International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

F.749.2

(03/2017)

SERIES F: NON-TELEPHONE TELECOMMUNICATION SERVICES

Multimedia services

Service requirements for vehicle gateway platforms

Recommendation ITU-T F.749.2

ITU-T F-SERIES RECOMMENDATIONS

NON-TELEPHONE TELECOMMUNICATION SERVICES

TELEGRAPH SERVICE	
Operating methods for the international public telegram service	F.1–F.19
The gentex network	F.20–F.29
Message switching	F.30–F.39
The international telemessage service	F.40–F.58
The international telex service	F.59–F.89
Statistics and publications on international telegraph services	F.90–F.99
Scheduled and leased communication services	F.100–F.104
Phototelegraph service	F.105–F.109
MOBILE SERVICE	
Mobile services and multidestination satellite services	F.110–F.159
TELEMATIC SERVICES	
Public facsimile service	F.160–F.199
Teletex service	F.200–F.299
Videotex service	F.300–F.349
General provisions for telematic services	F.350–F.399
MESSAGE HANDLING SERVICES	F.400–F.499
DIRECTORY SERVICES	F.500–F.549
DOCUMENT COMMUNICATION	
Document communication	F.550–F.579
Programming communication interfaces	F.580–F.599
DATA TRANSMISSION SERVICES	F.600–F.699
MULTIMEDIA SERVICES	**F.700–F.799**
ISDN SERVICES	F.800–F.849
UNIVERSAL PERSONAL TELECOMMUNICATION	F.850–F.899
ACCESSIBILITY AND HUMAN FACTORS	F.900–F.999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T F.749.2

Service requirements for vehicle gateway platforms

Summary

Recommendation ITU-T F.749.2 describes the service requirements and functional requirements for the vehicle gateway platform (VGP). The use cases and scenarios are described in Appendix I.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T F.749.2	2017-03-01	16	11.1002/1000/13183

Keywords

Intelligent transport system, ITS, service requirements, telematics, use cases, vehicle gateway platform, VGP.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g.,, interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T F.749.2

Service requirements for vehicle gateway platforms

1 Scope

This Recommendation specifies functional requirements for the vehicle gateway platform (VGP), including description, communication requirements and service requirements. Some use cases are included in Appendix I.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 functional entity [b-ITU-T Y.2012]: An entity that comprises an indivisible set of specific functions. Functional entities are logical concepts, while groupings of functional entities are used to describe practical, physical implementations.

3.1.2 intelligent transport systems (ITS) [b-ITU-R M.1797]: ITS can be defined as systems utilizing the combination of computers, communications, positioning and automation technologies to improve the safety, management and efficiency of terrestrial transport systems.

3.1.3 nomadic devices [b-ITU-T F.749.1]: Nomadic devices include all types of information and communication as well as entertainment devices that can be brought into the vehicle by the driver and/or passengers to be used while driving. Examples include mobile phones, portable computers, tablets, mobile navigation devices, portable media players and multi-functional smart phones.

3.1.4 telematics [b-ISO 15638-1]: Telematics is the use of wireless media to obtain and transmit (data) from a distant source.

3.1.5 vehicle gateway (VG) [b-ITU-T F.749.1]: A VG is a device in a vehicle that enables communications between a device in the vehicle and another device which may be physically located either inside the vehicle or outside the vehicle (e.g., roadside station, cloud-based server, etc.). A VG provides standardized interfaces and protocols, communications across heterogeneous networks, optimized network selection based on application needs and network QoS, arbitration and integration of network communications, security and switching network connections to maintain service continuity.

3.1.6 vehicle gateway platform (VGP) [b-ITU-T F.749.1]: A VGP is the collection of ICT hardware and software in a vehicle operating as an open platform to provide an integrated runtime environment for delivering the communications services of a VG. A VGP may also provide higher layer communications services such as interaction with the driver through the driver-vehicle access services and so on. Subsystems dedicated solely to vehicle operation are not considered part of the VGP. Supported applications/services include ITS and infotainment.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 driver-vehicle interface (DVI): The integrated user interface for the vehicle. It includes visual displays, loudspeakers, microphones, manual input controls, etc.

3.2.2 remote user interface: An approach to realize the interaction between applications in nomadic devices and the driver-vehicle interface (DVI). The UI of applications in nomadic devices can be displayed in the vehicle's touch screen, and drivers are able to control the applications through the DVIs (touch screen, buttons, etc.). A remote UI can help drivers avoid distraction from applications and thus reduce the probability of accidents.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2G	Second generation of cellular phone technologies
3G	Third generation of cellular phone technologies
4G	Fourth generation of cellular phone technologies
API	Application Programming Interface
ASR	Automatic Speech Recognition
DSRC	Dedicated Short Range Communication
DVI	Driver-Vehicle Interface
ECU	Electronic Control Unit
ETC	Electronic Toll Collection
FM-RDS	Frequency Modulation-Radio Data System
GNSS	Global Navigation Satellite System
INS	Inertial Navigation System
ITS	Intelligent Transport System
MAN	Metropolitan Area Network
NAT	Network Address Translation
NFC	Near-Field Communication
OSI	Open Systems Interconnection
POI	Point of Interest
PSAP	Public Service Answering Point
QoS	Quality of Service
RSU	Roadside Unit
TSP	Telematics Service Provider
TTS	Text to Speech
UI	User Interface
USB	Universal Serial Bus
VG	Vehicle Gateway
VGP	Vehicle Gateway Platform
VIN	Vehicle Identification Number
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network

5 Conventions

In this Recommendation:

– The keyword "shall" indicates a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

– The keywords "should" and "optional" indicate an optional requirement which is permissible. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the vendor. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Descriptions and characteristics of VGP

6.1 Descriptions

Figure 1 shows the VGP positioning in the intelligent transport system (ITS) reference model; six major sets of scenarios are defined:

1) Vehicle-to-vehicle

   The vehicle-to-vehicle scenario set mainly includes safety and auto-driving use cases in which some vehicles communicate with one another.

2) Vehicle-to-infrastructure

   The vehicle-to-infrastructure scenario mainly includes safety, electronic toll collection (ETC) and traffic information exchange use cases in which vehicles communicate with roadside infrastructures.

3) Vehicle-to-cloud-based server

   The vehicle-to-cloud-based server scenario set mainly includes emergency call and some telematics scenarios in which vehicles communicate with cloud-based servers.

4) Vehicle-to-nomadic device

   The vehicle-to-nomadic device scenario set mainly includes telecommunication and remote user interface (UI) use cases in which vehicles connect to nomadic devices.

5) Vehicle-to-pedestrian and bicycle

   The vehicle-to-pedestrian and bicycle scenario set mainly includes safety warning use cases in which vehicles communicate with devices carried by pedestrians and bicycles.

6) Interaction with in-vehicle network

   The interaction with in-vehicle network scenario set mainly includes vehicle diagnostics, remote data collection and vehicle remote control use cases in which the VGP communicates with the in-vehicle networks.

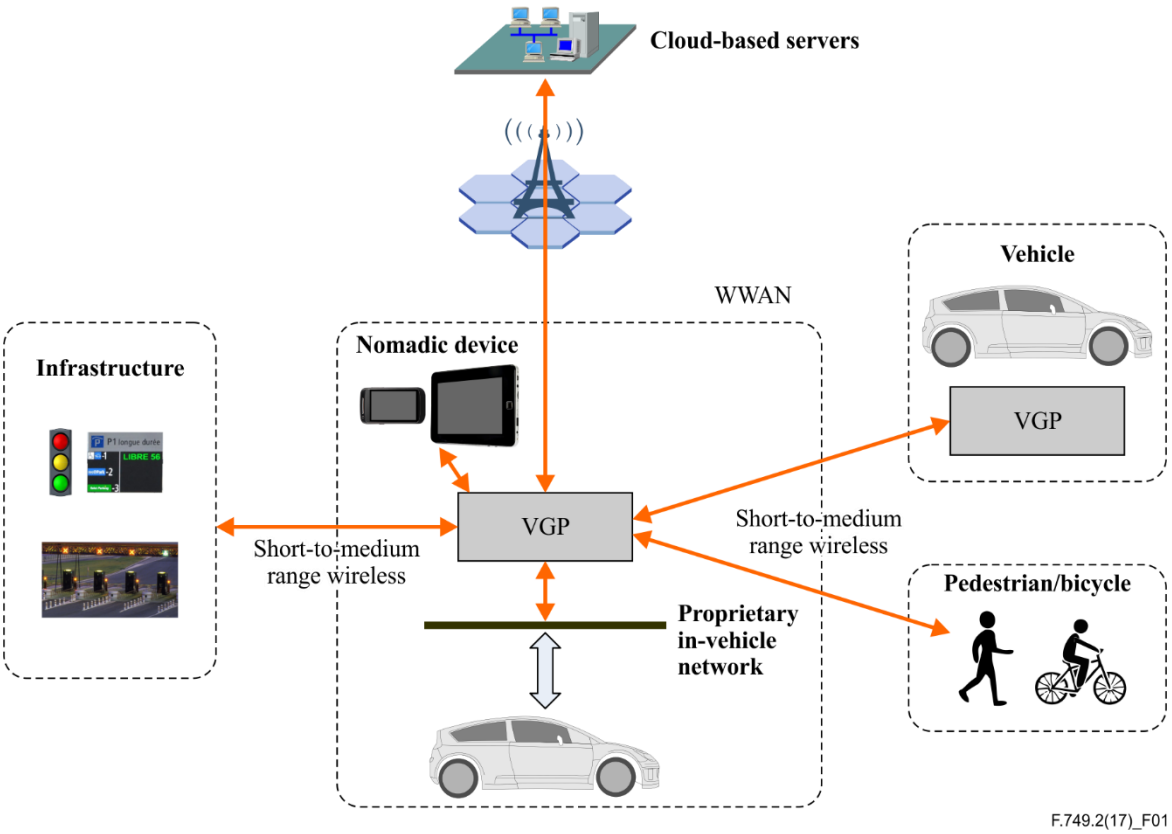

Figure 1 – VGP positioning in the ITS reference model

6.2 General characteristics

6.2.1 Access to external communication networks

The VGP has the ability to access communication networks including short-to-medium range wireless communication, such as the legacy dedicated short range communication (DSRC) or IEEE 802.11 (part of wireless access in vehicular environments) and wireless wide area network (WWAN).

6.2.2 Access to in-vehicle networks

The VGP shall support connectivity to in-vehicle sensors and controller networks in order to get information from, and/or control the vehicle.

6.2.3 Data process and transmission

The VGP shall support data transmission among in-vehicle networks, nomadic devices, cloud-based applications, roadside units (RSUs) and vehicle applications.

The VGP shall also support data formation, quality of service (QoS) management, priority management, etc.

6.2.4 Service or application interaction

The VGP shall encapsulate the communication and service capabilities as application programming interfaces (APIs) that can be invoked by external applications or services.

6.2.5 Secure data transmission

The VGP shall guarantee that data transmits securely, especially data exchanges between the external network and the in-vehicle data buses (vehicle diagnostics, vehicle control, etc.), and ensure that data cannot be tampered with or stolen.

The VGP shall support registration and authentication functions for nomadic devices and application access.

6.2.6 Management of the VGP

The VGP shall implement remote or local firmware and software updates, maintenance, configuration, priority strategies set and import, fault management and other functions.

The VGP shall provide fault prediction reports, diagnostics, recovery and log management.

7 Communication requirements for the VGP

7.1 External network connection requirements

The VGP should support ubiquitous connectivity to external communication networks. The network communication requirements for the VGP are as follows:

– The VGP should support two-way communications with local area wireless communication networks (e.g., DSRC ranges), WWANs (wireless metropolitan area network (MAN), 3G, 4G, etc.) and very short-range or near-field communication (NFC).

– The VGP should support wired (e.g., universal serial bus (USB)) and/or wireless connectivity with nomadic devices (e.g., smart phones, tablets, audio players) and other portable electronic equipment (e.g., cameras).

– The VGP should support communication with data broadcast networks such as frequency modulation-radio data system (FM-RDS).

– The VGP should be able to communicate with a fixed roadside infrastructure system via WWANs (e.g., wireless MAN, 3G, 4G) or wireless local area networks (WLANs) (e.g., DSRC).

– The VGP should be able to communicate with ad hoc roadside infrastructure (e.g., temporary roadwork beacons).

– The VGP should be able to communicate with other vehicles via WWANs (e.g., wireless MAN, 3G, 4G) or WLANs (e.g., DSRC).

– The VGP should be able to communicate with a road safety device carried by pedestrians and bicycles via WWANs (e.g., wireless MAN, 3G, 4G) or WLANs (e.g., DSRC).

7.2 In-vehicle connection requirements

In order to achieve vehicle diagnostics, control or vehicle data acquisition, the VGP should connect to the in-vehicle network. The in-vehicle connection requirements for the VGP are as follows:

– The VGP shall support the wired and wireless connectivity with the in-vehicle network and allow bidirectional communication with the connected electronic control units (ECUs) and sensors in the vehicle.

– The VGP shall support the control and management functions for communicating between external applications and the ECUs.

– When applications running on nomadic devices require access to in-vehicle networks, the VGP shall support authorisation management.

– When applications running on remote servers require access to in-vehicle networks, the VGP shall support authorisation management.

– The VGP shall support authorised access for services running within the VGP to access in-vehicle networks. When services running over the VGP require access to in-vehicle networks, the VGP shall support authorisation management.

7.3 Communication management requirements

The communication management requirements for the VGP are as follows:

– The VGP should allow external applications accessing the VGP to select the communication interface to use for transmission and reception of data.

– The VGP should allow services running over the VGP to select the communication interface to use for transmission and reception of data.

– The VGP should allow configuration of the transmission power level used for wireless communication with a device attached to the VGP in order to support a variable distance of transmission.

– The VGP should provide communication interfaces with different levels of QoS to cater to different communication scenarios.

– The VGP should provide communication interfaces with different levels of transmission priority settings to cater to different communication scenarios.

– The VGP should support selection of the access network according to certain criteria. For example, according to the type of service or network quality.

– The VGP should have a link layer address that identifies a radio transceiver attached to the VGP.

– The VGP should keep track of the connection status and quality of the connection for both the external networks and in-vehicle networks.

7.4 Communication security requirements

The communication security requirements for the VGP are as follows:

– The VGP shall support access security policies for external equipment and platforms.

– The VGP shall protect against cyberattacks.

– The VGP shall support data exchange security policies on open systems interconnection (OSI) 1-4 layer.

– The VGP shall support network end-to-end security functions to secure data transmission from the VGP to external devices (e.g., cloud servers, other VGP, nomadic devices).

– The VGP shall implement medium access security for communication between the VGP and the in-vehicle network as well as between the VGP and external networks.

– The VGP shall guarantee secure data exchange between the external network and the in-vehicle data bus.

– When the relaying function (see clause I.1) is available, the VGP shall support some security functions to authenticate the request for relaying.

– When the relaying function (see clause I.1) is available, the VGP data relaying service shall be secured at every layer of the data flow.

7.5 Networking requirements

– The VGP shall support the routing of packets between an external network and an in-vehicle network.

– The VGP shall support the routing of packets within a single external network or among multiple external networks.

– The VGP shall support IP-based and non-IP-based connections.

– The VGP shall support network address translation (NAT) functions for in-vehicle devices connected to in-vehicle networks and nomadic devices connected via an external network.

– The VGP shall support IPv4 and has optional support for IPv6 protocols.

– The VGP should support IP session handover across different IP sub-networks using the same wireless interface or different wireless interfaces.
– The communication devices attached to the VGP shall perform unicasting and should be capable of broadcasting and multi-casting messages to other VGPs or external devices.
– The VGP should be able to obtain its location information and transmit data within certain geographical boundaries (geo-casting).
– The VGP should provide data relaying services for a VGP using the same or different wireless communication interfaces.
– Relaying services should include configurable relaying service levels. The delay and bandwidth profile of the end-to-end relaying channel can be configurable based on user profiles and QoS settings.
– The VGP should be configurable to support data relaying.
– The VGP should implement one or several routing schemes to handle the relaying of the data.

8 Service requirements for VGP

8.1 Driver distraction management requirements

To mitigate driver distraction and workload, driver interaction with applications should be managed so that the driver is able to maintain situational awareness. Driver distraction management requirements for the VGP are as follows:

– The VGP shall acquire situational driving information from external entities.
– The VGP, to mitigate driver distraction, shall control when and how applications are used by the driver while driving the vehicle.

8.2 Session management requirements

The VGP is the hub of data/message exchange. Session management requirements for the VGP are as follows:

– The VGP shall support the routing and dispatching management of data/messages.
– The VGP shall support a data format process to guarantee high efficiency of data transportation.
– The VGP should support standard APIs to communicate with the local/cloud-based applications.

8.3 In-vehicle data resource access management requirements

In-vehicle data resource access management is an independent and isolated function to allow data exchange among external applications and the in-vehicle network. In-vehicle data resource access management requirements for the VGP are as follows:

– The VGP shall support selecting, organizing and converting in-vehicle data required for each managed function type (e.g., air conditioning, infotainment system, seat control, power train) in order to present data in a uniform and generic way.
– The VGP shall support access control functions so that an application or a service has access to only in-vehicle resources for which it has been authorized.
– The VGP shall support external application access to in-vehicle resources in a uniform way for the particular type of in-vehicle buses.

8.4 Driver-vehicle access management requirements

A driver-vehicle interface (DVI) is not included in the VGP. However, the VGP can control the interaction between applications and the DVI. The driver-vehicle access management requirements for the VGP are as follows:

– The VGP shall manage requests from applications to the DVI according to pre-configured policies or driving situations.

– The VGP shall manage instructions from the DVIs to applications according to pre-configured policies or driving situations.

– The VGP should manage the remote UI to approach the interface between applications and the DVI.

8.5 High-layer security requirements

If the higher-layer security policies are implemented, the high-layer security requirements for the VGP are as follows:

– The VGP shall protect against software attacks which target software vulnerabilities.

– The VGP shall support access control policies of applications.

– The VGP shall support user data privacy protection.

– The VGP shall support cipher, key, digital signature and certificate management.

8.6 Software management requirements

To maintain the VGP, improvements of current services and the potential deployment of new services inside and outside the VGP, it is required that the VGP provides the following requirements:

– The VGP shall support software management from external devices or servers in a safe, secure and flexible way. In particular, it shall be able to manage monitoring, adding, removing and updating of software packages.

– The VGP shall support software management of services running inside the VGP in a safe way.

– The VGP shall support software management of services running over in-vehicle devices connected to the VGP through in-vehicle buses in a safe way.

– The VGP shall support software version checking to ensure software version coherency between the various devices and services.

– The VGP shall maintain and provide access to a journal containing all management operations performed by the VGP. This journal must be protected with signature and encryption schemes in order to provide reliability and verifiability of the logs.

8.7 Application data management requirements

To maintain the VGP and improvements of current services, it is required that the VGP provides the following requirements:

– The VGP shall support application data management from external devices or servers in a safe, secure and flexible way. In particular, it shall be able to manage reading, adding, removing and modifying application data.

– The VGP shall support, in a safe way, application data management of services running inside the VGP.

– The VGP shall support, in a safe way, application data management of services running over in-vehicle devices connected to the VGP through in-vehicle buses.

– The VGP shall support application data version checking to ensure coherency with the software version running over the VGP or in-vehicle devices.
– The VGP shall support application data sharing among different services and access management (ownership, permissions).
– The VGP shall provide the capability to associate some metadata to data entries, such as size, data type.
– The VGP shall maintain and provide access to a journal containing all accesses and operations done to any data entries and their associated metadata. It must be protected with signature and encryption schemes in order to provide reliability and verifiability of the logs.

Appendix I

VGP use cases

(This appendix does not form an integral part of this Recommendation.)

I.1 Background

The following entities consume or initiate the interactions with the VGP. They are used to describe the various use cases:

– Vehicle gateway platform
– Vehicle sensors and input devices (e.g., global navigation satellite system (GNSS), cameras)
– Vehicle controller system (e.g., ECUs)
– Drivers
– Passengers
– Infrastructure systems (e.g., RSU)
– External mobile devices
– In-vehicle nomadic or mobile devices (e.g., navigation devices, tablet PCs)
– Servers (e.g., cloud servers)
– Pedestrians
– Call centres.

I.2 Vehicle-to-vehicle interaction use cases

Vehicle-to-vehicle interaction may occur under several usage scenarios and the interactions may be triggered by various entities, see Figure I.1.

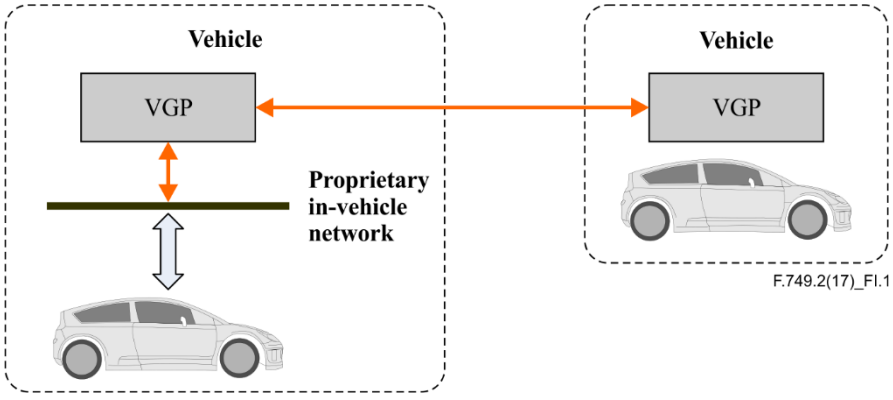

Figure I.1 – Vehicle-to-vehicle scenario

Examples of vehicle-to-vehicle use cases are described in the following clauses.

I.2.1 Vehicle-to-vehicle safety scenario

In the vehicle-to-vehicle safety scenario, real-time information of a vehicle such as its speed, direction, location, etc., is collected from in-vehicle sensors (within the VGP or possibly connected to vehicle controllers) by the VGP and is broadcast to the surrounding vehicles. The surrounding vehicles will then collect this information and use it to derive the safety context of the environment. Once the safety context is fully understood, the vehicles can then derive other safety warnings such as lane change warnings, forward collision warnings, etc. Besides sending raw sensor information, the VGP may also send processed safety context information in the form of alarms or warning

messages to other vehicles. For example, if a vehicle senses an obstacle ahead, the vehicle could send this information to other nearby vehicles. This information can be sent either in a broadcast, unicast, multicast or geo-cast manner. The processed safety information or warnings that are received by a vehicle may also be displayed by a UI attached to the VGP or sent to the UI of a nomadic mobile device associated with the VGP.

The vehicle-to-vehicle safety messages may be set as high-priority messages and transmitted over a dedicated wireless channel (frequency or timeslot) or a dedicated radio device. For this vehicle-to-vehicle safety scenario, security functions are implemented at every stage of information gathering, transmission and processing, to ensure the integrity of the data and processed information. Security functions are implemented to ensure that the integrity of the sensory data is not compromised by cyber security attacks. Transmission of data from one hardware/software block to another or from one vehicle to another is authenticated and secured along the entire transmission medium.

I.2.2 Vehicle-to-vehicle data relaying

In the vehicle-to-vehicle relaying scenario, the VGP of a vehicle is used to relay data such as software updates, telematics data or application data to an end destination, which could be a vehicle or an infrastructure system. Such a use case could happen if an infrastructure system, driver, passenger (via mobile device) or vehicle chooses to use a relaying approach to reach the end destination because of lower-cost communication or perhaps due to the lack of other viable communication methods.

The delay and bandwidth profile of the end-to-end relaying channel can be configurable based on user profiles and QoS settings. The transmission of the vehicle-to-vehicle relayed data could be based on either unicast, broadcast, multicast or geo-cast. Security functions are implemented to ensure end-to-end data integrity and security. The VGPs participating in the relaying of data should ensure that no cyber security attacks to the relayed information have occurred.

I.2.3 Platooning

The platooning scenario can be seen as a special case of a vehicle-to-vehicle safety use case. Real-time information of a vehicle such as its speed, direction or location is collected from the in-vehicle sensors (or possibly vehicle controllers) by the VGP and is broadcasted, unicasted or multi-casted to the vehicles in the platoon. The lead vehicle that controls the platoon uses this information to derive the movement control information and surrounding safety context information of the environment.

The processing of the movement control and surrounding safety context information, which is required to implement the platooning functions, can be carried out by a separate vehicle controller or by the VGP. In either case, the movement control information and safety context information is sent to the vehicles in the platoon to control their movement via the VGP. For the platooning scenario, security functions are implemented at every stage of information gathering, transmission and processing to ensure the integrity of the data and processed information. Security functions are implemented to ensure that the integrity of the sensory data is not compromised by cyber security attacks. Transmission of data from one hardware/software block to another or from one vehicle to another is authenticated and secured along the entire transmission medium.

I.3 Vehicle-to-infrastructure interaction use cases

Vehicle-to-infrastructure interaction may occur under several usage scenarios and the interactions may be triggered by various entities. Vehicle-to-infrastructure interaction may happen either through WWANs (e.g., cellular networks) or WLANs (e.g., DSRCs) and typically cover the interaction between vehicles and roadside infrastructure (which are normally transportation-related infrastructure physically located within the road networks); see Figure I.2.

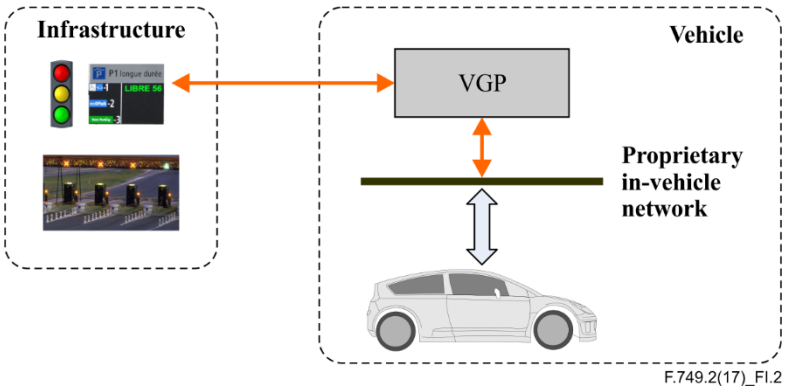

Figure I.2 – Vehicle-to-infrastructure scenario

Examples of vehicle-to-infrastructure use cases are described in the following clauses.

I.3.1 Vehicle-to-infrastructure safety

Vehicle-to-infrastructure safety scenarios involve the interaction between a vehicle and roadside infrastructure to provide navigation safety to drivers. One example is an intersection safety system which consists of roadside sensors that collect contextual information of positions and movement of vehicles and other road users. The system will then process the trajectory of the detected objects and provide warnings to vehicles or drivers navigating an intersection.

Another vehicle-to-infrastructure safety service is the traffic controller signal phase and timing information, which can be used by the vehicle or driver to plan their movement through an intersection. In these vehicle-to-infrastructure examples, processed safety information can be broadcast to the vehicles from the roadside infrastructure. Vehicles can also assist the safety system by sending their real-time information such as speed, direction, location, etc., which is collected from the in-vehicle sensors (within the VGP or possibly connected to vehicle controllers) by the VGP to the roadside infrastructure. For example, if a vehicle senses an obstacle ahead, the vehicle could send this information to nearby vehicles. The information from the roadside infrastructure can be sent either in a broadcast, unicast or geo-cast manner. The processed safety information or warnings that are received by a vehicle can be displayed by a UI attached to the VGP or the UI of a nomadic device associated to the VGP. Some vehicle-to-infrastructure safety services such as vehicle priority at intersections may require a longer distance communication with the roadside infrastructure. In such cases, the VGP in the vehicle requesting the service may select a different radio communication unit or change its power setting to ensure a longer distance communication. While the examples given above describe a permanent roadside infrastructure setup, there can also be ad hoc deployment of roadside infrastructure such as temporary road works. The interaction of such a system is expected to be the same as the permanent setup. The vehicle-to-infrastructure safety messages may be set as high priority messages and transmitted over a dedicated wireless channel. The messages sent from the roadside infrastructure and vice versa is secured at every stage of the message flow. Security functions are implemented to ensure that the integrity of the sensory data from the vehicle and the messages from the infrastructure are not compromised by cyber security attacks.

I.3.2 Vehicle-to-infrastructure traffic management

The vehicle-to-infrastructure traffic management use case involves the use of roadside infrastructure to provide traffic management functions and services such as ETC, probe data collection from vehicles, traffic information upload and download. The interaction between the VGP and the roadside infrastructure is similar for these services. In the road toll collection system, the VGP may be connected to a payment system (pre-paid or post-paid). The payment transaction for the ETC system involving the VGP and the roadside infrastructure must be secured to ensure no fraudulent payment. For the probe data collection, the VGP may upload a pre-recorded probe data collected by the VGP

or real-time data to the infrastructure device. Similar to the vehicle-to-infrastructure safety use case, security functions are implemented to ensure that the integrity of the data from the vehicle to the infrastructure and vice versa is not compromised by cyber security attacks.

I.3.3 Vehicle-to-infrastructure commercial and access control

Vehicle-to-infrastructure commercial and access control services could be services provided by commercial companies, transport authorities or other governmental agencies. For example, commercial services could include parking management, rental car transaction, vehicle diagnostic and fuelling station. In most cases, the interaction between the infrastructure and vehicle is similar to the vehicle-to-infrastructure traffic management use case, whereby there is an infrastructure device at the roadside. In some cases, it may involve the interaction between a third-party mobile device (external but nearby the vehicle) and the VGP. One such case is the use of mobile diagnostic equipment carried by vehicle service personnel to query information about a vehicle's status. In this case, the VGP will allow authorised access to the vehicle's ECUs. In another case, a parking attendant may use a mobile device to communicate with the VGP to request parking status from the vehicle. Some of these services may even use an NFC to communicate between the external mobile device and the VGP. Access control services include border crossing applications and drive-through applications. In these applications, the use of secure credentials and unique identification to identify the vehicle or its owner is important. In some cases, for example, when a vehicle is in a service centre, the authentication approach may even involve two-level authentication, which requires the user to key in a special code via the VGP's UI.

I.4 Vehicle-to-nomadic device interaction use cases

Vehicle-to-nomadic device interaction use cases include the interoperation among the VGP and nomadic electronic products such as mobile devices, personal productivity devices (e.g., notebooks, tablets) and navigation devices. See Figure I.3.

As nomadic devices can cause driving distractions, the interaction and interfaces to the applications of vehicle-to-nomadic devices need to be carefully designed. Nomadic devices may be used for starting voice calls or accessing telematics applications. Nomadic devices may also be used by drivers or passengers within a vehicle to access Internet applications. Some examples of vehicle-to-nomadic device usage categories are as follows:

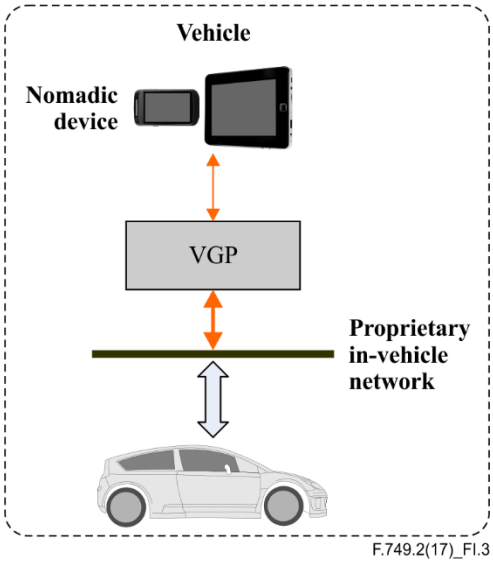

Figure I.3 – Scenario of vehicle-to-nomadic device interaction

Example 1: A driver can start/hang up a voice call through the UI (e.g., touch screen, button, microphone) attached to the VGP and through the communication link in a nomadic device. The VGP may synchronize the application data (e.g., address book) with the nomadic device.

Example 2: The VGP can be used as a personal hotspot for nomadic devices carried by a driver or passengers. Pre-configured pairing or per-session pairing (with perhaps manual password entry) to access to the in-vehicle hotspot is possible. In this scenario, the VGP must ensure that the UI operation causes minimal driver distraction.

Example 3: Nomadic devices may also interoperate with the VGP to access UI support functions such as automatic speech recognition (ASR)/text to speech (TTS)/remote UI technologies that can reduce driver distraction. For example, a personal navigation device can be used for navigation purposes. In this scenario, the device may have its own sensors such as GNSS/inertial navigation system (INS) or may access the VGP to obtain geographic information. The navigation device can use remote UI technology to project the applications on the vehicle's screen via the VGP. The navigation device may also access the audio devices through the VGP to output the audio feedback of route guidance or use the TTS/ASR applications to provide an audio input from the driver to control the navigation device. The VGP may connect to a sensor such as a video camera that can track a driver's distraction level to decide on what kind of UI can be used by the driver when using nomadic devices.

I.5 Vehicle-to-cloud interaction use cases

The vehicle-to-cloud use cases include the interoperation between the vehicle and the cloud-based servers; see Figure I.4.

Within a vehicle, the originator of information could be a passenger, the driver, in-vehicle mobile devices, VGPs or the vehicle owners. In the vehicle-to-cloud use cases, the interaction occurs through the WWAN (e.g., cellular networks) or short/medium range (e.g., DSRC, IEEE 802.11) communication infrastructure.

Some examples of vehicle-to-cloud use cases are described in the following clauses.

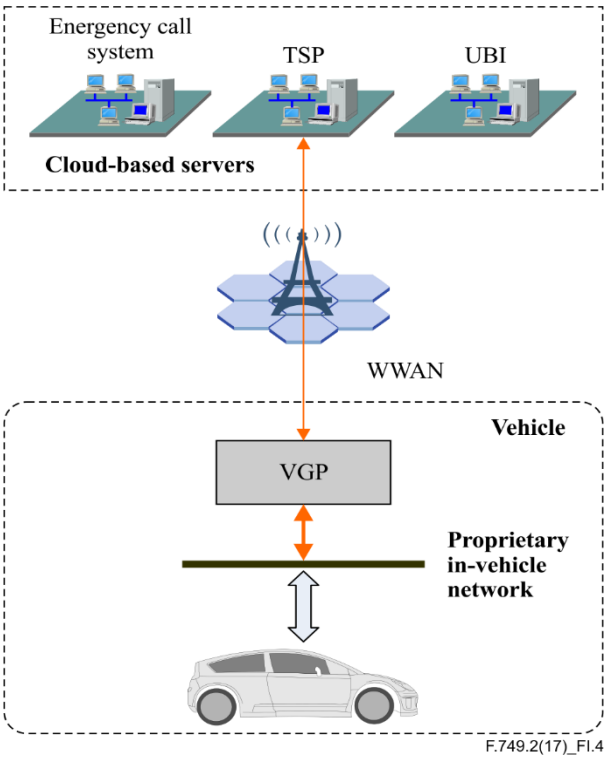

Figure I.4 – Scenario of vehicle-to-cloud-based server

I.5.1 Vehicle-to-cloud emergency scenario

When a crash or accident occurs, an emergency call to the call centre of the telematics service provider (TSP) or public service answering point (PSAP) is initiated automatically or by manually pressing the emergency call button in the vehicle. At the same time, the geolocation data, accident information and vehicle identification number (VIN) of the vehicle are transmitted to the TSP or PSAP. The TSP or PSAP operator communicates to the public rescue agency immediately to take action and provide medical and/or roadside assistance. A good example of this use case is the European Union's eCall plan for all of Europe, which strives to shorten rescue time in accidents and save many lives each year.

I.5.2 Vehicle-to-cloud telematics scenario

Some examples of a TSP's services include: emergency call, B-call, anti-theft, remote diagnostic and control, navigation assistance, eco-driving, infotainment and remote software update.

The following is a non-exhaustive list of vehicle-to-cloud telematics scenarios:

– B-call scenario: When a vehicle breaks down, the driver presses a button in the vehicle to start a call to the call centre and transmits the GNSS information of the vehicle. The operator at the call centre contacts the rescue agency to provide quick roadside assistance.

– Anti-theft scenario: When a vehicle is stolen, the driver can start a call to the call centre. The operator can communicate with the vehicle and remotely track the vehicle. The operator can take proper actions, such as alerting the police, immobilizing the vehicle, etc.

– Remote control scenario: Drivers can remotely control heating and ventilation in the vehicle to start during winter/summer by using a mobile phone or calling the call centre. Also, in this scenario, when a driver forgets their key, they can unlock the vehicle by using an authorised mobile phone or calling the call centre.

– Eco-driving scenario: Eco-driving can promote good driving behaviour, increase fuel-efficiency and reduce carbon emissions. The VGP collects real-time vehicle operation information and transmits this information to a remote telematics platform. The telematics platform analyses the data and sends driving suggestion reports to the driver.

– Navigation assistance scenario: Navigation assistance provides the functions of path planning and navigation. Drivers can press a button to start a call to the call centre and speak with an operator. The driver can provide their destination and require assistance. The operator searches for the best routes and sends this information to the VGP. The VGP can either transmit this information to the vehicle's built-in navigation system or to a nomadic device connected to the VGP.

Other examples of telematics applications are infotainment applications. These applications include: weather conditions, point of interest (POI) searching (e.g., gas stations, parks and restaurants), booking services (e.g., plane tickets, restaurants, hotels), online news and online music.

Most of the telematics applications mentioned above require a remote software update feature. Remote service or application update may occur in the VGP or nomadic devices attached to the VGP. The VGP may periodically connect to various service providers' cloud servers to retrieve software binary updates and to apply bug fixes or version updates to provide new features. Once the files are downloaded, the VGP can help coordinate the installation of the files to the corresponding modules. The entire process of software updates to the nomadic devices or the VGP must be secure to protect against cyber security attacks. For applications downloaded to a nomadic device, proper authentication with the VGP must be present to ensure secure communication.

I.5.3 Vehicle-to-cloud usage-based insurance

Usage-based insurance (UBI) service involves the collection, by insurance companies, of actual driver behaviour data and is used for linking premium pricing schemes in accordance with actual mileage and driving behaviour.

Data can be collected with the aid of the VGP, a digital map with current speed limits for various road links, etc., and matching how, where, when, and at what speeds the vehicle is driven. These data are transmitted to the insurance company and reduce ambiguous information about driving patterns making it possible to charge an individual a customised premium.

I.6 Vehicle-to-pedestrian and bicycle interaction use cases

The vehicle-to-pedestrian and bicycle use cases cover mainly the safety aspects of pedestrians or vulnerable users. In the vehicle-to-pedestrian and bicycle use cases, a mobile device carried by road users would send out its location via a dedicated short-range communication medium (e.g., DSRC) to warn drivers. For example, when a pedestrian appears from behind a parked car or other obstruction, the driver in the vehicle would receive an alert. The pedestrian may also get an alert on their mobile device. The authentication of the mobile device in this use case is important to protect against cyber security attacks or unwanted disruption to the operation of the vehicle.

Bibliography

[b-ITU-T F.749.1] Recommendation ITU-T F.749.1 (2015), *Functional requirements for vehicle gateways*.

[b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2010), *Functional requirements and architecture of next generation networks*.

[b-ITU-R M.1797] Recommendation ITU-R M.1797 (2007), *Vocabulary of terms for the land mobile service*.

[b-ETSI EN 302 665] ETSI EN 302 665 v1.1.1 (2010-09), *Intelligent Transport Systems (ITS); Communications; Architecture*.

[b-ISO 7498-1] ISO 7498-1 (1994), *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.

[b-ISO 15638-1] ISO 15638-1 (2012), *Intelligent transport systems – Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) – Part 1: Framework and architecture*.
[https://www.iso.org/standard/59184.html]

[b-ISO 21210] ISO 21210 (2012), *Intelligent transport systems – Communications access for land mobiles (CALM) – IPv6 Networking*.

[b-ISO 21212] ISO 21212 (2008), *Intelligent transport systems – Communications access for land mobiles (CALM) – 2G Cellular systems*.

[b-ISO 21213] ISO 21213 (2008), *Intelligent transport systems – Communications access for land mobiles (CALM) – 3G Cellular systems*.

[b-ISO 21214] ISO 21214 (2015), *Intelligent transport systems – Communications access for and mobiles (CALM) – Infra-red systems*.

[b-ISO 21216] ISO 21216 (2012), *Intelligent transport systems – Communications access for land mobiles (CALM) – Millimetre wave air interface*.

[b-ISO 24102-1] ISO 24102 (2013), *Intelligent transport systems – Communications access for land mobiles (CALM) – ITS station management – Part 1: Local management*.
[https://www.iso.org/standard/61561.html]

[b-ISO 24102-2] ISO 24102 (2015), *Intelligent transport systems – Communications access for land mobiles (CALM) – ITS station management – Part 2: Remote management of ITS-SCUs*.
[https://www.iso.org/standard/61563.html]

[b-ISO 24102-3] ISO 24102 (2013), *Intelligent transport systems – Communications access for land mobiles (CALM) – ITS station management – Part 3: Service access points*.
[https://www.iso.org/standard/61564.html]

[b-ISO 24102-4] ISO 24102 (2013), *Intelligent transport systems – Communications access for land mobiles (CALM) – ITS station management – Part 4: Station-internal management communications*.
[https://www.iso.org/standard/61565.html]

[b-ISO 24102-5] ISO 24102 (2013), *Intelligent transport systems – Communications access for land mobiles (CALM) – ITS station management – Part 5: Fast service advertisement protocol (FSAP)*.
[https://www.iso.org/standard/61566.html]

[b-ISO 29281] ISO 29281 (2011), *Intelligent transport systems – Communications access for land mobiles (CALM) – Non-IP networking*.
[https://www.iso.org/standard/45379.html]

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	**Non-telephone telecommunication services**
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017