-D4.1 –Specification of Connected Vehicle System

Security Assurance Framework for Networked Vehicular Technology

Abstract

SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-X (V2X) communications aiming at improving the cyber-physical security ecosystem of “connected vehicles” in Europe. The project will deliver innovative techniques, development methods and testing models for efficient assurance of security, safety and data privacy of ICT related to Connected Vehicles and V2X systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics, services and integration with 3rd party components and applications. The cornerstone of SAFERtec is to make assurance of security, safety and privacy aspects for Connected Vehicles, measurable, visible and controllable by stakeholders and thus enhancing confidence and trust in Connected Vehicles.

Dx.y & Title:	**D4.1 Specification of Connected Vehicle System**
Work package:	WP4 Connected Vehicle System
Task:	T4.1 Connected Vehicle System specification
Due Date:	30 September 2017
Dissemination Level:	PU
Deliverable Type:	R

Authoring and review process information	
EDITOR Alessandro Marchetto / CRF	DATE 19/07/2017
CONTRIBUTORS Alessandro Marchetto András Varadi / COMM Silvia Capato / SWR Elana Copperman /AUT Panagiotis Pantazopoulos / ICCS Nicolas Brailovsky / TOM	DATE 23/08/2017 28/09/2017 21/09/2017 18/09/2017 25/09/2017 28/09/2017
REVIEWED BY Nicolas Brailovsky / TOM Paul-Emmanuel Brun / CCS	DATE 29/09/2017 29/09/2017
LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?	
NO	

Document/Revision history

Version	Date	Partner	Description
V0.0	19/07/2017	CRF	Template with document structure
V0.3	23/08/2017	CRF	First draft
V0.4	01/09/2017	CRF	Second draft
V0.5	06/09/2017	CRF	ICCS feedbacks on section 2 and section 5
V0.6	06/09/2017	CRF	Executive Summary, Section 1 and Conclusions
V0.7	07/09/2017	TomTom	Contribution
V0.8	11/09/2017	TomTom	Contribution
V0.9	15/09/2017	Swarco	Contribution
V0.10	18/09/2017	Autotalk	Contribution
V0.11	21/09/2017	Commsigna Swarco	Contribution
V0.12	25/09/2017	ICCS	Contribution
V0.13	27/09/2017	CRF	Integration of partner contributions
V0.14	27/09/2017	CRF	Sent to TomTom and CCS for the internal review
V0.15	02/10/2017	CRF	Final version

Table of Contents

Table of Figures

List of Tables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Acronyms and abbreviations

Table 1: List of Abbreviations

Abbreviation	Description
ADAS	Advanced Driver-Assistance Systems
AFT	Assurance Framework Toolkit
C-ITS-S	Central ITS Station
CAN	Controller Area Network
CPS	Cyber-physical Systems
Dx.y	Deliverable x.y
DoA	Description of Action
DSRC	Dedicated Short-range Communications
EU	European Union
HAD	Highly Automated Driving
ICCS	Institute of Communication and Computer Systems
IoT	Internet of Things
OBU	On Board Unit
OCIT	Open Communication Interface for Road Traffic Control Systems
PND	Personal Navigation Device
R-ITS-S	Roadside ITS Station
SAE	Society of Automotive Engineers
SW	Software
T	Task
TTI	Traffic and Travel Information
V2I	Vehicle-to-Infrastructure
V2X	Vehicle-to-Everything
WLAN	Wireless Local Area Network
WP	Work Package

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Executive Summary

The objective of SAFERtec is to design and validate a flexible security assurance framework for Connected Vehicles. Towards that end, WP4 develop and integrate the ‘connected vehicle system’ to enable the framework’s validation. The aim of this deliverable is to present the WP4 specification work; namely, to (1) design and specify the SAFERtec hardware and software architectures, including relevant components, communication means and interfaces, for the reference connected vehicle system; and (2) introduce the motivation and rationale for the design and specification decisions made on each part of the envisioned and designed architecture.

In order to properly design and specify the connected vehicle system, all requirements and needs emerging from the use cases of interest for the SAFERtec project, detailed in the Deliverable D2.1 “Connected Vehicle Use Cases” (M6), have been considered and summarized in the initial sections of this deliverable, aiming at highlighting aspects that are relevant for the architecture design choices.

From a practical point of view, the reference connected system designed and specified in this deliverable will be implemented and realized along the following project tasks: T4.2 (“V2X HW & SW module”), T4.3 (“Implementation of RSU system (Component/System Level”), and T4.4 (“Implementation of 3rd Party Applications and Services”). Those three tasks will be detailed in Deliverable D4.2 (“Modules and Applications of Connected Vehicle” – M20) while the work of the final T4.5 (“Connected Vehicle System Integration”) will be reported in Deliverable D4.3 (“Integration of Connected Vehicle System” – M22).

The herein introduced architecture of the connected vehicle system will be (later) considered in the project task T5.3 (“Composite Evaluation”), to be described in the deliverable D5.4 (“Composite Evaluation of SAFERtec Assurance Framework”– M36) of WP5 (“Assurance Framework Evaluation”). The prescribed connected vehicle system, hence, will provide the means towards the evaluation of the SAFERtec assurance framework.

The present deliverable is mostly meant as a guideline for the implementation of hardware and software components of the reference connected system considered in SAFERtec. The starting point is a summary of requirements and technical aspects about the use cases of interest for SAFERtec. Then, the envisioned overall connected system architecture is presented. Subsequently, security aspects involved in vehicular communications are reported and summarized in terms of state-of-the-art. All relevant (hardware and software) components, communication interfaces and protocols are then detailed while associated risks and relevant mitigation plans are detailed in the Appendix A1. Finally, the conclusions of the final section summarize the deliverable content and highlight relevant points of the deliverable content.

1. Introduction

The present Deliverable D4.1 entitled "Specifications of Connected Vehicle System", as part of the WP4 work on the "Connected Vehicle System" presents the outcome of the task T4.1 "Connected Vehicle System Specifications". The deliverable describes the design, the architecture and specifications of a reference connected vehicle system. This designed reference system is to realize the use cases of interest of the SAFERtec project that are described in the deliverable D2.1 ("Connected Vehicle Use Cases" – M6).

In more detail, this deliverable specifies the architecture and all the involved components (e.g., embedded devices, on/off-board units, and vehicle networks) of the three main actors constituting the connected vehicle system: the vehicle (platform), the road side unit and the cloud infrastructure. Furthermore, it sheds some light on the involved public-key encryption and certificates needed to secure the exchange of data. Detailed descriptions of the hardware components and software modules available in the connected vehicle system are provided together with brief mentions to the adopted communication mean (ITS G5 and cellular technology) and the adopted (in-vehicle) communication protocols (with relevant security controls highlighted). Finally, the interfaces to facilitate the communication between all above modules and the hosted applications are introduced in this deliverable. In the Appendix A1 we elaborate on the risks that pertain to the architecture and technologies we herein proposed. We roughly estimate the possibility of their occurrence, assess their impact and highlight mitigations plans for each of the identified risks.

1.1 Purpose of the Document

The document seeks to specify and design both the hardware and software architecture of the reference SAFERtec' connected vehicle system that will be used to realize the project use cases and furthermore validate the proposed assurance framework. In more detail, the document the design and the specifications of the in-vehicle, the road side unit and the 3rd party cloud infrastructure architecture as well as the way in which these components (of the connected vehicle system) communicate.

1.2 Intended readership

Besides the project reviewers, this deliverable is addressed to any interested reader (i.e., PU dissemination level).

1.3 Inputs from other projects

No input from other projects was considered during the compilation of this deliverable.

1.4 Relationship with other SAFERTEC deliverables

A dependency exists between this deliverable and the deliverable D2.1, "Connected Vehicle Use Cases" (M6), related to WP2 ("Reference Modelling and Requirements"). The deliverable D2.1 details the use cases of interest for the SAFERtec project that have to be realized by means of the reference connected vehicle system which is specified and designed in this deliverable. Relevant aspects about such use cases are summarized in Section 3 of this deliverable (see below).

The content of this deliverable will impact other deliverables of the WP4 (“Connected Vehicle System”). In fact, it designs and specifies the reference system that will be physically realized in D4.2 (“Modules and Applications of Connected Vehicle” – M20) and integrated in D4.3 (“Integration of Connected Vehicle System” – M22). Additionally, this deliverable will also impact the deliverable D5.4 (“Composite Evaluation of SAFERtec Assurance Framework”– M36), related to WP5 (“Assurance Framework Evaluation”) since it designs and specifies the reference system that will serve as the basis for the assurance framework evaluation tasks.

2. Connected Vehicle System

The advent of ICT technologies and the spreading of digital computers have completely changed the way we live and interact. The number of services enabled by such technological artefacts is pushing the digitalization of vehicles and interconnection of vehicles giving rise to the emerging paradigm of "Connected vehicle systems". The connected vehicle system can be perceived as a dynamic Cyber-physical system comprised by highly-equipped infrastructure-connected vehicles with numerous third-party components.

The involved connected vehicles can dynamically retrieve information on road events/conditions, such as traffic data or weather conditions and thus, significantly improve driving safety and efficiency. Having in place a communication channel between vehicles and infrastructure enables the deployment of totally new services utilizing information collected by the infrastructure (or other peer-vehicles). Eventually, vehicles will no-longer act as isolated actors; they will be for instance enabled to cross intersections without the need of traffic lights or human intervention and/or exploit notifications received by dedicated infrastructure (or peer-vehicles) towards better traffic management.

In upcoming or near-future driving scenarios, the need to perform more complex manoeuvres without the driver intervention would require taking the control of engine, braking and steering systems from the drivers' command. These new capabilities clearly increase the vehicles' attack surface and may realize new dangers in terms of safety and privacy for the drivers. The connected vehicles would expose the in-vehicle systems (i.e., dedicated V2X hardware and applications) to remote attacks at distances that can range from several meters (through Bluetooth and Wi-Fi) to hundreds of meters (with DSRC/ITS-G5 technology) or even under an unlimited range (with the cellular connectivity).

In view of the numerous security solutions that become relevant under this paradigm, SAFERtec will lay the basis for assessing the confidence that the involved security needs are fulfilled. It will propose a flexible and efficient assurance framework for security and trustworthiness of connected vehicles and V2I communications. The way to realize an instance of the considered connected vehicle system (that will serve as the basis for the framework's validation) will be discussed in the following sections of the document.

3. SAFERtec’s use cases

The SAFERtec selected use-cases are the starting-point for this deliverable. The project has carefully selected a set of automotive use cases on the basis of safe-criticality, usefulness and problem-tractability (see D2.1 for detailed comments on the selection criteria). Having these use-cases realized using a prototype vehicle, dedicated (short and long range V2X communication technology and RSU) hardware as well as a number of relevant applications (e.g., infotainment, cloud-based etc.), the project seeks to create a realistic environment to test and validate the introduced security assurance framework.

Out of numerous instances of V2I communications the project will focus on a limited yet challenging set that may either involve the vehicle’s communication either with an RSU- or with a cloud-based service (see Figure 1 for indicative illustrations). An effort to identify use-cases that lend to both types of V2I communications (i.e., RSU and cloud) has been taken. Their comparative study can provide the project with useful hints on the way that different communication technologies influence the involved levels of security assurance.

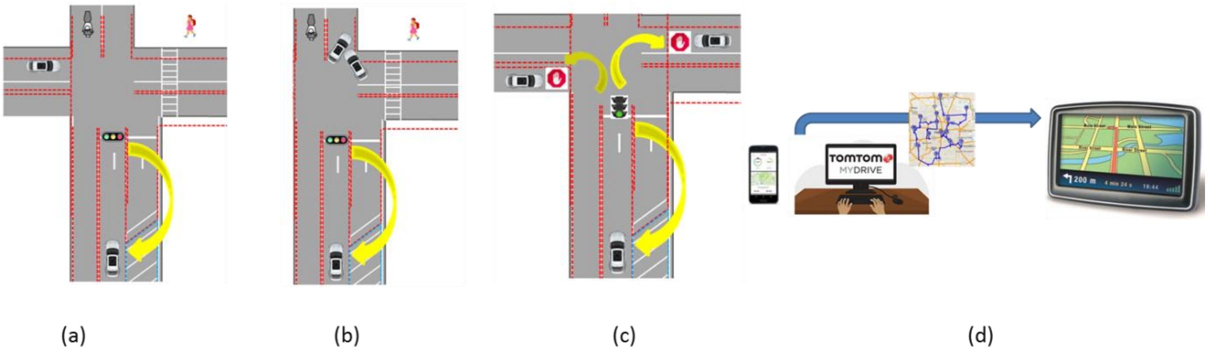

Figure 1: Indicative illustration of the SAFERtec use-cases: (a) optimal driving speed advice, (b) provision of real-time information, (c) priority request and (d) cloud-based route planning

When the above use-cases are considered under a WP4-specifications standpoint, then a number of requirements become relevant for the connected vehicle system architecture; they are highlighted in the following sub-sections together with a brief presentation of the involved scenario realised in the corresponding use-case. A detailed description of each SAFERtec use-case together with explanatory diagrams of all involved entities and communication means, appear in the deliverable D2.1 (“Connected Vehicle Use Cases and High Level Requirements). In the following we shortly introduce the SAFERtec use cases by mainly highlighting relevant requirements.

3.1 The Optimal Driving Speed Advice

The first SAFERtec use-case relates to informative messages received by the connected vehicle and used for more efficient and safe mobility. A traffic light status can be digitally communicated to the connected vehicles either through short-range communication (V2X, V2I) protocols or cellular connectivity (see Figure 1 - a), utilizing cloud-based services. Relevant messages may contain intersection geometry and signal identifiers as well as timing information for each light signal. Using this information, vehicles may calculate the behavior for the traffic light phases in their path (and compute an appropriate speed at which the vehicle will reach the intersection at the beginning of the next green phase).

The considered use-case requires:

- The vehicle to be able to establish communication channels with the infrastructure
- The RSU and cloud-based services to be enabled to transmit relevant messages (SPaT, MAP, TPEG-encoded messages)
- The connected vehicle to receive the above messages and to enable an appropriate process for them
- Dedicated software (i.e., Vehicle Safety Application) to trigger a relevant notification (that will include all needed information e.g., optimal speed)
- A relevant directive/notification to be projected to the driver (through an HMI system).

3.2 Provision of Real-Time Traffic-hazard information

The second selected use-case includes the retrieval of real-time warnings and traffic-flow information which typically takes place on motorways, major roads and/or central inter-city routes. There, a connected vehicle may receive V2X based information on hazardous road events either from an RSU or alternatively use cloud-based services (see Figure 1 - b).

Road events such as a traffic jam or hazardous incidents can be detected by traffic management centers or cloud-based intelligence and a relevant notification can be available at the RSU or cloud server. The use-case is realized when the ITS system (which avails the information) establishes a connection with the connected vehicle (and the appropriate in-vehicle application).

The considered use-case requires:

- A road event can be detected by the infrastructure
- The vehicle to be able to establish communication channels with the infrastructure (i.e., RSU or cloud-based services) and the available OBU to receive relevant messages (e.g., DENM) published by the infrastructure
- Dedicated software processes to control and verify the (DENM or TPEG-encoded) messages and trigger a relevant notification (if the information is relevant for the ego-vehicle)

- The relevant real-time traffic (V2X-based or TPEG-encoded) warnings to be projected to the driver (through an HMI system).

3.3 Priority request in intersection crossing

The priority (of emergency vehicle) in crossing an intersection can be digitized and thus become safer and more efficient. The priority can be requested and assigned by some responsible entity to the appropriate (emergency) vehicle while the rest (of the involved vehicles) can be notified to give priority. This scenario (see Figure 1 - c) constitutes the third SAFERtec use-case which is expected to involve an RSU-vehicle communication type.

A local central ITS Station can maintain a registry of connected vehicles in its area of control. The emergency vehicle will communicate its priority request to the local ITS station which subsequently communicates the right to drive for each lane to all vehicles (via a SPaT message)

The considered use-case requires:

- An ITS station and RSU back-end to avail and process information of connected vehicles approaching the intersection
- An emergency vehicle to be able to request priority rights (to the local ITS station)
- The RSU and back-end functionality to support priority assignment and communication of the corresponding priority (SPaT) messages
- The relevant acknowledgment (for granted priority rights) to be sent to the vehicle and projected to the driver (through an HMI system).

3.4 Privacy-preserving route planning and navigation

The last considered use-case relates exclusively to the use of cloud-based services and it is selected especially for the privacy issues that are involved. The scenario protocol (see Figure 1 - d) includes the selection of a destination by the user. This may become possible employing a web or smart-phone application. Then, a navigation device in the car is synchronized by a cloud-based service to provide the driver with a suggested route.

The considered use-case requires:

- A web or smart phone application to communicate with the dedicated cloud-service
- Cellular connectivity in order for the in-vehicle navigation application to import the selected route
- Dedicated software (infotainment or other HMI application) to provide the driver with the relevant directives/information (e.g., route and real-time traffic situation) through the dedicated navigation device
- All above information flow to respect certain privacy requirements (for the user's data)

The following sections of the deliverable will detail the SAFERtec connected vehicle system and how the proposed architecture is designed to meet the use-cases' requirements.

4. High-level view of the Connected Vehicle System

The use cases discussed in the previous section (Sect. 3 - "SAFERtec's use cases") foreseen two channels of communication:

- V2V/V2I – Vehicle to Vehicle and Vehicle to Infrastructure communication based on ETSI ITS-G5

  The European Telecommunications Standards Institute – ETSI (see (ETSI, 2017) and (ETSI Automotive Intelligent Transport Systems, 2017) for additional details) defines the European set of protocols and parameters based on the IEEE 802.11p standard, the short-range Wi-Fi standard (based on the IEEE 802.11 standard) for vehicular communication that supports low latency communication between vehicles and infrastructure enabling safety-related, time-crucial cooperative ITS applications. The communication between these actors held in license free bandwidth without the need of any centralized infrastructure. The authenticity, integrity and authorization check of the messages is required to perform reliable cooperative awareness applications. The standard concerns a connection with a Security Management System allowing vehicles to sign and verify the messages by mean of certificates emitted from a trusted authority. The communication channel for the update of the certificates can be the traditional Wi-Fi or the cellular connectivity and shall be renewed periodically (tentatively on yearly basis). Internet connectivity is required just for certificate update not for signing or verifies the messages. The same channel could be used also the send over the air updates and update of untrusted vehicles.

- Cloud Connectivity

  The evolution of tablet and smartphones together with the almost diffused availability of cellular connectivity allowed the proliferation of several services into automotive world, such as parking availability services, traffic information services, and electronic payment applications, among others. The number of services is growing day by day but usually they were not designed to deal with automotive safety concerns therefore they are the preferred way to perform attacks to vehicle equipment.

In Figure 2 is reported the architecture of the vehicle and all the actors involved in the communication.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

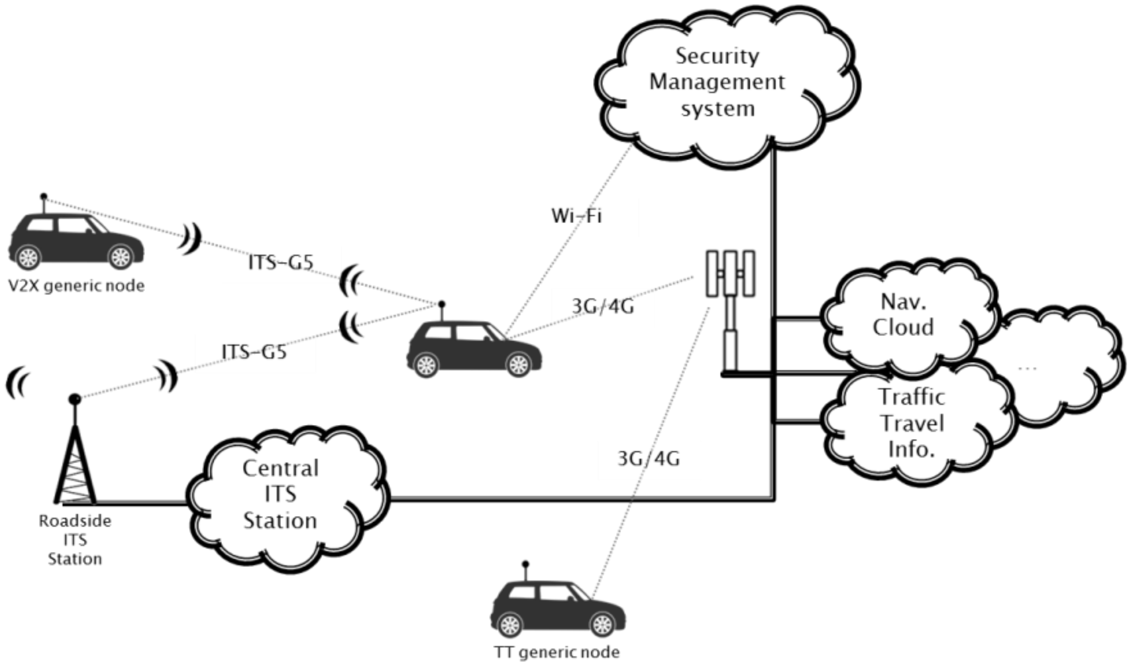

Figure 2: Vehicle connected to the world.

The vehicles (V2X generic nodes) are able to exchange information about their position, trajectories and on some extent of drivers' intentions (i.e. turn indicators status, acceleration, engaged brake, and so on) via ITS-G5 protocol. The infrastructure can install some Road Side ITS Stations (R-ITS-S) to collect the same information from the vehicles and vice-versa to disseminate data regarding dynamic changes of normal road rules: changes of speed limit or road geometry (due to roadwork or any other event) or to disseminate time-varying information such as the traffic-lights phases. The Roadside ITS station (R-ITS-S) are controlled by a management center (Central ITS Station or C-ITS-S) through wired network or cellular connection; in this way the road operators can collect real-time information from the vehicle equipped with ITS-G5 connectivity and can also disseminate specific warnings in case of danger. As an example, the approaching emergency vehicle could change the traffic-light phases to prevent vehicles from accessing an intersection. The ITS-G5 channel has been designed keeping in mind the security constraints therefore there is not additional need to design specific data protection for these messages. The vehicle requires to be connected to the cloud to access to other information: the certificates necessary to sign the V2X messages shall be periodically updated. The certificates shall be downloaded from the Security Management System via Wi-Fi or cellular connectivity. This communication is available from Car2Car – Communication Consortium service but the process is not standardized yet.

In addition there are some other cloud-based services: the vehicle can retrieve live information relevant to navigation services (such as live traffic information) from the TomTom cloud via cellular connectivity; in addition to that it's also possible to retrieve data from the C-ITS-S via cellular connectivity. Not only can a connected vehicle retrieve information from live online services, it can also access cloud services to store data. A driver's profile, favorite destinations or driven itineraries may be stored in TomTom’s cloud services. The current destination may be synchronized from the vehicle’s navigation OBU to a companion application being run in the driver’s smartphone. This information is highly privacy-sensitive. Additionally, there is not a uniquely recognized authentication system or API to register to these services therefore the security assessment is necessary to protect the car from possible attacks.

5. Detailed view of the Connected Vehicle System

This section describes the in-vehicle components that allow the proper implementation of the connected vehicles. Typically on-board-unit (OBUs) are connected to one or more Controller Area Network (CAN bus) following the standards ISO 11898-1 and ISO 11898-2 (Kvaser, 2017). In the network there is all the information that the vehicle collects from its sensors: accelerations, speed, brake engagements, ABS and ESC triggering, diagnostic data, and so on. The CAN bus is characterized by broadcast communication: the source, the destination and the content of the messages is not classified by any headers. The OBUs identifies the relevant messages basing on known message structure. In the modern vehicle these packets are the input source to perform autonomous activation of braking or steering wheel in order to provide ADAS functionality. The introduction of connected vehicles represents a new threat for this system in terms of security: without the connectivity an attacker attempting to get the control of the vehicle shall physically access the car to compromise the actuation systems (such as the braking system or longitudinal and lateral controller). For this reason, OEMs are introducing into their vehicle networks CAN gateway modules to isolate the OBUs with safety functionality from the one with remote interactions. In addition to that, this node can also monitor the traffic between the two CAN bus to detect anomalies into normal workload.

In the current project the V2X OBU, the HMI Android and the Safety Application components are connected to external source of information therefore they have been placed into a dedicated CAN bus beyond the vehicle CAN network. Standard Ethernet network (IEEE 802.3) is also available to connect these boards since some use-cases require cloud-connectivity to obtain updates or information from remote services. Concerning the interaction with the driver there are two possible HMIs available, both solutions are based on Android implementation: the integrated Android-HMI Head-Unit and the applications running into Android smartphone connected to car Wi-Fi. The main difference between the two HMI is that the Head-Unit can read hazard messages or sensor data directly from the dedicated CAN bus. In Figure 3 is reported the in-vehicle architecture with the description of each module right below.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

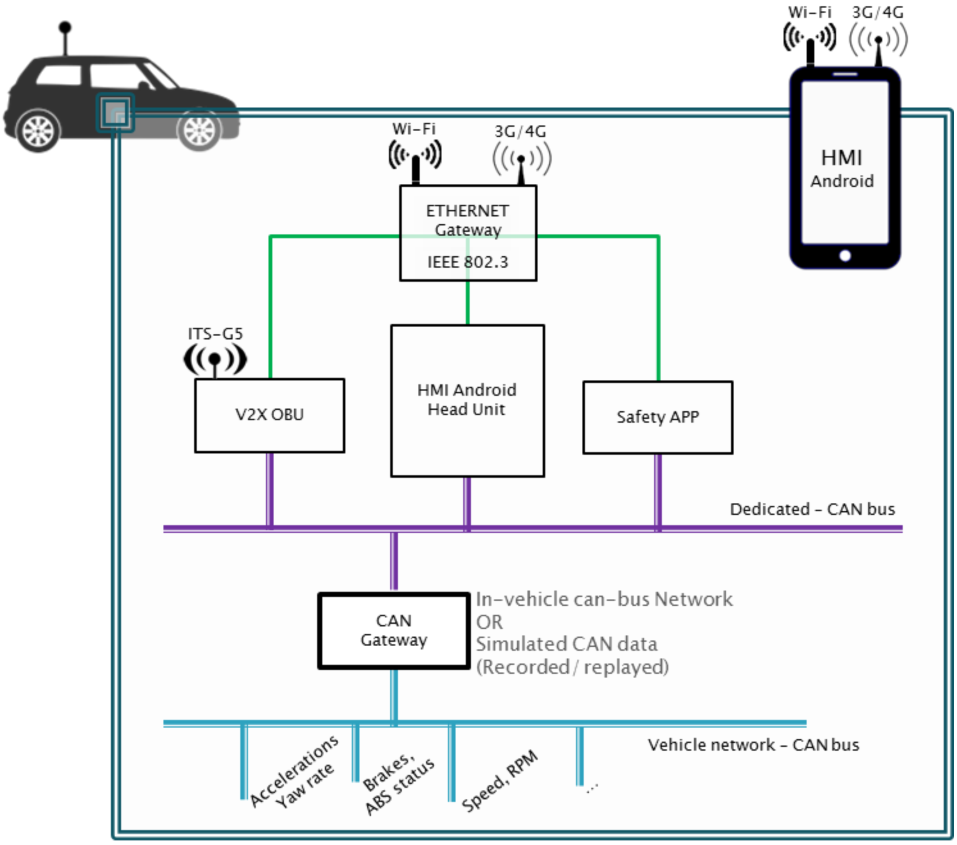

Figure 3 In-vehicle components.

In the SAFERTEC prototype there are the following OBUs connected with external components:

- CAN Gateway
  The CAN Gateway module is responsible to provide the vehicle signals necessary to the V2X OBU to generate the CAM messages. The module is equipped with two CAN networks in order to provide isolation between the connected components and the internal automated vehicle OBUs. The first one is connected to the internal vehicle CAN bus, here circulate the dynamic information of the vehicle such as speed, accelerations, steering wheel angle, and so on. The CAN gateway filter out the V2V relevant signal convert them into a new message database available to the V2X OBU, these messages are finally sent out to the dedicated CAN bus. No communication from the dedicated CAN bus into the internal CAN network is required for the selected use-cases. The CAN Gateway will also check anomalies of CAN traffic to detect anomalies to the expected data-flow.

- V2X OBU: Vehicle To Everything On Board Unit
  This unit is responsible of the ITS-G5 communication. As reported in Section 4 ("Detailed view of the Connected Vehicle System") the vehicle will communicate with authorized users only and with well-defined messages that the vehicles and the infrastructure are authorized to transmit.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The ITS-G5 standard is design to guarantee the integrity and authenticity of all the messages. The security stack of the V2X module requires certificates to sign and verify the V2X messages, for this reason the module is connected to the Ethernet HUB. Certificates can be downloaded from internet network, via Wi-Fi or 3G/4G cellular connectivity, or can be retrieved offline from PC or smartphone application. The connection is sporadic: it's not necessary to be continuously connected to the Security Management Component.

The messages sent from the V2X OBU must be fed with the vehicle dynamic data; these data are generated from the vehicle sensors and are available into the vehicle CAN bus. Since the V2X node could be connected to the external agents it cannot access directly to these signals but must get access to them through a CAN gateway. The CAN gateway is responsible to filter out the signals that are necessary to the V2X OBU from all the other CAN messages available into the vehicle network. In addition to that it can also perform an abstraction of the original data into a different data format to hinder the original structure. The V2X OBU can also write CAN messages into the dedicated CAN bus: these messages can be used from the HMI Head Unit or the Safety APP module to interact with the driver or to develop the specific safety application.

- Android HMI, Head Unit: Human Machine Interface
  This module represents the interface of the vehicle with the driver. In case of dangers due to a possible collision it may trigger an acoustic signal or display some hazard lights into the infotainment display. The HMI can also provide infotainment service such as the satellite navigation or, for instance, the parking availability service. In modern vehicles, this node could host a Wi-Fi access point and Bluetooth to communicate with smartphone applications. It's also growing the cellular connectivity availability to obtain dynamic update about traffic conditions, point of interests or specific services (like, e.g., parking availability or gasoline prices). The cellular connectivity is particularly critical from a security point of view since it's the only channels that allow to remotely access to the car everywhere seamlessly without the need to physically access the car or to close follow the driver. Traditionally the HMI is installed into the head unit where the user can interact to customize the vehicle behavior and ADAS systems therefore this module is connected the CAN bus. For the reasons mentioned above the HMI module is heavily exposed to attackers, more than any other OBU into the vehicle.

- Safety Application
  This module collects the data obtained from the V2X OBU and identifies if any danger could arise from the surrounding vehicles. This module doesn't require access to the original vehicle network: it just communicates with the V2X OBU and the HMI. Potentially could benefit with the connection to the Ethernet HUB to trigger specific warnings to the HMI module or to external users (call the rescue in case of breakdown or any other issue).

- Ethernet Gateway

The V2X OBU and the Safety APP OBU require the internet connectivity to access to remote services or to retrieve updates. The project requires also a connection with a smartphone to communicate with the driver. For these reasons the vehicle is equipped with standard IEEE 802.3 Ethernet gateway (not Automotive Ethernet) which provides also Wi-Fi and 3G/4G cellular connectivity. The OBUs in specific use-case can exchange information via TCP/IP or UDP streams but the traffic shall be regulated by proper isolation/security mechanism (e.g., see Section 8).

5.1 In-vehicle architecture

A V2X Software Stack is a piece of software, which enables a system to transmit V2X (Vehicle to Vehicle/Roadside/etc.) messages using standardized protocols and interfaces implemented in its core. This dedicated technology is used by the so-called C-ITS concept (Cooperative Intelligent Transport Systems) to increase traffic safety and efficiency.

Messages received are temporarily stored in a complex database (the LDM); all incoming messages must go through a chain of standardized processes in order to allow data extractions. Similarly, message generation also needs to follow a wide set of rules. As an example, CAMs are periodically built "here I am" messages, packaged in several layers of headers and container (e.g., the security header contains information about the signer). DENMs are triggered upon an event (e.g., a defined message received over the CAN bus). It uses the same set of lower layer functions, but might require different configuration (e.g., a high priority DENM will be dealt with differently than a normal one.

Figure 4 and Figure 5 show the two basic configurations V2X stack, LDM and applications may be deployed in a vehicular system. Both configurations will be investigated (one configuration for a specific use case).

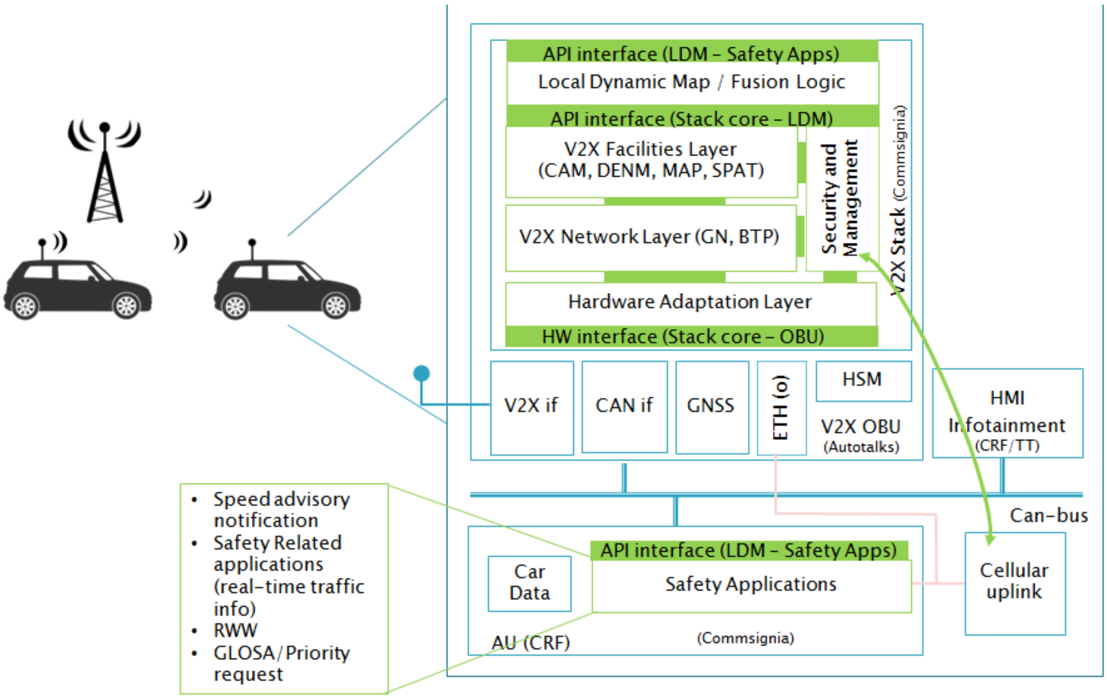
API interface (LDM – Safety Apps)
Local Dynamic Map / Fusion Logic
API interface (Stack core – LDM)
V2X Facilities Layer
(CAM, DENM, MAP, SPAT)
V2X Network Layer (GN, BTP)
Security and Management
V2X Stack (Commsignia)
Hardware Adaptation Layer
HW interface (Stack core – OBU)
V2X if
CAN if
GNSS
ETH (o)
HSM
V2X OBU
(Autotalks)
HMI
Infotainment
(CRF/TT)
Can-bus
Speed advisory notification
Safety Related applications (real-time traffic info)
RWW
GLOSA/Priority request
Car Data
API interface (LDM – Safety Apps)
Safety Applications
AU (CRF)
(Commsignia)
Cellular uplink

Figure 4: In-vehicle V2X software Stack architecture

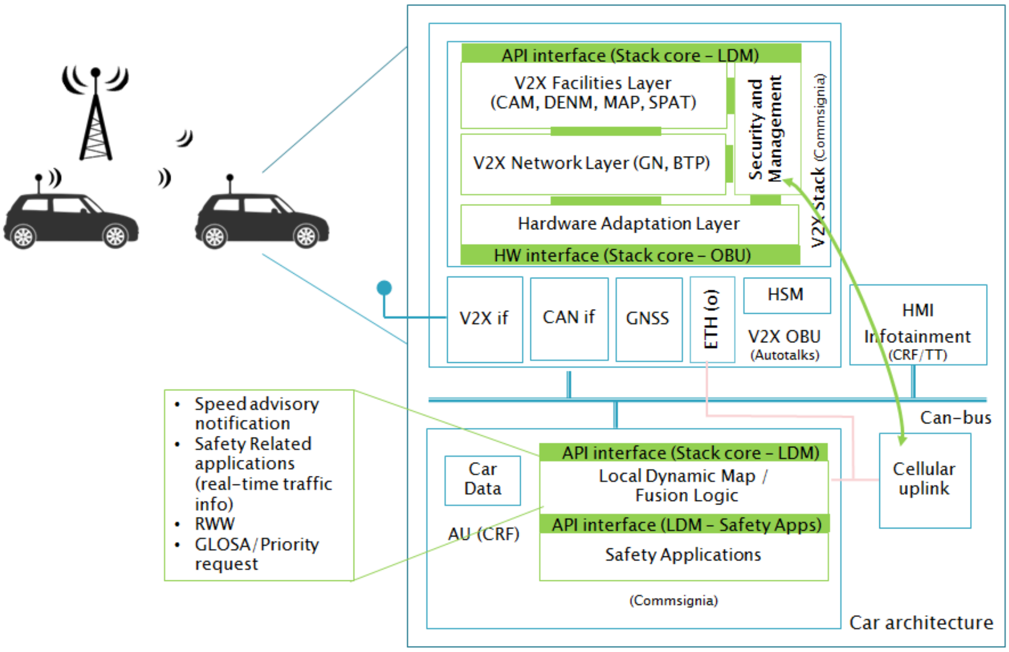
API interface (Stack core – LDM)
V2X Facilities Layer
(CAM, DENM, MAP, SPAT)
V2X Network Layer (GN, BTP)
Security and Management
V2X Stack (Commsignia)
Hardware Adaptation Layer
HW interface (Stack core – OBU)
V2X if
CAN if
GNSS
ETH (o)
HSM
V2X OBU
(Autotalks)
HMI
Infotainment
(CRF/TT)
Can-bus
Speed advisory notification
Safety Related applications (real-time traffic info)
RWW
GLOSA/Priority request
Car Data
API interface (Stack core – LDM)
Local Dynamic Map / Fusion Logic
API interface (LDM – Safety Apps)
Safety Applications
AU (CRF)
(Commsignia)
Cellular uplink
Car architecture

Figure 5: Alternative in-vehicle V2X software Stack architecture

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

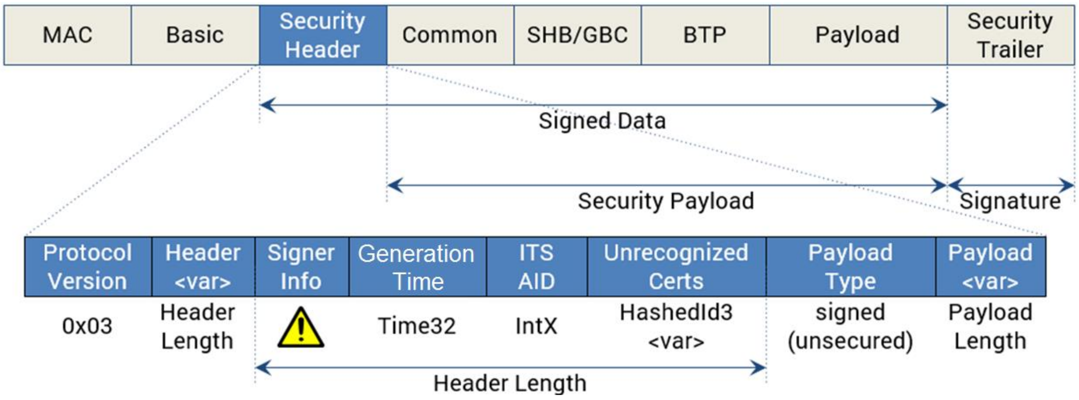

Figure 6: ECU secured message

EU secured message

V2X messages considered by the project (CAM, DENM, MAP and SPaT) are all broadcast messages, which are signed but not encrypted (see Figure 6). There is no communication link which is established, thus an ITS station will not know who receives the messages. DENM messages have the possibility to multi-hop from one node to another by using advanced GeoNet algorithms and functions, but the current set of applications do not trigger such messages. CAMs repetition rate follows various rules, e.g., if channel congestion is high, the rate is lowered, and while the rate is increased if vehicle dynamics change fast (e.g., a vehicle driving on a constant speed is sending fewer CAMs then a vehicle turning and/or accelerating).

The Stack implements layers defined by the ISO/CEN/ETSI/IEEE/SAE ITS architecture. In general, it covers functionality between the transmitting medium and the applications. The main building blocks are interfacing towards sensors (e.g. GNSS module) and transmitters (e.g. IEEE 802.11p radio), Network protocols, Management, Security and Facilities towards Applications.

Table 2 intends to identify the main standard references.

Table 2: V2X Communication Standards

Type	Standard
Safety Applications	ETSI TS 102 637-1, ETSI TR 102 638
Cooperative Awareness Message (CAM)	ETSI EN 302 637-2, TS 102 894-2
Decentralized Environmental Notification Msg. (DENM)	ETSI EN 302 637-3, TS 102 894-2
Signal Phase and Time message (SPaT)	ETSI TS 103 301
Road Topology messages (MAP)	ETSI TS 103 301
Local Dynamic Map (LDM)	ETSI EN 302 895
Security layers and functions	ETSI TS 102 940, ETSI TS 102 941,ETSI TS 102 942, ETSI TS 102 731,ETSI TS 103 097
V2X access layer (ETSI G5)	IEEE 802.11p, ETSI ES 202 663, ETSI EN 302 663,

	ETSI EN 302 571
Basic Transport Protocol (BTP)	ETSI EN 302 636-5-1
GeoNetworking	ETSI EN 302 636-4-1, EN 302 931

The Stack follows a modular approach in general: all protocol instances, services and other functions are identified as different modules. Modules are grouped into vertical and horizontal Layers. From bottom up, the following groups exist. The hardware dependent adaptation layers offering hardware independent upper interfaces, Network Layer, Facility Layer, and the Local Dynamic Map. The vertical layer(s) are Security and Management, while Applications sit on top of all other Layers.

Security functions

An ITS Station is able to verify that a given message is authentic by using the PKI (see dedicated Section 6 – “PKI entities and functionality”). The PKI also enables the use of pseudonym certificates and pseudonymity, which guarantees that all identifiers, used by V2X, of a vehicle are changed during a given trip (e.g., physical address).

The Stack applies the security headers shown on the picture above, i.e., Figure 6. It is made following the standard protocol as shown below, i.e., Figure 7.

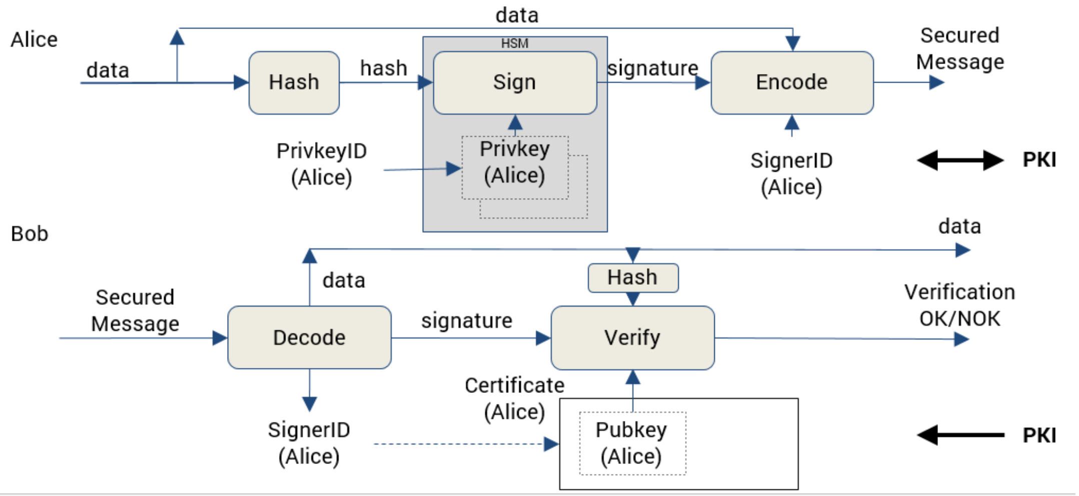

Figure 7: Protocol for message signatures and verification

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

5.2 Road Side Unit architecture

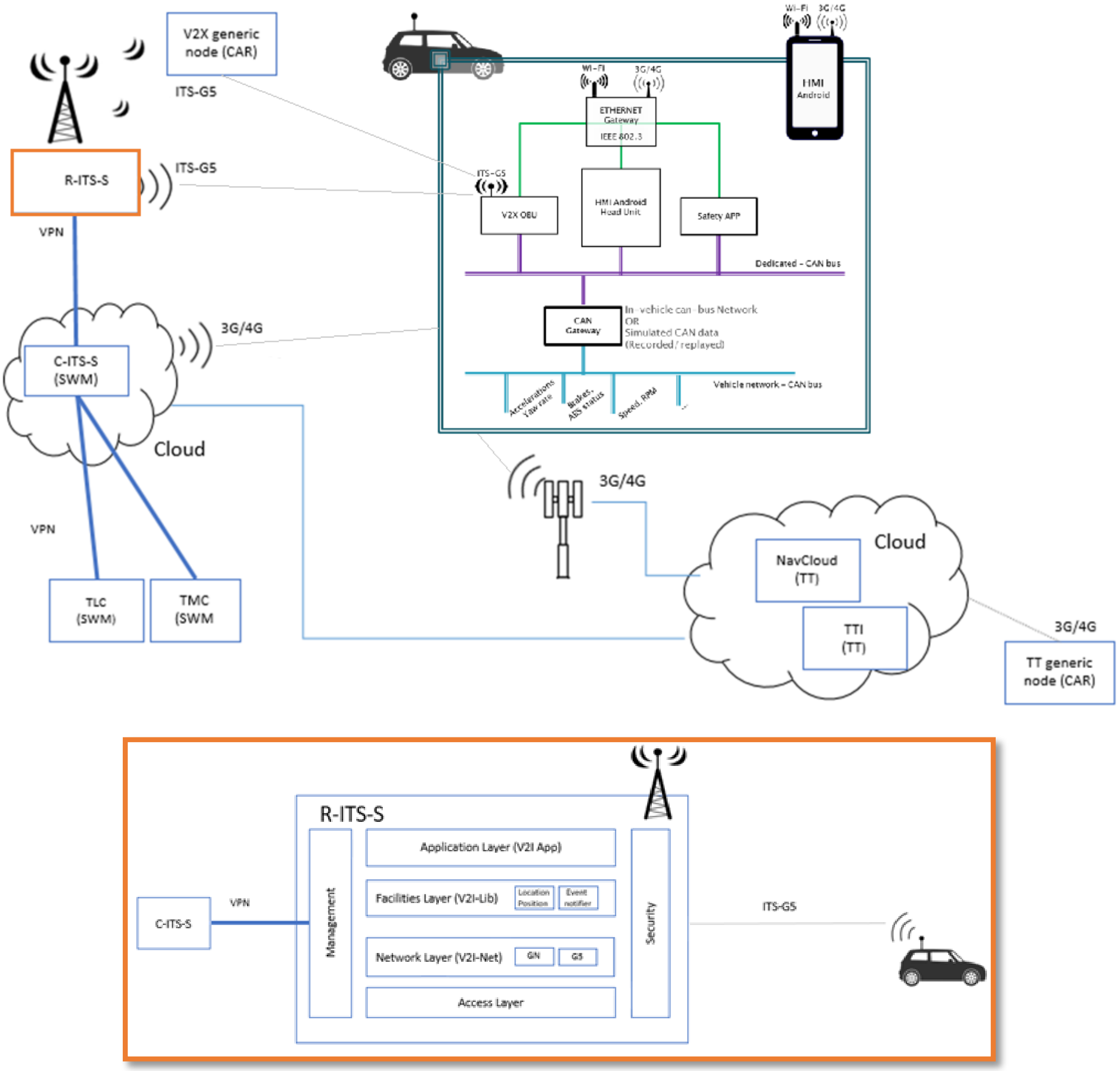

Figure 8: High-level view of the Road Side unit (top), and detail about internal architecture of the Road side unit (bottom)

The high-level view of the connected vehicle system with details about the road side unit is shown in Figure 8 (top) while the same figure (bottom) details the internal architecture of the Roadside ITS station (R-ITS-S). R-ITS-S is the gateway between the C-ITS-S and vehicles ITS G5 (V-ITS-S). The R-ITS-S receives and sends data from and to the C-ITS-S and also from vehicles. Some data is processed and

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

stored within the R-ITS-S, before being transferred. The R-ITS-S can be installed at a road works safety trailer or any other mobile device, for a mobile solution. It can also be installed inside the existing outstations at the gantries on the highway (fixed solution).

The R-ITS-S communicates with vehicles passing by via ITS-G5. It has the possibility to decode and encode C-ITS messages sent and received using the IEEE802.11p communication technology. The R-ITS-S has one interface to the C-ITS-S and another interface to the V-ITS-S (toward the vehicle), which is based on C-ITS specifications (e.g. ETSI-DENM, ETSI-CAM).

The R-ITS -S contains the ETSI ITS G5 – stack implementation (ITS access technology layer, ITS network & transport layer, ITS facility layer, ITS application layer). Through the application layer it is possible to access the ITS facility layer (ITS-G5), which contains the interfaces to the C-ITS-S.

For the data transfer to the C-ITS-S, an existing private IP network (e.g. fiber optic- or cellular network) will be used. The communication between the R-ITS-S and the C-ITS-S is done via an IP based connection initiated by the R-ITS-S. This means the C-ITS-S is always the OCIT-C (Open Communication Interface for Traffic Control Systems) Server and the R-ITS-S will always be the OCIT-C Client. A VPN tunnel is used to secure the communication link in case the communication is over internet. The C-ITS-S server may be the VPN Server and the R-ITS-S the VPN Client. Table 3 reports examples of R-ITS-S functionalities and their definition.

Table 3: R-ITS-S Examples of functionalities and their definitions

#	**Functionality**	**Definition, Example**
1	R-ITS-S management/maintenance	• Configuration • Logging • Monitoring • Remote access • Firmware update
2	Data processing	• Aggregation of CAM • Filtering to eliminate duplicated messages received from V-ITS-S • Logical functionalities
3	Interfaces • R-ITS-S <> C-ITS-S • R-ITS-S <> V-ITS-S	• Receive DENM and CAM from V-ITS-S • Send aggregated and special CAM to C-ITS-S • Receive DENM and SPAT/MAP data from C-ITS-S • Send DENM and SPAT/MAP data to V-ITS-S

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

4	Security PKI management (authentication, anonymization, legitimation)	The functionality of the system component PKI (certification authority) is not yet standardized for all the messages. There is a proprietary PKI-server implementation existing within the C2C-CC consortium.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

5.3 Cloud-based service architecture

This section will detail the logical architecture of the cloud-based services.

5.3.1 Central ITS Station

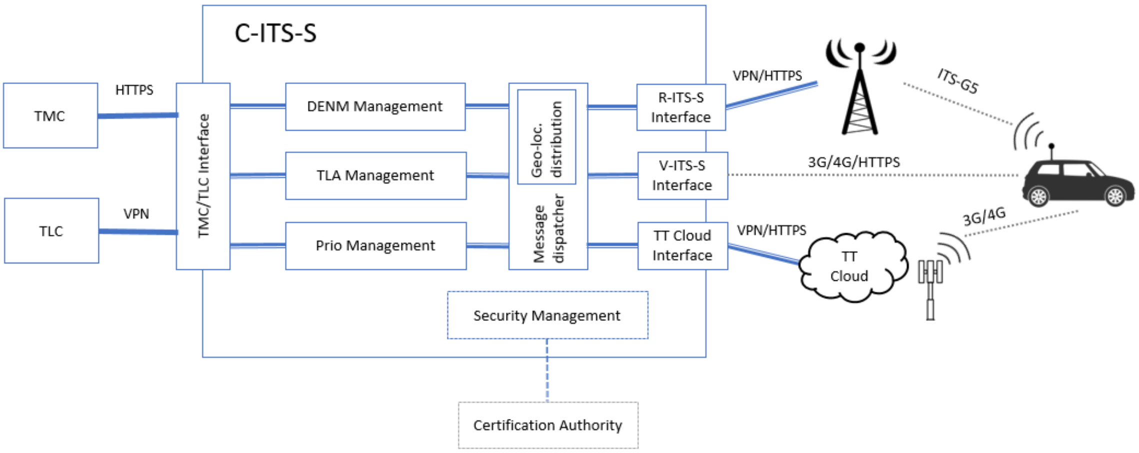

Figure 9: C-ITS-S logical architecture

The **Central ITS Station (C-ITS-S),** see Figure 9**,** is the core component of the C-ITS system. The C-ITS-S is connected on one side (input) to the urban/interurban traffic management center (TMC) and to the traffic light controllers (TLC), and on the other side (output) to one or more roadside-ITS-stations (R-ITS-S), to a V-ITS-S interface based on a web service for the provision of 3G/4G-messages and to the TT Cloud infrastructure.

The general concept of the C-ITS-S system is designed in a way that new modules can be easily connected without changing the general architectural concept of the system.

The C-ITS-S has one interface to the R-ITS-S, one to the TTCloud, another interface to the V-ITS-S, in addition to those with TCC and TLCs, see Figure 8. As mentioned before, the communication between the R-ITS-S and the C-ITS-S is done via an IP based connection initiated by the R-ITS-S.

The C-ITS-S is responsible for the accurate provision and delivery of the information to the V-ITS-S. The mechanisms that make available the information to be shared by several communication channels are developed and implemented within the C-ITS-S. It also supports the management of security mechanism of the system (e.g., access to the PKI).

The functionality of the system component PKI (certification authority) is not yet standardized and not yet implemented. The idea is possibly to enable the retrieval of PKI certificates by the C-ITS-S, to implement security across the system.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The data generated by the C-ITS-S (i.e., DENM, SPAT) can be delivered directly to the V-ITS-S through on ITS WEB server. The Communication between the WEB server and the C-ITS-S is done via an IP based Link initiated by the WEB server. This means that the C-ITS-S is always the OCIT-C Server and the WEB server is the OCIT-C Client. Table 4 reports examples of C-ITS-S functionalities and their definition.

Table 4: C-ITS Examples of functionalities and their definition

#	Functionality	Definition, Example
1	Basic System Functionality	e.g. architecture, modules like user interface, graphical representation of map, archive, user management, Device management/maintenance
2	Logging, archive	e.g. logging of sent and received messages (interfaces: TMC, TLC R-ITS-S, …)
3	Interfaces • C-ITS-S <> TMC • C-ITS-S <> TLC • C-ITS-S <> R-ITS-S • C-ITS-S <> TTCloud • C-ITS-S <> V-ITS-S • C-ITS-S <> Certificate Authority	• Receive DENM and special CAM from V-ITS-S • Receive aggregated and special CAM from R-ITS-S • Send DENM and SPAT/MAP data to R-ITS-S • Send DENM and SPAT/MAP data to V-ITS-S • Send DENM and SPAT/MAP data to TTCloud • Receive SSM data from TLC/TMC • Receive unplanned events from TMC • Send SRM data to TLC • Retrieve authorization ticket from Certification Authority
4	Data processing	Message processing and management: e.g. message generation/reception, processing of traffic information and traffic data / CAM data reception/processing.
5	Performance, Hardware	Hardware infrastructure and system architecture to ensure a proper function of the system even during peak periods.
6	Security PKI management	*Yet to be implemented.* The functionality of the system component Certification authority is not yet standardized.
7	Data dissemination	Location based message distribution.

5.3.2 TomTom Cloud Services architecture

TomTom Cloud Services are designed to maximize independence between the different services provided, so that customers may be enabled to consume services suiting their needs without

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

imposing the requirement to utilize the full stack of TomTom services. This means that each service must be designed to work independently of other services in TomTom's stack; for example, a live traffic service must be able to work for customers with different map versions and even maps from different vendors. To better characterize these services, a split between "live services" and "NavCloud" will be made.

The general high-level architecture of TomTom cloud services can be seen in the following diagram, i.e., Figure 10.

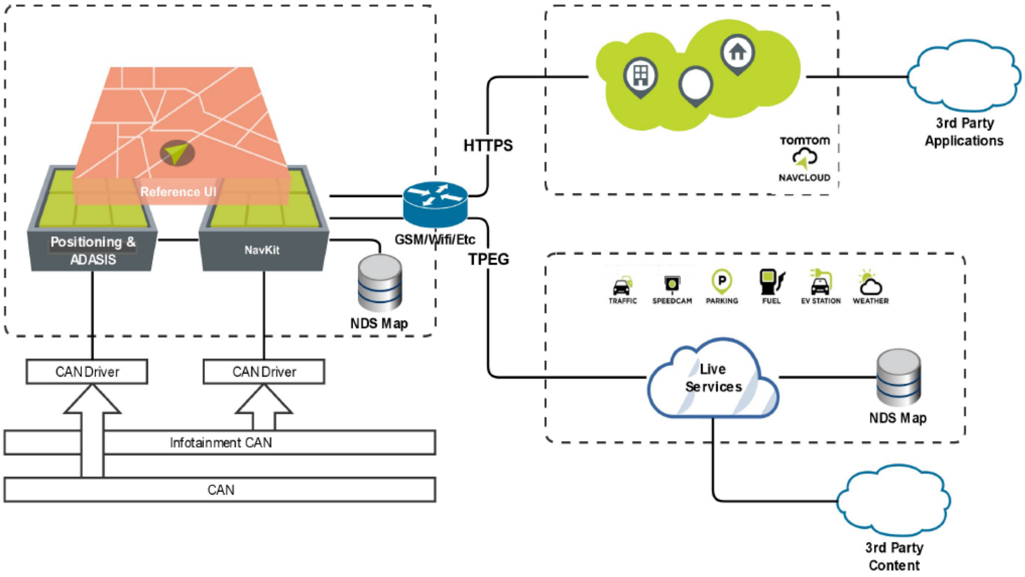

Figure 10: High-level TomTom cloud architecture

In the following, this diagram will be further detailed.

TomTom live services – Traffic and travel information (TTI)

TomTom live services enable consumers to develop applications based on real-time data aggregated by TomTom from traffic probes and fused with third party data. Traffic and travel information is then made available to end users through TPEG, which can be carried via any mean of connectivity a vehicle may have available.

In the use cases specific to SAFERtec, TTI cloud servers may source third party data such as DENM and SPAT/MAP data from a C-ITS-S to generate a traffic light profile. This data, fused with other information sourced by TTI servers, may then be delivered to the on-board units running NavKit, TomTom's navigation software. This data may be delivered through TPEG or any other means of communication available, together with other real time information pertinent to the driver's location, profile and requested services – such as traffic jam warnings, traffic flow information, weather information, and so on.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

The TTI services utilized for SAFERtec will have an interface with the C-ITS-S through a web-service API, as well as an interface through the vehicle's OBU through TPEG. The connection to the vehicle's OBU may be through Wi-Fi, cellular connectivity, or any other connectivity means available to the target platform. The TTI services will additionally have a connection to TomTom's working databases, to ensure access to TomTom's historical data.

TomTom NavCloud

NavCloud services are a set of comprehensive APIs that enable clients to create, store, organize and use across all navigation end-points (in-dash devices, web browser, mobile devices) data that has personal meaning to the end user. Such data includes, but is not limited to, user locations, itineraries, tracks, points of interest collection, personal user preferences (language, locale, etc.), historical data and more. This personal data is stored in a reliable and secure manner and in conformance with global and local laws.

NavCloud services are based on client-server architecture, see Figure 11. The server, composed of the APIs responsible of handling the personal data, is deployable to most commercial VPS (e.g., AWS or Azure). Complementing NavCloud server, NavCloud Client Libraries act as clients, being responsible for connecting, authenticating and synchronizing personal user data at the request of a specific navigation endpoint.

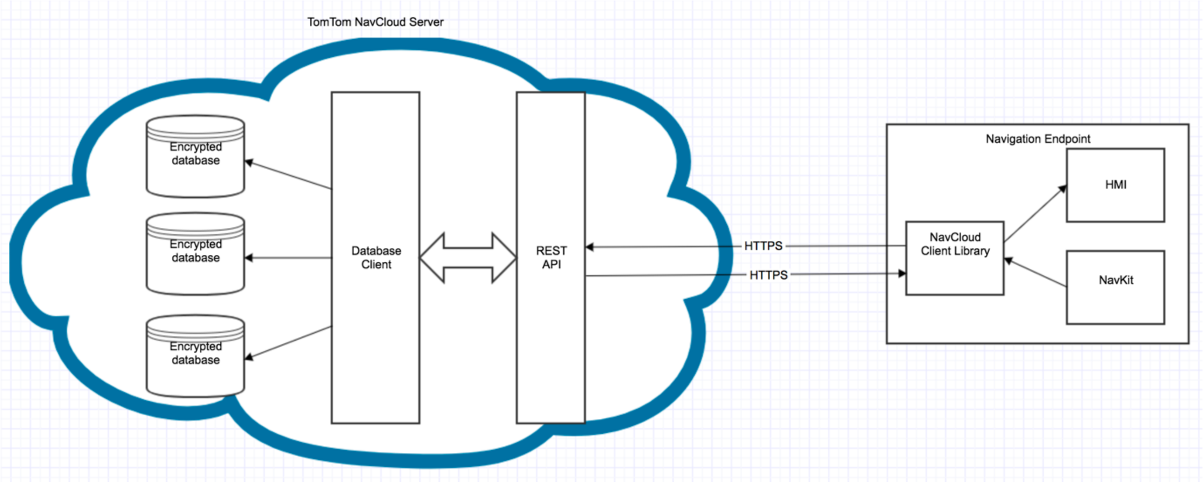

Figure 11: TomTom NavCloud architecture

NavCloud services are provided in an application-independent and map-independent way in order to enable interoperations between the users' different connected navigation clients (such as mobile companion applications, in-dash devices and web applications). NavCloud also provides wide range of client libraries so that clients can access this functionality from different parts of the stack.

All endpoints that require personal data shall always have access to the user personal data, if properly authenticated, however connection cannot be guaranteed in all situations. Therefore,

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

NavCloud client libraries will store a local version of the personal data for these cases. This data can be used or updated and it will be synchronized between all endpoints when connection becomes available.

Online storage security is achieved using state-of-the-art technology such as OAuth2 for authentication, HTTPS for communication and encrypted databases for storage. In situations where local replica of the data is required (e.g., there is no connection with the NavCloud Server) then securing the data is also performed offline, on the client side.

6. PKI entities and functionality

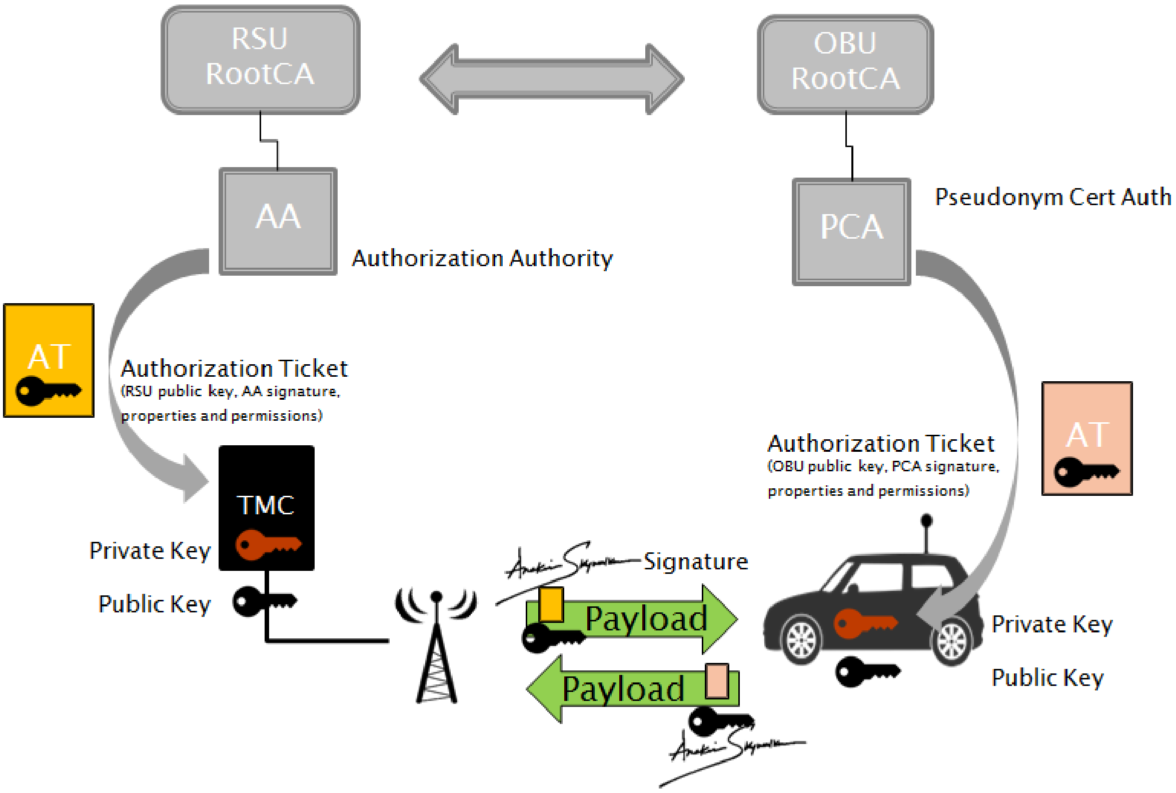

Figure 12: High-level flow of the PKI management and use

Figure 12 shows a high-level view of the flow about the PKI management and use. All V2X messages include cryptographically signed certificates, using pseudonyms. As defined in the General Data Protection Regulation (EU) 2016/679 Article 4 (5): a pseudonym is a cryptographic signed certificate, that corresponds to a public key certificate called authorization ticket. The authorization ticket represents the ITS Station, without revealing the identity of the vehicle or its driver.

This allows a Station to verify if a message has been changed since its original creation (and signature).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

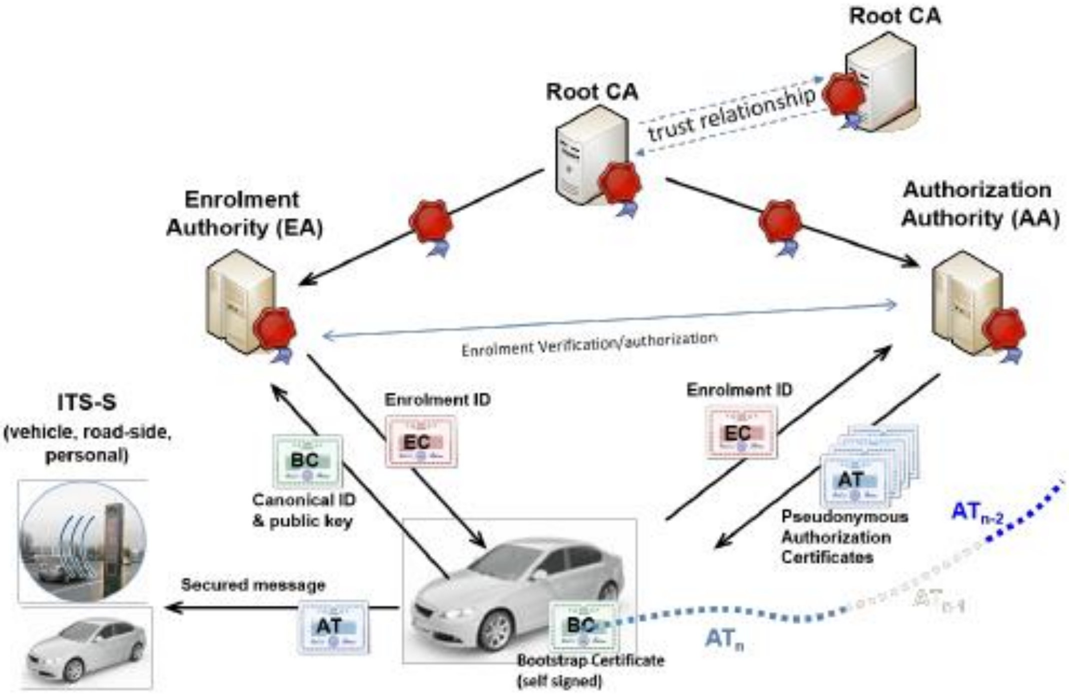
Root CA
Root CA
trust relationship
Enrolment Authority (EA)
Authorization Authority (AA)
Enrolment Verification/authorization
Enrolment ID
EC
Enrolment ID
EC
ITS-S
(vehicle, road-side, personal)
BC
Canonical ID & public key
AT
Pseudonymous Authorization Certificates
AT_{n-2}
AT_{n-1}
AT_n
Secured message
AT
BC
Bootstrap Certificate (self signed)

Figure 13: Public Key Infrastructure
(Curtesy of: Cooperative ITS Security Framework: Standards and Implementations Progress in Europe by Brigitte Lonc and Pierpaolo Cincilla)

The European V2X Certificate policy is currently being defined, however currently the PKI consist of the following entities (see Figure 13). The **Root certification Authority** supervises and establishes trust between the enrolment and the authorization authorities. In Europe it is foreseen that there will be more than one RootCA, e.g., different roots may exist for vehicles and for roadside equipment. Both types have been deployed already for use in pilots.

The **Enrolment Authority** provides Enrolment Certificates (also called as long term certificates) to ITS Stations that are part of the system (e.g., vehicles which have passed Compliance Assessment tests). These certs are then used to hide the identity of the vehicle/Station by using it instead of its ID. The certs used during V2X are provided by the **Authentication Authority** and are called authorization ticket. They are also standardized in Security Header and Certificate Formats (ETSI TS 103 097) and they are also sometimes referred to as short-term certificate or pseudonym certificate. They represent the proof that the system knows that ITS Station. The Authentication Authority provides ACs to vehicles which are verified using their EC by the EA.

New certificates are required due to their expiration.

The PKI also allows the so-called Revocation of Trust, meaning that a misbehaving ITS station is removed from the system by listing them untrusted (revocation list) and also by disabling the provision of valid certificates (and their certificates will expire).

7. Hardware components of the Connected Vehicle System

7.1 In-vehicle hardware

The following main in-vehicle components will be installed into the vehicle, according to Figure 3 (in-vehicle architecture): the CAN gateway, the V2X OBU, the HMI and the Safety App OBU. In this section, the candidate solutions are described.

- CAN Gateway

  The CAN gateway does not require any connection with external agents. Its job is to filter out unnecessary signals (concerning the SAFERtec framework) from the vehicle network and transmit the remaining into the dedicated CAN bus. For this purpose, we have two possibilities:

1. PEAK PCAN-Router Pro
   It allows to manage the data traffic from four High-speed CAN busses (see Figure 14). The behavior of the router is configured via the CAN bus with the provided Windows program PPCAN-Editor. As well as pure forwarding, the CAN data can be processed, manipulated, and for example, filtered in a number of different ways. As an alternative to the standard firmware, custom firmware based on the ARM microcontroller NXP LPC2294 can be created and implemented by mean of the Yagarto GNU ARM toolchain (it contains the GNU Compiler Collection GCC for C and C++).

Figure 14: PEAK PCAN-Router Pro

Specifications:

¬ 4 High-speed CAN channels via pluggable transceiver modules. Alternatively, Low-speed, Single-wire, and opto-decoupled High-speed modules, as well as High-speed modules without wake-up function available

¬ Wake-up function using separate input or CAN bus

¬ Complies with CAN specifications 2.0 A/B

¬ CAN connections are D-Sub, 9-pin

¬ CAN termination switchable, separately for each CAN channel

¬ CompactFlash card slot

¬ Battery buffered realtime clock (RTC), can also be used for wake-up

- Beeper
- Status LEDs for CAN channels, CompactFlash card, microcontroller, and power supply
- NXP microcontroller LPC2294
- Aluminium casing with flange. DIN rail fixing option available on request
- 8 - 27 V power supply, protection against overvoltage and reverse polarity
- Extended operating temperature range from -40 to 85°C (-40 to 185 °F)

2. Application Unit VBOX-3600

The Automotive-PC VBOX-3600 is composed by Intel Gen 3 Core i7-3517 1.7GHz, 8GB DDR3 RAM, 2 CAN interfaces, 4xGigabits Ethernet ports, Wi-Fi network and integrated GNSS receiver with Linux operating system (see Figure 15). CRF can provide CAN gateway application functionalities and other services (like Wi-Fi Hotspot) or running SAFERtec specific applications.

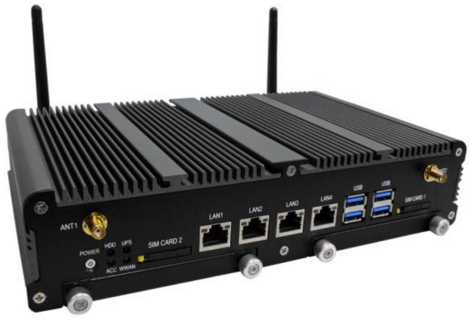

Figure 15: VBOX-3600

Specifications:

- CPU / SoC / Socket Intel Core i7-3517UE 1.7 GHz
- TDP (max.) 17 W
- Memory Onboard 2 GB
- Chipset Intel QM77
- Graphics Intel HD 4000
- Video signal 1x DVI-I, 1x VGA, 1x DisplayPort
- Network & wireless 4x LAN 1000
- Storage 2x 2.5'' disk drive (bay), 1x SATA DOM
- Connections 3 x SATA 2
- 1 x USB 2.0, 4 x USB 3.0
- 1 x RS-232, 2 x RS-232/485
- 2 x SIM card slot
- 4x SMA
- I/O 8x GPIO
- Expansion slots 4x Mini PCIe

- Fanless system
- Operating temperature: -40 to +70 (°C)
- System cooling Passive
- Mounting Wallmount
- Protection Vibration
- Dimensions Length: 235 (mm), Width: 155 (mm), Height: 50 (mm)
- Certifications CE, FCC Class A, eMark Compliance
- Input power +9 to +26 DC V
- Package contents VBOX-3600, Mount bracket, F-Type screws, Phoenix cabling CON male 3-pin
- Application market Automotive, Transportation

- V2X OBU:

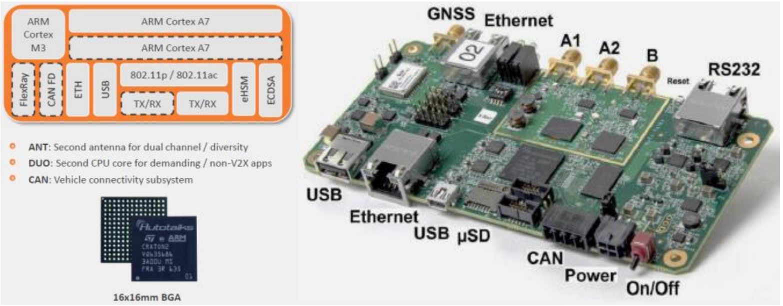

Figure 16: V2X OBU

Usages

- Evaluation of Autotalks technology in lab or field as RSU/OBU (see Figure 16)
- Software development platform

Features:

- CRATON2 –V2X Communication Processor
- PLUTON –V2X RF Transceiver
- Remote DSRC antenna support (optional HW flavour)
- CRATON2 EVK contains:
  - Dual PHY and MAC, supporting dual channel operation and optimized TX/RX diversity
  - Embedded on-board GNSS receiver (STMicroTESEO III)
  - On-chip accelerator for ECSDA verification

- On-chip Hardware Security Module (eHSM) for secure cryptographic operations
- On-chip ARM Cortex A7 CPU subsystem for V2X stack and application processing
- Upgradable Firmware

Note: EVK enclosure doesn't meet IP standards in terms of dust and water resistance

Interfaces:

- DSRC Ant A1* – SMA female Tx/Rx of channel A (Remote Phantom Compensator)
- DSRC Ant A2* – SMA female Tx/Rx of channel A (Direct antenna connection only)
- DSRC Ant B – SMA female Tx/Rx of channel B
- RS232 RJ45 – CRATON2 UART Connectivity to main CPU console interface
- 2xCAN - 2xHigh Speed CAN interface for Vehicle integration
- 2xRJ45 - Ethernet Data connectivity, Firmware upgrade and management interface.
- GNSS antenna – SMA female for GNSS active antenna port.
- USB 2.0 (Mini-B 5 pin) - Data connectivity, Firmware upgrade and management interface.
- USB 2.0 (Type A) - Data connectivity, Firmware upgrade and management interface.
- POWER - DC in power connector, supply voltage 9V - 16V
- uSD – Micro SD storage for data logging

- HMI:
  The following two possible HMIs can be tackled into the projects:

1. Android Car Stereo Navigation
   Our first attempt is to use an Android-based onboard vehicle infotainment unit, such as the one proposed by Smarty-trend (see Figure 17). The radio is equipped with Android 6.0.1 OS, 1.6 GHz Quad-core processor, 2 GB DD3 RAM, Bluetooth and Wi-Fi and CAN bus support. Here the specifications of 500L model.

Figure 17: Android Car Stereo

Specifications:

¬ 7 inches, capacitive multi-touch screen;
¬ HD 1024*600px LCD resolution;

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

- Android 6.0.1 (Marshmallow);
- 1.6 GHz Quad-core (Allwinner T3) processor;
- 2 Gb (Samsung DDR3) RAM;
- 16Gb, expansible through SD card;
- GPS / Glonass positioning system, external antenna is included;
- FM / AM radio with RDS and memory for 36 radio stations, high sensitivity NXP TEF6686 FM module;
- Hi-Fi sound processor, 4 x 50W sound amplifier MOSFET TDA 7850 class AB ;
- Equalizer: Bass / Middle / Treble, Loud. Cutoff frequency: BassF / MiddleF / TrebleF. Separate volume control for loud speaker (subwoofer);
- On-board WI-FI, Hotspot mode (access point for other Wi-Fi devices);
- 3G / 4G Internet is supported through an external USB modem (isn't included);
- Bluetooth HandsFree. Phonebook copy function and phonebook search. Separate volume control. A2DP music playback;
- TMPS (tire-monitoring pressure system) and OBD2 adapters, connection through Bluetooth;
- Steering wheel buttons, supporting 3 programmable functions for one button (short / long / repeat press);
- RGB front panel buttons backlight, every color can be adjusted;
- Faceplate buttons function can be changed, 3 programmable functions for one button (the same as steering wheel buttons);
- Backup camera, supporting every rear cameras (some models support original factory cameras, dynamic lines and park assistance system);
- Front parking camera supporting through the "FCAM" or "AUX Video In" port connection;
- Standby Mode (10, 30, 60 minutes), the unit will be switched on for 1 second;
- Android cold boot time for 20-25 seconds;
- Supporting of USB Flash, SD Card (up to 64 Gb) and hard drives (up to 1 Tb);
- Supported video formats: RMVB, MKV, MOV, WMV, AVI, MPG, TS with 1080P, H.264, etc.;
- Supported audio formats: MP3, WMA, WAV, OGG, FLAC, etc.;
- Support Full HD 1080p video playback;
- Video output - RCA Female (NTSC, PAL);
- External amplifier supporting, 4 channel (Left / Right Front + Left / Right Rear), RCA Female connectors;
- External loud speaker (subwoofer) supporting, RCA Female connector, separated sound level in the EQ settings;
- Dynamically changing the volume depends on the vehicle speed, 3 modes: low / medium / strong;
- Navigation voice prompts. You can choose speakers for voice navigation: front or all;
- Microphones, there are two kinds: on-board and external. You can use handsfree function and Android voice programs (Google Voice search, Skype, voice control, etc.);
- Video inputs: 1 x rear view camera (RCA Female connection), 1 x AUX In (RCA

Female connection), some models have 1 x Front CAM input (RCA Female connection);

- AUX Audio input, some models support factory AUX input;
- USB / SD card port, 2 x USB ports, some models support factory USB;
- Set up your car logo or custom logo;

Package includes:

- SMARTY Trend Car Stereo Head Unit for Fiat 500L;
- Main power cable for Fiat 500L;
- CAN-bus module (if applicable);
- USB 3G-modem and USB Flash Drive connection cables;
- Audio / Video connection cables;
- FM antenna connection adapter (if applicable);
- Adapters for original USB and AUX ports (if applicable);
- GPS / Glonass antenna;
- External microphone;
- Wi-Fi antenna;
- User manual.

2. Smartphone
   A secondary communication channel with the user will be a smartphone application able to communicate with the Safety Application OBU and/or with the V2X board. The connection could be established via Wi-Fi through infotainment unit or the router responsible of the communications (i.e., the Application Unit or standalone router Wi-Fi).

- Safety Application
  The Safety Application OBU allows the partners of the project to run the SAFERtec framework and other applications to check and test the reliability of the system proposed into the project. The first hardware solution for this component is the Application Unit VBOX-3600 previously described (see above in this list).

- Ethernet Gateway
  The Ethernet Gateway connects provide connectivity between V2X OBU, Safety APP, HMI Android Head-Unit and Smartphone HMI. The Gateway will provide the following networks: Ethernet IEEE 802.3, Wi-Fi and cellular 3G/4G.

  One option could be the Sierra Wireless AirLink® MP70
  The AirLink® MP70 is a high performance (see Figure 18), LTE-Advanced vehicle router developed specifically for mission critical applications in public safety, transit and field services. Offering high power, long range Gigabit Wi-Fi and Gigabit Ethernet, and up to 300 Mbps downlink speeds over LTE-Advanced, the AirLink MP70 unites the fleet with the enterprise network and enables multiple field applications to work simultaneously, further and faster from the vehicle than ever before.

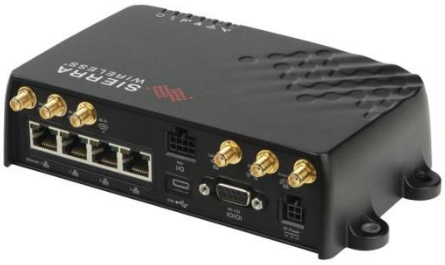

Figure 18 Sierra Wireless AirLink MP70

Specifications:

- LTE-Advanced (Carrier Aggregation) Wide Area Network (WAN) supporting up to 300 Mbps downlink speed
- State-of-the-art LTE coverage spanning 21 LTE frequency bands worldwide
- Two product variants: one product variant for all major NorthAmerican and European network operators, and one product variant for all major Asia Pacific network operators
- Automatic radio configuration based on the SIM
- Dual-SIM functionality to enable automatic failover between SIMs (Canada/EMEA/APAC)
- 4-port Gigabit Ethernet and next generation 802.11ac Gigabit Wi-Fi (3 x 3 MIMO) to support up to 1.3 Gbps, up to 128 clients, WPA2 Enterprise
- High power Wi-Fi provides long range Vehicle Area Network (VAN) and simultaneous AP/Client Mode
- Support for AirLink Vehicle Telemetry to collect OBD-II vehicle telemetry data and monitor engine diagnostics
- Built-in vehicle ready I/O for remote monitoring of auxiliary devices, such as light bars, sirens and gun racks
- Precision Geo-location via GNSS and Inertial Navigation System2, allow local data streaming over the serial port and remotely over NMEA, TAIP, RAP, XORA protocols
- Integrated Mobile Events Engine for real time monitoring and alert reporting of multiple devices, networks, and connected vehicle parameters
- Designed to meet IP64 for resistance to dust and water ingress, and exceeds the MIL-STD-810G specification for shock, vibration, temperature and humidity, and an aluminum chassis for heat dissipation
- Class-leading power supply with built-in surge protection that exceeds E-Mark, ISO 7637-2 and SAEJ1455 requirements, surviving 5V brownouts and spikes from -600 VDC to 200 VDC
- Remote monitoring, management and control with Sierra Wireless's Network Management Solutions—deployable in the cloud or in the enterprise data center
- Over twenty years' experience in cellular networking, and over 1.5 million AirLink gateways deployed
- Industry leading warranty, support, software updates and advance replacement

As an alternative, the Application Unit VBOX-3600 previously described can be used to handle all the traffic between the system components.

7.2 Road Side Unit architecture

The Roadside ITS-S provided is a Cohda MK5 RSU with an embedded NXP i.MX6 800MHz processor 512MB SDRAM and 4GB eMMC flash memory (see Figure 19). Its 802.11p Communication Unit allows the transmission and reception of ITS-G5 messages.

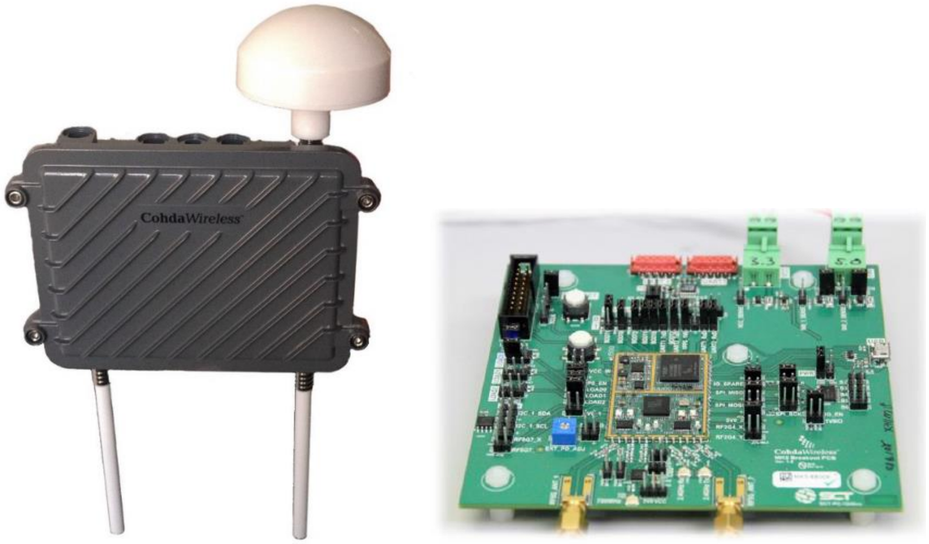

Figure 19: Cohda HW solution (MK5 RSU and Breakout Board)

Specifications:

- MK5 802.11p Radio Module with RF Frontend, security accelerator, operational temperature between -40°C to + 85°C, USB, SPI, UART, GPIO and RF (direct to antennas) interfaces, two x 5.9GHz omnidirectional antennas.
- MK5 RSU with an embedded processor, an embedded GNSS with optional dead reckoning, ETSI TC-ITS Network Layer software, V2X Facilities & Applications Layer software, Dual or single radio & antenna operation, Ethernet & CAN interface, USB 2.0 OTG interface, 12V & 24V Operation and NEMA4 / IP67 Alu-cast outer housing
- MK5 Breakout Board provided with an evaluation & development Kit, Provides full access to the MK5 Radio module, it has a micro-USB Interface, 3v3 and 5v Power Interface, two 5.9GHz RF Output Ports (R-SMA)

7.3 Cloud-based service architecture

7.3.1 Central ITS Station

The C-ITS-S software is deployed as virtual server on a physical server running the virtualization environment VMware vSphere ESXi.

The software runs on Microsoft Windows Server 2016 operating system, and makes use of MS SQL Server 2014 as DBMS.

The server farm on which the system is hosted is protected by redundant CISCO ASA 5500 firewalls.

7.3.2 TomTom Cloud Services architecture

TomTom cloud services, both for TTI servers and NavCloud servers, are based around the deployment of virtual servers in Docker containers, accessing other TomTom services through Virtual Private Cloud (VPC) peering. These services should be deployable in any VPS, such as AWS or Azure.

Even though TomTom services are designed to be deployable to any VPS infrastructure available, a standard hardware configuration for virtual nodes is available in the company, thus ensuring that minimal hardware requirements are always met for new server deployments. This allows teams to expect a baseline performance for new servers. The standard configuration guidelines recommend VPS instances with at least 8 cores, 64 GB ram and 1 TB SSD. All servers are reachable only when connected to the corporate VPN and must be behind a load balancer to avoid single point of failures.

8. Software modules of the Connected Vehicle System

8.1 In-vehicle software

8.1.1 Architecture data-flow

This section reports the data flow of the information between the in-vehicle components. They can be divided into two functionalities: periodic/normal and event based data-flow.

- V2X message generation
  According to ETSI ITS-G5 standard the vehicles are required to periodically send CAM messages (see Figure 20). The CAM messages are composed by: static data, such as vehicle type and identification, positioning data and dynamic data. The first cluster is managed into the configuration file of the V2X OBU. The positioning containers are updated by the GNSS receiver installed into the V2X board. The vehicle dynamic data instead are updated from the vehicle sensors: all the OBUs will send this information into the vehicle CAN bus with frequency rate up to 1-10[Hz], depending on standard transmission rules. The CAN gateway filter-out the signals required to fill the CAM messages and to transmit them into the dedicated CAN bus. The messages in this bus will be different from the original one, in this way it's possible to reduce the overall number of messages and obfuscate the original data-format. At the moment the CAN gateway shall not send back any information from the dedicated CAN bus into the original CAN bus. In addition to that the CAN gateway can also monitor the traffic into the CAN bus to detect anomalies of the expected behavior.

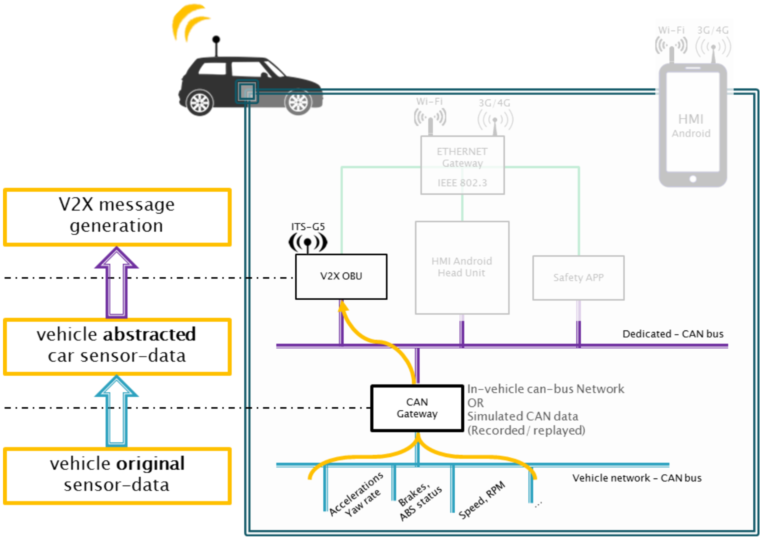

Figure 20: V2X message generation, input data from in-vehicle network.

- Hazard notification from V2X

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Whenever the vehicle approaches an R-ITS-S or another V2X vehicle the V2X OBU will receive information periodic messages (see Figure 21). Specifically from the R-ITS-S the vehicle could receive: road geometry data (MAP message), traffic-light phase information (SPAT messages) and traffic-jam information (DENM message). From the surrounding vehicles instead the receive CAM messages with exactly the same information described in previous point. The V2X OBU performs security check about signature and plausibility check (see description of Stack and chapter on PKI). After that it determines if the messages are relevant for the safety of the vehicle, if so it forwards the information to the safety application.

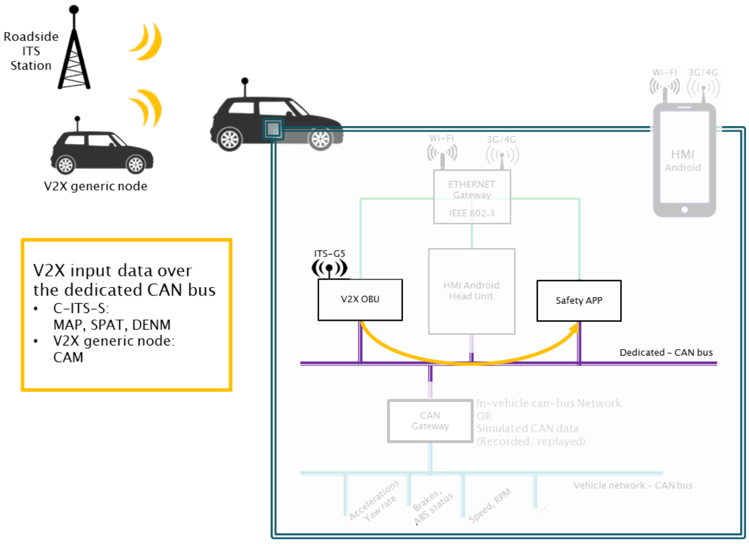

Figure 21 Processing of received I2V and V2V messages.

The Safety Application elaborates the incoming messages and triggers HMI hazard in case driver's intervention is necessary. Two HMI are foreseen into the project: the Android HMI head unit and the smartphone Android application. The first solution is integrated into the vehicle, the hazard triggering is raised through CAN messages sent into the dedicated CAN bus (see Figure 21). The second communication channel will use UDP protocol over Ethernet/Wi-Fi connectivity as depicted into Figure 22.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

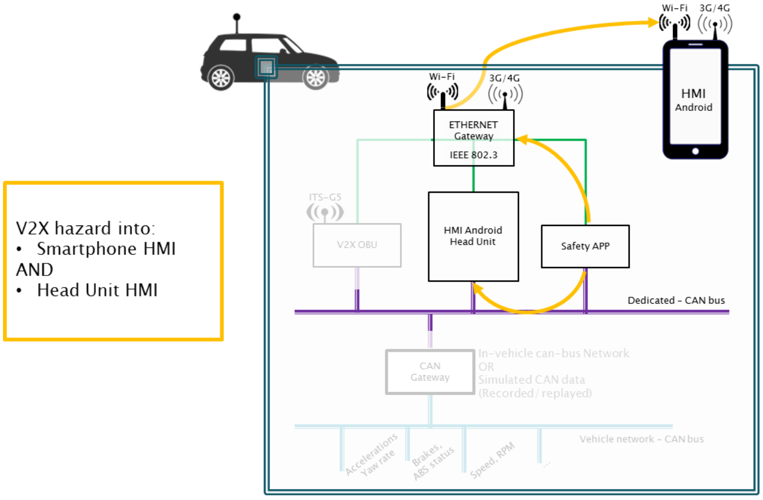

Figure 22: V2X hazards into HMI

As an alternative it's possible to deploy the Safety Application to be part of the OBU as shown in Figure 23, where the V2X OBU performs the hazard check and triggers the HMI warning into the Smartphone and vehicle Head Unit (HMI).

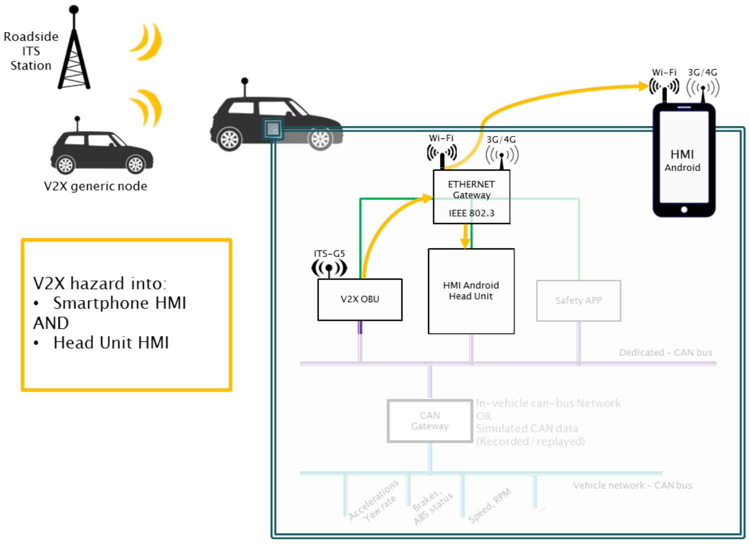

Figure 23 V2X hazards into HMI without Safety App intervention (alternative approach)

- V2X updates
  The V2X OBU requires to periodically getting pseudonym certificate update and Certification Revocation List (CRL), see Figure 24 and Figure 25. The Security Management System is not part of the standard so far but there are implementations of the service available for the OBY by the C2C-CC. The vehicle can reach the service via the internet by 3G/4G connectivity

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

or Wi-Fi. Since continuously connection is not required the system can perform the updates at home connecting to traditional Wi-Fi or any available Hot-Spot.

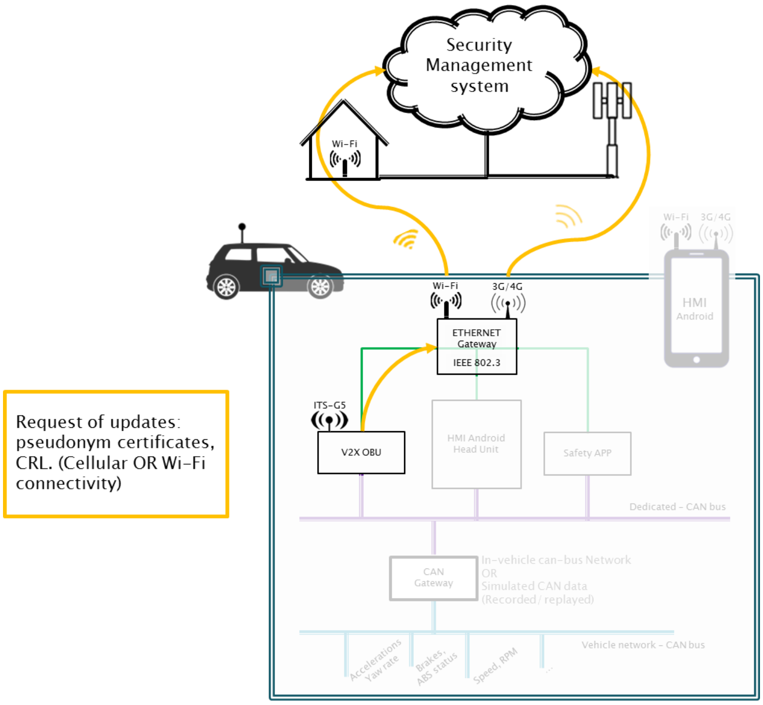

Figure 24 V2X OBU: request of updates: cellular or Wi-Fi connectivity.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

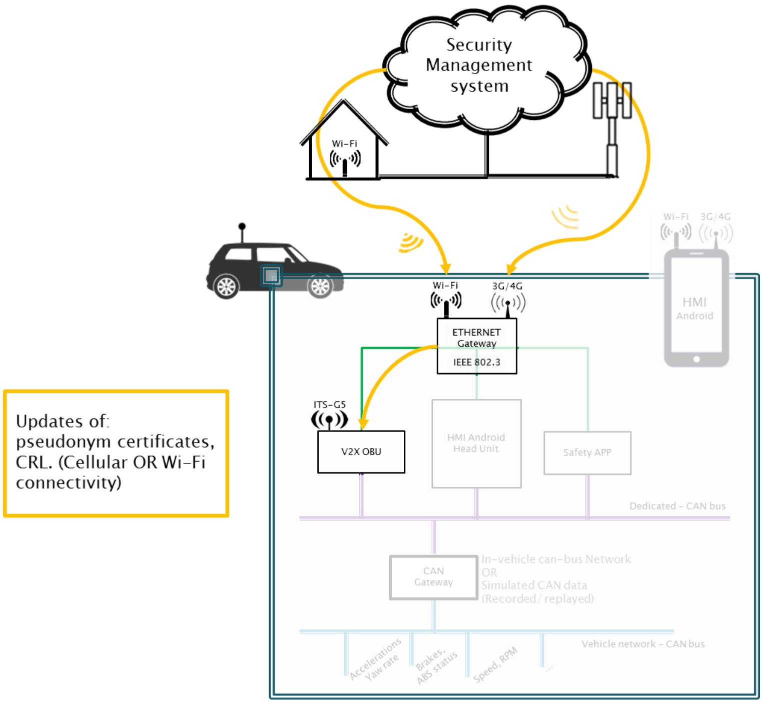

Figure 25 V2X OBU: service subscription

- Information notification from cloud service
  The navigation application fuses local sensor data with cloud services information to provide the driver with a stream of relevant and timely advice for his driving situation through the HMI. The navigation application may provide guidance advice based on a local (off line) map, but it may alter that advice according to live information received from one of TomTom live services, such as live traffic data. The navigation application may also alter the advice provided to a driver according to his personalized profile and settings, such as previous itineraries and favourite locations. Additionally, traffic jam warnings and speed advice may be provided depending on the driving situation and the information availability; this information may be generated by TomTom's services using traffic probes as data sources, but may also be sourced from third party information providers such as a C-ITS-S service to retrieve RSU information or SPAT data relevant to the driving itinerary. Figure 26 and Figure 27 show an example of flow for the application subscription to cloud services first and the subsequent information update, in case the HMI is hosting the application. Instead, Figure 28 shows an example of information flow in case of a hazard: the information is managed by the Safety app, if needed, and then provided to both the HMI as well as to the smartphone though Wi-Fi.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

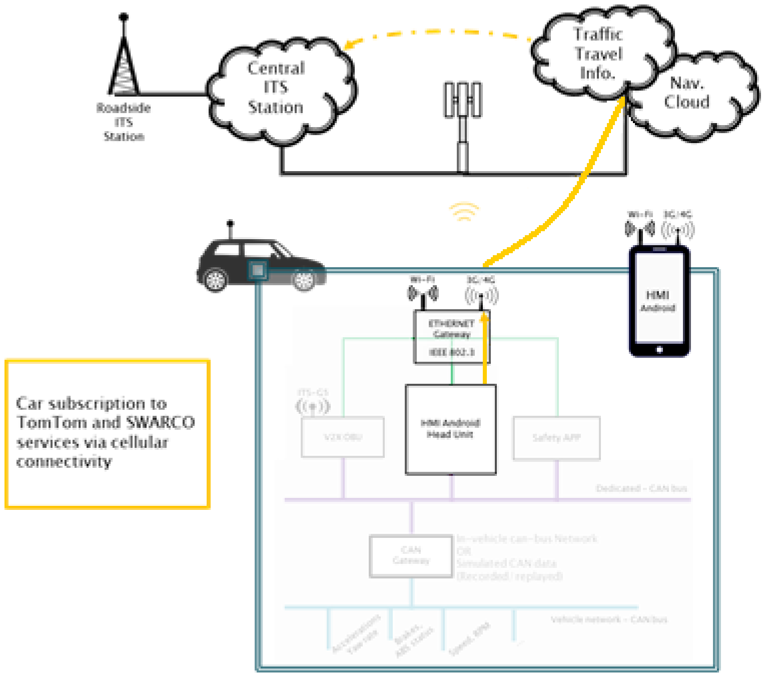

Figure 26: Application subscription to cloud services

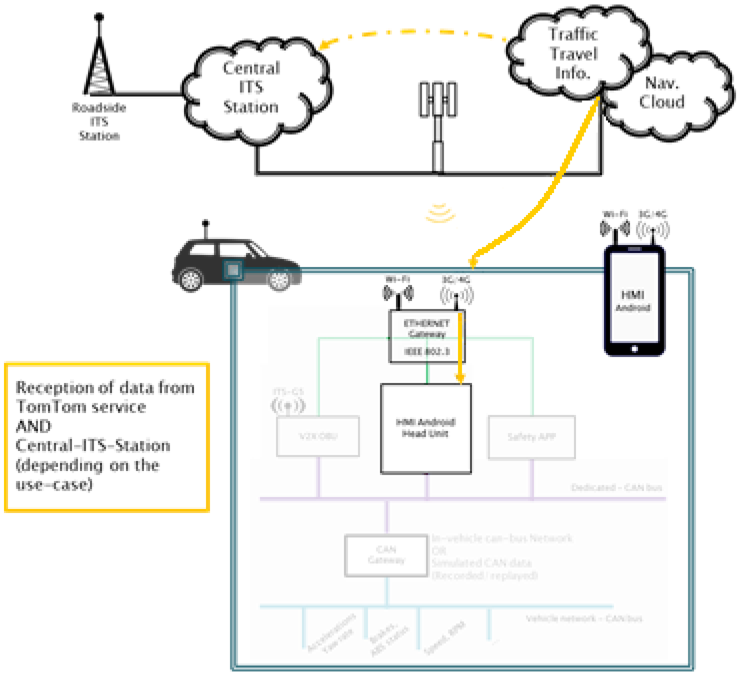

Figure 27: Information update of application on the HMI module

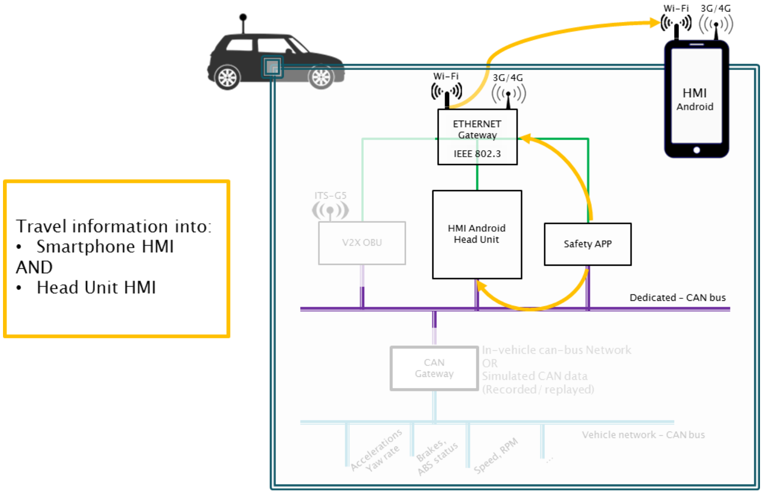

Figure 28: Example of notification of a hazard into both the HMI and the smartphone running Android-based apps

8.1.2 Software architecture security description

Given the complexity of the V2X system, as well as multiple internal and external interfaces, the architecture will support some necessary hardware and/or software based mechanisms in order to isolate critical functionality.

The purpose of isolation is to limit the attack surface of a given security vulnerability to a specific domain. For example, the infotainment service exposes a broad attack surface, which is commonly leveraged by hackers to gain entry into the system. The security architecture will be designed so that critical V2X messaging services or safety services are isolated from such vulnerabilities. The isolation does not guarantee that the complete system software will be secure. However, it provides added layers of security so that the impact of a single vulnerability may be constrained; and so that the hacker will be forced to break through multiple layers in order to stage an attack with any real impact, thus reducing the likelihood of a successful attack on the system.

In addition, the security architecture is designed to be certifiable by accepted hardening and isolation standards. This has fundamental implications:

1. The system may be tested and proven to satisfy market-mandated software security requirements.
2. In case of a security vulnerability is revealed in a particular isolated component, the update and mitigation process may be more readily defined and deployed.

Isolation mechanisms may be broadly classified by two types. A high-level block diagram which emphasizes the key differences is provided, see Figure 29.

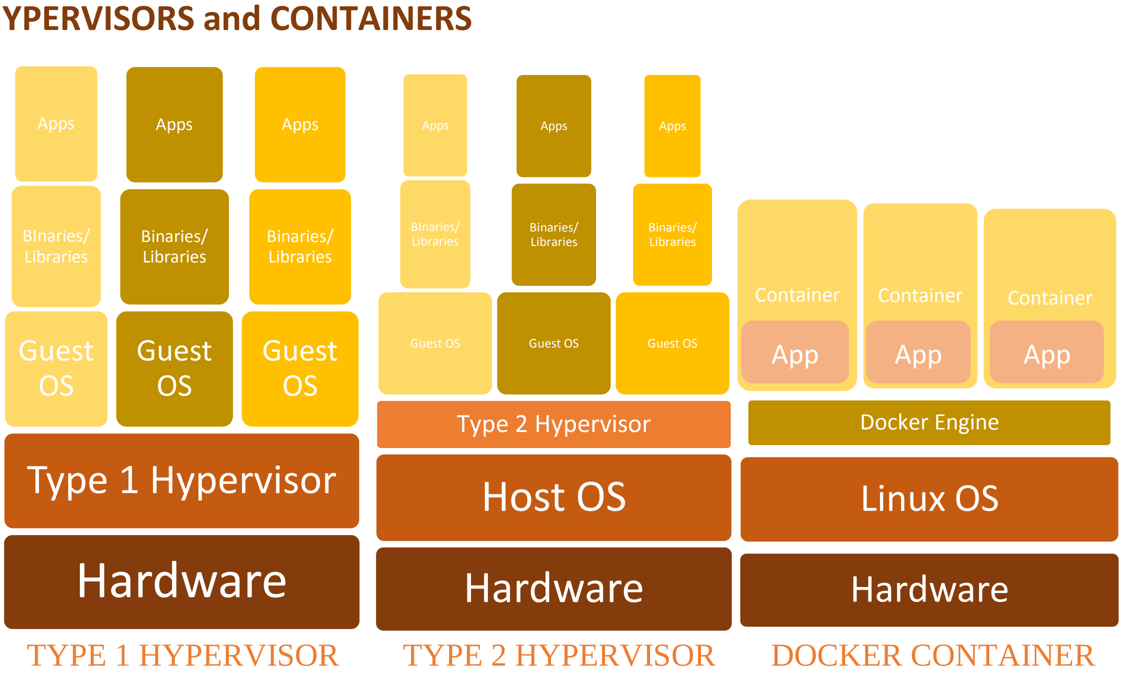

Figure 29: Hypervisors and Containers

1. Hypervisors, aka Virtual Machine Monitors (VMM), support multiple guest operating systems simultaneously on a single host machine. Hypervisors are further classified into 2 broad sub-types:
   a) Type 1 – VM runs directly on hardware. Normally provides better performance and security, given direct access to hardware security features. However, the hardware dependence is costly and more difficult to scale up/maintain long-term. Given these constraints, type 1 hypervisors are not expected to provide sufficient flexibility for the V2X domain.
   b) Type 2 – VM runs on top of some software (host operating system). The host OS controls hardware access, allowing for software flexibility and multiple OS's (each of which may support a separate software domain). However, the common host OS, as well as multiple guest OS's, provide lower security and an increased attack surface.

2. Linux-based containers, which support isolation on the operating system level. Some common examples:
   a) LXC (Linux containers).
   b) Docker containers, whose core is based on LXC.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

Hence, a VMM (in Figure 29 VMM of Type 1 and Type 2) virtually replicates the hardware of a machine and it is fully bundled with one, or more, guest OSs installed on top of such virtualized hardware. A container, instead, is installed on top of a given guest OS (e.g., Linux in Figure 29) and it packages the user software system for running it in isolation, i.e., without depending on a given OS and libraries. In other terms, while a VMM provides and abstraction of a physical machine in which run different guest OSs and the user software system on top of them; a container is a "host kernel" between the guest OS and the user software system, i.e., a container provides a sort of abstraction for the guest OS and contains only such libraries required to run the user software system.

As can be seen in the diagram in Figure 29 (depicting docker containers), the Docker engine replaces the Type 2 VMM. From security point-of-view, similar attack surfaces present themselves in both container as well as Type 2 VMM architectures. The underlying OS needs to be hardened as per accepted market standards, whether it is a Linux OS, for Docker, or host OS, for VMM. The containerization framework (Docker engine or VMM), as well as the individual containers or guest OS, all need to be configured securely as mandated by certification standards and as per specific product documentation. The extensive software base supporting Docker containers may present a broader attack surface; but, in case the added flexibility and ease of scalability are mandated, the effort to build a certifiably secure container infrastructure may be justified.

The Center for Internet Security (CIS) provides basic hardening guides (cisecurity.org); these will need to be evaluated and customized specifically for the V2X domain.

Current software architecture has identified the following domains to be isolated:

1. V2X messaging, including generate/sign/send; receive/authenticate/follow up.
2. Safety services.
3. Notification management (cloud, RSU, ITS).
4. Infotainment and HMI.
5. Ethernet gateway (including firewall and secure communication).
6. Cloud services. These are Android based, but may include native code; may be stored persistently on the device; currently expected low volume (<10). Device will also include web client(s) to interface with external web server.

In the scope of the SAFERtec project, it does not seem that the flexibility of Docker containers is strictly required. A basic VMM Type 2 hypervisor framework could be appropriate, with the specific product and granularity of necessary VM's yet to be determined. As the system functionality grows with time, a container sub-system, such as Docker, may be implemented within one or more individual VM. However, such extended functionality is out of scope for the SAFERtec project.

8.2 Road Side Unit software

The Roadside ITS-S software modules are deployed on the Cohda & NXP Dedicated Short Range Communications solution. It consists of Network and Higher Layer Software Stacks, available from Cohda and an Access Layer/Modem and Security chipset and firmware provided by NXP.

The Network Layer Software is compliant with ETSI ITS-TC:

- Stack Multi-Channel 11p (G5)
- GeoNetworking (GN)
- IPv6 over GeoNetworking (GN6)
- Decentralized Congestion Control (DCC)
- Basic Transport Protocol (BTP).

The Facilities Layer Software is proprietary while the Applications Layer (V2X-App) includes the several applications that have already been implemented and tested in other contexts:

- Hazard Location Warning
- Road Work Warning
- Green Wave
- Signal Violation Warning
- Ice Road Warning
- SPaT/MAP
- SCMS/PKI Interface.

8.2.1 Architecture data-flow

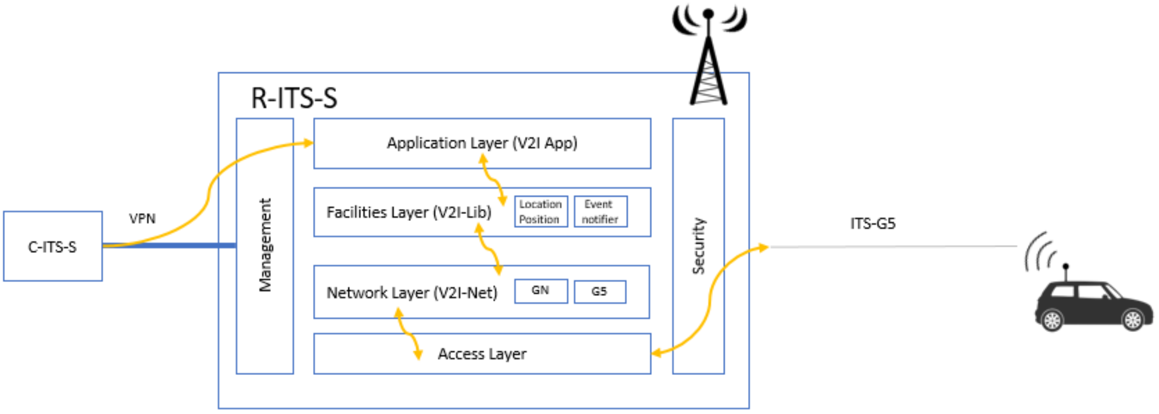

Figure 30: R-ITS-S Architecture data flow.

Figure 30 shows the R-ITS-S internal data flow architecture. The R-ITS-S periodically broadcasts the standardized messages, which are received by the vehicles present in the transmission range. More specifically, the vehicle will receive: road geometry data (MAP message), traffic-light phase information (SPAT messages) and traffic-jam information (DENM message). In return, the R-ITS-S will receive the CAM messages that are periodically sent by the vehicles.

Messages are digitally signed by using a private/public mechanism. Therefore, each box is individually registered at the corresponding PKI by the manufacturer. In turn the PKI issues a certificate for the individual public key stating its trustworthiness and service permissions. By usage of this enrolment certificate (long term validity) the box generates new private/public key pairs for which it requests authorization tickets, i.e. certificates with short term validity, from the PKI, which are included in the messages.

8.3 Cloud-based service software

8.3.1 Central ITS Station

In this section are reported the data flow of the information between the C-ITS-S and the other components of the Connected Vehicle System.

- Optimal Speed Driving use case

Figure 31 summarizes the architecture data flow in the case of the Optimal Speed Driving use-case. The TMC/TLC interface receives the signal feedback data from the field every second. Depending on the source, the communication protocol is different: from the TMC the data is received on REST interface that support HTTPS, optionally with mutual authentication, from the TLC the data is transmitted over a VPN using a proprietary binary protocol.

The data is processed by the TLA management that, with prediction algorithms, generates the SPAT messages. They include information on the status of traffic controllers and prediction of duration and phases.

The system can then either send the data through an endpoint where vehicles and RSUs can request data from when needed, or data can be sent to a specific endpoint in a Push modality. All these type of communication channels support the use of HTTPS, optionally with mutual authentication.

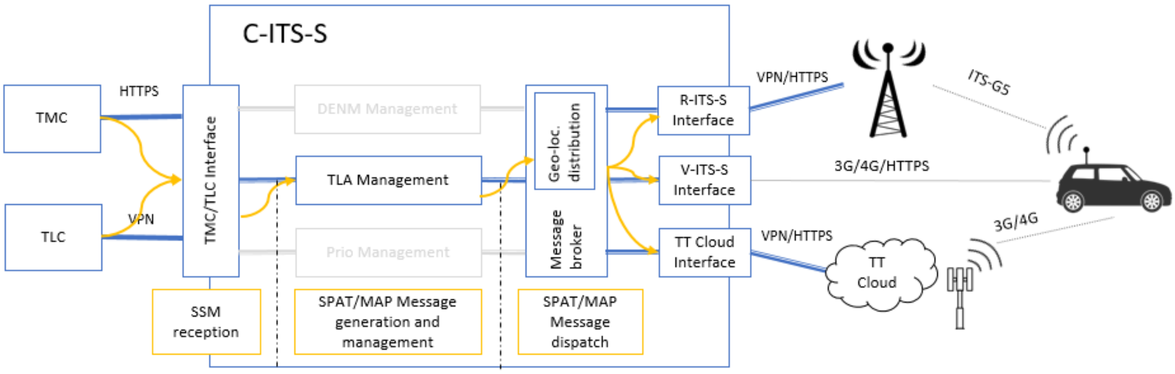

Figure 31: C-ITS-S Architecture data flow for the Optimal Speed driving use-case

- Real Time Traffic Info use case

Figure 32 summarizes the architecture data flow in the case of the Real Traffic Info use-case. The TMC interface receives the event data from the Traffic Management Centre. The data includes information about the position, description, severity, duration, etc. of the event. The communication protocol used by the TMC is a REST interface that supports HTTPS, optionally with mutual authentication.

The data is processed by the DENM management that generates the DENM messages. The DENM messages are composed by information related to the type of the detected event (e.g. traffic condition, accident, roadwork, etc.), information specific of the event location and location referencing.

The system can then either send the data through an endpoint where vehicles, RSUs or other service providers can request data from when needed. These types of communication channels support the use of HTTPS, optionally with mutual authentication.

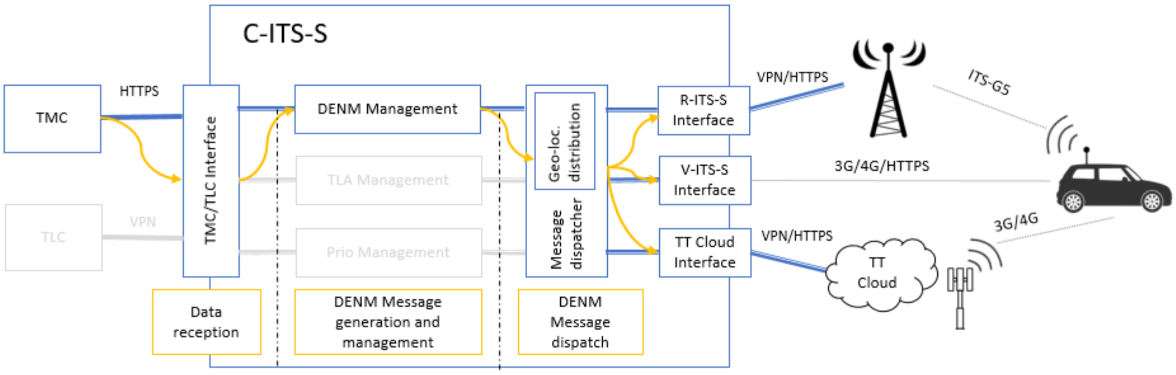

Figure 32: C-ITS-S Architecture data flow for the Real Time Traffic Info use-case

- Priority request use case

Figure 33 summarizes the architecture data flow in the case of the Priority Request use-case. The C-ITS-S receives the CAM messages that are periodically sent by the vehicles from either the Roadside ITS Station or directly from the vehicle. When an authorized vehicle sends a priority request, a special CAM message with an additional data element is sent, including the request of right of way.

The C-ITS-S receives the special CAM message either through the R-ITS-S or directly from the authorized vehicle. These types of communication channels support the use of HTTPS with mutual authentication.

The TLC interface will receive the priority request message from the Priority management, once the right of priority is granted. The data sent to the TLC is transmitted over a VPN using a proprietary binary protocol.

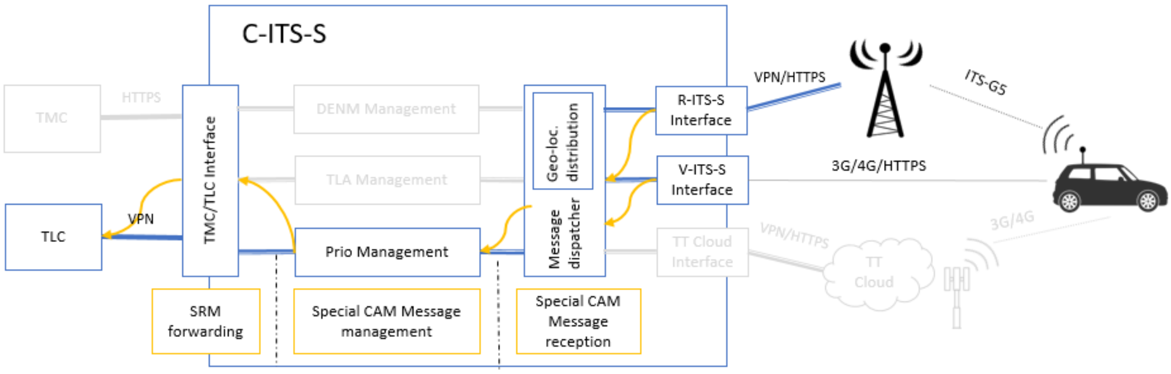

Figure 33: C-ITS-S Architecture data flow for the Priority Request use-case

8.3.2 TomTom Cloud Services architecture

The following section describes the expected data-flows of the use cases utilizing TomTom cloud services in a high level architecture overview representing TomTom cloud infrastructure and a subset of the components expected to be relevant for this use cases in a connected vehicle.

- Use case: Optimal Driving Speed Advice

Figure 34 describes the expected data flows for the optimal driving speed advice use case.

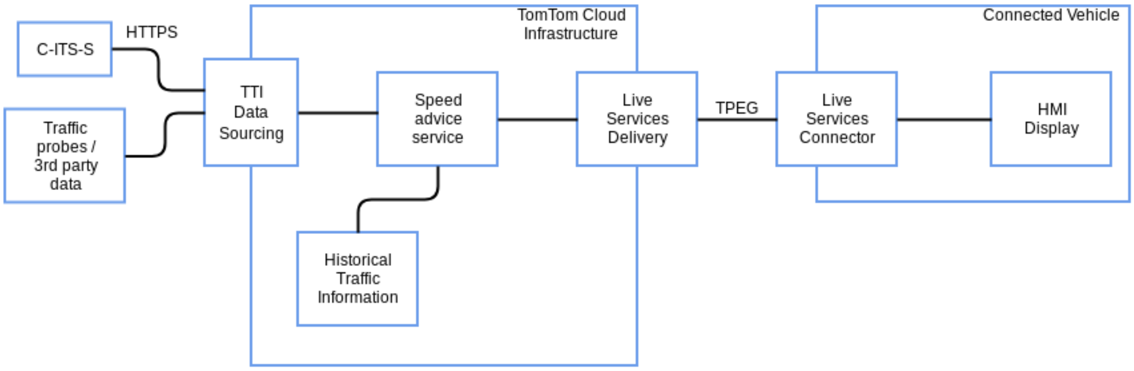

Figure 34: Data flow for the optimal speed advice

TomTom cloud services acquire on real time or semi real time infrastructure data through the C-ITS-S (such as a traffic lights phase information) as well as traffic probes (which may include 3rd party data) to determine the live traffic situation in a certain part of a road network. Fusing this information, TomTom TTI services can generate a speed advice for a driver relevant for certain roads in the road network, so that she may reach the next traffic light in its green phase. The speed advice is then relayed as part of the traffic information services transmitted to a connected vehicle using TPEG and a cellular network as a transport mechanism.

- Use case: Provision of Real-Time Traffic-hazard information

Figure 35 describes the expected data flows for the provisioning of Real-Time Traffic-hazard information.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

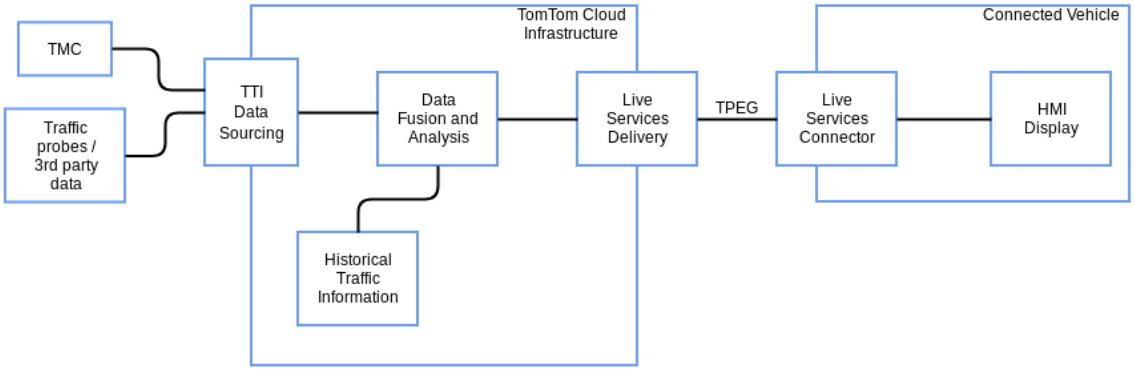

Figure 35: Data flow for real time traffic hazard

The data fusion components in TomTom cloud infrastructure aggregate data from traffic probes and TMC information. Depending on the number and reliability of real time data traces, the real time information may be complemented with historical traffic profiles. These aggregated information is then utilized to detect traffic situations such as traffic jams. Warning of traffic jams are then transmitted to connected vehicles through TPEG and displayed to drivers through and HMI if relevant.

- Use case: Privacy-preserving route planning and navigation

Figure 36 describes the expected data flows to plan a route on a companion app or website, then rely such a route to a connected vehicle so that a driver may navigate to his destination. Note that to emphasize the most relevant components in this diagram, details of TTI services and of the companion app or website are left incomplete; this diagram focuses instead on the connected elements that most closely interact with the connected vehicle.

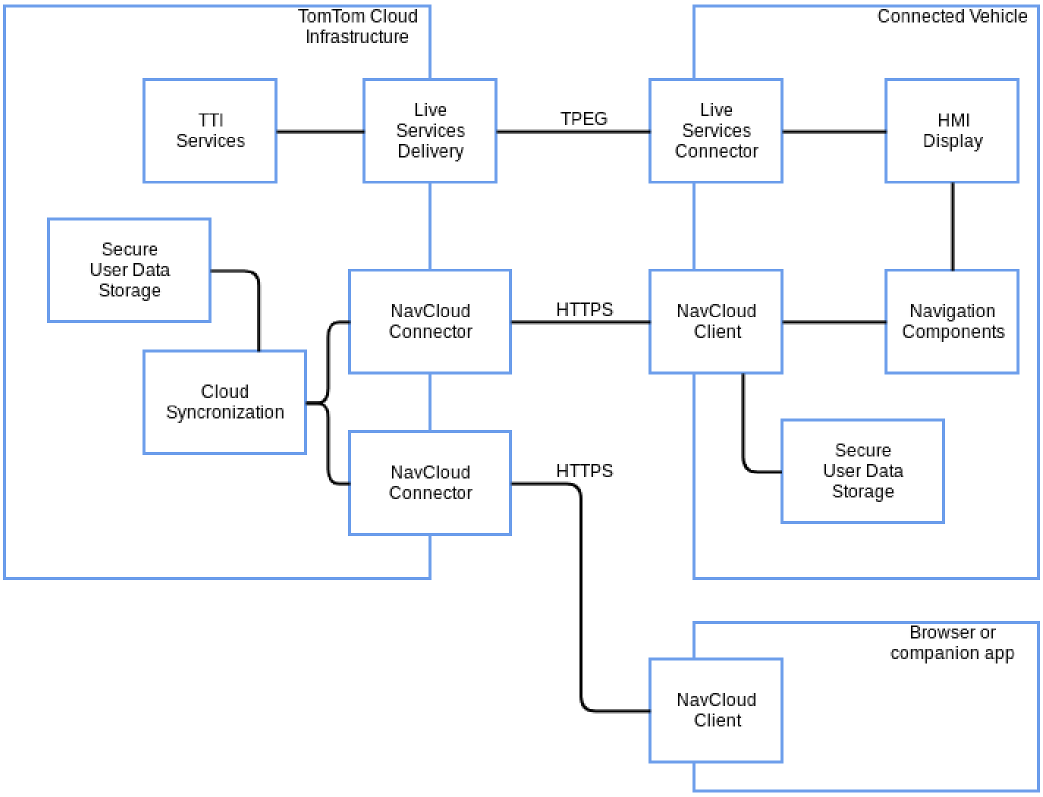

Figure 36: Data flow for route planning

When preparing for a trip, a driver may start by looking for his destination in his personal computer or using his personal phone with a companion app instead of the (usually more limited) HMI offered by a vehicle. Using cloud services, the destination and relevant preferences are synchronized to a secure storage in the cloud. Once the user is ready to commence his trip, this information is then synchronized to the vehicle from the cloud, and kept in a secure local storage in case connectivity is no longer available. Any changes to this information will in turn also be synchronized back to the cloud services once connectivity is restored, so that all of the driver's connected devices may remain in sync.

9. Interfaces of the Connected Vehicle System components/modules

- CAN Gateway

The CAN gateway module is responsible to filter out the vehicle network data required by the V2X OBU to send the V2V messages. The data written into the dedicated CAN bus will not follow the original structure in order to obtain some advantage in terms of channel efficiency and security. In Table 5 is reported the list of signals available for the V2X OBU.

Table 5 Information exchanged between CAN gateway and V2X OBU.

Interface	Information Keyword	Description	Transmission mean
Can Gateway →V2X OBU	ABS activation	ABS intervention ON/OFF	Vehicle CAN bus
Can Gateway →V2X OBU	Acceleration pedal position	[0-100]%	Vehicle CAN bus
Can Gateway →V2X OBU	Brake pedal	Brakes engaged ON/OFF	Vehicle CAN bus
Can Gateway →V2X OBU	Brake Pressure	Braking force	Vehicle CAN bus
Can Gateway →V2X OBU	ESC activation	ESC intervention ON/OFF	Vehicle CAN bus
Can Gateway →V2X OBU	Ignition position	Ignition status	Vehicle CAN bus
Can Gateway →V2X OBU	Lateral Acceleration	Lateral acceleration (ISO 8855) [m/s2]	Vehicle CAN bus
Can Gateway →V2X OBU	Turn indicator	Turn indicator status	Vehicle CAN bus
Can Gateway →V2X OBU	Longitudinal Acceleration	Longitudinal acceleration (ISO 8855) [m/s2]	Vehicle CAN bus
Can Gateway →V2X OBU	Reverse Gear	Reverse Gear inserted ON/OFF	Vehicle CAN bus
Can Gateway →V2X OBU	Steering Wheel Angle	Steering wheel position (counterclockwise) [deg]	Vehicle CAN bus

Can Gateway →V2X OBU	Vehicle Speed	[m/s]	Vehicle CAN bus
Can Gateway →V2X OBU	Yaw Rate	Angular velocity (ISO 8855) [deg]	Vehicle CAN bus

The V2X OBU get the vehicle dynamics data from the dedicated CAN bus and use them to generate the V2V messages.

- V2X OBU ←→ Safety App ←→HMI

The V2X OBU as responsible of the communication between vehicles and infrastructure generate the V2X messages, starting from the GNSS position and the vehicle data obtained from the CAN gateway, vice-versa it provide information of the surrounding vehicles and infrastructure to the HMI and Safety App module. The preferred channel for this communication is the dedicated CAN bus, to simplify the integration with other OBUs of the car, but it's also possible to send this information over the Ethernet network to reach different communication channels. Table 6 lists the V2X information sent and received by means of the V2X OBU.

Table 6: information concerning V2X OBU

#	Interface	Description
1	V2X OBU <> V2X Core Stack	Hardware interface of the Onboard unit for the core software, hardware adaptation (CAN, GNSS, eHSM, V2X radio)
2	V2X Core Stack <> Local Dynamic Map	V2X data is exchanged via TCP/IP using ASN.1 (Abstract Syntax Notation One) data abstraction as defined by e.g. CAM [EN 302 637-2], CDD [TS 102 894-2]
3	Safety APP <> V2X Core Stack (via Local Dynamic Map)	Custom (proprietary) TCP/IP API used to trigger V2X message via in-vehicle Ethernet (CAN alternative will also be investigated).
4	Local Dynamic Map <> Safety APP	Custom (proprietary) TCP/IP API for the safety applications via in-vehicle Ethernet (CAN alternative will also be investigated).
5	Safety APP <> HMI	XML-based warning data sent by means of the TCP/IP protocol though the in-vehicle Ethernet
6	Vehicle <> V2X OBU	Standard CAM and DENM messages
7	V2X OBU <> Road side unit	Infrastructural information (encoded as V2X CAM, DENM, MAP and SPAT messages) including, e.g., traffic light and traffic event information, signage and so on.

- TT Cloud

Table 7 lists the relevant information exchanged thought the components of the connected vehicle system for providing cloud-based services in the SAFERtec use cases.

Table 7 Information exchanged between through the cloud for the TT services

#	Interface	Description
1	TTI <> Connected vehicle	Updated traffic information relevant for the connected vehicle, to be used in the vehicle's OBUs and possibly displayed to a driver through an HMI
2	TTI <> C-ITS-S	Information exchange on infrastructure state
3	NavCloud <> Connected vehicle	Personal information storage relevant to a driver, such as locations, routes, favorites and others.

- Road side unit

Table 8 lists the information exchanged between the road side unit components and other components of the connected vehicle system.

Table 8: information exchanged between road side unit (C-ITS-S/S-ITS-S) and components of the connected vehicle system

#	Interface	Description
1	C-ITS-S <> TMC	Proprietary wired connection
2	C-ITS-S <> TLC	Proprietary wired or cellular connection
3	C-ITS-S <> R-ITS-S	The communication is done via an IP based connection initiated by the R-ITS-S. Standard OCIT-C communication protocol applied, with the utilization of a VPN tunnel for the communication link. OCIT-C interface between C-ITS-S and R-ITS-S for the Device Management operations and Cooperative data exchange
4	C-ITS-S <> TTCloud	Proprietary wired connection
5	C-ITS-S <> Web Server	The data generated by the C-ITS-S (i.e. DENM, SPAT) is delivered to the vehicle through an ITS WEB server. The web server behaves as a content provider and is in charge of the

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

		delivery of the information.
6	Web Server <> Vehicle	The connection from the web server to the vehicle is based on a set of methods that can be used to exchange data from/to the cloud C-ITS-S environment.
7	R-ITS-S <> Vehicle	The communications architecture of reference is the one defined in [ETSI 302 665]. The communications security architecture of reference is the one defined in [ETSI 102 940]. See "Figure 4: Architectural ITS security layers" in [ETSI 102 940].
8	C-ITS-S <> PKI	*Not yet implemented*

10. Conclusions

This document constitutes the SAFERtec deliverable D4.1 (entitled "Specifications of Connected Vehicle System) which is part of the WP4 (entitled "Connected Vehicle System") and presents the outcome of task T4.1 "Connected Vehicle System Specifications".

This deliverable includes a comprehensive description of the design and specifications for both hardware and software architecture required to implement the SAFERtec connected vehicle system. The latter will be used to realize all scenarios of interest for the project. The overall architecture has been defined aiming at fulfilling all the SAFERtec objectives; all technical requirements of the use cases have been considered in the design of the reference architecture which is expected to ease the subsequent SAFERtec implementation phase.

Concerning the final hardware architecture, the designed solution proposed in this document represents a good compromise in terms of integration and flexibility for the development of the reference connected vehicle system of modern vehicle-centric systems adopting ITS-G5 and cellular communication technologies.

Concerning the final software architecture, it has been designed to satisfy: all use cases prerequisites and requirements, the distribution of hardware components across the available platforms, and the consistency of the designed reference connected system with the actual (i.e., to be used in the project) and also envisioned (i.e., under development or produced by external to project vendors) connected systems.

All the input and output relations among hardware and software component and modules in the architecture of the connected vehicle system have been carefully considered and clearly designed, described and presented in the deliverable; as well as the data flow and control chain, especially concerning the use cases of interest for SAFERtec, have been detailed.

The actual implementation and realization of the designed and presented connected vehicle system will be realized in tasks:

- T4.2 ("V2X HW & SW module"), T4.3 ("Implementation of RSU system (Component/System Level") and T4.4 ("Implementation of 3rd Party Applications and Services") described in Deliverable D4.2 ("Modules and Applications of Connected Vehicle" – M20)
- T4.5 ("Connected Vehicle System Integration") described in Deliverable D4.3 ("Integration of Connected Vehicle System" – M22).

The architecture of the connected vehicle system which has been designed and specified in this deliverable will be mainly used in task T5.3 ("Composite Evaluation") described in the deliverable D5.4 ("Composite Evaluation of SAFERtec Assurance Framework"– M36) of WP5 ("Assurance Framework Evaluation") for evaluation purposes of the SAFERtec assurance framework.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

11. Bibliography

ETSI. (2017). Retrieved from European Telecommunications Standards Institute: http:// http://www.etsi.org

ETSI Automotive Intelligent Transport Systems. (2017). Retrieved from http://www.etsi.org/technologies-clusters/technologies/automotive-intelligent-transport

Kvaser. (2017). *CAN PROTOCOL Tutorial.*

Miller, C., & Valasek, C. (2015). *Remote Exploitation of an Unaltered Passenger Vehicle.*

National Highway Traffic Safety Administration. (2016). *Cybersecurity best practices for modern vehicles.* Washington DC: Report No. DOT HS 812 333.

Valasek, C., & Miller, C. (2014). *Adventures in Automotive Networks and Control Units.*

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement no 732319

Appendices

A.1: Risk Matrix

The following table constitutes a new addition to the SAFERtec Risk Matrix (presented originally in D1.2 – "Risk and Quality Procedures Manual"). As mentioned there, the table will be updated regularly as the work progresses and the consortium moves to important (technical) choices.

In the following entries, we identify a number of WP4 risks and highlight a mitigation plan for each of them (first and second column of the table respectively). In the two rightmost columns we approximately assess their probability of occurrence (using three levels: low, moderate, high) and the estimated impact (using a 1-10 scale). In the last column, finally, the other WPs impacted by the risk are listed.

The table presents the current view of the risks identified by the partners according to the presented architecture, architectural decisions as well as known challenging issues.

Risk	**Mitigation plan**	**Estimated probability** (3 levels)	**Estimated Impact** (1-10 scale)	**Other WPs Potentially Impacted by the RISK**
Delay in the architecture implementation, i.e., delay in the SAFERtec working and development process on WP4.	- Speed up the subsequent WP tasks as possible, such as the integration of the different architectural parts (i.e., in-vehicle architecture, road-side unit and cloud-based service) as well as the adoption of the designed connected vehicle system in the assurance framework refinement and evaluation	Moderate	5	WP3, WP5
Unavailability of hardware / software components used in the designed architecture. The following criticalities could be depicted: 1) unavailability of the adequate isolation mechanisms for the software architecture security (i.e., Linux-based containers); 2) unavailability of the in-vehicle Android-based HMI; 3) unavailability of a third-party cloud service; 4) unavailability of the expected PKI management system;	- Identifying alternatives of missing components by starting from alternatives already listed in the deliverable. For the listed risks, the following plan will be in place: 1) adoption of possible alternatives (hypervisors instead of Linux-based containers); 2) adoption of Android smartphone/tablet enriched with modules for accessing to the in-vehicle network 3) selection of an alternative and comparable cloud-based service that satisfied the requirements and lets us realize the use case of interest 4) emulation of the needed PKI service management	Moderate	6	WP3, WP5
Inability to realize a use case of interest of the project, i.e., not meeting the use-case requirements and needs	- The whole project consortium to promptly identify another use-case that will be achievable by the available architecture and of interest for the project - Promptly identifying, specific aspects of the use-case that could be realized by the architecture and that are in line with the project goals	Low	7	WP2, WP5
Non interoperable V2X communications, use of different standard versions/releases.	- Clearly (re)define the message set used - Reserve resources to align to a common set of standard implementation	Low	3	WP3, WP5
Inability to implement conflicting security and privacy requirements	- Redesign the conflicting relationships and provide alternative implementation paths using	Moderate	5	WP3, WP5

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement no 732319

	the already implemented protocols/techniques.			
Conflict resolution among safety and privacy requirements	- Determine the set of personal information per use case against the safety requirements and provide adequate Privacy Enhancing Technologies that will provide adequate level of users' privacy without compromising safety. Also provide alternative security profiles that the system will adopt in case of conflicting requests.	Moderate	6	WP3, WP5