5GAA Automotive Association

Road traffic operation in a digital age A holistic cross-stakeholder approach

5GAA Automotive Association
White Paper

DOCUMENT UNDER INTERNAL UPDATING PROCESS
NEW UPDATE TO BE RELEASED SOON

CONTACT INFORMATION:
Lead Coordinator – Thomas Linget
Email: liaison@5gaa.org

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

VERSION:	3.0
DATE OF PUBLICATION:	3 June 2025
DOCUMENT TYPE:	White Paper
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	24 April 2025

Contents

Contents

1 Executive summary

The societal ambitions of zero fatalities and climate neutrality in road transportation, as well as future ambitions of automated driving require a new approach to the handling of road traffic information. The key stakeholders of the ecosystem, global automotive OEMs, service providers (SPs) and infrastructure owner-operators[1] (IOOs), need new digital methods of operating and interworking.

This White Paper describes a solution-based approach, including methods for scalable digital data exchange, services infrastructure and associated processes to govern operations and both the availability and quality of data. It leverages bidirectional communication channels in a connected ecosystem to deliver static, semi-static and near real-time road traffic and road operation information to all kinds of road users, traffic operators, supporting agencies, and to fleet operators. This is essential in order to deliver on society's demands for safe and efficient road transportation, and for more effective road management using a digital representation of the physical world.

Scalable digital data exchange and services infrastructure are also considered to be essential enablers of new business and cooperation models necessary for the ecosystem delivering the expected benefits to function sustainably. The role of providing data with clear quality KPIs and making them available via well-aligned interfaces in secure environments are underlined.

[1] In this paper IOO is used as an umbrella term for a number of actors, e.g. road authorities, road operators, cities, parking area providers.

Given the needed scale and highly distributed responsibilities, a federated architecture is seen as the most appropriate way to handle the complexity, expected volumes of data and service usage, as well as the demanding latency requirements (depending on the use cases). It also protects and combines the natural business interests of private and public stakeholders in the transport ecosystem. Public-private partnerships and governance are seen as an important instrument to secure investment and ensure the whole ecosystem functions smoothly.

The outlined architecture, including deployment and governance recommendations, has been validated in a number of projects, in different countries, and with many use cases. This White Paper describes verified solutions and includes references to initial operational deployments of parts of the suggested application-level reference architecture. The Annex also provides detailed descriptions of various use cases and demonstrates how the architecture supports their implementation in line with the role of the participating ecosystem stakeholders.

The White Paper concludes with recommendations to public authorities and other stakeholders which should be taken into consideration for the digitalization of the transport infrastructure. Examples are:

- Define a National Roadway Digital Strategy, including the concept of roadway operations data exchanges, and data-sharing guidelines.
- Consider the establishment of a nation-wide information-sharing domain, in a federated structure, with loosely coupled information-sharing instances.
- Investing in digital road infrastructure always needs to be directly combined and implemented with aligned investment in data-sharing and services infrastructure.
- Set up and finance a public-private governance structure and sustained operation to drive stepwise implementation.

To complement the whitepaper, 5GAA have produced a technical report that provides additional details about the system architecture, various deployment options and end-to-end (E2E) implementation examples of V2N2X communications for V2X services.[2]

Additionally, 5GAA have also produced a technical report that describes the V2N2X market from a business perspective. It contains a brief description of market values, stakeholders needs, factors driving market growth as well as an analysis of business models that exist in a number of exemplary V2N2X system deployments.[3]

[2] "Vehicle-to-Network-to-Everything (V2N2X) Communications: Architecture, Solution Blueprint, and Use Case Implementation Examples", available at https://5gaa.org/vehicle-to-network-to-everything-v2n2x-communicationsarchitecture-solution-blueprint-use-cases/

[3] "Business Perspectives on Vehicle-to-Network-to-Everything (V2N2X) Deployments", available at https://5gaa.org/business-perspectives-on-vehicle-to-network-to-everything-v2n2x-deployments/

2 Motivation

The evolution of transportation technologies coupled with innovation in wireless technologies and networks opens our future to continued – and accelerating – improvements in transportation, as the integration of pre-trip and en-route information guides the individual traveler and transportation systems manager toward evermore optimized decisions to positively impact mobility, safety, and environmental stewardship. The key to realizing these improvements will be the effective harnessing of these communications and digitization efforts, and the clever use of data to provide salient, near real-time information to transportation system users and managers. An important feature of this will be an implementable and extensible system that at once derives and provides value to key data stakeholders; the traveler, automotive OEM, communication SP, and IOO.

In the end, the system will hinge on the holistic combination of technologies, digitization, and interoperable systems. This approach clearly resonates with 5GAA's integral mission to develop the components and systems to usher road traffic operations into the digital age. Representing both the automotive and digital spheres, we are pleased to share our point of view, then roll up our sleeves and work with stakeholders to implement solutions and realize the benefits.

3 Evolving steps in road traffic management

As the world industrialized, a well-functioning road network was considered essential for society and the national economy. Governments established dedicated departments for building and maintaining roads and subsequently engaging in active road traffic management.

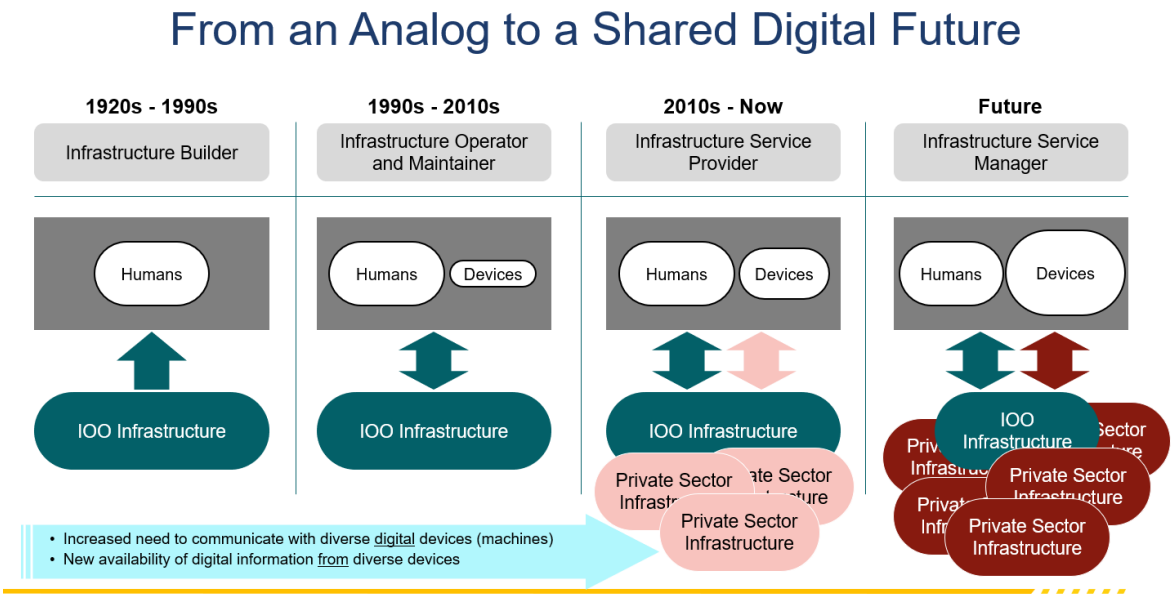

Figure 1: Major evolution steps in road traffic management (Source: FHWA[4])

Over time, static traffic signs have been complemented or replaced by variable and electronic messaging and signs, connected and controlled by the responsible road traffic management and operation center (TOC and TMC). Road traffic and weather sensors were later installed, and CCTV cameras[5] provided traffic operators at TMCs with real-time views of the road traffic situation. This era of **road traffic management in the 'analogue age'** still focused on human drivers as the prime recipients of information. One-way communication from TMCs and traffic signs to drivers and pedestrians was the norm.

The 21st century, however, has been marked by the transition to digital and individualized communication. The internet and cloud operation centers made all kinds of information ubiquitously available. Smartphones became indispensable and navigation apps spread widely. Crowd-sourcing apps help users navigate roads and traffic more efficiently and safely.

[4] US Department of Transportation, Federal Highway Administration, December 2023.

[5] Closed-circuit television (CCTV) cameras are also known as road video surveillance cameras.

These two-way communication channels between 'connected vehicles' and 'drivers' and the 'IOO infrastructure' also introduced a new source of road traffic information. Figure 1 illustrates the major evolution steps in connected road traffic management.

In response to changing consumer and vehicle driver demand for real-time road traffic information and digital navigation services, vehicle manufacturers added cellular communication solutions in their vehicles . Today, 'connected vehicles' and 'connected vehicle services' are first-line users of road traffic and navigation information in concert with human drivers.

Going forward in the evolution to **road traffic management in the 'digital age'** we see 'human drivers' turning into 'connected vehicles' as the new receiver/user. With advances in connected vehicles' onboard sensors, such mobile sensors provide information that is highly relevant to public road traffic authorities and overall road traffic operations. Commercial and societal interest in accessing vehicle and road traffic information is increasing.

Open questions remain: How can we organize the (real-time) exchange of digital information between connected vehicles from different vendors with other road traffic participants, including vulnerable road users, and with the road operators and authorities, their TMCs, and the various agencies in a consistent and agile way? Furthermore, how we set up and operate a 'digital twin' for road traffic management duties?

Further improvements in road safety and traffic efficiency remain essential ingredients for a prosperous society and economy. This White Paper outlines a possible commercially viable and ready-to-deploy solution. An approach that leverages bidirectional communication channels in a connected ecosystem setting. An attempt to balance societal and commercial interests in scalable 'connected vehicle' operations.

3.1 Prime stakeholders and interactions

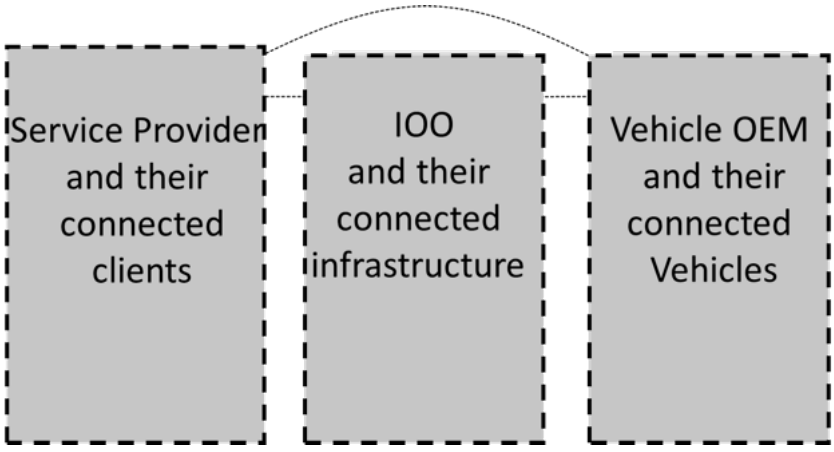

Figure 2: Schematic illustration of SPs, IOOs and OEMs and their operational trust domains

Smarter and better road traffic management in the digital age calls for a networked ecosystem delivering timely and relevant information where it matters, when it matters.

Figure 2 illustrates three stakeholder groups with prime relevance in such a connected ecosystem:

Global OEMs operate their connected vehicle services from central IT backends. They reach their vehicles via factory fitted software modules in a client-server structure. In many cases, the various OEMs operate their connected vehicle services with cross-regional and cross-country IT systems, under their control. Every OEMs' connected vehicle operations constitute a dedicated trust domain, indicated by the grey OEM rectangle in Figure 2.

Service providers adopt a similar client-server operational structure. Their software clients appear most often as smartphone apps on a consumer device. Smartphones and apps are used as 'assisting services' when driving, either with no vehicle integration or with loose vehicle integration (Apple Car-Play, Android Auto, or Mirror-Link). Examples are navigation, road-weather updates, and traffic information services.

Irrespective of where a particular SP client service is executed, its integration into the SP backend system constitutes another trust domain.

Road traffic operation centres (IOO box in Figure 2) are a third stakeholder group. Different to the former stakeholders, IOOs most often have regional responsibilities. Their road traffic operations are executed by one or several road TMCs operating with sub-regional authority or with responsibility per road category. The connected road infrastructure (i.e. client devices) interacts with TMC IT systems using mobile or wired networks. This structure represents a third trust domain considered for simplicity as an 'IOO trust domain' in the above figure.

These three stakeholder groups (SPs, IOOs and OEMs) typically operate their client services in self-contained isolation. Thanks to commercial interest, some stakeholders have established bilateral B2B agreements to better serve their B2C clients. Such B2B agreements translate as proprietary system integration efforts between the B2B partners. Corresponding B2B contracts result in the implementation of a system interaction channel and interface between the actors' operational domains, to facilitate the exchange of relevant road traffic and vehicle safety data.

As a result, enhanced customer services are becoming available in some locations (e.g. a certain city or a local region), from a given OEM, or from a specific road TOC. Such commercially minded relations and interactions are indicated by the dotted lines between the three trust domains in Figure 2.

Despite the collaborative spirit and intention behind these interacting ecosystem partners, the gap to a seamless and consistent vehicle-to-everything (V2X) service experience for 'connected vehicles', driving across a country or nation, remains huge. A gap that relies on more than commercial (or private) stakeholder interests and investments.

To resolve this and facilitate seamless road traffic operations and services requires a new approach to information management and delivery tailored to the individual recipient's requirements and the road context – where and when needed[6]. Real-time and safety related traffic information (RTTI and SRTI) must be included across stakeholders, devices, and jurisdictions. [7]

[6] Example of such an approach in the EU is the Data For Road Safety initiative. For more information, visit: https://www.dataforroadsafety.eu

[7] More information on RTTI and SRTI specifications can be found at: https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/action-plan-and-directive/safety-related-traffic-information-srti-real-time-traffic-information-rtti_en

Given the current spread across regions, countries and road categories, a **national roadway digital strategy** is needed. The strategy should address the need for a regulatory framework covering what data must be made available for public and commercial use, with data quality ensured and privacy preserved, for a nationwide and scalable approach to road traffic management. Other considerations include how to manage mixed fleets with human drivers and automated vehicles as well as cross-regional system operations including financial means and cross-actor communication.

Such a holistic approach must align with public (societal) and private (commercial) interests, and not emphasize one at the expense of the other. The result may emerge as a new way of performing road traffic control and management. That would be a major step towards **road traffic management in the digital age**, involving all road participants and enabling mutual awareness.

Ultimately, this would result in more efficient road traffic operations, with corresponding economic and environmental gains, and most importantly it would lead to fewer accidents, injuries, and fatalities.

3.2 Information flows in a holistic stakeholder approach

The key to success is information that is relevant to individual road traffic participants, available for digital processing, suitable for humans to use, and capable of assisting automated vehicle operation and enriching driver assistance systems. Relevant information emerges from any of the three stakeholder groups introduced in Section 3.1.

The question is, how can such information be delivered with quality and consistency where it matters, when it matters, and at a scale matching the needs of receivers and ecosystem actors, and with millions of 'information elements' processed and delivered within seconds?

A holistic approach must **balance private and public interest in a complementary manner**. This requires a systemic solution and calls for a common regulatory framework dealing with data-sharing and quality aspects, diverse ecosystem partners and their expected behavior, and with system-wide operations and financial considerations.

In a nutshell, **a dedicated trust domain for V2X data-sharing is needed**, equipped with measures that ensure data provided via such a domain can indeed be trusted in practice and at scale, and that any misuse can be detected and treated. This points to the concept of an overarching 'information-sharing domain', as outlined below, which connects the various actors and provides bridges between today's largely isolated ecosystems.

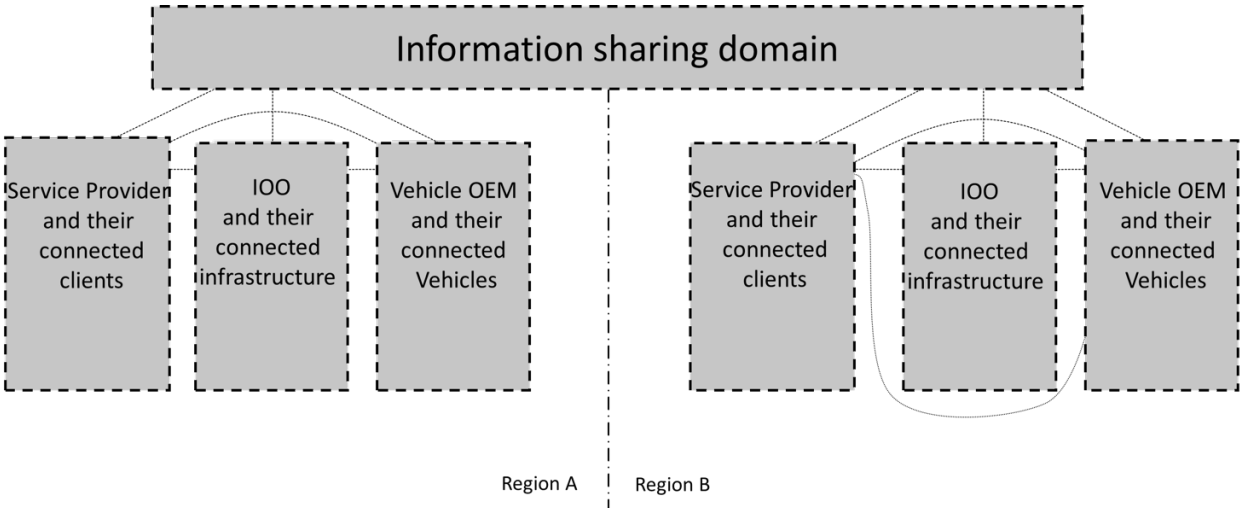

Figure 3: High-level example of an ecosystem for interconnecting actors

The interfaces between the 'information-sharing domain' at Figure 3, and the ecosystem actors point to cross-stakeholder interactions in public relations involving various cross-sector ecosystem partners, as well as operational agencies, such as IOOs or emergency responders. The latter are representing societal demands for safe and efficient road traffic operation.

But what does a C-ITS data-sharing system and distribution architecture look like? How can it be deployed nationwide and across jurisdictions/regions/countries, and among different service providers and OEMs? A system structure which scales and provides resilience by design is needed; one with a common data-sharing governance that ensures data quality and consistency; one that is open in its structure and capable of supporting a wide range of use cases.

Data elements can be sensitive. **Trust in system operation** and in the **provided information** is indispensable. Correspondingly, ecosystem actors and the data elements they share via such a sharing infrastructure should be guided by a so-called data-sharing framework. Such a framework could be shaped in the form of a **common code of conduct** (CCoC) applicable to all ecosystem stakeholders engaging in V2N2X data-sharing.

All actors sending information to (or receiving information from) the overarching information-sharing domain should commit to such a CCoC. Signatories would then receive a digital key/ID giving them permission to access the shared infrastructure. Such an 'actor certificate' should accompany all digital interactions with or within the information-sharing system. It thereby establishes a solid foundation for trust in the information-sharing system operation.

Eventually, the CCoC should provide authoritative guidance on what data can be shared, with what quality and accuracy, and what data usage principles should be applied. Data elements with valid (digital) signatures boost all actors' confidence (sharers and receivers) in the data quality and its origin, delivering greater transparency and overall trust in the exchange. The outcome would see the **information-sharing domain** transformed into a **dedicated trust domain** (see Figure 3).

Information-receiving actors would then have confidence in incoming B2B information, delivered via the managed public information-sharing domain, enhancing their ability to deliver better-quality services to their connected clients. The system technologies

underlying the communication and interaction methods should follow global standards and established IT best practices. (See Annex 7.2 for details.)

Different deployment structures for such an information-sharing domain are possible. All would facilitate 'seamless' data exchange between the various actors. The simplest structure is a centralized data-sharing instance (illustrated in Figure 4-b). Such a structure has been used in many proofs-of-concept (PoC) and C-V2X demonstrations. It is similar to the European concept of having so-called **national access points** (NAP)[8] for C-ITS data-sharing. Given the different flavors of EU NAP implementations, a NAPCORE[9] project has been launched to harmonize the various mobility data platforms in Europe.

The main concerns with such a **centralized operation** are system resilience, single point of contact and dependency issues, and scalability with hundreds or thousands of stakeholders connected, and millions of data elements handled per second or minute. Many of those data elements would carry strong real-time requirements, such as SRTI and RTTI[10] [11].

Another stakeholder interaction structure is a **full mesh network** (Figure 4-a). This structure avoids having a dedicated information-sharing domain and operation instance. However, it requires system integration interfaces with all relevant stakeholders (e.g. all kinds of service providers and road traffic operation centers and agencies). These many integration points call for multiple B2B contracts to be in place. It also largely extends the operational risk/exposure of a connecting actor. With just 100 ecosystem actors 10,000 integration interfaces (with contracts, SLAs and security monitoring) are required per actor. Cost and complexity argue against such ambitions.

Thus, 5GAA favors a networked structure or **mesh federation,** as illustrated at Figure 4-c. This information-sharing structure contains myriad **information-sharing instances** connected to each other in a network topology (e.g. a mesh or any other interconnect structure). It is sufficient for ecosystem actors to integrate only one sharing instance, and with that connection they then gain access to all data handled within an information-sharing domain.

Such a network federated structure embeds resilience by design. It scales easily across geographic areas and jurisdictions and avoids single dependencies. It requires, however, dedicated operational instances that interact under a common governance framework, and deliver internal data-sharing services according to a CCoC.

[8] National Access Points are nodes facilitating the exchange of ITS and ITS-related data. more information available at: https://napcore.eu/description-naps/

[9] National Access Point Coordination Organisation for Europe (NAPCORE) Project, more infromation available at: https://napcore.eu/

[10] Data For Road Safety initiative, available at https://www.dataforroadsafety.eu/

[11] SRTI and RTTI data information, available at https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/action-plan-and-directive/safety-related-traffic-information-srti-real-time-traffic-information-rtti_en

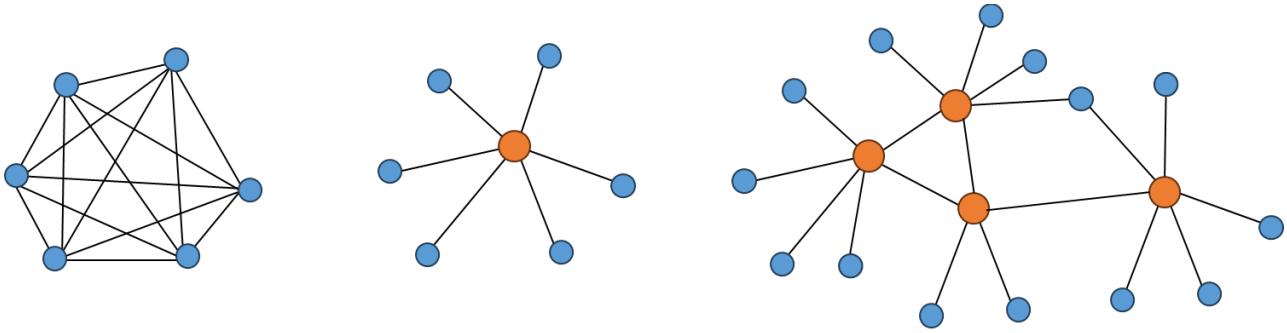

Figure 4: Fundamental interconnect structures and B2B implications

The technical and operational feasibility of a federation-based data-sharing structure, along the lines of Figure 4-c, has been piloted by road traffic operators from Norway, Sweden, Finland, and Denmark as part of the Scandinavian NordicWay[12] project, by the Belgian and Dutch RTOs in the Mobilidata program[13], and by the Talking Traffic[14] partnership, with around 20 use cases deployed[15].

Based on the above considerations, 5GAA recommends the establishment of a **dedicated information-sharing domain**, consisting of loosely coupled **information-sharing entities** in a federated structure shown in Figure 4-c.

3.3 The V2N2X architecture blueprint

The V2N2X application-level reference architecture, illustrated at Figure 5 below, introduces an information-sharing domain in a federated structure for real-time V2X data-sharing. It stresses the demand for system governance (upper dashed box). It includes SPs, IOOs and OEMs as prime ecosystem stakeholders, their operational domains and prime client-server operational components, as well as logical interfaces at the application layer. Application-level interfaces, indicated by the dotted cross-domain lines, are needed for any end-to-end (E2E) implementation of a given cross-stakeholder V2X service.

Interaction interfaces, reflecting commercial B2B relations, are indicated as P3, O2, O5; and if available P4. Interfaces reflecting public interest and corresponding data flows are I4, I1 and I3.

The interface I5 between the networked information-sharing instances in Figure 5 facilitates the federation requirement within the information-sharing domain. The C-Roads consortium[16] has specified[17] interfaces related to the public interest, i.e. details of I4, I1, I3 interfaces and the I5 federation interface. Implementations of such an operating structure have been tested and used in various cross-country cross-IOO live deployments (e.g. in NordicWay, BeMobile, Talking Traffic deployments). The applied

[12] NordicWay road authority data sharing projects and use case implementation available at: https://www.nordicway.net/

[13] Mobilidata programme defined 31 traffic solutions in 5 different categories (intelligent traffic lights, navigation and parking management, Risk and hazard notifications, Traffic rules notifications and Policy support) based on road-vehicle data collection and sharing https://www.mobilidata.be/en

[14] Talking Traffic initiative for smart and sustainable urbanisation, more information available at https://dmi-ecosysteem.nl/en/theme-page-urban-traffic/talking-traffic/

[15] BeMobile C-ITS use cases information available at https://be-mobile.com/solutions/traveler-information/cooperative-intelligent-transport-systems-c-its

[16] C-Roads: The platform for harmonized C-ITS deployment in Europe: https://www.c-roads.eu/platform.html

[17] IP-based interface profile, which is part of release 2.0.x of the C-Roads harmonised C-ITS specifications: https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/Harmonised_text_v2.pdf

meta-data enhancements to raw data-elements turn, in fact, raw-data into information suitable for further processing or final consumption. For more details, see Annex 7.3.

Details on how application-level interoperability can be achieved, from an E2E service perspective, and how meta-data can be used to filter and facilitate mechanisms for data format transcoding, are provided in Annex 7.3. Similar mechanisms facilitate the decoupling of protocol versions and software releases per connecting actor.

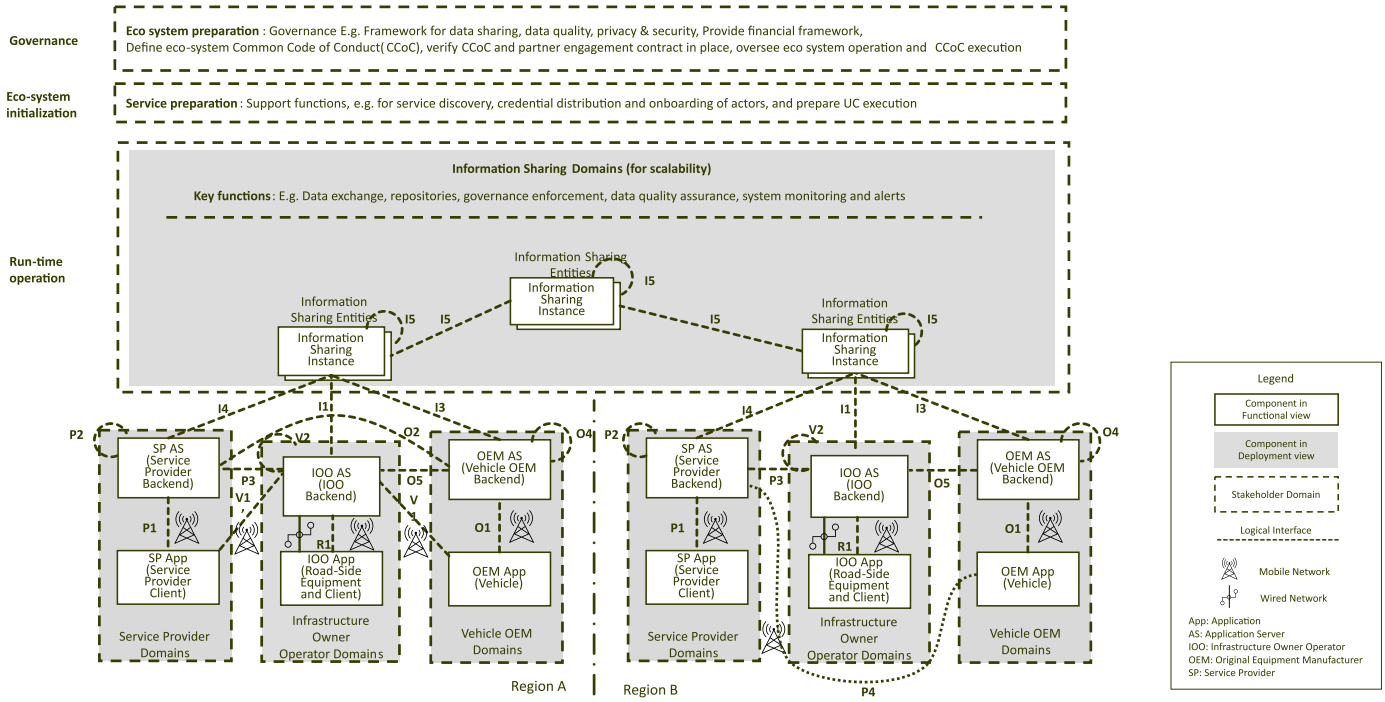

Figure 5: Applied cross-domain application-level reference architecture

The actors, as exemplified in Figure 5, constitute the SP domain, the local road traffic management domain (IOOs) and the vehicle OEM domain. They are the consumers and producers of information. They may share information using bilateral/multilateral agreements, as exemplified with the cross-domain interfaces (O2, O5, P3, P4, V1 and V1'). These actors comprise of a backend 'application server' (AS) with its clients on a cellular connected device (app). Within an actor's domain the corresponding interfaces (P1, R1[18], O1) are internal and therefore can be designed according to the actor's needs.

For a larger ecosystem, especially comprising many information-sharing entities, governance mechanisms are required, as indicated by the dashed boxes across the top in Figure 5. **Governance** would for example comprise a 'governing body' that sets the rules (e.g. a framework for data-sharing, data quality, privacy and security). It provides the financial framework and defines an operational CCoC reflecting the public interest in the cross-stakeholder V2X information-sharing. **Key functions** comprise, for example, databases for static or semi-static data, information about system status, operation and data-quality monitoring, including alert management and information about internal operational events in the system.

[18] As indicated in Figure 5, R1 that connects the IOO AS with the IOO App (e.g., road-side equipment including road traffic light controllers, variable electrified message signs, and sensors, or parking facilities) in the IOO domain may be implemented using cellular network, wired network, or combination of both.

Only those **ecosystem stakeholders agreeing to a CCoC** for information-sharing, -retrieval and -usage, and committed to behaving according to the CCoC principles, should be allowed to access the information-sharing domain and integrate their IT systems with an information-sharing instance.

Upon confirmation of compliance, an ecosystem actor will receive a digital certificate and become an authorized V2N2X actor. Having signed the CCoC, a system function linking the validation of a joining actor to a digital certificate for that actor is part of the '**ecosystem initialization**' functions, indicated by the second horizontal dashed box in Figure 5.

To **enable automated data processing** methods, such as publish-subscribe data selection methods, search and filter procedures, data-routing and query-forwarding algorithms, or automated data format and protocol conversions, all data elements provided by a data source should be enhanced with a meta-data record describing the nature, purpose, and format of a given data element. Such **meta-data enhancements turn raw data into information elements.** For more information about interoperability and meta-data see Annex 7.3.

Adding a payload agnostic message queuing protocol beneath all communication to or from the information-sharing instances in Figure 5 would **decouple the real-time systems of all such instances and of all connecting ecosystem actors.** See Annex 7.2 for more details on recommended IT technologies and best practices.

Every information element that an authorized ecosystem actor provides to the information-sharing domain should be traceable to its source. This is to provide any receiving party information about the source of and responsibility for provided information. An ecosystem service provider who enhances information from the information-sharing domain – and injects a newly created (enhanced) information element back into it – becomes the new owner of that enhanced information element. This helps to create trust in the information. Various trust models can be used to achieve this, one way would be based on secure connections between trusted actors bound by agreements, each actor allocates an identifier to be added to the information, and communication is to be monitored and logged.[19] Another way of linking data elements (including meta-data) to the sender is by having the message content signed with a digital certificate; in this case, presumably the certificate that was provided to the corresponding actor in the ecosystem initiation phase.

Having only signed information elements, from trusted actors, handled within the information-sharing domain strongly enhances the **trust and confidence** that all ecosystem actors have **in using such information for their own clients and operations.** Data quality issues, should they occur, can be reported to a quality assurance system with evidence and source information attached. Such operation principles **turn the information-sharing domain into a dedicated trust-domain** for data- and information-sharing across independent ecosystem parties.

[19] Section 6.4.2 of the 5GAA Technical Report "Vehicle to Network to Everything (V2N2X) Communications; Architecture, Solution Blueprint, and Use Case Implementation Examples" provides technical solution details for handling security and privacy requirements in the information sharing domain.

4 Reference use cases and best practice examples

All the various real-time elements and instances of the suggested application-level V2N2X reference architecture, illustrated in Figure 5, have been tested in live deployments by different projects and initiatives, or they are presently in live commercial operation via B2B agreements between ecosystem stakeholders and actors. 5GAA is thereby confident that the suggested approach is technically feasible and adheres to the various deployment and operational requirements.

In Section 3.3, we have already provided links to reference implementations of the federation concept, depicted as the information-sharing domain in Figure 5. These links point to technical specifications, applied to many V2X use case implementations. The reference links also include use case descriptions and video feeds.

Next to these reference implementations, with a focus on the information-sharing mechanisms, there are also several commercial V2X deployments. The matching of such deployments to the V2N2X reference architecture is described in greater details at Annex 7.1.

In commercial operation:

7.1.1 UC-1 Road operator work zone warnings (including maintenance vehicles)

7.1.2 UC-2 Crowd-sourced data collection (e.g. road maintenance)

7.1.3 UC-3 Crowd-sourced wrong way driver alert

7.1.4 UC-4 Emergency vehicle awareness – Talking Traffic NL

7.1.5 UC-5 Private initiative for smart city and connected infrastructure

Tested in a live deployment:

7.1.6 UC-6 Protection of unconnected VRUs

5 Deployment and operation aspects

Large-scale V2N2X deployments are ecosystem efforts requiring thorough groundwork and attention. Without that, participation and hence impact will be limited.

Existing deployments show that initial agreements on the following matters are highly recommended:

- Set of launching use cases, preferably those that can be deployed nation-wide within a reasonable time
- Interfacing, data standards and messages to use
- Security arrangements (e.g. organization certification, security framework compliancy, and technical measures)
- Service definitions, including service levels
- Connectivity-, data- and use-case quality levels
- Conditions for data-sharing and consumption (e.g. privacy preserving agreements, ecosystem contribution, FAIR[20] data principles or contracts)
- Optional but recommended are testing standards and certification procedures

Ideally these matters are initially agreed upon and managed during operation, e.g. by a public-private governance structure involving authorities and industry experts.

[20] FAIR: findability, accessibility, interoperability and reusability: data principles defined by Wilkinson, Dumontier, et al, in "The FAIR Guiding Principles for scientific data management and stewardship", March 2016, available at: https://www.nature.com/articles/sdata201618

Governance and operation example: Talking Traffic, The Netherlands[21]

Talking Traffic is a successful innovation program to bring digital infrastructure and connected vehicles to large-scale deployment in The Netherlands, leveraging the existing cellular networks.

In the preparation phase of the program a group of authorities, led by the Ministry of Infrastructure and Waterworks, agreed on a set of use cases suitable for their country, mainly around signaled intersections. These use cases were: Priority/pre-emption for designated road users, leveraging vehicle probe data for improved traffic flow efficiency, and GLOSA/TTG.

With the use cases selected, a public-private governance structure was created consisting of:

- A committee of senior policymakers responsible for authority alignment
- A committee of subject matter experts from the authorities, involved in operational aspects
- A joint body of senior representatives from the industry and representatives from the previous mentioned committees, called the Strategic Council (SC)
- The Change Advisory Board, a committee open for participation by all stakeholders

This structure worked together to create the initial Common Code of Conduct[22], consisting of technical and non-technical arrangements:

- Examples of non-technical elements:
  - Standardized privacy (data processor) agreements
  - Long-term funding for the governance structure (small deposit by authorities for every smart intersection, fund controlled by the SC)
- Examples of technical elements:
  - Agreement on message types and usage (e.g. ETSI C-ITS messages)
  - An open standard for the exchange of real-time messages with field equipment called the C-ITS subject interface (SI)[23], adopted by all suppliers of traffic light controllers
  - Quality levels/KPIs on uptime, connection quality (clock synchronization, latency), message conformity and use-case quality
  - Latency budgets, for the individual components as well as a target for the end-to-end latency
  - Standards on interoperability (open interfacing only, no custom end-to-end solutions, no silos)
  - Security arrangements: TLS, PKI, MFA etc.

During these processes the Ministry of Infrastructure and Waterworks procured a platform (information-sharing instance) for data exchange, data quality control, stakeholder dashboarding, governance, and the enforcement of security and privacy – open for use by all participating authorities.

After the initial development phase, a large-scale deployment of the services followed. By October 2023, this program connected field equipment and traffic management from over 50 authorities with over 25% of motorized vehicles in The Netherlands. Data is shared bi-directionally leading to a daily exchange of over 1.3 billion messages.

During the deployment many lessons were learned and significant changes and additions were made in the initial CCoC. With the foundation in place, a set of inter-urban use cases was selected for large-scale deployment, such as wrong way driver warning, emergency vehicle awareness, jam-tail warning, and road inspector vehicles/shock absorbers in action. Also, a testbed was created and a process for certification of digital services with field equipment was realized. All these changes where initiated and supervised by the public-private governance structure.

Annex 7.4 provides additional details about best practices on deployment and operation.

[21] Talking Traffic website: https://dmi-ecosysteem.nl/en/theme-page-urban-traffic/talking-traffic/
[22] Many elements of the CCoC can be found at https://www.crow.nl/thema-s/smart-mobility/landelijke-ivri-standaarden
[23] C-ITS Subject Interface: https://www.citsinterface.org/

6 Recommendations

Zero road fatalities, climate neutrality and ambitious automated driving goals require a new approach to handling road traffic information. Service providers, OEMs and IOOs thus need new digital ways and strategies to enhance the way they operate and work with one another.

A digital data exchange, services infrastructure and associated processes are the core of those changes. Given the needed scale and the highly distributed responsibilities, a federated architecture is seen as the most appropriate way to handle the complexity and expected volumes of data and service usage.

5GAA recommends the following steps to progress on the path towards a fully digitalized road operations management:

- A comprehensive national data-sharing strategy (including data privacy and security) needs to be part of any V2X deployment plan, including the use of cellular networks for wide area service availability.
- Investment in digital road infrastructure needs to go hand in hand with investment in data-sharing infrastructure, suitable to enable a wide variety of services relying on data being available in machine-readable form, with corresponding meta-data attached.
- Establish clear guidelines and measures toward the digitalization of road transportation systems and operation.
- The framework for data-sharing between actors should build on the use of standard IT technology, harmonized to ensure interoperability and onboarding of new ITS actors and mobility service providers.
- Set up and finance a public-private governance structure and sustained operation to drive the stepwise implementation, and to ensure sustained nationwide operation.

Data availability is a prerequisite for successful implementation:

- IOOs and mobility service providers in the public sector (e.g. bus operators) need to make traffic-related digital twin information available via public interfaces.
- Clear priorities and timelines need to be set with respect to data scope and availability – e.g. starting with safety-related traffic information and real-time traffic information[24] examples[25]: road works (semi-static data); and moving road works, accident locations, road worker locations (dynamic data), traffic flow information, road hazard warnings, etc.

[24] More information on RTTI and SRTI can be found at: https://transport.ec.europa.eu/transport-themes/intelligent-transport-systems/road/action-plan-and-directive/safety-related-traffic-information-srti-real-time-traffic-information-rtti_en

[25] Data for Road Safety (EU) live map: https://data-intelligence.post.lu/dfrs/

- IOOs should ‘stimulate’ special fleet operators (own vehicles, emergency vehicles, etc.) to provide data to publicly available interfaces – e.g. through regulation, contractual obligations – and in a consistent, nationwide way.
- Stimulate other mobility and transportation service providers to share road safety-related data for the greater good of society.

Data accessibility needs to be organized by the recommended public-private governance structure to enable scale and to attract globally acting players such as OEMs:

- Provide federated data-sharing capabilities with nationally aligned interfaces and ensured data quality.
- Organize the data-sharing infrastructure, operation, availability, real-time capabilities, data throughput/scalability as well as comprehensive and trustworthy data security mechanisms.
- Organize and finance the data-sharing infrastructure operations, including data quality assurance procedures, testing, and certification.

For further information, please contact 5GAA and explore the 5GAA website (5GAA.org).

7 Annexes

7.1 Use case reference implementations

7.1.1 UC-1 Road operator work zone warnings (including maintenance vehicles)

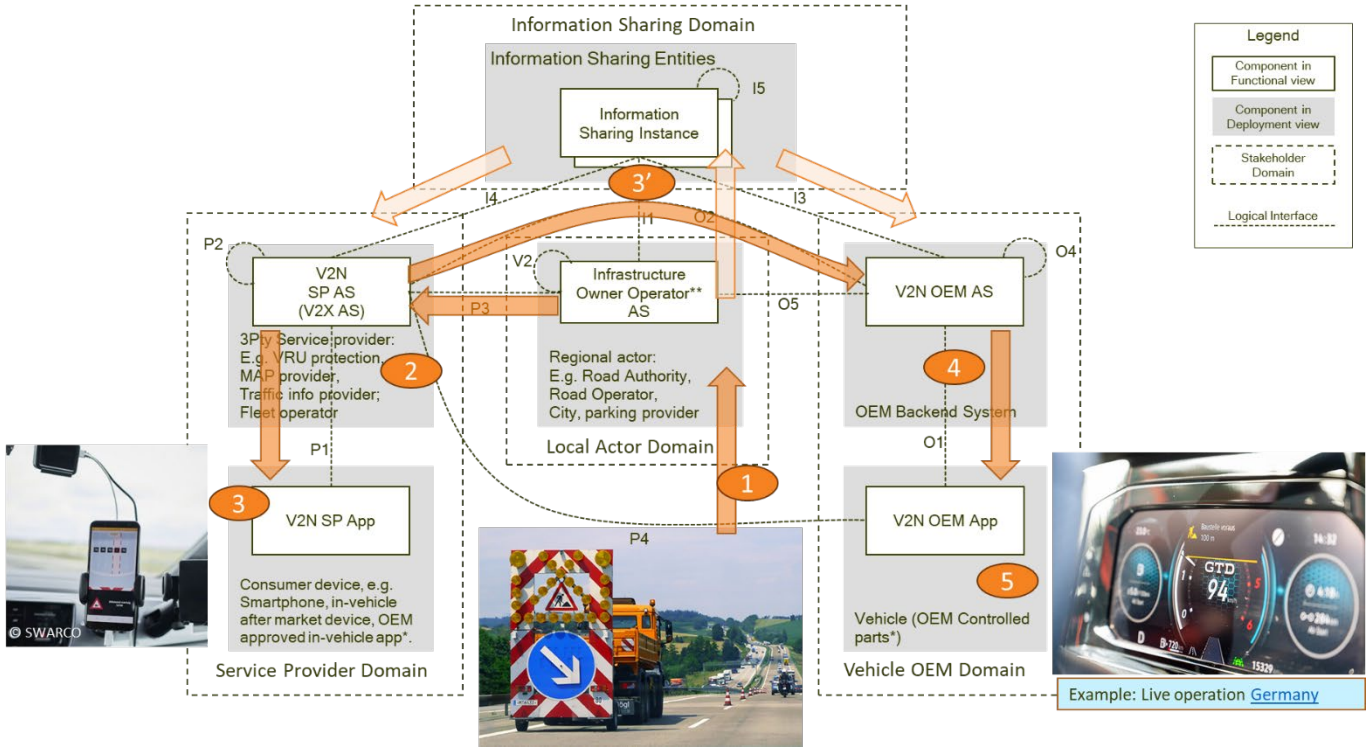

Figure 6: Work zone warnings (including maintenance vehicles)

In Figure 6 the actual information flow is overlaid on the 5GAA applied application reference architecture.

The use case illustrates a maintenance vehicle periodically updating its backend system (e.g. the road operator) about its location. For example, using Basic Safety Message (BSM), the backend system shares information about the road works underway with OEMs and service providers it has prior agreements with. The OEM and SP backend systems forward information about the maintenance vehicle to respective clients (e.g. connected vehicles and smartphone clients) affected or heading towards the road works. Finally, the clients visualize the information (e.g. live operation in Germany[26]).

To include multiple OEMs, service providers and road operators in the scenario, a more scalable solution would be required, i.e. use of an information-sharing domain for sharing related data and information. In such a scenario the road operator publishes the information about roadworks as an 'instance' using the 'I1' interface, e.g. using

[26] Example of a visualization on vehicle dashboard in Germany: https://www.main-echo.de/ressorts/politik/schnelle-warnung-vor-baustellen-art-7732471

advanced messaging queuing protocol (AMQP) including meta-data that identifies the format of the message (e.g. ETSI DENM, BSM type 2), the location of the roadworks (e.g. latitude/longitude, and/or an area identified by quadTree tiles [27]), the originator of the message, etc. This meta-data then allows backend systems to subscribe to 'I3' and 'I4' interfaces for information of interest and receive notification when something matching the subscription filter is published. For more information about interoperability and meta-data see Annex 7.3

The 'I5' interface may be used for federating data, e.g. if an OEM backend system (OEM AS) is connected to an information-sharing instance other than the producer of the data, the OEM backend can still subscribe to this information published by a certain road operator.

One way to interact with and within the **information-sharing domain** is described in the C-Roads 'IP-based interface profile', which is part of the 'Harmonised C-ITS specifications for Europe' and provides a profile for use of AMQP. (C-Roads terms for I1/I3/I4 and I5 interfaces are 'BI' and 'II' respectively).[28]

[27] **QuadTiles** are a geo-data storage/indexing strategy, often referred to as hierarchical binning. For more infromation visit: QuadTiles - OpenStreetMap Wiki

[28] The C-Roads 'IP-based interface profile' can be requested at: https://www.c-roads.eu/platform/get-in-touch.html (Free of charge, but requires registration to receive updates.)

7.1.2 UC-2 Crowd-sourced data collection (e.g. road maintenance)

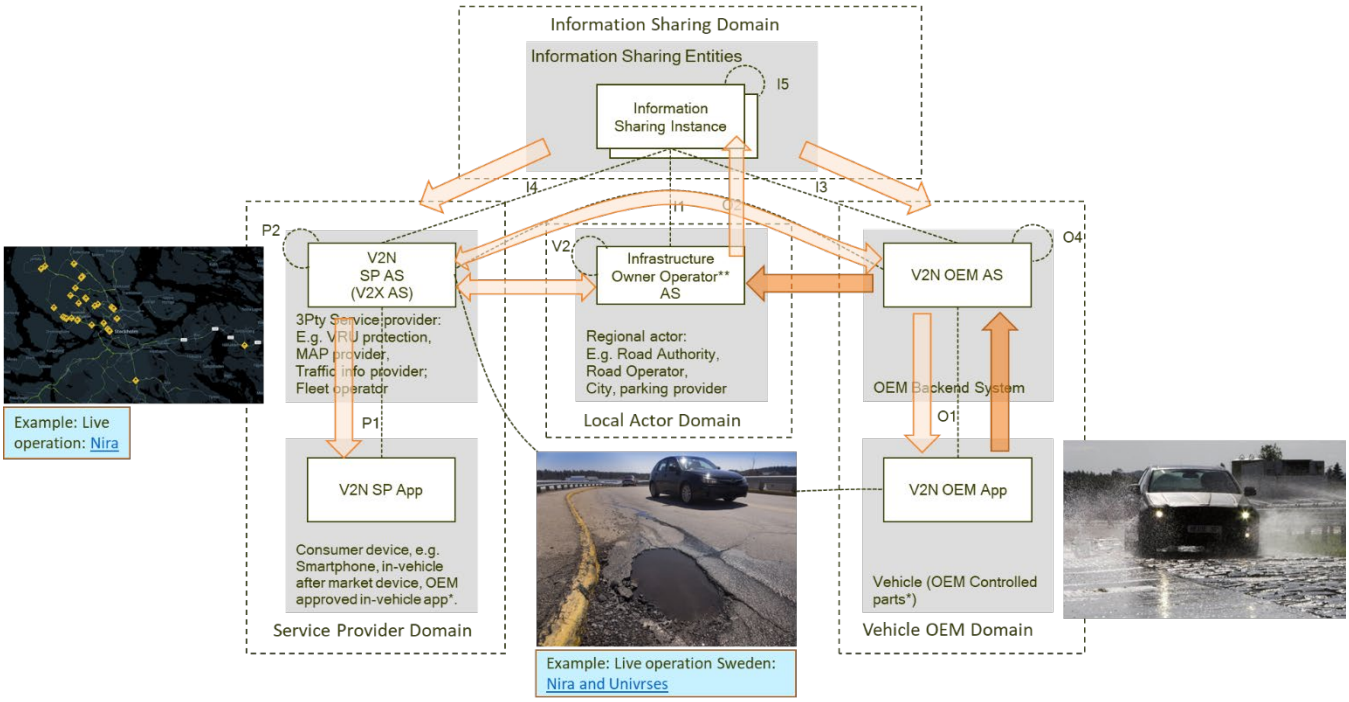

Figure 7: V2N2X Application architecture for crowd-sourced data collection (e.g. road maintenance)

In Figure 7 the information flow for crowd sourced data collection for road maintenance services is overlaid on the 5GAA applied application reference architecture.

In premium car brands, vehicle sensors continuously monitor/measure various road surfaces to provide input to advanced driver-assistance systems (ADAS) such as anti-lock braking systems (ABS). As a side effect, these measurements can be analyzed and used for detecting road conditions e.g. potholes where road maintenance would be required. The use case illustrates that the connected vehicle (a OEM fleet car) informs its backend system about such certain road surface conditions, including the exact location. This information can be transmitted from the vehicle to the car OEM backend (OEM AS) in a proprietary data format, because the transmission is internal between the vehicle and the related backend. Alternatively, standardized data formats can be used (e.g. SENSORIS)[29].

The OEM AS uses this information to calculate road surface condition heat maps. Based on commercial contracts, this information can be exchanged with IOOs (see for example the contract signed by the Ministry of Infrastructure and Water Management in The Netherlands with Mercedes[30], in the US/Ohio Department of Transportation with

[29] Example of a standardised interface to exchange information between in-vehicle sensors and cloud, more information at https://sensoris.org/

[30] Mercedes-Benz vehicle data and advanced software tools push efficiency and safety to a next level with large-scale digital infrastructure agreement, Press Release, March 2022, available at https://data.mercedes-benz.com/news/mercedes-benz-wins-landmark-road-monitoring-programme-in-the-netherlands

Honda[31], or the operation in Sweden[32]). On the IOO level, this information can be used for the organization of maintenance activities. It can also be used to provide a service to other OEMs and SPs, e.g., navigation service providers, to inform road users about possible dangerous road conditions. In that case, the customer would be informed either by the SP they are subscribed to or by the OEM AS (if the service is offered by the OEM AS to the vehicle fleet).

To include multiple OEMs and SPs in the solution, an information-sharing domain for sharing/disseminating information could be a workable and scalable solution. In such a scenario the road operator publishes the information (an instance) about potholes using the 'I1' interface, including meta-data that identifies the message format (e.g. ETSI DENM, BSM type 2), the location of the pothole (e.g. latitude/longitude, and/or an area identified by quadTree tiles[33]), the originator of the message, etc. This meta-data then allows backend systems to subscribe to 'I3' and 'I4' interfaces for information of interest and receive relevant notices when something matching the subscription filter is published. All other methods of data exchange are equal to what was already described in UC-1.

7.1.3 UC-3 Crowd-sourced wrong way driver alert

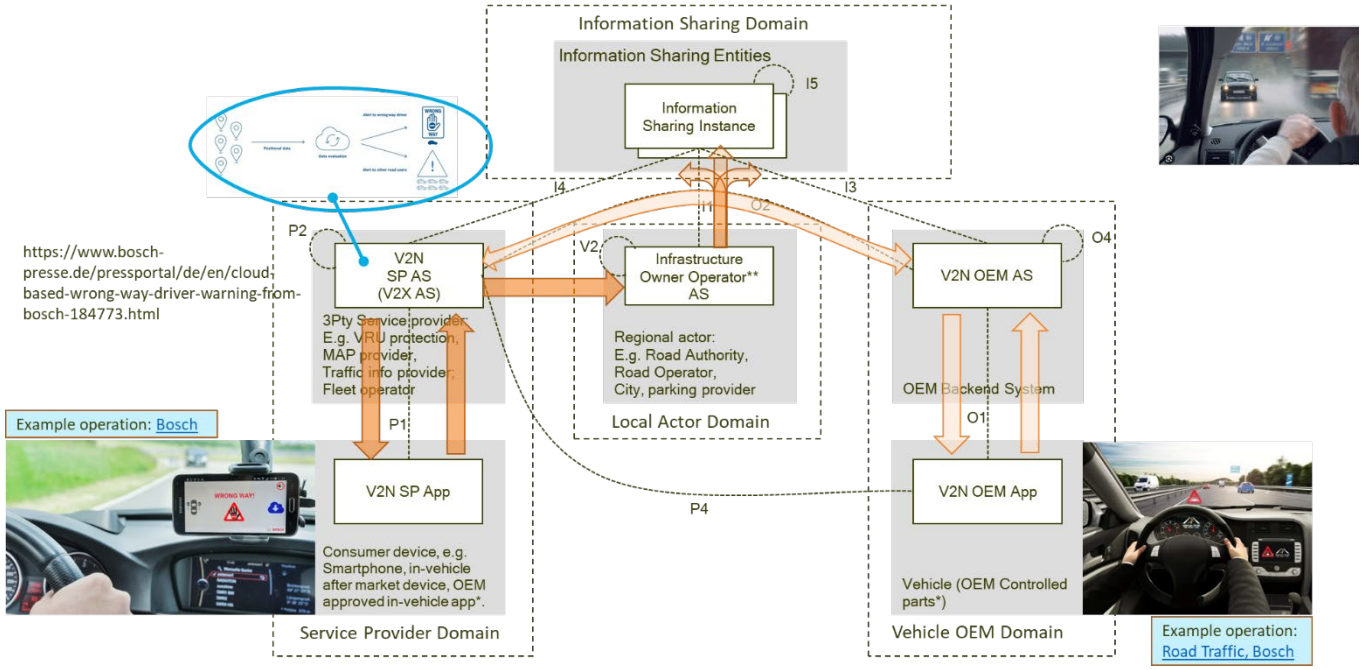

Figure 8: V2N2X application architecture for crowd sourced wrong way driver alert

[31] M. Miller, "UC joins Honda and ODOT to show how cars can collect data to prioritise road improvements", November 2023, available at https://www.uc.edu/news/articles/2023/11/uc-joins-honda-and-odot-to-show-how-cars-can-improve-road-safety.html

[32] D. Arminas, "Nira and Univrses in Swedish road data project", April 2023, available at https://www.worldhighways.com/wh1/news/nira-and-univrses-swedish-road-data-project

[33] QuadTiles - OpenStreetMap Wiki

In Figure 8 the information flow for crowd sourced data collection for wrong way driver warning services is overlaid on the 5GAA applied application reference architecture.

In most modern vehicles the position of the vehicle is measured continuously for navigation purposes either by the in-car navigation system or by an app provided by a services provider, used while driving. As a side effect, these position measurements can be analyzed by an additional app and used for detecting wrong way driver behavior. This use case illustrates how an SP application informs its backend system (SP AS) about such wrong way driver behavior, including the exact location and driving direction. This information can be transmitted from the connected vehicle to the SP AS, e.g. using the P4 interface, in a proprietary data format, because the transmission is internal between the service provider app and the related SP backend.

For privacy reasons, the location information is analyzed only in case the location is inside a predefined entry/exit location on a motorway/freeway (physically separated lanes).

The SP backend system uses this information to ascertain a wrong way driver and issue an immediate alert the person and other drivers subscribed to this service who may be approaching the vehicle in question, giving them time to take appropriate action. Based on commercial contracts the service can be provided to other OEMs and SPs, e.g. navigation service providers, to inform more road users about a potentially dangerous situation (wrong way driver) approaching. In turn, car OEMs as well as other services providers can provide position and speed information about their subscribers within the predefined areas mentioned above. The wrong way driver alerts can be exchanged with IOOs; example in practice include Road Traffic, Bosch[34] and participating service providers, e.g. Flitsmeister app, which is used to warn drivers about speed cameras, and public broadcaster apps, e.g. 'Antenne Bayern'/Bavarian local radio broadcaster. Customers of the service would thus be informed either by their service provider or in the case of fleet vehicles by the OEM AS offering such a service.

To involve multiple OEMs and SPs in this solution, again an information-sharing domain is a smart, scalable solution. In this scenario the wrong way driver service provider or the road operator (IOO) publishes the instance using the 'I1' interface, including meta-data identifying the message format (e.g. ETSI DENM, BSM type 2), location and direction of the wrong way driver (latitude/longitude and heading), the originator of the message, etc. This meta-data then allows backend systems to subscribe to 'I3' and 'I4' interfaces for information of interest and receive notification when something matching the subscription filter is published. All other methods of data exchange are equal to what was already described in UC-1.

[34] Bosch Cloud based wrong way driving warning solution, more information available at https://www.bosch-mobility.com/en/solutions/assistance-systems/cloud-based-wrong-way-driving-warning/

7.1.4 UC-4 Emergency vehicle awareness – Talking Traffic NL[35]

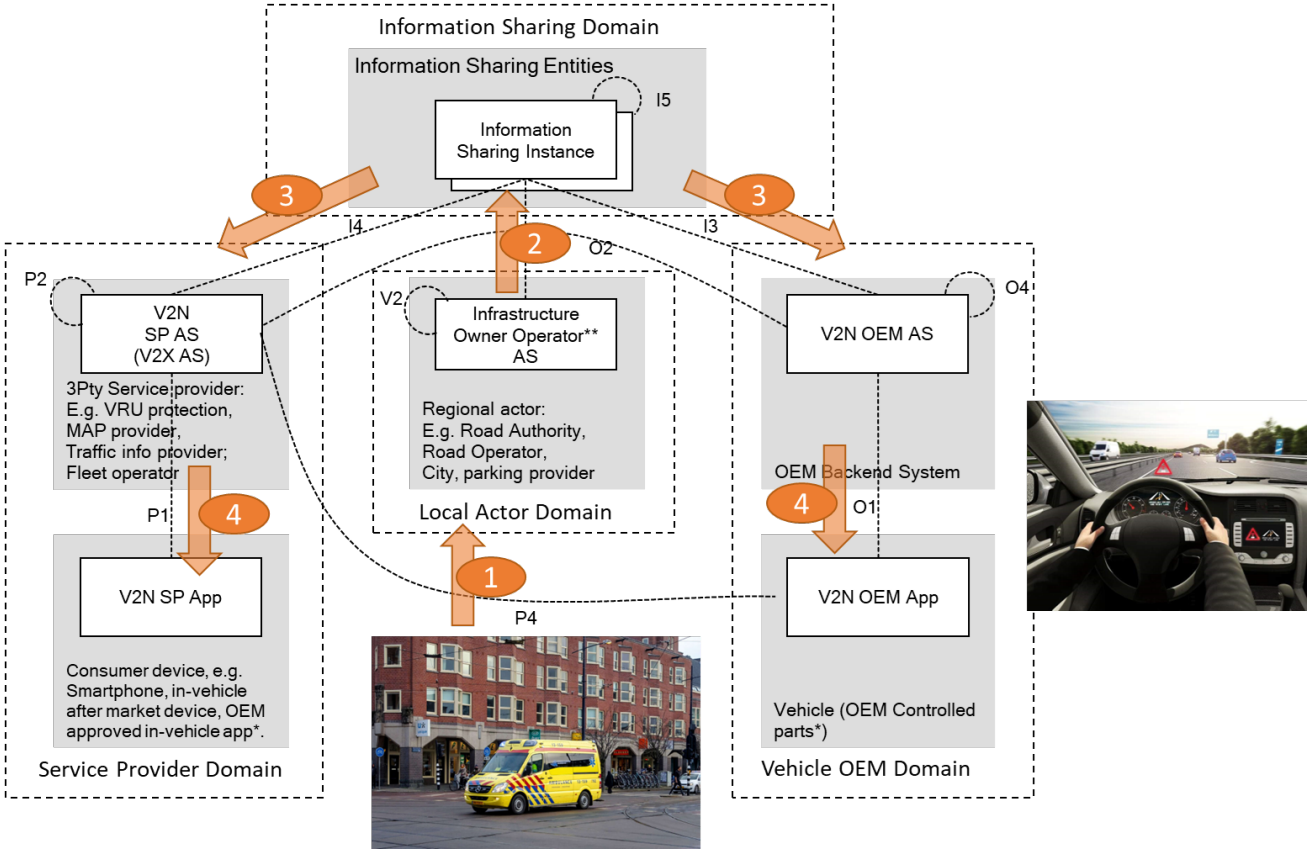

Figure 9: Emergency vehicle awareness – Talking Traffic NL

In The Netherlands, road users are informed about approaching ambulances thanks to a V2N2X setup. For this service to work, all ambulances share their route and status with connected road users. Approximately 25% of all motorized vehicles receive these awareness messages through apps and on-board units, according to an October 2023 statement by the Dutch Ministry of Infrastructure and Waterworks.

Figure 9 illustrates the information flow overlaid on the 5GAA applied application reference architecture:

1. Ambulances services are organized in regional organizations. During an emergency trip individual ambulances share their route and status with a frequency of approximately one-message-per-second with the backend system of the regional ambulance organization.
2. The backend systems convert these updates to ETSI DENM messages and forwards them to a national information-sharing instance using the C-ITS subject interface (I1).
3. The instance manages data quality and authorizations and shares these messages with connected service providers (In October 2023: ANWB, Be-Mobile, Hyundai, INRIX, KIA ,TomTom).

[35] This use-case was part of the Safety Priority Services sub-programme: https://dutchmobilityinnovations.com/spaces/1275/safety-priority-services/landing-sps

4. The service providers forward these messages to connected road users, tailoring the in-car message (smartphone app or dashboard) to the position of the individual vehicle (e.g. 'Ambulance 700 meters behind').

7.1.5 UC-5 Private initiative for smart city and connected infrastructure

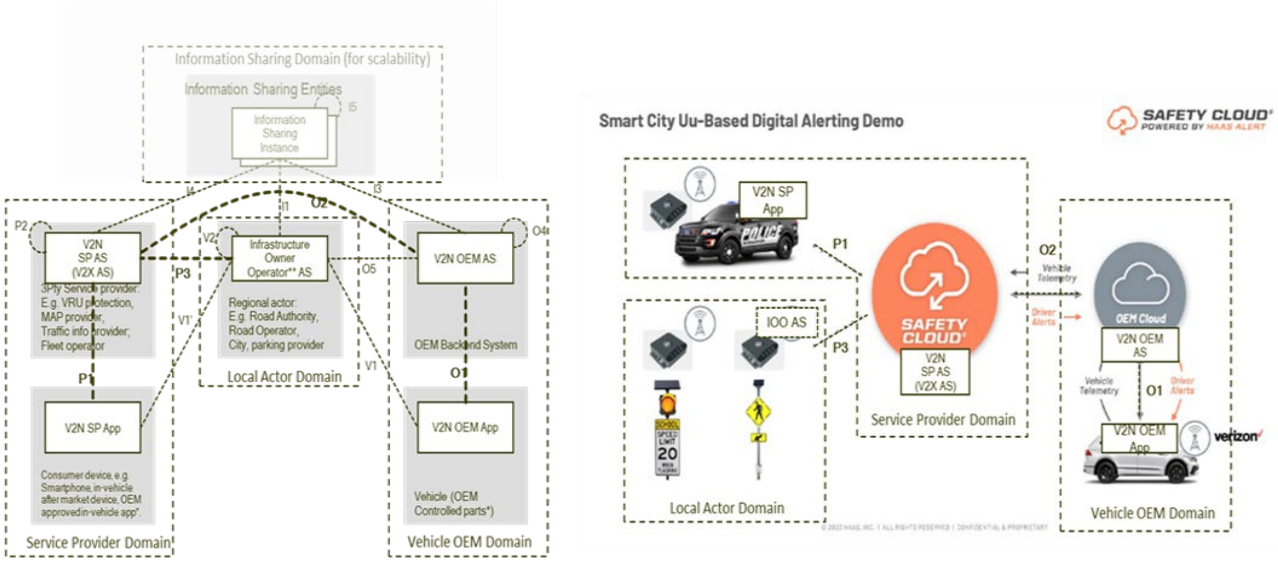

Figure 10: Private initiative for smart city and connected infrastructure

The right part of Figure 10 is from a Verizon and HAAS Alert demonstration of a smart city and connected infrastructure using a cellular-based (Uu) solution, 5GAA Detroit Demonstration October 2023[36]. The left part of Figure 10 shows the 5GAA applied application reference architecture to facilitate mapping it to the deployed solution.

One use case for this solution is an 'emergency vehicle approaching' where a 'Safety Cloud' collects input from emergency vehicles on a mission and forwards it to the OEM AS which, in turn, relays the information to affected vehicles for display on their human-machine interfaces (HMI).

Similarly, information about active school zones and pedestrian crossings can be collected by the 'Safety Cloud' and forwarded to the OEM backend who then relays it to an approaching vehicle for display on its HMI.

The information-sharing domain (greyed out) in the 5GAA application reference architecture is not used in the existing solution, but will be needed when the solution is scaled up to multiple OEMs, emergency departments, and school zones/pedestrian crossings. In such a scenario the 'Safety Cloud' could publish the information about active emergency vehicles and school zones on an information-sharing instance subscribed to by a myriad of OEMs. Alternatively, or additionally, the 'Safety Cloud' could play a more active role in the information-sharing instance process i.e. support a backend interface allowing other backend systems to subscribe to this information.

[36] 5GAA Live Showcase of C-V2X Technology, M-City Test Facility, Ann Arbor, Michigan , October 2023, available at 5gaa-detroit-showcases-brochure.pdf

7.1.6 UC-6 Protection of unconnected VRUs

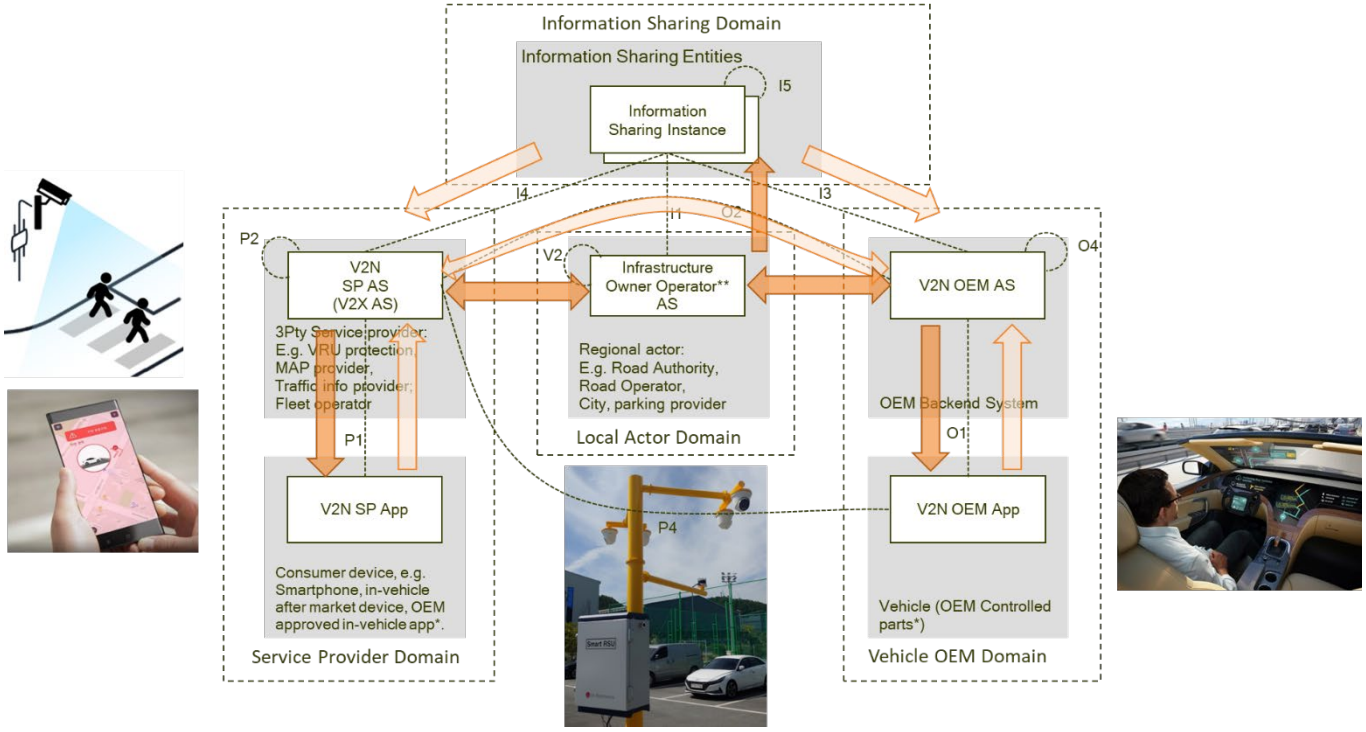

Figure 11: Protection of unconnected VRUs

Figure 11 illustrates how a vehicle's app receives a V2X message about unconnected pedestrians at intersections generated by IOO equipment (camera with object detection and artificial intelligence/machine learning, AI/ML). Through an exchange of V2X messages, drivers are alerted to the presence of pedestrians. The driver perceives this information on a user interface (HMI) and can slow down in advance, enabling a safer road environment.

Connected to intelligent equipment, an IOO AS collects data related to pedestrian patterns in crossings and enables more accurate predictions through AI/ML systems. A series of V2X messages can be created based on information collected by the IOO AS and can be sent to the SP AS and OEM AS through V2N2X interfaces, or they can be spread out through the information-sharing instance, facilitating wider distribution. [37]

In the V2N2X ecosystem, IOOs can perform a crucial role in providing infrastructure-related services, confirmed through the successful demonstration and validation of practical use cases during collaborative efforts with V2N service providers and multi-access edge computing (MEC) platform providers. Live deployment cases conducted by 5GAA include the following:

At a 5GAA event in Turin[38] held in December 2021, Telecom Italia, Telefonica, BT/EE, and Stellantis demonstrated passive vulnerable road user (VRU) detection using smart cameras to alert vehicles about pedestrian movements, even those without connected devices. Meanwhile, active VRU detection carries out a data exchange between vehicles

[37] An example of the use case described can be found at: 'Pedestrian safety service utilizing information detected via CCTV, LG Electronics. Video available at: http://www.soft-v2x.com/static/media/video_1_eng.9bdf3406.mp4

[38] 5GAA Live Trial of 5G Connected Car Concept, Turin, Italy, December 2021, available at: https://5gaa.org/live-trial-of-5g-connected-car-concept-to-launch-in-turin-italy/

and pedestrian devices for real-time location and movement tracking.

The 5GAA live showcase on the Virginia Smart Road in Blacksburg[39], in March 2022 (Verizon, Telus, American Towers, Capgemini, Harman, Intel, Stellantis, Virginia Tech Transportation Institute) used smart cameras with AI/ML to detect 'unconnected' pedestrians at crossings and provided safety-enhancing alerts to nearby drivers. Moreover, the trial included a system where pedestrians with smartphones could communicate with nearby cars via MEC proxy servers.

The 5GAA Detroit[40] live showcase in October 2023, facilitated by Uu interface-based communication, involved T-Mobile, Verizon, Commsignia, Bosch and LG Electronics, and an IOO AS deployed on the V2N MEC platform. It demonstrated a V2N2X structure to deliver V2N safety-enhancing services with reduced latency, ensuring efficient and seamless communication.

7.2 Software system and operation design principles

- Design for flexibility, automation and IT best-practices:
  - Provide the system foundation for a growing set of use cases. Facilitate data and information flows between private and public entities, cross-industry, cross-service providers, and between cross-jurisdictional stakeholders.
  - Extend data elements for cross-domain communication with descriptive meta-data (see Annex 7.3). This facilitates machine-readable and automated processing with protocol conversions on the application level. It also helps to decouple software life-cycles and versioning between the various stakeholder systems and domains.

– Allow proprietary protocols and data formats within a stakeholder domain (see P1, R1[18] or O1 in Figure 5), e.g. for commercial or for stakeholders' client-server interactions.

  - Encourage a state-less and event-driven software-design pattern. Avoid period message repetitions and timeout dependencies.

- Utilise best-practices for communication protocols and application programming interface (API) technologies:
  - The V2N2X communication protocols should be IP-based and use standard IT technologies for security, e.g. TLS (for TCP) or DTLS (for UDP).
  - Between the V2N2X information-sharing instances, use HTTP REST APIs for federation of information and for process automation.

[39] Live Trial of 5G Connected car Concept, Blacksburg, VA, USA, March 2022, available at https://5gaa.org/live-trial-of-5g-connected-car-concept-launches-in-blacksburg-virginia-va/

[40] 5GAA Showcases Cutting-Edge C-V2X Technology, Pioneering the Future of Vehicle Connectivity, Press Release, October 2023, available at https://5gaa.org/5gaa-showcases-cutting-edge-c-v2x-technology-pioneering-the-future-of-vehicle-connectivity/

- Design for large-scale operation and cross-country/cross-state/cross-stakeholder interactions:
  - Avoid the need for many-to-many system integration efforts and stakeholder contract relations. A stakeholder that aligns with the V2N2X information-sharing domain would have indirect access and reach all networked stakeholders, without further integration effort.
  - For stakeholders to have their IT systems interacting with the V2N2X information-sharing domain, which constitutes a dedicated trust domain, they must provide confirmation/proof that they will adhere to the data-sharing governance model, superseding the V2N2X information-sharing domain (e.g. by signing a CCoC). The proof or evidence may trigger the appropriate authority (CA) to issue a digital certificate (permission) for the stakeholder to communicate with a V2N2X data-sharing instance.
  - Support functions for automation, system and information resilience, security and trust in exchanging data should all be based on interactions via standard DNS for discovery of 'approved' actors and on a CA for handing out standard X509 certificates to approved actors.
  - For scalability within a the V2N2X information-sharing domain use a 'message queuing protocol' with a publish/subscribe mechanism for data-sharing, filtering or forwarding of data elements or queries; e.g. the standardized advanced message queuing protocol (AMQP).
- Keep the additional standardisation efforts minimal:
  - Allow use case specific data formats to travel via generic and well-established application-level communication protocols. Provide meta-data with suitable data-elements to facilitate the transcoding of data formats and interaction protocols (for more information about interoperability and meta-data see Annex 7.3).

7.3 Interoperability and use of meta-data

For network communication, interoperability is on the application-level, not on the radio-level, so mobile users on cellular networks can use different radio technologies (e.g. 4G, 5G, and beyond), and fixed assets operated by IOOs can be connected by different wired communication technologies or cellular. This means that a road user connected to a 4G cellular network, provided by one communication service provider (CSP), can communicate with other road users on a 5G cellular network, provided by another CSP. Application servers provide the bridge between users on different CSP networks, using different generations of cellular networks. In fact, it is the application data (IP packets) passed from the user (device or vehicle) on the mobile network to an AS. The radio-specific parts of the protocols are only used within the mobile networks. The AS can then provide service-level interoperability, i.e. pass the application-level information on to other actors, such as external service providers and road operators, or convert the application-level information to an agreed format before passing it on.

The application itself should make use of well-defined ITS message sets, as they are standardized by SAE or ETSI on the application level. For example, hazard warnings messages can be described in DENM or TIM[41] format, signalized intersections conditions by SPAT/MAP messages, or traffic light pre-emption by SREM/SSEM messages. Note: the message format on an application level can be re-used, however message frequency should be used in an adapted way.

To facilitate information filtering and/or data format conversions, the actual application-level information is tagged with meta-data, which provides information about the actual application-level input. The suggested ISO standard advanced messaging queuing protocol 1.0 (AMQP)[42] is available from a number of vendors, including Linux distributions; AMQP refer to meta-data as 'application properties'.

Table 1 is an example from the 'C-Roads IP-based interface profile'[43] of what such meta-data can indicate. Left-most column 'Name' is the meta-data (application property).

[41] Traveler Information Message, as defined by SAE/J2735 Message Set Dictionary

[42] More information on the ISO standard advanced messaging queuing protocol can be found at https://www.amqp.org/

[43] C-Roads: "IP based interface profile", which is part of Release 2.0.x of the C-Roads Harmonised C-ITS Specifications: https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/Harmonised_text_v2.pdf

Name	Value and type	Description	Mandatory/ Optional
publisherId	string A two-letter country code (based on ISO 3166-1 alpha-2) and a numerical identifier (value between 0 and 16383 including leading zeroes) based on ISO 14816:2005 (same as used for providerIdentifier in IVIM), e.g. "AT00001", "DE15608"	Unique ID of the publisher. It is linked to the country where the provider wants to register. It could be in one country or several.	M
publicationId	String Concatenation of publisherId and a unique identifier for the dataset/publication with a ":" in between, e.g. "DE15608:IVIM_BERLIN_067" or "NO73944:679ABX92"	Each dataset/publication identifier needs to be unique for the given publisher.	O
originatingCountry	string Country code (based on ISO 3166-1 alpha-2)	Country code where the C-ITS message is created	M
protocolVersion	string E.g. "DENM:1.3.1" or "IVIM:1.2.1"	Represent the version of standard used to create the message, i.e. for DENM the version of ETSI EN 302 637-3, for IVIM, SPATEM the version of ETSI TS 103 301	M
serviceType	string E.g. "HLN-RLX"	Acronym defined in latest version of Common C-ITS Service and Use Case Definitions	O
messageType	string DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, CAM	For this version of the specification the string shall be one of the following: DENM, IVIM, SPATEM, MAPEM, SREM, SSEM, and CAM. The list may be subject to changes in future versions of the specification	M
longitude	float Decimal degrees According to WGS84/ EPSG:4326	Longitude of the event published; for DENM (eventPosition) and for IVI and SPATEM/ MAPEM/SSEM/SREM (referencePosition)	O
latitude	float Decimal degrees According to WGS84/ EPSG:4326	Latitude of the event published; for DENM (eventPosition) and for IVI and SPATEM/ MAPEM/SSEM/SREM (referencePosition)	O
quadTree	string Comma separated list of quadtree tiles starting and ending with a comma, e.g. ",202320120232120101," (single value) or ",2023201202321201012023201202321201012023201202321201032," (multiple values chained)	Relevant spatial index location of the C-ITS message	M

Table 1: Meta data (AMQP application property) example

Meta-data (application properties) can be user defined for AMQP and thus tailored to the needed applications and operation. In this example the meta-data is tailored for C-Roads use with ETSI-type messages, as can be seen in the row 'messageType'. An actor publishing information to an information-sharing instance thus includes these 'application properties'. An actor subscribing to an information-sharing instance provides a filter[44] of what information it is interested in. For example, if only ETSI DENM messages of a certain revision are supported by an actor, the filter would indicate that if that actor publishes information matches the filter, this information is pushed to the subscribing actor. Further filters and subscription properties could, for example, be using 'quadTree'[45] (bottom meta-data in Table 1) to provide only road traffic information with relevance to a certain geographic area or for certain types of vehicles, e.g. to heavy-duty trucks driving in a certain geographic area.

[44] AMQP uses 'Structured Query Language' (SQL) for filter expressions, this mean that powerful conditions can be expressed, e.g. including 'And', 'Or', 'If', Comparison operators etc.

[45] QuadTiles - OpenStreetMap Wiki

7.4 Deployment and operation best practices

- Governance
  - Ideally a public-private governance structure is set up with participating authorities and industry experts. This should be a permanent structure consisting of permanent bodies responsible for decision-making as well as temporary technical workgroups.
  - The governance structure should lead in:
    - Identifying and managing standardized use-cases
    - Maintaining/updating standards, security arrangements and quality levels
    - Resolving discussions
    - Optionally: community platform, test facilities and certification requirements
- Data quality management
  - Data quality and consistency is key for adoption by service providers and OEMs, and therefore for the large-scale adoption and impact.
  - The 'network character' of V2N2X allows for high-quality control and due to their central position in the ecosystem the information-sharing instances are the designated place to manage data quality.
  - Quality control is a continuous effort and should at minimum include:
    - Verification of security arrangements (e.g. message signing)
    - Continuous inspection of connection- and data quality
    - Alerting producing actors and relevant stakeholders in case of diminished quality
    - Provide quality labelling of data for consuming actors (continuously monitored and updated)
- Authentication and access
  - Traditional IT access features (passwords, tokens etc.) can be applied to identify and authenticate connecting actors. For added trust it is possible to use a designated CA to sign messages. This allows all actors in the chain to identify the source of every message.
  - the information-sharing instances should provide supervising authorities with the possibility to manage access to published public data, e.g. because consumers need to comply to certain privacy policies. In a later phase it is advised to set up a national register for trust, centrally administering authorization policies that all information-sharing instances can use.

- Interfaces and protocols
  - Typically static and dynamic public data are exchanged using HTTP REST-based protocols. Data types for these kinds of data types are usually text based (e.g. DATEXII[46], WZDx[47]).
  - For real-time data, streaming channels are used, based on AMQP[48] (C-Roads IP-based interface profile[49]) combined with an 'orchestration API' to establish subscriptions and facilitate load balancing, both on the side of the information-sharing instance as well as on the side of the publishers/consumers. As these data channels facilitate the exchange of large volumes of messages, encoded message types are used specifically for ETSI C-ITS or SAE C-ITS message types.
  - Between information-sharing instances, a HTTP REST-based protocol is used for federating data and automation. The C-Roads II interface is a mature protocol for federation. The actual data exchange between instances is then handled using streaming data channels.
  - Providing/administering standardized meta-data concerning data sources is a key element to facilitate machine reading, interoperability, and scale-up. The information-sharing instance uses the meta-data to provide filtering mechanisms for data consumers and serves as a basis for quality control.

[46] Information model for road traffic and travel infromation in Europe, DATEX II more infromation can be found at https://datex2.eu/about/

[47] Work Zone Data Exchange, US DOT, available at https://www.transportation.gov/av/data/wzdx

[48] More information on the ISO standard advanced messaging queuing protocol can be found at https://www.amqp.org/

[49] C-Roads: 'IP-based interface profile', which is part of Release 2.0.x of the C-Roads Harmonised C-ITS Specifications: https://www.c-roads.eu/fileadmin/user_upload/media/Dokumente/Harmonised_text_v2.pdf

7.5 Glossary of terms

ABS:	Antilock Brake System
ADAS:	Advanced Driver Assistance System
AI/ML:	Artificial Intelligence/Machine Learning
AS:	Application Server
App:	Client part of an application (e.g. in smartphone or vehicle)
B2B:	Business-to-Business
B2C:	Business-to-Consumer
BSM:	Basic Safety Message
C-V2X:	Cellular Vehicle To Everything Communication (including cellular network and direct communication)
C-ITS:	Cooperative Intelligent Transport System
CCoC:	Common Code of Conduct
CSP:	Communication Service Provider (alias MNO)
DENM:	Decentralized Notification Message (ETSI 'Event based' message)
DNS:	Domain Name Server
E2E:	End-to-End
FHWA:	Federal Highway Administration
GLOSA:	Green Light Optimization Speed Advice
HMI:	Human Machine Interface
IOO:	Infrastructure Owner Operator
IP:	Internet Protocol
IT:	Internet Technology
KPI:	Key Performance Indicator
MAP:	Intersection Map (geometry of intersection)
MFA:	Multi Factor Authentication
MNO:	Mobile Network Operator
OEM:	Original Equipment Manufacturer
PKI:	Public Key Infrastructure
RO:	Road operator (alias IOO)
RTTI:	Real-Time-Traffic-Information
SPAT:	Signal Phase And Timing
SREM:	Signal Request Extended Message
SSEM:	Signal Status Extended Message
SRTI:	Safety-Related-Traffic-Information
TCP:	Transmission Control Protocol
TIM:	Traveler Information Message, as defined by SAE/J2735 Message Set Dictionary
TLS:	Transport Layer Security
TOC:	Traffic Operation Center
TMC:	Traffic Management Center
TTG:	Time-To-Green
UDP:	User Datagram Protocol
UI:	User Interface
Uu:	Name of cellular network radio interface
VRU:	Vulnerable Road Users
V2N2X:	Vehicle-to-Network Communication to Everything Communication
V2N:	Vehicle-to-Network Communication

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


5GAA
Automotive Association