Abstract
SAFERtec proposes a flexible and efficient assurance framework for security and trustworthiness of Connected Vehicles and Vehicle-to-Everything (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 Connected Vehicle and V2X systems, with increased connectivity of automotive ICT systems, consumer electronics technologies and telematics applications, 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.X & Title:** D2.1 “Connected Vehicle Use Cases and High Level Requirements”  

**Work package:** Reference Modeling and Requirements  

**Task:** Task 2.1 Connected Vehicle Use Cases  

**Due Date:** 31 June 2017  

**Dissemination Level:** PU  

**Deliverable Type:** R

---

**Authoring and review process information**

<table>
<thead>
<tr>
<th>EDITOR</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panagiotis Pantazopoulos / ICCS</td>
<td>15-10-2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CONTRIBUTORS</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Panagiotis Pantazopoulos / ICCS</td>
<td>16-03-2017</td>
</tr>
<tr>
<td>András Váradi / COMM</td>
<td>12-07-2017</td>
</tr>
<tr>
<td>Elana Copperman / AUT</td>
<td>24-07-2017</td>
</tr>
<tr>
<td>András Edelmayer / COMM</td>
<td>14-09-2017</td>
</tr>
<tr>
<td>Andrea Steccanella / CRF</td>
<td>20-09-2017</td>
</tr>
<tr>
<td>Gildas Koudessi / CCS</td>
<td>02-10-2017</td>
</tr>
<tr>
<td>Silvia Capato / SWR</td>
<td>03-10-2017</td>
</tr>
<tr>
<td>Kostas Lambrinoudakis / UPRC</td>
<td>09-10-2017</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REVIEWED BY</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elana Copperman / Autotalks</td>
<td>30-10-2017</td>
</tr>
<tr>
<td>Matthieu Gay / CCS</td>
<td>30-10-2017</td>
</tr>
</tbody>
</table>

**LEGAL & ETHICAL ISSUES COMMITTEE REVIEW REQUIRED?**  
NO
Document/Revision history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Partner</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>29/03/2017</td>
<td>ICCS</td>
<td>Starting draft</td>
</tr>
<tr>
<td>V0.2</td>
<td>10/04/2017</td>
<td>ICCS</td>
<td>ToC update</td>
</tr>
<tr>
<td>V0.3</td>
<td>23/05/2017</td>
<td>ICCS</td>
<td>Section 1, introduction</td>
</tr>
<tr>
<td>V0.4</td>
<td>14/06/2017</td>
<td>ICCS</td>
<td>Appendix A, updates in structure</td>
</tr>
<tr>
<td>V0.5</td>
<td>19/07/2017</td>
<td>ICCS/ALL</td>
<td>Section 2, Section 3, Section 4</td>
</tr>
<tr>
<td>V0.6</td>
<td>30/08/2017</td>
<td>ICCS/ALL</td>
<td>Updates in Section 2 and Section 3</td>
</tr>
<tr>
<td>V0.7</td>
<td>18/09/2017</td>
<td>COMM</td>
<td>Comments in Section 2</td>
</tr>
<tr>
<td>V0.8</td>
<td>09/10/2017</td>
<td>UPRC</td>
<td>Comments across the document, security and privacy concerns for each use-case</td>
</tr>
<tr>
<td>V0.9</td>
<td>30/10/2017</td>
<td>AUT, CCS</td>
<td>Internal review comments</td>
</tr>
<tr>
<td>V1.0</td>
<td>31/10/2017</td>
<td>ICCS</td>
<td>Comments included. Final version produced and submitted</td>
</tr>
</tbody>
</table>
Table of Contents

Acronyms and abbreviations ........................................................................................................... 6
Executive Summary .......................................................................................................................... 8
1. Introduction ................................................................................................................................. 9
   1.1 Purpose of the Document ........................................................................................................ 9
   1.2 Intended readership ................................................................................................................ 10
   1.3 Inputs from other projects ..................................................................................................... 10
   1.4 Relationship with other SAFERtec deliverables ................................................................. 10
2. The SAFERtec Connected Vehicle Use Cases ....................................................................... 10
   2.1 Application scenarios under Vehicle to R-ITS-S communications ..................................... 11
       2.1.1 The optimal driving speed advice .................................................................................. 12
       2.1.2 Provision of real-time traffic-hazard information ......................................................... 14
       2.1.3 Priority request in intersection-crossing ...................................................................... 17
   2.2 Application scenarios under Vehicle to Cloud communications ....................................... 20
       2.2.1 The optimal driving speed advice .................................................................................. 20
       2.2.2 Provision of real-time traffic information ...................................................................... 22
       2.2.3 Privacy-preserving route planning and navigation ....................................................... 23
3. A SAFERtec reference architecture to support the selected Use Cases .................................. 26
   3.1 Modules in the vehicle platform ............................................................................................. 27
   3.2 Modules outside the vehicle platform ..................................................................................... 30
       3.2.1 The SAFERtec C-ITS-S and R-ITS-S ......................................................................... 30
       3.2.2. The SAFERtec Cloud-based Services ...................................................................... 31
4. Attack entry points and high level security and privacy requirements .................................... 33
   4.1 Attack entry points and security/privacy requirements in the vehicle platform ............... 34
   4.2 Attack entry points and security/privacy requirements outside the vehicle platform .......... 35
       4.2.1. R-ITS-S and C-ITS-S infrastructure and services ........................................................ 36
       4.2.2. Cloud infrastructure and services ................................................................................... 38
       Provision of real-time traffic information .............................................................................. 38
       Provision of real-time traffic information .............................................................................. 39
5. Conclusions ............................................................................................................................... 40
References ....................................................................................................................................... 41
Appendices .................................................................................................................................... 42
A. Related standards ....................................................................................................................... 42

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

Figure 1 R-ITS-S communicates optimal speed to the connected vehicle ........................................... 12
Figure 2 Entities, communication means and responsible partners involved in the UC1 implementation ........................................................................................................................................................................... 13
Figure 3 R-ITS-S communicates a warning for hazardous event ahead .......................................................................................................................................................................................................................... 15
Figure 4 Entities, communication means and responsible partners involved in the UC2 implementation .......................................................................................................................................................................................................................... 15
Figure 5 R-ITS-S signals to coordinate the intersection-crossing .......................................................................................................................................................................................................................... 18
Figure 6 Entities, communication means and responsible partners involved in the UC3 implementation .......................................................................................................................................................................................................................... 19
Figure 7 A cloud-based service communicates the optimal speed to the connected vehicle ............. 20
Figure 8 Entities, communication means and responsible partners involved in the UC4 implementation .......................................................................................................................................................................................................................... 21
Figure 9 Cloud-based service communicates a warning for hazardous event ahead ................................................ 21
Figure 10 Entities, communication means and responsible partners involved in the UC5 implementation .......................................................................................................................................................................................................................... 23
Figure 11 Online route-planning informs vehicle device ............................................................................. 24
Figure 12 Entities, communication means and responsible partners involved in the UC6 implementation .......................................................................................................................................................................................................................... 25
Figure 13 Draft of the SAFERtec architecture for the vehicle platform .................................................... 27
Figure 14 Draft of the SAFERtec architecture for the C-ITS and R-ITS systems .................................. 30
Figure 15 Draft of the SAFERtec architecture for the cloud services ....................................................... 32

List of Tables

Table 1: List of Abbreviation .......................................................................................................................... 7
Table 2: Identified entry points of attacks for the vehicle platform .............................................................. 34
Table 3: Preliminary high-level requirements for the vehicle platform ......................................................... 35
Table 4: Identified entry point of attacks for the R-ITS-S and C-ITS-S services ........................................ 36
Table 5: Preliminary high-level requirements for the C-ITS-S/R-ITS-S functionality ................................... 37
Table 6: Identified entry point of attacks for the cloud-based services ....................................................... 38
Table 7: Preliminary high-level requirements for the cloud-based services ................................................ 39
### Acronyms and abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BTP</td>
<td>Basic Transport Protocol</td>
</tr>
<tr>
<td>C-ITS-S</td>
<td>Cooperative Intelligent Transport Systems</td>
</tr>
<tr>
<td>C2C-CC</td>
<td>Car 2 Car Communication Consortium</td>
</tr>
<tr>
<td>DoA</td>
<td>Description of the Action</td>
</tr>
<tr>
<td>DSRC</td>
<td>Dedicated Short Range Communication</td>
</tr>
<tr>
<td>ECU</td>
<td>Electronic Control Unit</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>GLOSART</td>
<td>Green Light Optimized Speed Advisory</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite System</td>
</tr>
<tr>
<td>HMI</td>
<td>Human-Machine Interface</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware security module</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>LDM</td>
<td>Local Dynamic Map</td>
</tr>
<tr>
<td>LTE</td>
<td>Long-Term Evolution</td>
</tr>
<tr>
<td>MAP</td>
<td>Map Data</td>
</tr>
<tr>
<td>OBU</td>
<td>(Vehicle) Onboard Unit</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>PC</td>
<td>Project Coordinator</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PO</td>
<td>Project Officer</td>
</tr>
<tr>
<td>PP</td>
<td>Protection Profile</td>
</tr>
<tr>
<td>QRM</td>
<td>Quality and Risk Manager</td>
</tr>
<tr>
<td>R-ITS-S</td>
<td>Roadside ITS Station</td>
</tr>
<tr>
<td>SME</td>
<td>Small and Medium-sized Enterprise</td>
</tr>
<tr>
<td>SPaT</td>
<td>Signal Phase and Time</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
</tbody>
</table>

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

D2.1 – Connected Vehicle Use Cases and High Level Requirements

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIM</td>
<td>Technical and Innovation Manager</td>
</tr>
<tr>
<td>TLC</td>
<td>Traffic Light Controller</td>
</tr>
<tr>
<td>TMC</td>
<td>Traffic Management Center</td>
</tr>
<tr>
<td>TRL</td>
<td>Technology Readiness Level</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>V-ITS-S</td>
<td>Vehicle-ITS-System</td>
</tr>
<tr>
<td>V2I</td>
<td>Vehicle-to-Infrastructure</td>
</tr>
<tr>
<td>V2X</td>
<td>Vehicle-to-Everything</td>
</tr>
</tbody>
</table>

*Table 1: List of Abbreviation*
Executive Summary

This deliverable, entitled “Connected Vehicle Use Cases and High Level Requirements” lays the ground for the SAFERtec modeling and implementation work. It essentially singles-out a number of timely use-cases where the project will set its focus-on when realising instances of real-world V2I communications. Those will be used to help us validate the proposed security assurance framework.

The work carried out in the context of SAFERtec Task 2.1 is presented in this document; it first discusses the use-cases selection criteria, describes each use-case, the corresponding information flow as well as the major security concerns that become relevant in each one. At the same time the involved project partners that will subsequently contribute to the implementation of each use-case, are noted.

The following paragraphs of the document explain the main technical choices regarding the implementation of the (prototype) ‘connected vehicle system’ in a way that will allow to efficiently realize the selected use-cases. Software design choices for the architecture of the vehicle platform as well as the Roadside ITS Station and the cloud-based infrastructure/services, are discussed.

The final part of this deliverable is dedicated to a first approach to the identification of the entry points of attacks associated with the selected use-cases and the foreseen software and hardware modules. Then, a number of relevant high level security (safety, privacy and reliability) requirements are presented for both the vehicle platform and the corresponding infrastructure. This preliminary study will be considered as an initial input to the subsequent attack modelling and vulnerability analysis tasks, where it will be thoroughly enhanced and explored to become the basis for the SAFERtec security assurance framework.
1. Introduction

Even if today’s vehicles already integrate devices that provide connectivity (e.g., Internet), in the very near future commercial vehicles are expected to directly interact with the road infrastructure (as well as with each other). On the one hand, this interaction will allow road users and traffic managers to share and exploit information previously not available and then, accordingly act. On the other hand, the established connectivity will facilitate information exchange of increased quality and reliability about the vehicles, their location and the road environment. This is to significantly improve road safety, traffic efficiency and comfort of driving, by helping either the driver or the automation software to take the right decisions and adapt to a given traffic situation.

Benefits that will go beyond stand-alone driver assistance services can be further magnified if individual vehicles are enabled to continuously communicate with the road infrastructure (R-ITS-S). Likewise, a number of new services to road users are becoming available when vehicles connect to cloud services. On a more visionary note, V2I communications are crucial to increase the safety of fully automated vehicles and most notably their integration into the overall transport system.

The document at-hand presents relevant automotive scenarios (i.e., the SAFERtec use-cases) where the connected ego-vehicle communicates either with the road-side/traffic management infrastructure or with cloud-based services to access information of relevance. Each use-case scenario is detailed pointing to the software design, implementation choices and brief references to the identified security and privacy challenges (associated with each one). It is those use-cases that will be implemented (through the so-called SAFERtec connected vehicle system) to serve as the basis for the SAFERtec assurance framework evaluation.

Under the emerging digitized transport ecosystem the involved software (and even hardware) entities become more vulnerable to hacking and cyber-attacks. Connected vehicles that integrate numerous 3rd party components need to exchange information with the infrastructure about complex traffic situations where not only safety but also security and the protection of personal data remain highly critical. The focus of the SAFERtec project is to analyse the above V2I automotive landscape and propose a framework that would quantify the involved (security, safety, privacy, reliability) assurance levels rather than devising new security controls. With the set of SAFERtec use-cases carefully selected to cover a broad range of the V2I attack surface, the project will proceed with the modelling tasks (i.e., attack modelling, vulnerability analysis) and at the same time implement the SAFERtec connected vehicle system. As such, a considerable task to serve the SAFERtec purposes and contribute to the successful deployment of the connected vehicles has been accomplished.

1.1 Purpose of the Document

The document seeks to present the result of the work carried-out in the context of Task2.1 (entitled ‘Connected Vehicle Use-cases’). Entry points of attacks, access methods and high level security, safety, privacy and reliability requirements will be derived to feed the subsequent WP2 tasks.
1.2 Intended readership

Besides the project reviewers, this deliverable is addressed to any interested reader (i.e., Public 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

The content included in this document is related to numerous other SAFERtec deliverables. Essentially the subsequent WP2 tasks as well as the majority of the WP4 work will evolve around the herein presented use-cases. The SAFERtec security assurance framework will be designed to meet the generic V2I requirements but its evaluation will be conducted over a reference vehicle connected system that would realize the SAFERtec use-cases.

2. The SAFERtec Connected Vehicle Use Cases

This section details the automotive use cases that the project will consider. Central to the SAFERtec research is the so-called ‘connected vehicle system’ that essentially realizes the V2I (Vehicle-to-Infrastructure) communication paradigm. 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. In the context of V2I security and communications, the consortium carefully considered more than a dozen (V2I) use cases and finally selected the ones that are herein presented. The main criteria considered for our selection are listed in the following points:

- The extent to which a use-case is (or may become) safety-critical.
- The level of pervasiveness, or anticipated deployment, in current and emerging automotive settings. This does not necessarily imply that the project seeks to focus
on ‘radically new’ settings. On the contrary, existing use cases can be challenging to study from a security- and privacy-assurance standpoint, in various infrastructure frameworks.

- The feasibility of a detailed exploration with respect to the available resources. In-depth exploration of the most relevant use cases is targeted so as to derive effective, deployable and measurable results.

- The extent to which a certain use-case can be realized under two different counterparts i.e., one that requires a Roadside-/Central- ITS Station (C-/R-ITS-S) and another that requires cloud communication. Interesting outcomes can result from a side-by-side comparison.

Finally, it is worth mentioning that the set of selected use-cases will be studied with primary focus on the so-far under-explored areas involved, such as identifying specific security- and privacy-vulnerabilities and/or requirements of the R-ITS-S and cloud infrastructure.

Likewise, other entities that are typically present in the considered setting such as the public key infrastructure (PKI) and the related functionality\(^1\) (e.g., messages, protocols, etc.) will be herein simply mentioned. Their role and security impact will be discussed in detail in future deliverables (see for instance the SAFERtec D4.1), as relevant for the overall security context.

For the sake of completeness we provide pointers to the related standards (i.e., mainly V2I messages) in Appendix A.

### 2.1 Application scenarios under Vehicle to R-ITS-S communications

One major part of the V2I setting that the SAFERtec work will focus-on involves scenarios that realize the connected vehicle system through the communication with Roadside ITS Stations (R-ITS-S). The corresponding information can originate from the infrastructure back-end (e.g., TMC), reach the C-ITS-Station [1] and become relevant in numerous current as well as emerging (i.e., of higher-automation level) automotive settings. In what follows, we present a high-level description of those RSU-related use-cases that will be considered in SAFERtec.

---

\(^1\) PKI typically enables authentication, authorization of senders, integrity of data through verification of digital signatures and confidentiality principles as well as certificates’ management.
2.1.1 The optimal driving speed advice

In this use-case a vehicle can rely on the received phase-and-timing messages in order to calculate the appropriate speed for reaching the intersection at the beginning of the next green phase (see Figure 1) i.e., the so called “Green Light Optimized Speed Advisor” (GLOSA). That speed value can be made known to the driver of the connected vehicle through an HMI application, either using the vehicle’s infotainment system or a customized application in some handheld device. (Additional information such as the intersection topology may be employed by highly automated vehicles to calculate trajectory data for safe and comfortable intersection crossing [3]).

The traffic light status can be digitally communicated to the connected vehicles through short-range communication (V2X) protocols based on the ETSI-ITS G5 technology [2]. When using V2X, a message pair (MAP-SPaT) is transmitted: a MAP message [ETSI TS 103 301] contains intersection geometry and signal identifiers, while a SPaT (Signal Phase and Time, ETSI TS 103 301) message contains timing information for each light signal. Using this information, vehicles may calculate the behaviour for the signal in their path.

![Figure 1 R-ITS-S communicates optimal speed to the connected vehicle](image)

Figure 2 highlights the involved modules and communication means required to implement this use-case². The C-ITS-S application server can aggregate data received from several sources (i.e., TMC: an entity being responsible for monitoring and regulating the traffic in a specific area, TLCs) over proprietary communication channels. The traffic signal status and timing data is forwarded to

---

² In this deliverable we omit details on the security management system and the way to generate and distribute certificates. All relevant issues will be studied in the subsequent WP2 tasks.
the R-ITS-S which then broadcasts the data to all connected vehicles in its area of control via a SPaT/MAP messages (see Appendix A).

Figure 2 Entities, communication means and responsible partners involved in the UC1 implementation

Figure 2 also lists the SAFERtec partners that will provide the corresponding hardware infrastructure and/or lead the software development needed for the realization of the current use-case in the SAFERtec connected-vehicle system. In WP4 this use case will be realised as a sequence of events:

1. Vehicle approaches the intersection to cross
2. R-ITS-S receives SPaT and MAP messages from the C-ITS-S
3. The R-ITS-S transmits (broadcasts) assembled SPaT and MAP messages including signal information for the given path of the vehicle, via the V2X module
4. Vehicle OBU receives SPaT and MAP via V2X transmission
5. Vehicle V2X Stack (i.e., responsible applications over the V2X dedicated hardware) receives, verifies and processes each message and aggregates signal information relevant for the vehicle
6. Vehicle Safety Application triggers a notification containing the time and optimal speed for the vehicle
7. HMI receives the notification and displays the information for the driver
Foreseen security issues: Along the events constituting the first SAFERtec use case the challenging safety, security and privacy issues are:

1. An appropriate balance should be reached between various constraints, such as safety, security, privacy and functionality. The offered services and system expectations should be defined, so as to satisfy necessary requirements and effectively resolve any potential conflicts. Security and privacy related requirements should be precisely and completely defined, based on the chosen use cases, during the modelling phase. This is considered fundamental for future project phases.

2. If, for any reason, the calculated optimal speed that has been communicated to the driver is not the correct one, safety issues are raised. This may be due to functional defects (e.g., inaccuracy of sensor measurements), or malicious intervention with hardware, software, or communication paths.

3. Various underlying communication parameters will be continuously sampled, in order to generate relevant data such as time and optimal speed. Appropriate integrity checks should be defined, to ensure that this information is accurate and untampered during broadcast.

4. The transmission of the traffic signal status and timing data to the R-ITS-S should occur in a secure manner to avoid a breach in the functional chain.

5. Privacy protection is also a key aspect in this use case (based on strict EU regulations). Transmitted data should not contain any personal identifiable information or vehicle related information that may directly or indirectly refer to the driver’s id. User profiling is also a key privacy concern.

2.1.2 Provision of real-time traffic-hazard information

Real-time traffic information is increasingly available in the emerging paradigm of the connected vehicles. Such information may include data about road events and traffic-flow (i.e., anonymous data) that can be continuously-retrieved by mobile apps from the cloud or directly from public authorities; alternatively, modern built-in navigation systems may also collect, display and use such data.
Numerous driving instances can be included under this use-case; without loss of generality, the project will consider the scenario of communicating notifications for a traffic-jam (ahead of the ego-vehicle) as the most indicative one.

Typically, on motorways, major roads and central inter-city routes a connected vehicle moving by an R-ITS-S may receive V2X based information and can retrieve real-time warnings and traffic-flow information (see Figure 3). The information-flow relevant to this use-case is shown in Figure 4. Note that the vehicle-to-vehicle communication depicted in the figure is essentially beyond the SAFERtec scope and is presented as an optional part for the considered information flow.
A noteworthy remark here involves the presence of a parallel communication channel (to the RSU-based one) from the C-ITS-S to the connected vehicle utilizing the cellular network (see grey arrows in Figure 4). C-ITS-S is enabled to transmit messages (of proprietary XML format) directly to all vehicles in its area of surveillance.

The selected use-case can essentially be used to investigate the way to communicate notifications (i.e., traffic jams or other road events) to the connected vehicle utilising three different routes. Notifications may:

- come from the TMC, through the C-ITS-S, and be dispatched by a local R-ITS-S to the vehicle via V2X
- be sent directly by the C-ITS-S (or occasionally the Road Authority / Infrastructure operator) to the vehicle application /navigation software through cellular channels
- broadcasted by vehicles moving at the event location to other peer-vehicles. (The latter option essentially lies out of the SAFERtec scope)

This use-case (to be realised by the HW/SW contributions of SAFERtec partners in the context of WP4) can be seen as a sequence of events. When the hazardous event is a traffic jam ahead (of the ego-vehicle) we identify the following sequence:

1. A traffic jam situation is taking place or the TMC (or a similar entity) can foresee an (near-future) event which requires the issue of a warning.
2. The C-ITS-S publishes information towards the R-ITS-S about the controlled area and the latter through signed\(^3\) DENM messages [ETSI EN 302 637-3], which forwards the relevant information to the vehicle OBU. In parallel, appropriately-encoded information is also published in the cloud to be read by subscribed applications.
3. The vehicle’s V2X OBU receives the message.
4. The V2X stack processes and verifies the DENM message and V2X applications create a warning if the information is relevant for the given vehicle. In parallel the cloud application requests and receives messages from the server.
5. The received cellular- and V2X-based real-time traffic warnings and event-notifications are displayed to the driver\(^4\).

---

\(^3\) The entity and process of signing the involved messages is out-of-scope for the current deliverable. Details will be provided in future deliverables (e.g., D4.1)

\(^4\) Real-time traffic flow information can be shown on a digital map.
The scenario may also contain a third source of V2X DENM messages which in event sequence shall be broadcasted along with the RSU’s DENM.

**Foreseen security issues:** Along the above sequence of events the challenging safety, security and privacy issues are:

1. The integrity of the transmitted messages. In addition to the security concern that some kind of unauthorized modification of the transmitted information may cause, tampered V2X messages will clearly impact safety as well.

2. The confidentiality of the transmitted messages should be guaranteed, while at the same time the V2X OBU vehicle should be able to prove its authenticity without having its own identity revealed to a third party.

3. Unlinkability between the driver/vehicle and the OBU should be also satisfied. Unlinkability is important for protecting driver’s identity especially in cases where a small number of vehicles are simultaneously using the same service.

4. As in the previous use case, it is essential to identify and resolve any potential conflicts between safety, security and privacy requirements.

### 2.1.3 Priority request in intersection-crossing.

The priority (of an emergency vehicle) in crossing an intersection has been traditionally demanded by (human) drivers using sound signals (i.e., siren) and/or flashing lights. When moving to the connected vehicles paradigm, intersection-crossing can be digitized and thus become safer and more efficient (see Figure 5). The priority can be requested and assigned by the C-ITS-S to the appropriate vehicle while the rest (of the involved vehicles) can be notified to give priority.
In terms of information flow (see Figure 6), the relevant scenario includes:

1. The C-ITS-S which maintains a registry of connected vehicles (of various level of automation) in its area of control, for example by receiving (special) CAM messages.

2. The emergency vehicle communicates its priority request to the C-ITS station. (Additionally, the emergency vehicle could communicate its planned route, for example preferred lane or next turn).

3. The C-ITS station communicates the right to drive for each lane to all vehicles in its area of surveillance, via a SPaT message, thus emptying the appropriate lane for the emergency vehicle.
What is challenging in this use-case is the existence of a parallel communication path from the vehicle (either using a 3G/4G-enabled V2X chipset or a hand-held device) to the C-ITS system through a cellular channel. Then, the R-ITS-S involvement can be circumvented and through the cellular connectivity the spatial limitations of the DSRC can be overcome. The reverse path (i.e., from the vehicle to the infrastructure) can be used to send acknowledgements to the infrastructure (of messages being received), if needed.

**Foreseen security issues:** In this case an indicative set of challenging safety, security and privacy issues are:

1. A strong authentication mechanism is required for approved prioritized vehicles in order to detect fake emergency vehicles. (The application of a mechanism for integrity checks between the communicating entities is considered critical for the vehicle safety).
2. Assurance of physical security of the C-ITS Station is essential in this scenario.
3. The data stored in the ITS infrastructure should be anonymised in order to protect users’ privacy. Data protection regulation should be enforced regarding the storage and processing of the stored personal information.
4. As in previous use cases, it is essential to identify and resolve any conflicts between safety, security and privacy requirements.
2.2 Application scenarios under Vehicle to Cloud communications

In what follows we discuss how the aforementioned use-cases are shaped and which other becomes relevant under the second major part of the SAFERtec V2I setting; this involves scenarios that realize the connected vehicle system through the communication with the cloud infrastructure. The corresponding information can originate from the cloud-based services and become relevant in similar automotive settings (to those considered in the previous section) but occasionally can support different ones. We next present a high-level description of those cloud-based use-cases that will be considered by SAFERtec.

2.2.1 The optimal driving speed advice

The optimal driving speed advice use-case can be highly challenging when considered under the cloud-based communication paradigm (see Figure 7). In this counterpart, the vehicle can exploit the cellular connectivity and receive the relevant speed advice while driving beyond the DSRC scope (i.e., at large distance from the local R-ITS-S).

![Figure 7 A cloud-based service communicates the optimal speed to the connected vehicle](image)

The cloud-based service avails the involved speed data; the latter can be estimated and delivered to the cloud by the corresponding traffic management entity via the Internet. The cloud-based service establishes connectivity with appropriate software that resides over the (cloud-service compatible)
OBU using the cellular network (see Figure 8). The advice is finally presented to the driver using the in-vehicle HMI board (or a customised Android mobile app).

Two remarks are relevant here. First, an alternative path can be realized through cellular connectivity, from the C-ITS Station to the vehicle application and vice-versa. The latter can use functionality implemented over the OEM (i.e., CRF) cloud. TPEG-encoding (or XML-based proprietary solutions) can be used for the involved messages that are directed either to an OEM-specific application (that realizes the vehicle-end part of this communication) or to the C-ITS system, if needed.

The second comment has to do with the exchange of SPaT messages over cellular channels; the latter can be implemented but remains largely under-explored, especially when security and privacy issues are considered.

**Foreseen security issues:** In this use case the challenging safety, security and privacy issues are summarised in the following points:

1. The protection of the stored data in the cloud infrastructure through the isolation of the VMs where drivers’ data are stored that may directly or indirectly lead to data leakage or user profiling.

2. Vehicle Authentication: Security measures to comply with relevant cellular standards which are implemented and supported by each entity. Typically, without a reliable authentication mechanism for cellular communications, a malicious user could impersonate the network itself and intercept or modify communications.
3. Confidentiality of the exchanged information through encryption and authentication mechanisms used for higher level protocols.

4. Accessibility of the devices to the mobile broadband network: The mobile broadband network can be a privileged entry point for a malicious user as it is accessible from all over the world and the necessary equipment is inexpensive and widespread. If vulnerabilities are remotely exploitable through direct incoming IP traffic and no reliable perimeter security measures are implemented, then every connected device may be at risk.

5. Availability of the service (avoiding denial-of-service attacks).

6. Calculated optimal speed that has been communicated to the driver should be accurate and untampered, to avoid safety as well as security issues.

2.2.2 Provision of real-time traffic information.

In view of the emerging 5G technologies and the expected reduced latency (compared to the LTE standard) the provision of real-time traffic information can be efficiently facilitated by cloud-based services. SAFERtec will put the relevant scenario (depicted in Figure 9) under the microscope.

Events (such as a traffic jam or road incidents) can be detected and a relevant notification can be available at the cloud server. This may be realised connecting the C-ITS system (which avails the information) with the cloud application; in an alternative way other peer-vehicles that are registered
as users in the same application can provide real-time feedback regarding the road situation to the cloud-server (see Figure 10). As before, the vehicle-to-vehicle communication depicted in the figure is essentially beyond the SAFERtec scope and is presented as an optional part for the considered information flow.

![Diagram](image)

*Figure 10 Entities, communication means and responsible partners involved in the UC5 implementation*

The rest of the information flow in this use-case includes:

1. The cloud-based service communication with the in-vehicle associated application (i.e., OBU SW by the cloud-service provider)
2. The projection of relevant notifications to the user by HMI visualizations.

Similar to the previous use-case, a parallel bi-directional communication path may be used to a) provide real-time traffic information to the C-ITS-S and/or b) download real-time information from the ITS station.

*Foreseen security issues*: In this use case the challenging security issues are the same with those discussed in the previous one.

### 2.2.3 Privacy-preserving route planning and navigation

Trip planning is the use of specialised search engine/software to find an optimal means of travelling. Relevant searches may be optimised on different criteria. When it comes to the case of a
(connected) vehicle being the single means of travelling, the task called route-planning can benefit from the proliferation of highly-capable (hand-held) smart devices.

In the SAFERtec project we will reproduce an instance of route-planning scenario using a part of the TomTom MyDrive infrastructure and functionality\(^5\) (see Figure 11).

![Figure 11 Online route-planning informs vehicle device](image)

The origin of relevant information is a web or a smart-phone application with which the user plans her trip. A route (i.e., starting point and destination) is selected and the application automatically plans the route for the destination; the corresponding itinerary appears on the user’s screen. The information necessary to plan this route is stored in TomTom’s cloud services, together with other user preferences and locations.

Once the driver is in the vehicle and before driving starts, the information stored in TomTom’s cloud services is automatically synchronized using any available connection (i.e., most often, cellular connectivity) to a local storage in the vehicle (see Figure 12). Using the information retrieval from the cloud services, the previously planned route to the driver’s destination is recalculated in the vehicle through its dedicated HMI. The actual (real-time) traffic situation can be also projected to the driver along with estimated arrival timings.

\(^5\) TomTom MyDrive planner can be found at: [https://mydrive.tomtom.com/en_gb/](https://mydrive.tomtom.com/en_gb/)
Clearly, the use-case includes the collection and usage of users’ private data rendering it appropriate for studying the identification of the involved privacy assurance levels.

**Foreseen security issues:** In this use case the challenging safety, security and privacy issues are:

1. Anonymization of the driver/vehicle (The transmission of users’ private information over the IP stack raises data privacy issues).
2. Unlinkability between the vehicle and the communicating Cloud Service instance.
3. Avoiding user profiling capabilities of potential attackers. The disclosed personal information should be kept to the minimum required for satisfying the service functionality.
4. Ensuring the integrity of the route information since unauthorised alteration of this information may cause discomfort, or even safety issues, to the driver.
5. The regulatory requirements regarding the collection, communication and processing of personal information.
3. A SAFERtec reference architecture to support the selected Use Cases

This section discusses the architectural design of the SAFERtec connected vehicle system which is a reference system to assist the validation of the proposed framework over the aforementioned V2I use-cases. Details and specifications of this proposed reference architecture can be found in the SAFERtec D4.1. Herein, we will highlight the main choices and explain why the proposed architecture is adequate to realize the SAFERtec use-cases.

Before moving to the high-level description of the architecture, broken down to two distinct parts i.e., the vehicle platform and the modules outside the vehicle, we make a very short mention to the involved PKI modules and relevant security- and privacy-related features.

ETSI ITS security architecture appears in various standards and profile specifications. One basis is the security header standard, which defines the structure and data of a secured (signed) message [ETSI TS 103 097]. However, the chosen method of verification requires the existence of a Public Key Infrastructure (PKI), which main function is to issue certificates for a given ITS Station (R-ITS-S or OBU). It also has supporting duties, e.g. to enrol new stations or to revoke misbehaving ones. In general, the PKI enables authentication and authorization of senders, integrity of data through verification of digital signatures and confidentiality principles with secure connections between different ITS stations extending transport layer security (TLS). Each ITS station has a pool of pseudonym certificates that are regularly updated.

Currently there is no Standard or Europe wide specification of a common PKI approach, instead several National PKI systems are in operation, which are currently being harmonized by the ITS Platform, the C2C-CC (Car 2 Car Communication Consortium) and other stakeholder groups and initiatives. The project considers at least 3 PKI reference systems which are deployed in France, Germany and Austria, however implementation and deep analysis of the infrastructure and operation of the PKI is out of scope of the project. The focus is set on the R-ITS-S and OBU communication, however the existence of a PKI service is assumed (certificates and other security assets are assumed to be acquired by each unit e.g. the OBU targeted for investigation)
3.1 Modules in the vehicle platform

The project’s Vehicular software architecture enabling V2X communication follows the standard set of European V2X protocols standardized by ETSI (e.g. by EN 302 663). All fundamental protocols, services and other blocks (e.g. hardware drivers) are fitted into a layered network architecture. All above use cases and the corresponding functionality (i.e., applications such as the Cooperative Awareness Basic Service which is responsible to broadcast CAMs) share a common base of facilities and services.

Functions may be distributed on several different ECUs or target platforms. In the SAFERtec system, core elements of V2X functionality will be deployed to a dedicated V2X platform (developed by AUT), while higher level functions (e.g. application level modules) can be deployed to an ECU within the vehicle eco system.

In Figure 13, the **hardware adaptation layer** groups all hardware dependent software blocks which are required by the V2X middleware. The following key interfaces need to be adopted:

The V2X subsystem needs to have an interface towards the following internal (in-vehicle) subsystems or components:
- Vehicle dynamics, via e.g. CAN: provides information on vehicle status (e.g. steering wheel angle)
- Position via GNSS module
• interconnection to safety related / critical subsystems, via e.g. CAN or ETH: connection to other (non-V2X middleware) software modules, e.g. HMI, safety applications, ADAS subsystem
• eHSM – Embedded Hardware Security Module: certified tamper proof crypto unit for private key storage and secure V2X message signing.

The V2X subsystem needs to communicate with the following external (to the vehicle) systems/networks:
• V2X network via V2X radio
• Public Key Infrastructure via cellular / conditionally WiFi

The hardware adaptation layer may be considered to act as the Access layer of the standard V2X architecture defined by the aforementioned standard set.

The Network Layer includes the Basic Transport Protocol (BTP) software module and the GeoNetworking module. This layer is tightly coupled to both the V2X air interface (radio) below and to the V2X facilities above (e.g. CAM service).

The Facilities layer uses the vehicular dynamic data (e.g. via CAN) and position and time (e.g. via GNSS) received to maintain its basic services (transmit CAMs and DENMs). It also processes all incoming V2X messages and provides it to upper layers.

The Security and Management Layer(s) offer cross layer functions, where the most important one is encryption, decryption, signage and verification of V2X traffic in both directions. It uses the eHSM to safely store keys for signing and may establish a link to the PKI to request new certificates.

The Security and Management, Facilities, Network and Access layers may also be referred to as the Core Stack component.

The Facilities are used by several entities to realize various applications and functions, such modules are the Local Dynamic Map, which maintain a digital map of the surrounding. Safety Applications may rely on the LDM database or communicate directly with the Core Stack to realize basic V2X functionality (e.g. stationary vehicle ahead warning) or to allow more complex applications (e.g. priority request).

The SAFERtec architecture has been designed to fulfil the requirements of the connected vehicles. The objective was to create a flexible platform with remote services implemented with short range communication (i.e. ITS-G5) and cellular connectivity. The proposed vehicle-platform solution allows the (equipped) vehicle to obtain information from the road-side-units and vice-versa to send the vehicle-data to the road-side-units via V2X communication. In addition to that, the vehicle is able to subscribe to cloud services and retrieve updates or received geo-localized information. The security threats coming from these two channels are different, for this reason some applications, like the
Optimal Driving Speed Advisory, will be developed both via V2X and via cellular connectivity. Then, our study is expected to shed some light on how different technologies influence the involved security assurance levels. Likewise, the vehicle platform is designed to support two different HMI systems: one integrated into the vehicle and another connected via Wi-Fi connectivity. Thanks to this redundancy it is possible to perform a complete assessment of the vehicle vulnerabilities of all the use-cases described in the current document.
3.2 Modules outside the vehicle platform

The ‘world-outside’ of the SAFERtec connected vehicle includes the R-ITS-S and the cloud infrastructure and functionality.

3.2.1 The SAFERtec C-ITS-S and R-ITS-S

The Central ITS Station (C-ITS-S) is the central component in the C-ITS system. The C-ITS-S is connected on one side (input) to the urban/interurban traffic management centre (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 that way, that new modules can be easily connected without changing the general architectural concept of the system.

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 PKI).

The functionality of the system component PKI (certification authority) is not yet standardized and not yet implemented. The idea is to enable the retrieval of PKI certificates by the C-ITS-S, to implement security across the system.
The data generated by the C-ITS-S (i.e. DENM, SPaT) is delivered to the V-ITS-S through to an 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.

The encoding of the ITS-message payload (DENM, SPAT, etc.) is defined by the WEB server implementation. The rest of the scenarios (upstream data transfer, i.e. receiving sensor information and DENMs) are not considered by this interface.

The V-ITS-S can be seen either as a vehicle equipped with ETSI ITS-G5 and/or mobile internet (3G/4G) communication or as a mobile device running an application able to interact with the C-ITS-S. Mobile internet over cellular communications (e.g., 3G/4G) is seen as a communication channel for content; similar purposes can be served by ETSI ITS-G5 services.

The Roadside ITS station (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/or 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 de- 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, 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.

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 Server and the R-ITS-S will always be the OCIT-C Client. A VPN tunnel is used for the communication link. The C-ITS-S server may be the VPN Server and the R-ITS-S the VPN Client.
3.2.2. The SAFERtec Cloud-based Services

In this section we briefly present the current view of the cloud architecture needed to realise the above use-cases. (The current analysis will be further detailed in the WP4 deliverables)

In Figure 15 we present the 4 main modules that comprise the architecture; they are the Navigation, TTI, NAVCLOUD and UI module:

- **Navigation** module is responsible for providing navigation features. It is meant to be part of the vehicle or installed on a device. It’s composed of several sub-modules:
  - NavKit - library that is used to accomplish various navigation tasks like reading maps (usually NDS), search, routing, map matching, map visualization, map updates, and more.
  - NDS Map – On board map database in NDS format
  - Other modules such as a positioning engine amongst others. These are not relevant to SAFERtec and won’t be further detailed.

- **TTI** module is responsible for gathering, aggregating and feeding traffic information. This service gathers traffic information from various trusted 3rd party content providers, aggregates the data and sends it to the Navigation module.

- **NAVCLOUD** module is in charge of storing and managing sensitive user data and preferences.

- **UI** is a customizable module closely related to Navigation, that is responsible for providing a friendly user interface to the navigation software: displaying maps, helping the driver to plan routes, live navigation and more
Further attributes of the architectures are presented below:

- The Navigation module communicates with TTI module using https as a channel and TPEG (see Appendix A) as an encoding protocol
- The Navigation module communicates with TTI module using https as a channel and protobuf as an encoding protocol
- TTI and NAVCLOUD services are implemented as cloud services.

4. Attack entry points and high level security and privacy requirements

In this section we highlight some preliminary (high-level) security and privacy requirements associated with each selected use case. Furthermore, we present our first approach to the exploration of the involved attack surface that would become relevant when realizing the interactions of the connected (prototype) vehicle with the infrastructure.

What is important to note here is the scope of our study (in the area of attack modelling and implementation). Essentially the security and privacy issues that emerge under the SAFERtec concept of connected vehicles can intensely scale in number as the diverse involved technologies and 3rd party modules are increasingly more complex. To cope with that complexity and render the considered problem tractable we focus on threats stemming from attackers that have no physical access to the vehicle. (Vulnerabilities and attacks related to physical access remain out of the V2I communications scope where SAFERtec has originally set its focus)

A second note relates to the provided level of details. This study does not aim to provide an exhaustive presentation and analysis of the potential entry points; it neither studies the whole set of security and privacy requirements. The main idea is to provide a preliminary study, identify the fundamental issues involved and lay the ground for the T2.2 and T2.3 tasks that will follow.
4.1 Attack entry points and security/privacy requirements in the vehicle platform

As a preliminary study we identify an indicative set of potential entry points of attacks (over the vehicle platform) that can be relevant in the aforementioned use-cases. The list is indicative yet it demonstrates the broad range of the exposed vulnerabilities. The exploration of the threats on those entry points will be determined by our future modelling and implementation work.

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2X radio</td>
<td>external</td>
<td>Malware to affect LDM (e.g. phantom vehicle, corrupt infrastructure information (wrong signal, wrong closed lane))</td>
</tr>
<tr>
<td>Cellular uplink</td>
<td>external</td>
<td>Authentication and identity threat (all PKI related issues here) The cellular uplink is used by the security layer of the V2X stack to acquire pseudonym certificates, however neither the enrolment or standard (new certificate reception) vehicle-PKI communication is part of the interfaces used in the use cases.</td>
</tr>
<tr>
<td>GNSS</td>
<td>external</td>
<td>Spoofed position&lt;br&gt;Blocked signal (function stop)</td>
</tr>
<tr>
<td>eHSM APIs</td>
<td>internal</td>
<td>Identity / privacy breach</td>
</tr>
<tr>
<td>internal API</td>
<td>internal</td>
<td>Data injection, alteration or sniffing between core stack, LDM and Safety application modules. (trusted entities)</td>
</tr>
<tr>
<td>external API</td>
<td>internal</td>
<td>Data injection, alteration or sniffing between Safety application module and (third party) HMI. (untrusted entities)</td>
</tr>
<tr>
<td>CAN bus</td>
<td>internal</td>
<td>CAN traffic anomalies (compared to normal conditions)</td>
</tr>
</tbody>
</table>

Table 2: Identified entry points of attacks for the vehicle platform

We complement the study presenting a high level security, safety, privacy and reliability requirements posed for the vehicle platform that will be involved in the realization of the above use-cases.

<table>
<thead>
<tr>
<th>Asset</th>
<th>High level (Security and Privacy) Requirement</th>
<th>Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2X message reception (CAM, DENM, SPAT, MAP, IVI)</td>
<td>Avoid Untrusted/ illegitimate sources/devices / Shall be signed by a trusted third-party (message shall have valid and verified certificate and signature)&lt;br&gt;Avoid the corruption of messages / Message shall be intact and uncorrupted</td>
<td>All use cases</td>
</tr>
<tr>
<td>HSM module</td>
<td>In process of security certification as per FIPS 140-2 Level 3; as well as C2C-CC PP’s for eHSM and V2X Gateway.</td>
<td>All use cases</td>
</tr>
<tr>
<td>GNSS position</td>
<td>Avoid corruption or unauthorized access to this data</td>
<td>The optimal driving speed advice</td>
</tr>
</tbody>
</table>
Table 3: Preliminary high-level requirements for the vehicle platform

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Requirement</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2X message Transmission (CAM, DENM)</td>
<td>Preserve the confidentiality of sources and content / pseudonymity shall be assured, vehicle and passenger identity shall be preserved. Transmitted data validity shall be ensured.</td>
<td>All use cases</td>
</tr>
<tr>
<td>CAN bus data</td>
<td>Avoid any untrusted and unauthorized access to CAN data</td>
<td>All use cases</td>
</tr>
<tr>
<td>external API</td>
<td>No privacy related data shall be exploited to third party (untrusted) software components. Anonymization.</td>
<td>All use cases</td>
</tr>
<tr>
<td>internal API</td>
<td>Data connection between non co-located software modules shall be secure.</td>
<td>All use cases</td>
</tr>
</tbody>
</table>

Those requirements will be further analysed and are subject to change as the work for the identification of the full set of requirements will proceed. The outcome will appear in the following WP2 deliverables.

### 4.2 Attack entry points and security/privacy requirements outside the vehicle platform

The ‘world-outside’ of the SAFERtec connected vehicle includes the C-ITS-S/R-ITS-S and the cloud infrastructure and functionality. We briefly study the involved attack surface and discuss relevant requirements for the SAFERtec use-cases.
4.2.1. R-ITS-S and C-ITS-S infrastructure and services

In this section we summarize an indicative set of potential entry points of attacks over the Roadside- and Central-ITS Stations. Those entry points constitute only a preliminary set to be considered in the modelling and implementation of the described SAFERtec use-cases. The subsequent WP2 work (to be presented in D2.2 and D2.3) will result in a comprehensive analysis of the relevant attack surface and vulnerabilities.

In the table that follows, we categorise each of the identified ‘point’ (in the leftmost column) as internal/external and explain why it constitutes a potential attack entry (rightmost column). A systematic study will be carried-out in the following WP2 stages.

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C-ITS-S</td>
<td>Internal/External</td>
<td>System based on a software platform which serves as distributor of the data, providing either cooperative or basic functionalities for a proper operation of the system. The data exchanged among the different modules is organized by the software platform.</td>
</tr>
<tr>
<td>R-ITS-S</td>
<td>Internal/External</td>
<td>The roadside ITS-S gateway provides functionalities to connect the components of the roadside system.</td>
</tr>
<tr>
<td>C-ITS-S &lt;&gt;</td>
<td>External</td>
<td>The data generated by the C-ITS-S (i.e. DENM, SPAT) is delivered to the V-ITS-S through an ITS Web server. The web server behaves as a content provider and oversees the delivery of the information.</td>
</tr>
<tr>
<td>Web Server &lt;&gt;</td>
<td>External</td>
<td>The connection (via cellular network) from the web server to the V-ITS-S is based on a set of methods that can be used to exchange data from/to the cloud C-ITS-S environment.</td>
</tr>
<tr>
<td>C-ITS-S &lt;&gt;</td>
<td>External</td>
<td>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</td>
</tr>
<tr>
<td>R-ITS-S &lt;&gt;</td>
<td>External</td>
<td>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].</td>
</tr>
<tr>
<td>C-ITS-S &lt;&gt;</td>
<td>External</td>
<td>Not yet implemented</td>
</tr>
</tbody>
</table>

*Table 4: Identified entry point of attacks for the R-ITS-S and C-ITS-S services*
Next, we consider some of the involved assets (i.e., anything valuable for the V2I communications) in the (R-ITS-S and C-ITS-S -based communications) and derive the main high-level security, safety, privacy and reliability requirements associated with the selected use-cases.

<table>
<thead>
<tr>
<th>Asset</th>
<th>High level (Security and Privacy) Requirement</th>
<th>Use cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>DENM/RWW message</td>
<td><strong>Integrity</strong> (of the probe data from the vehicle ITS-S and of the message originated by the C-ITS-S based on TMC information): the data coming from the vehicle and sent by the C-ITS-S/R-ITS-S must contain correct, untampered information  &lt;br&gt; <strong>Availability</strong>: the messages are sent to the vehicles in a timely manner, and should not be blocked by any unauthorized entity  &lt;br&gt; <strong>Accountability</strong> (of the message originated by the C-ITS-S based on TMC information) possibility of tracing events back in time to the C-ITS-S/R-ITS-S to establish responsibility for actions or omissions  &lt;br&gt; <strong>Authenticity</strong> (of the probe data from the vehicle ITS-S and of the message originated by the C-ITS-S based on TMC information): assurance that the message is indeed from the C-ITS-S/R-ITS-S (proof of identity).</td>
<td>Real time traffic information</td>
</tr>
<tr>
<td>SPAT/MAP Message</td>
<td><strong>Integrity</strong> (of the probe data from the vehicle ITS-S and of the message originated by the C-ITS-S based on TMC information): the data coming from the vehicle and sent by the C-ITS-S/R-ITS-S must contain correct, untampered information  &lt;br&gt; <strong>Availability</strong>: the messages are sent to the vehicles in a timely manner and should not be blocked by an unauthorized entity.  &lt;br&gt; <strong>Accountability</strong> (of the message originated by the C-ITS-S based on TCC information) possibility of tracing events back in time to the C-ITS-S/R-ITS-S to establish responsibility for actions or omissions  &lt;br&gt; <strong>Authenticity</strong> (of the probe data from the vehicle ITS-S and of the message originated by the C-ITS-S based on TMC information) assurance that the message is indeed from the C-ITS-S/R-ITS-S (proof of identity).</td>
<td>Optimal speed driving</td>
</tr>
<tr>
<td>CAM Message</td>
<td><strong>Confidentiality</strong>: personal user information must be kept private;  &lt;br&gt; <strong>Integrity</strong>: the data coming from the vehicle must contain correct, untampered information  &lt;br&gt; <strong>Authenticity</strong>: assurance that the messages comes from the involved vehicles</td>
<td>Priority request</td>
</tr>
</tbody>
</table>

Table 5: Preliminary high-level requirements for the C-ITS-S/R-ITS-S functionality

Those requirements are to be enhanced and thoroughly considered in the subsequent WP2 tasks.
4.2.2. Cloud infrastructure and services

We now discuss an indicative set of potential entry points of attacks over the cloud infrastructure and related services that can be relevant in the above SAFERtec use-cases. The list is not exhaustive but presents some of the most significant entry points.

<table>
<thead>
<tr>
<th>Entry Point</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation</td>
<td>External</td>
<td>NavKit stores a sensitive user data (i.e. history of all trips performed by the user, user specific locations, etc.) in encrypted SQLite databases. The encryption keys are specific to the device.</td>
</tr>
<tr>
<td>Navigation</td>
<td>External</td>
<td>NavKit allows for map updates. The update source can be remote and is configurable. The update packages are signed. Communication can be HTTP or HTTPS</td>
</tr>
<tr>
<td>TTI</td>
<td>External</td>
<td>Unauthorized access to TTI servers will violate confidentiality of private data and may open up NavKit for further attacks</td>
</tr>
<tr>
<td>NAVCLOUD</td>
<td>External</td>
<td>Unauthorized access to NC servers will violate confidentiality of private data and may open up NavKit for further attacks</td>
</tr>
</tbody>
</table>

Table 6: Identified entry point of attacks for the cloud-based services

The threats associated with those entry points will be studied in our future modelling and implementation work. We now conclude this section with a short presentation of a set of high-level security/privacy requirements posed for the cloud-related use-cases. This is again subject to future elaboration.

<table>
<thead>
<tr>
<th>Asset</th>
<th>High level (Security and Privacy) Requirement</th>
<th>Use case</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAVCLOUD</td>
<td>Confidentiality – personal user information must be kept private; Data integrity – packages coming from NAVCLOUD servers must contain correct, untampered client information stored by TT in the cloud. Availability – NAVCLOUD servers must provide a reliable service to clients, service should not be blocked by unauthorized entities</td>
<td>Privacy-preserving route planning and navigation</td>
</tr>
<tr>
<td>TTI</td>
<td>Authentication – TTI traffic information must come from genuine TTI servers Data integrity – traffic information provided by TTI servers must be valid and trusted Availability – TTI servers must provide a reliable service to clients, service should not be blocked by unauthorized entities Unlinkability – it must be impossible for anyone to reveal sensitive client information based on multiple TTI requests sent out by the same client</td>
<td>The optimal driving speed advice Provision of real-time traffic information</td>
</tr>
</tbody>
</table>
### Table 7: Preliminary high-level requirements for the cloud-based services

<table>
<thead>
<tr>
<th>Requirement Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Navigation</td>
<td>Confidentiality – map data, client settings and other information kept by NavKit must remain private&lt;br&gt;Availability – this component is vital to navigation, service should not be blocked by unauthorized entities</td>
</tr>
<tr>
<td></td>
<td>Provision of real-time traffic information&lt;br&gt;Privacy-preserving route planning and navigation</td>
</tr>
</tbody>
</table>
5. Conclusions

This deliverable presents the output of the work carried-out in the context of the SAFERtec Task 2.1 which focused on the connected vehicle use-case scenarios. The document considers the two classes of V2I communications i.e., the one that involves roadside units and the other that involves cloud-based services. For each class, it details a set of use-cases that have been carefully selected according to a number of criteria as defined by the SAFERtec team and described in this document.

The document also elaborates on a broad set of related issues. It briefly presents security and privacy concerns for each selected use-case. Then, it highlights the software design of the connected vehicle system that will realize the SAFERtec use-cases presenting technical details for each of the three major entities i.e., the prototype vehicle, the roadside units and the cloud services.

The deliverable concludes with a section that discusses the relevant attack entry points for each use-case and a ‘first-approach’ to the involved security and privacy requirements. What is presented in that section will serve as an input to the subsequent WP2 tasks (of modelling work) where its comprehensive analysis will take place.

The herein presented work marks a considerable step-forward for the project as the selection of the use-cases lays the ground for the modeling as well as implementation work that follow; all of which constitute cornerstones to the development of the SAFERtec security assurance framework.
References


http://www.etsi.org/deliver/etsi_en/302600_302699/302663/01.02.00_20/en_302663v010200a.pdf


Appendices

A. Related standards

In this appendix we list the related standardization work and its current status. The interested reader should direct to the corresponding official releases of the involved standardization bodies.

- SPAT-MAP and pre-emption:
  - SAE J2735 release January 2016
  - CEN/ISO TS 19091-3 Currently being drafted
  - ETSI TS 103 301 (protocol) Currently being drafted
- CAM: ETSI EN 302 637-2, V1.3.1
- DENM: ETSI EN 302 637-3, V1.2.1
- TPEG: www.TISA.org