.

It should be noted that such a matrix may only be needed for the evaluation criteria that have been identified as relevant for the Use Case, and have been given the most significant weighting when the evaluation was made.

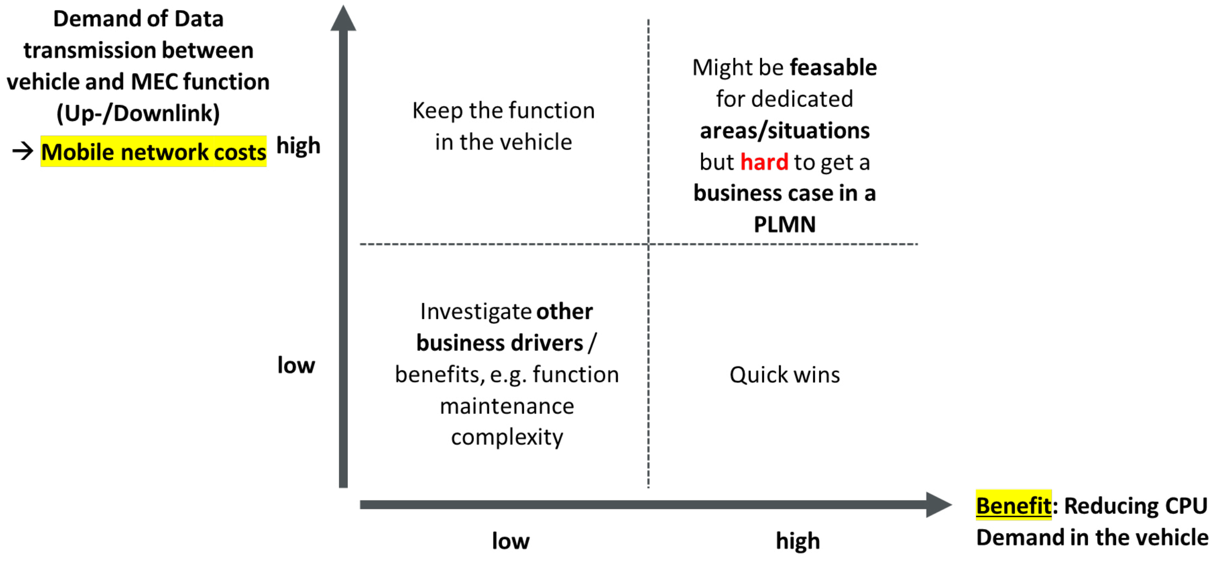


Figure 7.4-3: Matrix representation of proposed MEC evaluation results

7 MEC APIs and introduction of conformance test specifications for V2X interoperability

Section 5.1.3 already described consumption of MEC services as one of the most important benefits of edge computing, thanks to the availability and exploitation of local and context information, providing the opportunity to produce (and thus consume) edge services in close proximity to the application endpoint. In this perspective, the selected 5GAA Use Cases (together with the usage of MEC APIs and their relevance for each Use Case) has been described in Section 6. Based on that description, a summary of some APIs relevant for the Use Cases is provided in the following table.

Table 8.1-1: Outline of relevant Use Cases for select APIs

Use Case	Relevant APIs and information	Notes
Use Case 1: See-Through	MEC application support API [6], V2X API [15], Location API [11]	Context information on all cars in the cluster
Use Case 2: In-Vehicle Entertainment (IVE)	MEC application support API [6], V2X API [15], Location API [11]	Context information on all cars in the cluster
Use Case 3: Intersection Movement Assist (IMA)	MEC application support API [6], V2X API [15], Location API [11]	Context information on all cars in the cluster
Use Case 4: Vulnerable Road User (VRU)	MEC application support API [6], V2X API [15], Location API [11], network API (vehicle/user mobility), compute power (AI-based detection)	Location and network API are suitable for the VRU variant on: 'Infrastructure sensor-based approach'
Use Case 5: Vehicle Platooning in 'steady state'	MEC application support API [6], V2X API [15], Location API [11], RNI API [8], UE app [14]	information to the platoon vehicles, possibly also to multiple platoons
Use Case 6: Automated Valet Parking (AVP)	MEC application support API [6], V2X API [15], Location API [11]	Vehicle Motion Control (VMC) information to multiple vehicles.

As an important clarification, not only ETSI specified APIs should be considered for providing V2X services, but also proprietary implementations are possible (while guaranteeing interoperability). In fact, the MEC009 specification [7] defined a guideline for generic API design, following the RESTful paradigm and messages (see also OpenAPI standard representation[5]). For this purpose, in case of a proprietary implementation of a new MEC API (i.e. not standardised in ETSI), a proper definition of new MEC API resources and error message handling is sufficient (i.e. according to MEC009 guidelines), in order to provide interoperable language for all MEC applications. For further background, the reader can have a look at the ETSI Forge Repository (https://

[5] Note: The OpenAPI Specification (originally known as the Swagger Specification) is for machine-readable interface files describing, producing, consuming, and visualising RESTful web services.

forge.etsi.org), where many API representations are implemented. It is also a suitable tool for SW developers, to test the REST messages and error codes in the consumption of MEC services (the figure below shows an excerpt of the Forge site, for the RNI API).

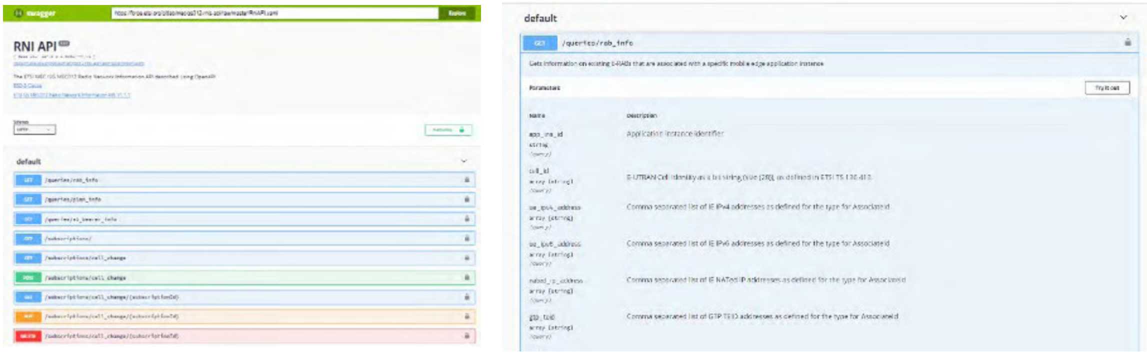


Figure 8.1 – Example of OpenAPI representation of radio network information (RNI) API (Source: https://forge.etsi.org)

When it comes to interoperability in multi-stakeholder environments, compliancy with the standards is essential. For this purpose, recently ETSI published a deliverable [23] listing all functionalities and capabilities required by a MEC compliant implementation. This document also specifies a testing framework defining a methodology for interoperability and/or conformance test strategies, test systems and the resulting test specifications for MEC standards. In addition, the testable requirements are listed and prioritised. More recently, the group also released a stable draft of the MEC API conformance test specification, in three parts [24][25][26]:

- Part 1: Test requirements and implementation conformance statement (ICS)
- Part 2: Test purposes (TP)
- Part 3: Abstract test suite (ATS)

Test specifications are key for all stakeholders (MNOs, but also technology providers and application developers), to verify and test the correct implementation of APIs, in order to ensure proper communication with MEC applications. For this purpose, ETSI is also organising Plugtests events[6] with the aim of offering network function virtualisation (NFV) and MEC solution providers and open source projects an opportunity to meet and assess the level of interoperability of their NFV and edge solutions, while they validate their implementation of NFV and MEC specifications and APIs.

The certification process is outside the scope of ETSI, but starting from this work, the Global Certification Forum (GCF)[7] established at the end of 2018 a task force on MEC

[6] The NFV and MEC Plugtests 2020 (https://www.etsi.org/about/10-events/1683-nfv-mec-plugtests#pane-5/) will include different types of test sessions covering: NFV Interoperability and API Conformance, MEC and MEC-in-NFV Interoperability and API Conformance. The test plans will be based on NFV-TST007, NFV-TST010, NFV-SOL016, MEC017, MEC-DEC025 and MEC-DEC032.

[7] https://www.globalcertificationforum.org/about/organisation.html

(as an initiative triggered by operators), called 'Multi-access Edge Computing Task Force' (GCF TF MEC), with the goal of working on MEC certification, and planning to leverage the above work in ETSI on conformance tests.

8 Conclusions

MEC4AUTO stakeholders have analysed several Use Cases defined by WG1 and down selected five which are relevant to MEC in further analysing Task 2, Task 3 and Task 4. The table below summarises the selected Use Cases for MEC4AUTO.

	Technical criteria and relevance					Preliminary analysis on business criteria and relevance
Use Case	Interoperability (type and relevance, Low/ Mid/High)	E2E Latency (against SLR)	Security and privacy (Low/Mid/ High)	MEC service consumption (list of APIs)	Other technical criteria (e.g. throughput, bandwidth saving, energy efficiency...)	Business role: Who buys MEC service and receives business value from MEC?
See-through	All dimensions (MNO, MEC, OEM). High relevance	Only SLR compliance	High	Location API, context information on all cars	Better service discovery phase, more reliability	MNOs can exploit their network and edge cloud to offer to road operators and car OEMs a key point-of-presence of edge instances that can enable interoperable 'see-through' functionality and other high-performing services. Road operators and municipalities can improve the quality of life of citizens, and the safety of the population, e.g. reducing accidents and obtaining more funds from central governments. Car OEMs can integrate this service in their in-vehicle platforms, increasing the added value of the vehicle and services package. ISVs like app vendors, VNF vendors, MEC vendors, MANO players and OEMs/ODMs (Dell, HPE, server vendors and RSUs vendors like Harman, etc.) can provide the MNOs the hardware/software components of the solution stack that constitute the service. MNOs will monetise the service through the road operators, city governments/ municipalities who will host the service on their premises (traffic poles, street light poles, uCPE, etc.) as an add-on to the MNO infrastructure in their NGCOs or regional data centres. Essentially, the vehicle owners/drivers would use the service and pay for it directly/ indirectly through the city authorities. Latency/response time KPIs are key as an in-car solution because of the better response time for this case vs. through a MNO service.

In-Vehicle Entertainment (IVE)	All dimensions (MNO, MEC, OEM) High relevance	High relevance	High	Location API, context information on all cars	Reduced load on the transport network	End-customers may buy premium services from content providers enabled by MEC functionalities. MNOs and content/service providers can benefit from the introduction of MEC, to offer added-value services. The ISV partners the CDN enablers (e.g. Qwilt, etc.) will play a role here along with the content creation and distribution companies like Netflix, Walt Disney, etc.
Intersection Movement Assist (IMA)	All dimensions (MNO, MEC, OEM) High relevance	Only SLR compliance	High	Location API, context information on all cars	Scalability Saving in terms of signalling (and network capacity)	MNOs can exploit their network and edge cloud to offer to road operators and OEMs a key point-of-presence of edge instances that can enable interoperable IMA and other high-performing services. Road operators and municipalities can improve the quality of life of citizens, and the safety of the population, e.g. reducing accidents and gaining more funds from central governments. Car OEMs can integrate this service in their in-vehicle platforms, increasing the added value of the vehicle and services package. Same as Use Case 1

Vulnerable Road Users (VRU)	All dimensions (MNO, MEC, OEM) High	High	High	Location API, network API (vehicle/user mobility), compute power (AI-based detection)	Scalability, service availability and reliability, savings in terms of network backhaul traffic and capacity.	MEC HW/SW vendors can provide the relevant components. MNO can receive value from application hosting as well as providing service and communication savings in terms of network backhaul traffic and capacity, centralised resources are used more efficiently. OEMs can integrate this AI-based service in their in-vehicle platforms increasing the added value of the vehicle and services package. Road operators and municipalities can improve the quality of life of citizens, and the safety of the population, e.g. reducing accidents.

Vehicle Platooning	All dimensions (MNO, MEC, OEM) High	High	High	Location API Radio network information API UE application	Scalability Service availability and reliability	MEC vendors: use case can be enabled by many platforms MNO: more business opportunities, reuse of edge cloud infrastructure, OEM: performance: use case requires low E2E latency, business: enable edge-hosted applications with low-cost in-vehicle frontend, Road operator/insurance companies/society (incentives, regulations)
Automated Valet Parking (AVP)	All dimensions (MNO, MEC, OEM) High	High	High	Location API Radio network information API UE application	Availability/reliability of network at the AVP operating location.	Expect multi-MNO, multi-OEM, connecting to MEC hosted services of parking service provider. MEC provides suitable environment to ensure SLR's (e.g. latency and reliability) for Vehicle Motion Control (VMC) service, connecting between vehicle and RVO AS. OEM AS and AVP SP AS locating in MEC, for efficient support of VMC logical interface for geographically static garage locations.

9 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1]	5GAA TR "C-V2X Use Cases and Service Level Requirements Volume I", December 2020 Available at: https://5gaa.org/wp-content/uploads/2020/12/5GAA_T-200111_TR_C-V2X_Use_Cases_and_Service_Level_Requirements_Vol_I-V3.pdf
[2]	5GAA TR "C-V2X Use Cases and Service Level Requirements Volume II", January 2021 Available at: https://5gaa.org/wp-content/uploads/2021/01/5GAA_T-200116_TR_C-V2X_Use_Cases_and_Service_Level_Requirements_Vol_II_V2.1.pdf
[3]	ETSI GS MEC-IEG 006 V1.1.1 (2017-01), 'MEC Metrics Best Practice and Guidelines', Available at: https://www.etsi.org/deliver/etsi_gs/MEC-IEG/001_099/006/01.01.01_60/gs_mec-ieg006v010101p.pdf
[4]	3GPP TS 23.501 V16.1.0 (2019-06), 'System Architecture for the 5G System; Stage 2 (Release 16)', Available at: https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/
[5]	ETSI MEC webpage, https://www.etsi.org/technologies/multi-access-edge-computing
[6]	ETSI GS MEC 011 V2.0.10 (2019-06), 'MEC Platform Application Enablement', Available at: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/011/02.02.01_60/gs_MEC011v020201p.pdf
[7]	ETSI GS MEC 009 V2.1.1 (2019-01), 'General principles for MEC Service APIs', Available at: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/009/02.01.01_60/gs_MEC009v020101p.pdf
[8]	ETSI GS MEC 012 V1.1.1 (2017-07), 'Mobile Edge Computing (MEC); Radio Network Information API', Available at: www.etsi.org/deliver/etsi_gs/MEC/001_099/012/01.01.01_60/gs_ MEC012v010101p.pdf
[9]	ETSI ISG MEC 028 V2.1.1 (2020-06), 'Multi-access Edge Computing (MEC); WLAN Information API', Available at: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/028/02.01.01_60/gs_MEC028v020101p.pdf
[10]	ETSI GS MEC 029 V2.1.1 (2019-07), 'Mobile Edge Computing (MEC); Fixed Access Information API', Available at: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/029/02.01.01_60/gs_MEC029v020101p.pdf
[11]	ETSI GS MEC 013 V1.1.1 (2017-07), 'Mobile Edge Computing (MEC); Location API', Available at: www.etsi.org/deliver/etsi_gs/MEC/001_099/013/01.01.01_60/gs_MEC013v010101p.pdf
[12]	ETSI GS MEC 014 V1.1.1 (2018-02), 'Mobile Edge Computing (MEC); UE Identity API', Available at: www.etsi.org/deliver/etsi_gs/MEC/001_099/014/01.01.01_60/gs_MEC014v010101p.pdf
[13]	ETSI GS MEC 015 V1.1.1 (2017-07), 'Mobile Edge Computing (MEC); Bandwidth Management API', Available at: www.etsi.org/deliver/etsi_gs/MEC/001_099/015/01.01.01_60/gs_MEC015v010101p.pdf
[14]	ETSI GS MEC 016 V1.1.1 (2017-09), 'Mobile Edge Computing (MEC); UE Application Interface', Available at: www.etsi.org/deliver/etsi_gs/MEC/001_099/016/01.01.01_60/gs_MEC016v010101p.pdf
[15]	ETSI GS MEC 030 V2.1.1 (2020-04), 'Mobile-Edge Computing (MEC); MEC V2X Information Service API', Available at: https://www.etsi.org/deliver/etsi_gs/MEC/001_099/030/02.01.01_60/ gs_MEC030v020101p.pdf
[16]	ETSI ISG MEC, DGS/MEC-0033IoTAPI' Work Item, 'Multi-access Edge Computing (MEC) IoT API', Available at: https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=56918

[17] IETF RFC 7519: 'JSON Web Token (JWT)', May 2015

Available at: https://tools.ietf.org/html/rfc7519

[18] MEC PoC#13 on 'MEC infotainment for smart roads and city hot spots',

Available at: https://mecwiki.etsi.org/index.php?title=PoC_13_MEC_infotainment_for_smart_roads_and_city_hot_spots

[19] DOT HS 812 312, 'Crash Avoidance Needs and Countermeasure Profiles for Safety Applications Based on Light-Vehicle-to-Pedestrian Communications,' National Highway Traffic Safety Administration, US Department of Transportation, August 2016,

Available at: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812312_v2ppedestrianreport.pdf

[20] J. Scholliers et al., 'Integration of vulnerable road users in cooperative ITS systems', European Transport Research Review, vol. 9, no. 2, DOI 10.1007/s12544-017-0230-3, March 2017, Available at: https://etrr.springeropen.com/track/pdf/10.1007/s12544-017-0230-3.pdf

[21] AECC Document V3.0, 'Use Case and requirement Document (URD)', January 2020 Available at: https://aecc.org/wp-content/uploads/2020/03/AECC_WG1_URD3.0.0_ToC-3.pdf

[22] AECC Technical Report V2.0, 'Driving Data to the Edge: The Challenge of traffic Distribution', July 2020, Available at: https://aecc.org/wp-content/uploads/2020/07/AECC_WG2_TR_v2.0_July2020.pdf

[23] ETSI GR MEC-DEC 025 V2.1.1 (2019-06), 'Multi-access Edge Computing (MEC); MEC Testing Framework', Available at: https://www.etsi.org/deliver/etsi_gr/MEC-DEC/001_099/025/02.01.01_60/gr_MEC-DEC025v020101p.pdf

[24] ETSI GS MEC-DEC 032-1 V2.1.1 (2020-12), 'Multi-access Edge Computing (MEC); API Conformance Test Specification Part 1: Test Requirements and Implementation Conformance Statement (ICS)', Available at: https://www.etsi.org/deliver/etsi_gs/MEC-DEC/001_099/03201/02.01.01_60/gs_MEC-DEC03201v020101p.pdf

[25] ETSI GS MEC-DEC 032-2 V2.1.1 (2020-12), 'Multi-access Edge Computing (MEC); API Conformance Test Specification Part 2: Test Purposes (TP)', Available at: https://www.etsi.org/deliver/etsi_gs/MEC-DEC/001_099/03202/02.01.01_60/gs_MEC-DEC03202v020101p.pdf

[26] ETSI GS MEC-DEC 032-3 V2.1.1 (2020-12), 'Multi-access Edge Computing (MEC); API Conformance Test Specification; Part 3: Abstract Test Suite (ATS)', Available at: https://www.etsi.org/deliver/etsi_gs/MEC-DEC/001_099/03203/02.01.01_60/gs_MEC-DEC03203v020101p.pdf

[27] 3GPP TR 23.722 V15.1.0 (2018-04), 'Study on Common API Framework for 3GPP Northbound APIs (Release 15)', Available at: https://www.3gpp.org/ftp/Specs/archive/23_series/23.722/

[28] 3GPP TS 23.682 v16.3.0 (2019-04), 'Architecture enhancements to facilitate communications with packet data networks and applications (Release 16)'

[29] 3GPP, TS 29.522 v16.0.0 (2019-06) '5G System; Network Exposure Function Northbound APIs; Stage 3 (Release 16)'

[30] 3GPP, TS 29.122 v15.4.0 (2019-06) "T8 reference point for Northbound APIs (Release 15)"

[31] 3GPP, TR 23.786 v16.1.0 (2019-06) "Study on architecture enhancements for the Evolved Packet System (EPS) and the 5G System (5GS) to support advanced V2X services (Release 16)"

[32] Akraino Edge Stack API sub-committee website. https://wiki.akraino.org/display/AK/API+Sub- committee?desktop=true&macroName=view-file

[33] 5GAA, 'Making 5G Proactive and Predictive for the Automotive Industry', December 2017, https://5gaa.org/news/5gaa-releases-white-paper-on-making-5g-proactive-and-predictive-for-the-automotive-industry

[34] 5GAA, 'Toward fully connected vehicles: Edge computing for advanced automotive communications', December 2017, http://5gaa.org/wp-content/uploads/2017/12/5GAA_T-170219-whitepaper-EdgeComputing_5GAA.pdf

[35] IETF RFC 6749, 'The OAuth 2.0 Authorization Framework', October 2012, https://tools.ietf.org/html/rfc6749

[36] Montanaro, U., Fallah, S., Dianati, M., Oxtoby, D., Mizutani, T., & Mouzakitis, A, Cloud-assisted distributed control system architecture for platooning. In IEEE 21st International Conference on Intelligent Transportation Systems (ITSC) (pp. 1258-1265) 2018.

[37] Virdis, Antonio, Giovanni Nardini, and Giovanni Stea. "A Framework for MEC-enabled Platooning." 2019 IEEE Wireless Communications and Networking Conference Workshop (WCNCW). IEEE, 2019.

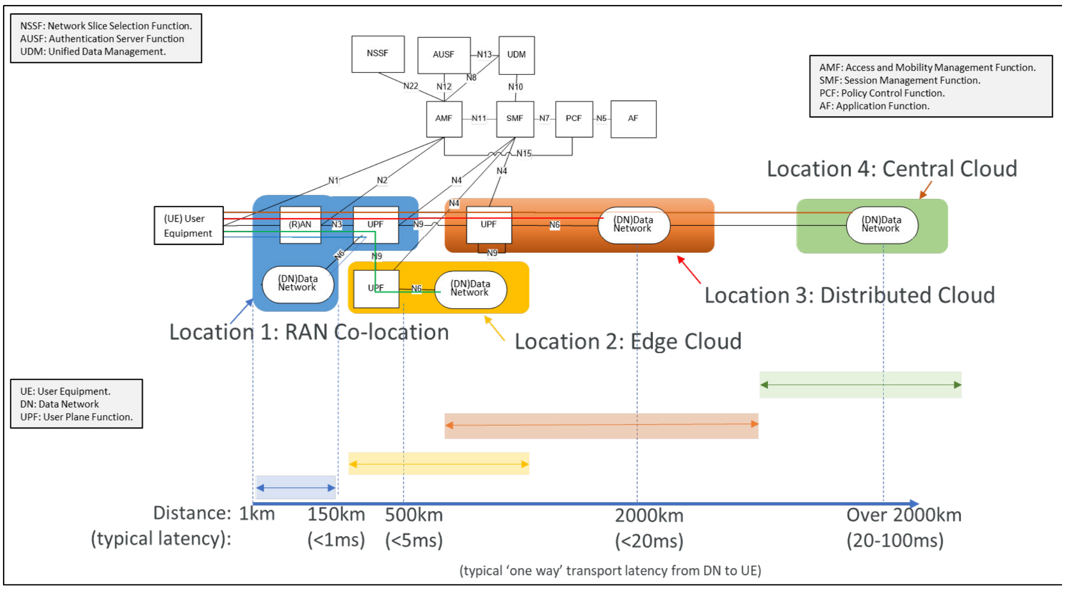
[38] 3GPP TR 22.886 v15.1.0, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on enhancement of 3GPP Support for 5G V2X Services, March 2017

Annex A: Cloud and MEC routing options

Deployment architecture considerations

Reference 3GPP architecture for 5G SA network

- The User Plane Function (UPF) provides the routing of User data between the RAN and external Data Network (DN).
- The Session Management Function (SMF) controls and configures multiple UPF, and can provide simultaneous routes for different data traffic for the same User Equipment.
  - Different routes may need to be configured and maintained for each UE.
  - configures each application to related PDN sessions, using "rules" that map applications (traffic types) to different access routes (PDU sessions within specific network slices, and access types).
- The Policy Control Function (PCF) provides the UE Route Selection Policy (URSP).
  - TS 23.503. Section 6.6.2.



3GPP network architecture for 5G SA is shown above, with four different user plane data routes from the User Equipment (UE) to an external Data Network (DN), via the 3GPP defined Radio Access Network (RAN) and User Plane Function (UPF). Four different generic classes corresponding to the location of the DN which is hosting a requested function are described as follows.

<u>**Location 1**</u> shows the shortest possible route from UE to DN, with the DN co-located with the RAN (the UPF is co-located with the RAN network, and then the DN is also

co-located with the UPF). It is assumed here that all the RAN, UPF and DN are co-located at the RAN site to minimize latency. The RAN Distributed Unit (DU) function is usually co-located or within 20 km of the Radio Unit (RU) on the cell site (due to latency requirements), and the RAN Centralised Unit (CU) is within 150 km of the cell site. So RAN co-location with the CU would require the DN function to also be within 150 km of any supported cell site.

UE to DN latency range may be < 1ms.

Location 2 shows the DN located within an Edge Cloud data centre, which is normally an edge location close to the RAN site (e.g. within 500 km), and intended to support low latency services. Example might be an MNO MEC data centre.

UE to DN latency range may be 1-10 ms.

Location 3 shows the DN located within a Distributed Cloud data centre, which is a cloud location in the region of the RAN site (e.g. within 2000 km). Example might be MNO or Cloud Service Providers regional data centre.

UE to DN latency range may be 5-30 ms.

Location 4 shows the DN located within a Central Cloud data centre, which is a cloud location that may be outside of the region of the RAN site (e.g. more than 2000 km). Example is that the DN is located in a Global HQ Datacentre (e.g. for MNO, vehicle OEM, Cloud service provider) that may be outside the region where UE (vehicle) is used.

UE to DN latency range may be typically 30-100 ms.

Where an 'inter-connect' between DN's is used (e.g. an IXP, Internet eXchange Point) to link from an available DN to the DN connecting to the Central Cloud (e.g. in Route 4, connecting between DN's), then an additional latency may be incurred. This additional delay may typically be also in the range 20-100 ms.

Additional notes

5G Ultra Reliable/Low Latency Communications (UR/LLC) features can achieve lower than 1 ms latency within the RAN 'air interface', for example by using 'self-contained sub-frame'. But it is assumed here that 'normal' data traffic is used, with an additional 'air interface' latency of 1 ms for the scheduling latency between RAN and UE.

The latency figures shown here are given as 'typical' values seen within networks, for the one way Edge/Cloud to UE transport latency. The two factors that determine the latency delay are the propagation along fibre (roughly equal to 5 μs per km for single-mode fibre), and the switching delays for inter-connect (usually a few μs per switch). However, as the distance increases then the possibility to have more complex switching/routing and relaying can create longer delays in the packet latency. So, the overall latency presented here is a 'typical' value seen with modern network infrastructure today, but actual values for the switching delays can vary significantly across different network architectures and implementations.

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of over 115 members, including leading global automakers, Tier-1 suppliers, mobile operators, semiconductor companies, and test equipment vendors.
5GAA members work together to develop end-to-end solutions for future mobility and transport services.
5GAA is committed to helping define and develop the next generation of connected mobility, automated vehicles, and intelligent transport solutions based on C-V2X.
For more information, please visit https://5gaa.org

5GAA Automotive Association