Submitted by the Informal Working Group on
Intelligent Transport System

Informal document **WP.29-194-23**
194th WP.29, 12-15 November 2024
Agenda item 2.3
(Based on ITS-10-03)

Vehicular Communications Definition, Types, Value, Uses, and Considerations

Prepared for the Task Force on Vehicular Communications (TF on VC)

This document provides an overview of Vehicular Communications (VC) including its definition, types, value, uses, and considerations. This document has been prepared to provide background information about VC to WP.29 participants.

The advancement of VC capabilities will benefit from collaboration between policymakers, industry stakeholders, and researchers to deploy and protect relevant communications technologies.

At its 188th session in November 2022, the World Forum for Harmonization of Vehicle Regulations (WP.29) requested the Informal Working Group (IWG) on Intelligent Transport Systems (ITS) to perform preparatory activities and to explore the potential role of WP.29 related to VC (see: ECE/TRANS/WP.29/1168, para 19). This document is the outcome of those preparatory activities. The purpose of this document is to identify potential activities for further consideration at WP.29.

This document is focused on the use cases and does not detail communications technologies used or to be used, some of which are already available in markets.

This document was created by input from WP.29 participants with tremendous support by communications and automotive experts from 5GAA, AAPC, CAR 2 CAR Communication Consortium, CATARC, CLEPA, ERTICO, ETSI, IMMA, OICA, and SAE International.

I. VC Definitions

In this document, the wording:

'*ADS*' is an Automated Driving System as defined in WP.29 document GRVA-18-50e ("the vehicle hardware and software that are collectively capable of performing the entire Dynamic Driving Task (DDT) on a sustained basis").

'*Built-in system*' refers to components that have access to vehicle-state information other than through external indications (for example, that can access brake and indicator state other than through viewing the brake lights or turn signals). Built-in system includes components with read-only access to the vehicle as well as components that might have write access to vehicle interface or control systems. For example, any device in the vehicle that can directly cause ADS features to activate is a built-in system. Built-in system does not include devices brought into the vehicle that have communications capabilities. Built-in systems might be added to a vehicle after its manufacture.

'*DCAS*' means Driver Control Assistance System as defined in UN Regulation No. 171 ("the hardware and software [that are[1]] collectively capable of assisting a driver in controlling the longitudinal and lateral motion of the vehicle on a sustained basis").

'*Multihop*' refers to the concept in communications networking where information is transmitted across a communications network by passing through multiple intermediate nodes (or "hops") before reaching its final destination. Instead of a direct link between the source

[1] Likely to be added in UN Regulation No. 171 update for consistency.

and destination, the information to be transmitted "hops" from one node to another, each forwarding the packet closer to its target.

'*PII-leakage*' refers to the accidental or unauthorised exposure of Personally Identifiable Information (PII), such as names, addresses, identification numbers, and financial data, to individuals or systems that should not have access. This can occur through security breaches, improper data handling, and inadequate privacy protections, leading to privacy risks or potential misuse of personal data.

'*Road occupants*' includes vehicles, VRUs, and animals.

'*Road transport infrastructure components*' include roadside units, electronic signs, traffic control and management systems, and other road transport infrastructure.

'*Surroundings*' is drivers/vehicle owners outside their vehicle, household elements, other vehicles, VRUs, road transport infrastructure components, service providers, cloud-based operations, etc.

'*Transmitted information*' includes data and commands.

'Trust' refers to the concept that information received by a processing system is accurate, comes from a source appropriate for that information, and has not been maliciously generated, modified in transit, or otherwise manipulated to be incorrect or misleading.

'*VC*' is communications in public-accessible areas from and to systems built in vehicles and from and to mobile communications devices connected to these built-in systems.

Note: Communications by mobile communications devices that are not a built-in system are not included in VC, even if the built-in system serves as the communications device's connection to a cellular network (e.g., by a built-in Wi-Fi hotspot).

'*Vehicle*' includes passenger vehicles, goods vehicles, agricultural and forestry vehicles, emergency vehicles, special purpose vehicles, delivery robots, and any other motorised equipment that uses a public roadway.

'*Vulnerable Road Users (VRU)*' includes people (i.e., pedestrians, persons with disabilities or reduced mobility and orientation, authority personnel, road workers, animal riders, herders, etc.), and occupants and riders of motorcycles, tricycles, bicycles, scooters, and similar road transport equipment.

II. VC Types

This section provides general background about types of VC.

VC includes the following broad categories:

a. Wired and wireless.

b. One to one (unicast), one to a group (multicast), and one to many (broadcast).

c. Unidirectional and bidirectional.

Current wired communications components in vehicles primarily are:

a. The On-Board Diagnostic (OBD) port.

b. Universal Serial Bus (USB) ports.

c. The Electrical Vehicle (EV) charging equipment.

While these communications components often utilise wired connections, they might also use wireless communications.

Vehicles commonly have wireless communications technologies installed. The wireless communications technologies, listed below in approximate range order, might appear in a vehicle now or in the future, including, but not limited to:

a. Very-short range communications, such as access control technology using Radio-Frequency IDentification (RFID) or Near-Field Communications (NFC) for short-range identification data exchange in the range of centimetres.

b. Close-range communications, such as Bluetooth, Ultra-Wide-Band (UWB), or infrared for communications in the range of a few metres.

c. Radio Local Area Networks (LAN), such as wireless LAN (IEEE 802.11 family) for transmission of information over tens to hundreds of metres or as a wireless communications link between a built-in internet router and vehicle occupants' mobile communications devices, often referred to as a Wi-Fi hotspot.

d. Direct short-range communications between vehicles (V2V), between vehicles and road transport infrastructure components (V2I), and between vehicles and VRUs (V2VRU, sometimes V2P), such as technologies standardised by 3GPP or IEEE.

e. Cellular communications providing voice, text messages, and mobile internet access via International Mobile Telecommunications (IMT).

f. Radio, such as AM, FM, shortwave, or DAB+.

g. Satellite, such as Global Navigation Satellite Systems (GNSS), satellite radio, or satellite internet.

In the future, vehicles might have wireless rather than wired internal communications. Those communications are not considered VC.

III. VC Value

VC has the potential to:

- Improve road occupant and vehicle safety.
- Reduce the environmental impact of road transport.
- Enhance the road transport efficiency.
- Improve the road transport experience.
- Improve driving experience and comfort.
- Reduce road transport costs.
    - Optimisation of routes will reduce traffic congestion, which will reduce fuel costs and tyre wear due to shorter journeys, and less time spent by vehicles in queues with the vehicles idling, thus wasting energy and causing additional pollution.

VC enables built-in systems and vehicle occupants to receive transmitted information from their surroundings.

VC enables built-in systems to provide their surroundings with transmitted information including, but not limited to:

- State of the vehicle, such as:
    - Vehicle location, speed, heading, and trajectory.
    - Vehicle acceleration and braking.
    - Externally viewable and hearable signals, such as turn signals
    - Use of vehicle features, such as DCAS and ADS.
- The state of driver engagement (including sudden health issues).
- Identified road conditions.
- Identified weather and environmental conditions.
- Identified other road occupants.

Note that a carry-in system could provide some of the above information. For example, using position / accelerometer information, a carry-in system could provide approximate vehicle dynamics information. This type of information provision is not in scope of VC as defined in this document.

IV. VC Uses

This section provides general information on possible uses of VC, grouped according to the type of use case. Some elements appear in multiple use case descriptions below, as common terminology does not always have precise boundaries.

VC that might impact safety or vehicle control should be secure and trusted.

VC should respect privacy rules and regulations.

The inclusion of a use case in this section is not an endorsement of that use case or a suggestion that it be mandated. This list is a list of technical possibilities whose use might be decided on by appropriate stakeholders.

Possible use cases include, but are not limited to:

1. Safety and Emergency

a. *Safety information for vehicle occupants*: VC makes it possible to provide real-time notifications and warnings to built-in systems and vehicle occupants about possible hazards. These notifications and warnings are based on received information, integrated with direct sensing by the vehicle.

   VC makes it possible to report various types of possible local hazards, allowing for a more comprehensive risk assessment.

   Notifications and warnings include, but are not limited to, information about wrong-way driving, traffic congestion, VRU presence, slippery roads, vehicles with excessive speed, presence and directions of emergency vehicles, and other road hazards.

b. *Safety information for road-transport operations:* VC makes it possible for built-in systems to transmit real-time information to their surroundings, allowing road transport infrastructure operators to improve their traffic management operations. These real-time notifications and warnings can be used to improve service operators' information and overall traffic management, possibly leading to infrastructure improvements or can be used for notifications on Variable Message Signs (VMS).

c. *Emergency services:* VC makes it possible to improve conditions for first responders and emergency services by providing real-time information about crashes, road hazards, and other incidents. Also, see the *Traffic signal priority* and *Emergency vehicle support* use cases below.

d. *Automated Emergency Call Systems (eCall/AECS)*: VC makes it possible to support built-in AECS that can automatically detect the occurrence of a crash to call emergency services and provide vital information, such as location, crash severity, number of vehicle occupants, and other vehicle information. This process can reduce emergency response times and improve the effectiveness of the emergency response. Also, see the *Emergency services* use case above.

e. *Collision warning and avoidance:* VC makes it possible to support drivers and vehicles systems detect and avoid possible collisions by sharing real-time information about other road occupants' location, speed, heading, and trajectory. This information could be used as additional input to built-in safety systems complementing the built-in sensors, enhancing collision prevention capabilities.

   VC, combined with good vehicle positioning, makes it possible both to improve the vehicle's detection capability of the 360°surrounding conditions and to increase the

likelihood that the vehicle is detected by other vehicles. This capability is especially useful in supplementing recognition in challenging scenarios such as bad weather as well as identifying non-line-of-sight objects, such as intersections with obscuring items, where visual recognition by built-in sensors (e.g., radar, camera, lidar) is compromised or not possible.

In addition, safety can be improved by collective perception, when road transport infrastructure components or vehicles identify road occupants not transmitting VC information and inform the surrounding road occupants with VC equipment about it. Also, see the *Safety information for vehicle occupants* use case above.

f. *VRU protection*: VRUs could be protected from vehicles and other road occupants through VC.

VC makes it possible for communications devices carried by VRU to provide information to built-in systems and vehicle occupants about the VRU.

In addition, the detected presence of a VRU could be communicated to vehicles by capabilities such as:

- Road transport infrastructure sensors detecting the presence of a VRU and sending the detection (including position and, if available, direction) to vehicles and VRUs to make them aware (collective perception).
- Vehicle sensors detecting the presence of a VRU and sending the detection (including position and, if available, direction) to other vehicles, VRUs, and road infrastructure components to make them aware. Vehicles equipped with VRU detection systems could share the information that they identify with surrounding vehicles and road transport infrastructure components (collective perception).

All of this information could then be used to implement VRU protection strategies. This information – if reliable, relevant, reasonably accurate, and real-time – could be used as additional input for collision-related and other safety systems. Safety is improved when road transport infrastructure components identify VRUs and send the information to surrounding road occupants with VC equipment in real time. See the *Collision warning and avoidance* use case above.

g. *Natural disaster and crisis management:* VC makes it possible for built-in systems and vehicle occupants to receive notifications and warnings about various disasters and crises, including tsunamis, typhoons, other weather conditions, and wildfires as well as human disruptions, shootings, terrorist attacks, etc. VC could support evacuations, by enabling sharing information from authorities.

In situations where the primary communications infrastructure is disrupted, vehicle-to-vehicle communications might be able to relay information across the road network using a vehicle-to-vehicle multihop approach or a satellite approach. Such approaches might allow for comprehensive notifications and warnings to reach built-in systems and vehicle occupants even in areas where there are communications infrastructure outages. Similarly, vehicles in areas where there are communications infrastructure outages could use such approaches to deliver information to road transport operators and authorities responsible for the disaster response and management.

h. *In-vehicle notifications and warnings*: VC makes it possible for vehicles to receive notifications and warnings from their surroundings of special situations ahead on the road. Such situations include road closures and rerouting, materials spills, and crashes. Also, see the *Safety information for vehicle occupants* use case above.

2. Traffic Management

a. *Road transport infrastructure management:* VC makes it possible for road transport operators to improve traffic flow, reduce congestion, and improve overall road transport efficiency and safety. Vehicles could provide real-time information on their location, movement, intended manoeuvres (e.g., lane changes, upcoming turns), etc. In addition, vehicles could report local hazards, such as road surface issues and areas with frequent braking or electronic stability control activation. This information could help identify areas for targeted maintenance and repair of road transport infrastructure components.

b. *Road works:* VC makes it possible for road transport infrastructure components to inform built-in systems and vehicle occupants about road works, including detours, lane changes, revised speed limits, and possible delays. Real-time warnings could reduce crashes and improve safety for both vehicle occupants and road workers.

c. *Optimised traffic signal handling*: VC makes it possible for vehicles to receive intersection Signal Phase and Timing (SPaT) information, along with intersection topology, from road infrastructure components. With this information, vehicle software could optimise vehicle speed for energy efficiency to achieve green-light-optimal speeds. Road infrastructure components could provide red-light violation warning information to built-in systems and vehicle occupants as well as passing the warning to built-in systems and vehicle occupants in other vehicles approaching the intersection.

d. *Optimised traffic signal management*: VC makes it possible for vehicles to provide information about their activities to traffic management systems. With this information, traffic signal controllers could adjust their signal timing. In the future, VC might act like inductive-loop detectors as well as support red-light violation prevention, reducing crashes and improving safety. Also, see the *Safety information for vehicle occupants* use case above.

e. *Traffic signal priority*: VC makes it possible for emergency vehicles (police vehicles, ambulances, fire vehicles, rescue vehicles, etc.) and public transport vehicles to request priority, including pre-emption, at traffic signals, facilitating a swift change to green and/or extending the length of the green light.

f. *Real-time traffic information:* VC makes it possible for built-in systems and vehicle occupants to receive information on road network status. VC could also support built-in systems sending information to the road transport infrastructure components about situations that the vehicle encounters.

g. *Traffic management for major events*: VC makes it possible for traffic management systems to provide information about road closures, detours, and other route changes during special traffic situations, such as events, parades, protests, and VIP travel. This information could help drivers and vehicles with ADS features plan their routes and avoid congested areas.

3. Advanced Vehicle Capabilities

a. *ADS support:* VC could improve the performance of ADS. With transmitted information received as additional input, ADS features might improve performance within their Operational Design Domain (ODD) and even extend their ODD. This supplementary transmitted information, complementary to the built-in software's own sensor interpretations, might allow for earlier and smoother automated actions.

   VC could allow road transport infrastructure components to provide ADS features with crucial, real-time information, including, but not limited to:

   - Changed road conditions, such as special traffic situations, road works, crash locations, and obstacles on the road.
   - Information about challenging topological situations, such as existence of tunnel entries, highway entries and exits, reversible lanes, roundabouts, and complex intersections.
   - Road traffic participant detection at tunnel entries or complex intersections.
   - Traffic signal information and variable message sign information.

   Similarly, DCAS features might benefit from VC.

   When approaching their ODD limits, vehicles with ADS features without a fallback user could indicate this condition, enabling remote human interaction or automated guidance from road transport infrastructure components.

   Also, see the *Road works* and *Traffic management for major events* use cases above.

b. *Automated Vehicle Marshalling (AVM)*: VC could support slow-speed vehicle control services such as remote parking, hire and freight vehicle positioning, and Automated Valet Parking (AVP).

c. *Emergency vehicle support*: VC could allow emergency vehicles to transmit their location, speed, heading, and trajectory, ensuring earlier awareness of these emergency vehicles and facilitating safe interaction with them. Emergency vehicles might send instructions to ADS vehicles without a fallback user.

d. *Cooperative manoeuvre coordination*: VC could support collaboration between vehicles to improve safety and efficiency. Such collaboration includes platooning and intersection movement coordination for vehicles with ADS features (and possibly DCAS features).

   VC could assist vehicles with ADS features (and possibly DCAS features) to safely and reliably complete challenging manoeuvres, such as lane changing, merging into crowded lanes, and handling four-way stops.

   Also, see the *Collision warning and avoidance* use case above.

e. *Remote interaction*: VC could make it possible for out-of-vehicle humans and equipment to interact with vehicles with ADS features without a fallback user. Such interaction could include remote supervision of, sending instructions to, and supporting on-site traffic authorities' interaction with vehicles with ADS features without a fallback user.

   When approaching their ODD limits, vehicles with ADS features without a fallback user could indicate this condition, enabling remote human control or possibility even automated guidance from a road transport infrastructure component.

f. *Remote driving*: VC could make it possible for an authorised person outside a suitably equipped vehicle to remotely control it and perform driving manoeuvres if permitted by the local regulatory authorities.

4. In-Vehicle Experience and Convenience

a. *Infotainment and convenience:* VC can support an enhanced in-vehicle experience for vehicle occupants by delivering multimedia content, internet access, and personalised services. This delivery includes providing real-time information, such as location of rest areas for people and vehicles; availability of overnight parking for lorries; status of facilities for campers; location, availability, and pricing of EV charge points and fuel stations; and availability of parking spaces. In addition, reservations could be made for parking, EV charging, and other services, such as dining and lodging.

b. *Remote activities*: VC makes possible remote initiation of vehicle actions, such as door locking and unlocking, accessing the temperature control, managing EV charging, and opening the trunk for delivery and pickup. VC supports locating a parked vehicle. In addition, VC could be used from the vehicle for controlling communications-equipped home and destination items, such as home appliances and garage doors.

   VC could be used for services such as vehicle sharing, vehicle rental, and automated transport.

c. *EV Charging support:* VC could make it possible for information from the grid to be transmitted to control EV charging times and support bidirectional electricity flows, enabling EVs to power the grid or the user's home or other facility. Such activities could play a role in supporting electrical energy storage and electric grid balancing.

d. *Payment services*: VC can be used for in-vehicle purchases, such as payments for tolls, road pricing, parking, fuelling, EV charging, and drive-thru purchases.

e. *Wide area information provision*: VC can be used to provide general information to built-in systems and vehicle occupants via broadcast through FM, AM, shortwave, and DAB+ radio; terrestrial TV; satellite radio; etc. This includes the use of TMC coding using ALERT-C or TPEG over FM RDS and DAB+.

5. Vehicle Management and Maintenance

a. *Geofencing*: VC makes possible notification of vehicle owners and managers when a vehicle exceeds pre-set geographic limits and speed limits. VC could provide information relevant to vehicle operations within those limits, such as traffic rules.

b. *Vehicle software maintenance*: VC makes it possible to update remotely in-vehicle software, firmware, map data, etc.

c. *Vehicle diagnostic and maintenance information***:** VC makes possible access to real-time information on the health and performance of built-in components, and transmitting the status of built-in components to vehicle owners, vehicle manufacturers, and independent repairers.

d. *Function Control*: VC makes it possible for vehicle manufacturers to enable and disable remotely a built-in system capability across a set of vehicles.

6. Support for Authorities

a. Regulatory *reporting:* VC supports vehicle manufacturers in providing regulatory reporting to vehicle-regulatory authorities.

b. *Investigation and information collection*: With proper local legal authorisation, VC could make it possible for information to be retrieved from vehicles, including whether an ADS feature is active or was active at a specific time.

c. *Remote vehicle actions*: Under the direction of local law enforcement authorities, VC makes it possible for a vehicle to be remotely slowed, stopped, and disabled. Also, see the *Remote interaction* use case above.

d. *Stolen vehicle tracking*: If allowed under the jurisdiction's privacy rules and regulations, local law enforcement authorities can utilise VC to track a stolen vehicle.

7. Fleet and Logistics

a. *Public transport*: VC makes it possible to provide waiting passengers with information about public transport arrival times and service variations, as well as to assist public transport fleet operations and management, including prioritisation of public vehicles at traffic signals. Also, see the *Traffic signal priority* use case above.

b. *Fleet management*: VC makes it possible for fleet operators to collect information remotely from their managed vehicles and control their operations. Also, see the *Geofencing* use case above.

c. *Freight movement*: VC makes possible activities such as tracking freight movement, improving freight transport efficiency, and lorries transmitting weight and digital documentation to relevant authorities, including traffic management centres and customs authorities.

V. VC Considerations and Challenges

VC can provide many benefits, but also comes with challenges to consider. Challenges might vary across countries or country groups.

a. *Trustworthy data sources*: Data sources used to originate information that is transmitted over VC to built-in systems and vehicle occupants should be trustworthy, i.e., they should meet stakeholder expectations for the reliability of the data for its intended use.

   Possible solutions include:

   - Data sources undergo a validation process to provide assurance that the data is of the expected reliability (by self-certification or third-party certification).
   - Systems that create VC messages based on data sources (a) validate the trustworthiness of the data sources that they use and (b) use mechanisms to provide assurance that data sources remain trustworthy over time.

   These or other solutions, including the verification and validation methods used, can be determined within a country or country group.

b. *Trustworthy VC senders*: Senders that create messages within a VC system should be trustworthy, i.e., the processing that creates messages from data should not impact the property that the data in the message meets stakeholder expectations for the reliability of the data for its intended use.

   Possible solutions include:

   - Design of the sending system is reviewed for assurance that data is not modified (or added to) in a way that impacts its trustworthiness.
   - Sending systems are validated or certified to meet these requirements (by self-certification or third-party certification).
   - VC messages include integrity protection applied at the data source that can be checked by the receiver.
   - VC messages and/or protocols include mechanisms to allow receivers to validate that the sender is trusted and considered reliable in meeting these requirements.

   These or other solutions, including the verification and validation methods used, can be determined within a country or country group.

c. *Identification of sender*: Knowledge of sender identity or other properties (for example, that the sender is an emergency response vehicle) is important for some VC applications.

   Possible solutions include:

   - VC senders are issued with credentials asserting their identity or other properties following a process that establishes assurance that those properties truly apply.
   - VC receivers validate the identity and attributes of senders and the accuracy of their sources via standardised communications security mechanisms.

   The validation methods used by credential-issuing systems or by receivers can be determined within a country or country group.

d. *Data security*: Some types of VC could be subject to attacks on the communications security, such as breaches in confidentiality, breaches in authentication, replay attacks, traffic analysis attacks to impact security, etc.

   Possible solutions include: Use standardised communications-security techniques with the necessary properties to block identified threats.

e. *Reliability*: If transmitted information used for safety or vehicle control does not have the expected accuracy and reliability, it might be used in ways that degrade road occupant safety or impact other goals of the system.

   Possible solutions include:

   - Data sources and VC message senders are validated for reliability and trustworthiness as described in *Trustworthy data sources* and *Trustworthy VC senders* above.
   - Mitigate accuracy limitations by receive-side application approaches that use the information transmitted as a guide that is supplemented by information from other sources such as built-in sensors in vehicles.

f. *Privacy*: Information exchange among vehicles and road transport infrastructure components can raise privacy issues, especially with regard to the PII of vehicle occupants and other road occupants.

   Possible solutions include:

   - Authentication to access vehicle information.
   - Anonymisation and pseudonymisation of the information.

   Note that access and processing of PII is allowed:

   - With a vehicle occupant´s consent.
   - When necessary to protect vital interests of a vehicle occupant or another person.
   - Based on public interest.
   - In compliance with legal obligations.

g. *Cybersecurity*: VC is sensitive to cybersecurity threats, including hacking attempts and unauthorised access. Malicious actors might attempt to exploit vulnerabilities in communications protocols and compromise the integrity of transmitted information exchanged between vehicles and external systems.

   Possible solutions include: Implement systems by vehicle manufacturers to secure vehicles and their information (e.g., following ISO 21434 in conforming to UNR 155), often named CyberSecurity Management System (CSMS).

   Similarly, implement systems by road transport infrastructure operators to secure their components and information (e.g., following ISO 27001), often named Information Security Management System (ISMS).

h. *Information overload for human drivers and riders*: The amount of information provided to drivers and riders might increase with VC. Safety-related messages such

as warnings and cautions might be difficult for some drivers and riders to recognise when surrounded by other information.

Possible solutions include: The design of the in-vehicle Human Machine Interface (HMI) for such messages can take account the driver and rider workload and follow appropriate HMI guidelines.

i. *Vehicle service lives, backward compatibility, and future proofing*: Many vehicles have service lives of 15 years or more. This presents a significant challenge for vehicular communication, which need to function effectively over this extended period.

   Possible solutions include: Backward compatibility with futureproofing. Backward compatibility ensures that newer communication systems can still interact with older vehicles already on the road. Futureproofing, on the other hand, guarantees that the system can adapt to new technologies and evolving communication standards that will emerge in the coming years. New features and functionalities might not work with older vehicles, while a system overly focused on backward compatibility may struggle to integrate with future advancements. Vehicular communication systems should bridge this gap to be effective and safe over the long term.

j. *Communications interference*: VC can be disrupted by interference, either within the same frequency range (in-band) and from outside that frequency range (out-of-band). Such interference can disrupt or limit information exchange between vehicles, road transport infrastructure components, and the communications infrastructure.

   Possible solutions include: State of the art interference mitigation techniques. Adherence to relevant regulations on radio spectrum and its use can reduce interference to an acceptable level when implemented in communications devices.

k. *Damage to communications infrastructure*: Physical attacks, mishaps, fake infrastructure, environmental effects, power outage, etc. might cause roadside units and base stations to malfunction, disrupting communications. Also, see the *Cybersecurity* consideration above.

   Possible solutions include: Applications and communications systems can be designed resiliently with protections to handle potential issues. In addition, relevant service organisations can patrol regularly to ensure that the infrastructure is well maintained.

l. *Damage to built-in communications components*: Physical damage to built-in communications components, such as antennas and other built-in communications equipment, might compromise functions reliant on information exchange.

   Possible solutions include: Notifications about such issues can be provided to built-in systems, vehicle occupants, fleet managers, and vehicle manufacturers. Failsafe or fail-operational designs are possible. Physical designs can provide fall back or make repair easy.

m. *Latency*: Communications are subject to delays due to communications network equipment processing time, protocol setup time, radio-spectrum bandwidth limitations, transmission rate, transmission throughput, etc. In addition, delays can come from communications technology limitations. For example, cellular communication systems contain many communications network components (radio

base stations, gateway, etc.), which can cause delay. Satellite communication transmission paths are relatively long and lead to intrinsic delays.

Possible solutions include: VC applications can be designed so that the delays for the chosen communication methods match the latency requirements for the application. Factors such as the maximum number of communications participants at any time, the coverage of the chosen methods, and the supported vehicle speed can be considered. The minimum quality of service for VC applications can be ensured when designing the application.

n. *Limited Coverage*: Communications infrastructure can have areas of limited or no signal (dead spots). Such limits might disrupt information transmission.

Possible solutions include: Applications using VC can be designed to expect dead spots and areas of poor coverage. Information on VC coverage can be sent from in-vehicle applications and added to maps sent to vehicles. Alternative communications approaches, such as vehicle-to-vehicle Multihop or (possibly LEO) satellite, might provide an alternative for natural disaster and crisis management VC, even if the communications speed and bandwidth is lower.

o. *Service Outages*: Communications infrastructure can experience service outages due to technical failures (e.g., power cuts), tropospheric interference, maintenance activities, etc. Outages can range from short to lengthy in disaster situations. Also, see the *Damage to communications infrastructure* consideration above.

Possible solutions include: VC applications can be designed to be resilient to interruptions by communications infrastructure outages, both local and wide area. Temporary VC infrastructure can be provided by communications operators and authorities in disaster situation. Alternative communications approaches, such as vehicle-to-vehicle Multihop or (possibly LEO) satellite, might be an alternative for natural disaster and crisis management VC, even if the communications speed and bandwidth is lower.

p. *Geographic requirements*: VC is subject to rules, regulations, and practices that vary among countries and country groups. Different jurisdiction can have different (incompatible) communications infrastructure and/or communications regulations.

Possible solutions include: As with any other products and system sold internationally, planning and coordination between authorities, manufacturers, and users is required. Creating international regulations might help minimising variations. If the differences can be expressed digitally as rules, table-driven implementations, with relevant data for each jurisdiction, can allow software in a product to handle variations between jurisdictions. Flexible structures are possible, such as cellular eSIM.

q. *Protection and harmonisation of automotive safety-related radio spectrum*: Some radio spectrum has been allocated, and additional spectrum might be allocated, for safety-related VC. There can be inconsistencies in the frequency bands used for VC between countries and country groups. There is a risk of safety-related radio spectrum being used for other purposes due to demand for radio spectrum from other stakeholders.

Possible solutions include: The preservation or allocation of adequate, protected radio spectrum for safety-related VC might become a priority for communications regulators. Prompt commercial use of radio spectrum allocated for safety-related VC will help.

r. *Market Penetration*: Some VC applications require a substantial number of communications devices be deployed to function effectively.

   Possible solutions include: Authorities can encourage deployment, possibly with incentives. VC technologies can first expand using pre-existing, widely deployed communications infrastructure while bundling it with other VC technologies requiring a longer time to be effective due to the penetration constraint. If there is a substantial safety benefit from VC deployment for a specific use, harmonisation or regulation might be appropriate.

s. *VRU detection*: The communications devices used by VRUs can have limited positional accuracy. In addition, such communications devices might also have issues with reliability, availability of information (independent of whether a communications device is charged or switched on), etc.

   Possible solutions include: Built-in components for VRU protection can treat VC from VRU communications devices as supplementary information to the vehicle's sensors. Vehicles can use cameras, radars, and other technology, to capture information on VRUs to share with other vehicles using VC.

t. *Aftermarket equipment*: Aftermarket equipment with communications capabilities might have inferior capabilities to the capabilities of systems included in the vehicle at its manufacturer.

   Possible solutions include: Determining that the VC is coming from aftermarket equipment and taking possible lower reliability into account. VC applications can treat VC from aftermarket equipment as supplementary information.

   Aftermarket equipment should meet required standards for the accuracy of information including location. VC applications might be able to account for minor inaccuracies from aftermarket equipment and warn other vehicles.

   Aftermarket equipment can be required by regulation to indicate itself as aftermarket and not built-in.

u. *Interoperability*: The ability of vehicles and road transport infrastructure components to seamlessly exchange information in support of common services like collision avoidance or cooperative adaptive cruise control and achieving true interoperability is required.

   Possible solutions include: A unified approach can be created that ensures that vehicles from different manufacturers and road transport infrastructure components from different road operators or different service providers communicate effectively. Some applications using VC can use multiple communications technologies with different service levels according to availability and needs.

v. *Harmonised services*: Triggering conditions and minimum Key Performance Indicators (KPI) for senders and receivers of VC are varied and complex.

   Possible solutions include: Harmonised structurers can achieve effective communications-based services using recognised standards and practices. Industry organisations might create recommended KPIs for different parts of VC. Different service levels might be appropriate for different applications using VC. The service levels required might vary between communications device type.

w. *Compliance assessment*: Minimum performance of harmonised services using VC and the communicated information are expected.

   Possible solutions include: Achieve the required quality and accuracy and timeliness of transmitted information as well as the appropriate level of security for the communications services offered and information transmitted using recognised standards and practices.

x. *Costs vs. benefits*: Communications infrastructure, road transport infrastructure components, information exchange, maintenance, and built-in communications components as well as licenses and fees for some communications technologies might be expensive, depending on the benefits achieved by the applications using VC.

   Possible solutions include: A comprehensive investment by vehicle manufacturers and manufacturers of road transport infrastructure in VC which will depend on the benefits achieved by the applications using VC.

   Much of the communications infrastructure required is already in place in many markets. Additional expenditure on road transport infrastructure and systems for information exchange might be required for more benefits from VC.

   Costs can be handled as a policy issue when benefits accrue to society and not the manufacturer and suppliers.