Project acronym:	OVERSEE
Project title:	Open Vehicular Secure Platform
Project ID:	248333
Call ID:	FP7-ICT-2009-4
Programme:	7th Framework Programme for Research and Technological Development
Objective:	ICT-2009.6.1: ICT for Safety and Energy Efficiency in Mobility
Contract type:	Collaborative project
Duration:	01-01-2010 to 30-06-2012 (30 months)

Deliverable D1.1:
Use Case Identification

Authors:	Cyril Grepet (Trialog)
Reviewers:	Rafael Grote (TUB) Marko Wolf (Escrypt)

Dissemination level:	Public
Deliverable type:	Report
Version:	1.5
Submission date:	01 July 2011

Abstract

The next generation of intelligent vehicular Information and Communication Technology (ICT) applications for advanced traffic management, active vehicle safety, or “green” electric cars strongly depends on the availability of an ICT infrastructure combining both dependability and security attributes.

To meet these challenges, OVERSEE will develop an open vehicular IT platform that provides a protected standardised in-vehicle runtime environment and an on-board access and communication point.

This document describes use cases of automotive applications or areas directly related to automotive issues. These use cases will serve as a basis for the deduction of security and dependability requirements for the OVERSEE platform.

Contents

List of Figures

List of Tables

List of Abbreviations

ADAS **A**dvanced **D**river **A**ssistance **S**ystems

AES **A**dvanced **E**ncryption **S**tandard

ARINC **A**eronautical **R**adio **Inc**orporated

CAN **C**ontroller–**a**rea **N**etwork

API **A**pplication **P**rogramming **I**nterface

COTS **C**ommercial **O**ff-**T**he-**S**helf

CPU **C**entral **P**rocessing **U**nit

DSRC **D**edicated **S**hort-**r**ange **C**ommunications

ECC **E**lliptic **C**urve **C**ryptography

ECU **E**lectronic **C**ontrol **U**nit

FLOSS **F**ree**/L**ibre and **O**pen **S**ource **S**oftware

FPGA **F**ield **P**rogrammable **G**ate **A**rray

GPRS **G**eneral **P**acket **R**adio **S**ervice

GPS **G**lobal **P**ositioning **S**ystem

GSM **G**lobal **S**ystem for **M**obile Communications

GWN **G**lobal **W**ireless **N**etworks

HSM **H**ardware **S**ecurity **M**odule

HMI **H**uman **M**achine **I**nterface

ICT **I**nformation and **C**ommunication **T**echnology

IT **I**nformation **T**echnology

ITS **I**ntelligent **T**ransportation **S**ystems

IVN **I**n-**v**echicle **N**etwork

LWN **L**ocal **W**ireless **N**etwork

ID **Id**entity

MOST **M**edia **O**riented **S**ystems **T**ransport

NDs **N**omadic **D**evices

OBU **O**n-**B**oard **U**nit

OEM **O**riginal **E**quipment **M**anufacturer

OS **O**perating **S**ystem

OVERSEE **O**pen **Ve**hicula**r** **Se**cur**e** Platform

PCIe **P**eripheral **C**omponent **I**nterconnect **E**xpress

PCO	**P**oint of **C**ontrol and **O**bservation
PKI	**P**ublic **K**ey **I**nfrastructure
POI	**P**oint **o**f **I**nterest
PS	**P**ositioning **S**ervices
RE	**R**untime Environment
RSA	**R**ivest, **S**hamir and **A**dleman algorithm for public-key cryptography
RSU	**R**oad**s**ide **U**nit
RTOS	**R**eal-**t**ime **O**perating **S**ystem
SMod	**S**ecurity **Mod**ule
SMem	**S**ecure **M**emory
S&D	**S**ecurity and **D**ependability
Tetra	**Te**rrestrial **T**runked **Ra**dio
TOC	**T**raffic **O**perations **C**enter
UC	**U**se **C**ase
UMTS	**U**niversal **M**obile **T**elecommunications **S**ystem
UN	**U**ser **N**etwork
USB	**U**niversal **S**erial **B**us
V2I	**V**ehicle-to-**I**nfrastructure
V2V	**V**ehicle-to-**V**ehicle
V2X	**V**ehicle-to-**X**
WAVE	**W**ireless **A**ccess for **V**ehicular **E**nvironment
Wi-Fi	**Wi**reless **Fi**delity

Document History

Version	Date	Changes
V1.5	01-07-2011	Final Version

1 Introduction

1.1 OVERSEE Objectives

The next generation of intelligent vehicular Information and Communication Technology (ICT) applications for advanced traffic management, active vehicle safety, or "green" electric cars strongly depend on the availability of an ICT infrastructure combining both dependability and security attributes.

Thus, future intelligent vehicles (i) have to provide an appropriate wireless access point to their on-board IT systems and in-vehicle applications, (ii) need appropriate access to external information and applications, and (iii) have to execute multiple independent applications with different level of criticality concurrently in a trusted manner.

To meet these challenges, OVERSEE will develop an open vehicular IT platform that provides a protected standardised in-vehicle runtime environment and on-board access and communication point.

Therefore, the main objectives of the OVERSEE platform will be IT security and dependability, which means enforcing a strong level of isolation between independent applications and ensuring that vehicle functionality and safety cannot be harmed by any application.

OVERSEE will first carry out a requirement analysis based on security risks and dependability analysis. It will then specify the in-vehicle platform architecture based on the following key elements:

- Efficient resource virtualisation that meets the stringent real-time and security requirements,
- Trusted access to security services protected by a vehicular hardware security module
- Flexible trusted dynamic administration of application deployment
- Monitoring capabilities based on trusted points of control and observation (PCO).

OVERSEE will also specify and develop the capabilities that are needed to validate future open platform implementations. This will involve an assurance approach, validation tools, and run-time building blocks. Finally, OVERSEE will develop at least two novel ICT applications to prove the feasibility of the approach.

1.2 Scope

This document describes use cases of automotive concerns or in areas directly related to automotive issues. These use cases will serve as a basis for the deduction of security and dependability requirements for the OVERSEE platform. The deliverables D1.2/D1.4 and D1.3/D1.5 defining respectively functional and non-functional requirements for the OVERSEE platform from the use cases identified as well as the partners expertise.

The extracted requirements will be refined and used to define the fitting architecture and abilities that must be provided by the platform. These topics will be treated in the future OVERSEE project report.

From a wide choice of use cases, this report will detail for some of them:

- The scenarios
- The involved component
- The actors and their benefices
- The security aspect

To avoid safety considerations regarding safety-relevant use cases and to keep the focus on security in OVERSEE, the consortium decided to decouple OVERSEE completely from safety-relevant in-vehicle systems (e.g. steering system and airbag system). Safety-relevant use cases will be executed on a dedicated OVERSEE unit in an isolated vehicle-safety-domain. This unit has to be SIL-certified in addition by considerations on top of the results of the OVERSEE project.

1.3 Document Outline

The remainder of the report is structured as follows:

- Section 2 gives details about the template used in OVERSEE for the use cases as the chosen categorisation. It also provides a comprehensive list of the use cases.
- Section 3 contains the description of some selected use cases among the list from the previous section.

2 Use Cases

2.1 Process of Definition and Selection

2.1.1 Overview of the Process

Task 1.1 defines and organises use cases. The following process was followed in order to improve collaboration and efficiency.

1. Step 1 was to propose a list of use cases by name and/or a short description in a few words. Some use cases come from other projects (e.g. SEVECOM[1], EVITA[2], TECOM[3], and others describe current or future needs for in-vehicle embedded applications directly from partners.
2. Step 2 was to consolidate and try to identify similar use cases and combined use cases. A combined use case includes more than one other previously defined use case. In this document combined use cases are denoted as *meta use cases*. This phase restricts unnecessary effort and creates a wide enough set of use cases.
3. Step 3 consisted of the first description and review phase. Each partner had to define a number of items in the list but none of those it proposed. The original proposer of the use case reviewed it based on common understanding and agreement. It was also a phase of improvement for the template. For instance, the various components were unified among the use cases to provide a complete list of terms which define the component used in or interacting with the OVERSEE platform. The used template is described in section 2.2.
4. In Step 4 the work previously done was refined. According to the purpose of OVERSEE, the use cases have to be classified according to a precise category, to clearly identify the assets to secure, and to sort them by order of “priority”. As the OVERSEE partners specialise in various areas, each of them selected and ranked 15 use cases. From this primary ranking, a study of the arguments leading to each decision was completed to reach a compromise and an accurate selection. Moreover, the categories and application type was taken into account to provide the best coverage of the future needs in ICT.

The overall results provided 20 use cases from various areas and concerns to illustrate the capabilities of the OVERSEE platform with respect to current and future needs of in-vehicle embedded systems.

2.1.2 Information about the Process Methodology

2.1.2.1 Selection Criteria

The OVERSEE project aims to propose a unique platform to support various applications. These applications can be part of different kinds. In the description of work and along the first discussions of the consortium, the following applications’ domains have been identified from our expertise:

- Intelligent Transport Systems
- Infotainment
- Driving Assistance System
- Car Manufacturer Interest

These domains have usually constraints that are not the same. Most of the driving assistance systems are real-time applications unlike infotainment's ones. Therefore, the use cases to be used in this document have to take into account this kind of constraint:

- Real-Time application
- Non-Real-Time application

Finally, OVERSEE is not foreseen to be used only for current applications but also to be able to support the upcoming ones. Thus, the two following parameters have to be considered:

- Near-term application
- Long-term application

The overall process has been based on the expectation of the European Commission (mandatory ITS application, e.g., eCall), the expertise of the involved partners and the existing on-going and ended projects defined as input for OVERSEE.

2.1.2.2 **Consolidation Aspects**

All along the different phases of the definition and selection of use cases some consolidation has been done. In the following, the different consolidation steps are described.

The first step described in section 2.1.1 results in 72 proposed use cases (cf. Appendix 5.2) described only by a name or a short sentence.

As each use cases has been proposed without knowing the proposition made by the other partners some use cases seem to be described twice, or some of them are quite the same. Therefore, to avoid unnecessary work a first consolidation phase (Step 2 in section 2.1.1) has taken place on the following criteria:

1. Identification of redundancy between UC proposed by different partners (e.g. eToll is equivalent to Electronic Toll Collection systems, theft intervention is similar to active theft management, and Point of Interest is similar to 3rd-party infotainment [POI, tourist info]
2. Identification of similar UC (same concern but different treatment)
3. Identification of meta use cases (e.g. "Traffic information from/to other entities" and "Road surface conditions to TOC" are part of "Cooperative awareness ")
4. Results 52 unique elementary use cases, 2 meta use cases and 3 similar use cases (cf. 5.2) for a total of 57 use cases

Later on 3 more use cases were added by one partner to reach 55 unique elementary use cases, 2 meta use cases and 3 similar use cases for a sum of 60 use cases (cf. 5.2).

Behind this consolidation the idea was to provide an interesting set of use cases that addressed a wide set of concerns and took into account all of the criteria defined in Section 2.1.2.1. The partners knowledge help a lot to reach quickly a sound set of use cases to illustrate the wanted capability of the OVERSEE platform.

2.1.3 Description and Review Phase

The third step of the process (see 2.1.1) consisted of describing each use case according to the template in section 2.2. During this description phase the partner who proposed the use case acted as a reviewer. Another partner acted as writer of the use case.

This decisions aims to help the whole consortium to reach a common understanding by coping with the other partners' concerns and points of view, and to allow each one to work with unknown partners.

In case of different understandings or opinions between the writer and the reviewer, they discussed the issue to find a solution.

During this phase, some redundancy between several use cases has been discovered and therefore twice two use cases have been merged. Moreover, three misuse cases have been proposed, but have been considered out of scope of this task. Actually, this task focuses more on use cases to illustrate the capabilities of the upcoming OVERSEE platform, and allow us to extract requirements both functional and non-functional. The decision was taken to provide description of required security aspects in each use case and not to describe unrelated or hard to link misuse cases. The misuse cases are left in charge of the proof of concept use cases (T5.1) and can be easily derived from the description of the use cases and the security aspects.

2.2 Use Case Template

A template has been defined to provide a workable and flexible format. It aims to provide a high-level use case but with enough information to extract requirements, both functional and non-functional. In order to perform a more synthetic job some common glossary is used mainly for security aspects and for the component involved in the use case. As the use cases rely on concrete applications some information provided could not be in the OVERSEE scope but are mandatory to be explicit enough.

The following subsection describes the components of the template.

2.2.1 Use Case Label and Name

This field contains a codename for the use case and its complete name.

2.2.2 Domain

This field defines the application domain concerned by the use case. It can be

- Intelligent Transportation Systems (ITS)
- Infotainment
- Advanced Driver Assistance Systems (ADAS)
- Car Manufacturer Interest

2.2.3 Category

These categories mainly rely on definitions from Volkswagen's current practice and were refined by OVERSEE partners

- Operation: All use cases during vehicle operation over life cycle. This includes all monitoring and maintenance services, software updates, data gathering for leasing companies, etc.
- Driver assistance systems (DAS) or Advance Driver Assistance System (ADAS): All use cases that assist the driver during a specific driving scenario.
- Convenience: All use cases that increase or influence the driver's convenience. This includes all inner- and outer-vehicle driver information systems.
- Mobility: All use cases that contribute the driver's mobility. This includes all data aggregation to increase the driving efficiency.
- Security services: All security-driven use cases like theft warning systems, etc.
- Others: All use cases that do not fit into existing categories

2.2.4 Functional/Technical Category

This field indicates the technical category of the use case. Most of them are related to "application" or "communication". Nevertheless, other categories have been proposed too. These categories are more technical and not based on business.

- Application: All mainly software based use cases
- Communication: Use cases relying mainly on communication
- Hardware: All mainly hardware based use cases
- Platform: All use cases focusing on connection to an existing in-vehicle platform

2.2.5 Originator

This field denotes the instance, which assembles or releases the application.

- OEM
- Public authority
- Third Party
- User or passenger
- Component supplier

2.2.6 Operation Description

This section addresses the overall description of the use cases. It should contain at least a description of the sequential actions. It could also define:

- Summary of the use case

- Precondition not depending on the OVERSEE platform
- Post condition not depending on the OVERSEE platform

2.2.7 **Roles, Actors and Stakeholders**

Each use case could imply various actors. Classical and well-identified roles are Road Sign Unit, Driver, or OEM.

2.2.8 **Benefits**

The benefits are high-level merits for each actors/roles defining previously. It could be practical ones (faster reaction, safer roads, etc.) or could address some future business models.

2.2.9 **Involved Components**

Any logical components both hardware and software involved in the implementation are depicted in this section. During the use case definition process, a list of components has been defined to formalize the section and the various constraints on the system.

2.2.9.1 **Communication Unit (CU)**

The "Communication Unit" of the OVERSEE platform is the capability of the platform to send and receive data through networks which are connected to the OVERSEE platform. If the CU is necessary, the type of network (see sub items) should also be specified.

- *Global wireless networks (GWN)*:
  Global Wireless means networks, which are widely available throughout (at least) Europe. These networks are able to offer uninterrupted communication connections even over wide distances, due to their cellular architecture (including the necessary handover mechanisms). If GWN is specified the conceivable networks for the implementation should also be fixed (e.g., UMTS, GSM/GPRS, Tetra).
- *Positioning services (PS)*:
  Positioning services means the capability of the OVERSEE platform to provide the current position of the vehicle by the use of appropriate receivers. If PS is specified the conceivable technologies for the implementation should also be fixed (e.g., GPS, Galileo).
- *User networks (UN)*:
  User networks means networks which are used to connect nomadic devices of the user to the OVERSEE platform. This networks can be wireless, too. If UN is specified the conceivable networks for the implementation should also be fixed (e.g., USB, Ethernet, Bluetooth).
- *In-Vehicle networks (IVN)*:
  In-Vehicle networks means networks, which connects the vehicle internal

components (ECUs). If IVN is specified the conceivable networks for the implementation should also be fixed (e.g., CAN, FlexRay, MOST).

- *Local wireless networks (LWN)*:
  Local wireless networks means networks, which are only available in a narrow area and for a short time period (if the vehicle is moving). If LWN is specified the conceivable networks for the implementation should also be fixed (e.g., DSRC, Wi-Fi).

2.2.9.2 **Runtime Environment (RE)**

Runtime Environment is a software execution environment of the OVERSEE platform to execute software applications. This component is necessary if an application needs to be installed on the OVERSEE platform (in most cases this means that the application needs more than the simple communication capabilities of OVERSEE). REs can offer a temporal and spatial isolation of applications (should be specified for each use case within the requirement analysis).

2.2.9.3 **Security Module (SMod)**

The security module of the OVERSEE platform provides Hardware Security Module-based security services. The necessary security services for each application should be fixed within the requirement analysis.

2.2.9.4 **Secure Memory (SMem)**

Secure memory means the capability of the OVERSEE platform to store data in a protected manner. This means that the data is stored in a confidential or immutable form. The SMem capability will probably reuse some functions of the HMS-based SMod. The requirements concerning secure memory should be considered for each application within the requirement analysis.

2.2.9.5 **Provider's System**

Provider's system means the internal (BackOffice) IT-system of the system provider. This component is out of the project scope of OVERSEE, but connected to the OVERSEE platform through at least one of the networks provided by the OVERSEE platform.

2.2.9.6 **Peripherals**

Peripherals are components which are out of the project scope of OVERSEE, but which are connected to OVERSEE through at least one of the connections provided by the OVERSEE platform. If Peripherals are mentioned within a use case the expected type of the peripheral should also be fixed (e.g., small printer, credit card terminal)

2.2.9.7 **Sensors**

Access to sensors is available through the IVNs. Sensors are out of the project scope of OVERSEE, but the type of the sensor should be fixed within the use case description.

2.2.9.8 **Actuators**

Access to actuators is available through the IVNs. Actuators are out of the project scope of OVERSEE, but the type of the actuator should be fixed within the use case description.

2.2.9.9 **Electronic Control Units (ECUs)**

Access to ECUs is available through the IVNs. ECUs are out of the project scope of OVERSEE, but the type of the ECU should be fixed within the use case description.

2.2.9.10 **Road Side Units (RSUs)**

Connections to RSUs are available through LWNs. RSUs are out of the project scope of OVERSEE, but the type and usage of the RSU should be fixed within the use case description.

2.2.9.11 **Nomadic Devices (NDs)**

Nomadic devices are connected through user networks (UN). NDs are out of the project scope of OVERSEE, but the type and usage of the ND should be fixed within the use case description.

2.2.9.12 **Public Key Infrastructure (PKI)**

A PKI provides certificates with public keys for asymmetric cryptography functions in a reliable manner. The PKI is out of the project scope of OVERSEE, but if a PKI is necessary for a use case the PKI and its usage should be fixed within the use case description.

2.2.9.13 **Human Machine Interface (HMI)**

The HMI is the capability of the OVERSEE platform to present information to the vehicle occupants and to receive input from them.

2.2.9.14 **Navigation or Positioning Capability**

Navigation or positioning capability means the function to locate the vehicle on a map, based on the information from the PS. It should also be possible to locate other objects (e.g., vehicles, POIs) on this map and bring up geographical relations between the own vehicle and the other objects.

2.2.9.15 **Others**

Any other involved components, which are not specified in the collection of involved components, should be treated as “others”. This component should be exactly defined within the use case description.

2.2.10 **Security Aspects**

Security aspects section covers *potential misuses* and (counteracting) security objectives/properties. Some properties are widely used and could be defined as following.

2.2.11 **Authentication**

- *ID authentication*: Receiver should be able to verify unique ID of sender.
- *Property authentication*: Receiver should be able to verify that sender has certain properties, e.g. sender is a car, a traffic sign, etc.
- *Location authentication*: Receiver should be able to verify that sender is actually at the claimed position or that message location claim is valid.

2.2.12 **Integrity**

It should be ensured that information cannot be tampered or the tampering could at least become detected.

2.2.13 **Confidentiality**

Information must not be accessible to unauthorized entities. Eavesdropped data does not reveal any information on the transmitted clear text to any third party or to assure that transported information cannot be eavesdropped on its way.

2.2.14 **Privacy**

Since privacy is rather a second level or sociological term than a clear technical or cryptographic property, in the following just the concrete aspects regarding privacy covered by OVERSEE.

- *ID privacy:* Sender does not want to reveal its identity without his explicit approval and never want to reveal its identity to any unauthorized entities.
- *Location privacy:* Sender does not want to reveal its location without his explicit approval and never want to reveal its identity to any unauthorized entities. The location privacy issue can be also spread into subdivision:
    1. Location information can be freely distributed throughout the network
    2. Current location information is relevant for neighbouring nodes; collection of sequences of location information for user tracking should be prevented

3. Other nodes (knowing the identity of a node) in the network cannot retrieve the (exact) location of this node

2.2.15 **Availability**

Authorized entities (e.g., hardware modules, software processes, users) must have proper and timely access to their dedicated data, functions, and services.

2.2.16 **Access Control**

Access control mechanisms (e.g., discretionary access control and/or mandatory access control) prevent unauthorized access to access-restricted vehicular data or access-restricted vehicular resources (e.g., networks, computing power). Access rules to restricted data and resources are defined in the corresponding security policy derived during the overall security requirements engineering process, which determines the access rights for each authorized entity.

2.2.17 **Auditability**

Application needs to track/reconstruct what was going on in the past. This might also include non-repudiation requirements, where senders or receivers can prove that messages have been received or sent respectively. For some applications, messages may only be stored for a very limited time (e.g. the last 10 seconds in a ring buffer) and made permanent only in case of an incident (e.g. fault entry).

2.2.18 **Testing Requirements**

This optional section proposed some hint to validate or verify the capability in term of security and dependability of the use case.

2.3 Overview of the Resulting Template

Use Case Label & Name	
Domain	
Category	
Functional/Technical Category	
Originator	
Operation description	
Roles, Stakeholders, Actors	
Benefits	
Involved components	
Security aspect	
Testing Requirements	

Table 1 Use Case Template

2.4 Use Case List and Overview

After the previous work, a list of use cases has been defined. The original list is a bit longer but some of the use cases are actually equivalent to some others or were identified as non-relevant for the project after the second step of the definition process. Some of the use cases are defined as meta use cases, i.e., they encompass at least two other pre-defined use cases. The overall list is stated below:

1) Parking lot reservation
2) E-Toll
3) Remote car control
4) Secure integration
5) Stolen vehicle tracking
6) Electronic licence plate
7) Remote flashing
8) Local Danger Warning Between Cars
    a. Vehicle-based road condition warning

   b. Emergency vehicle signal pre-emption (1 & 2)
   c. Work zone warning
   d. Intersection collision warning
9) Cooperative awareness
   a. Traffic information between entities
   b. Road surface conditions to TOC
10) Record driving data
   a. Electronic driver logbook
   b. Pay as you drive (Eco)
   c. Pay as you drive (Safety)
11) Point of interest
12) Dynamic traffic management
13) Safety reaction : activate break
14) Flashing per OBD
15) eCall
16) Map download/update
17) Install applications
18) Personalize the car
19) Replacement of engine ECU
20) Remote feature activation
21) Vehicle to home to business
22) Remote vehicle rental
23) Point to point connectivity across multiple vehicles
24) Misuse case: causing accidents, traffic jam and aggro by faking or manipulating messages
25) Application for cabs
26) Application for parcel services
27) Vehicle access control
28) Interactive Web 2.0
29) Break down call live check
30) M-Commerce
31) Car finder
32) Software test container
33) Monitoring system
34) Parking sensor system
35) Request for automobile club assistance
36) System management
   a. Deployment
   b. Mode change
37) Wi-Fi hotspot
38) Extended floating car data

2.5 **Use Case Selection**

The selection has been made on the following criteria:

- Is the use case representative of a class of problem or technical category?

- Is the use case providing hints for defining new requirements for the next step of the project?
- Is the use case important according to future business and coming automotive evolution?
- Is the use case feasible within the project?

Not all the criteria are relevant for the selected use cases but all have been taken into account to make the selection.

Each partner selected and ordered 20 use cases based on these criteria and on the relevance for the OVERSEE platform. The combination of the ranking has been used to discuss and propose a list of 20 final use cases. The main goal was to provide in this deliverable only a representative number even if all the use cases have been completed.

2.6 Use Cases versus Misuse Cases

As we originally depicted some misuse cases, none of them are in this deliverable. The intent of this document is to provide a sufficient kind of use cases to extract requirements in the future steps of the project, both functional and non-functional ones. In this way, we did not address misuse cases for three main reasons:

- Requirements are not easily extracted from general (high level) misuse cases
- Misuse cases will be derived from the security aspect section of each use case
- Misuse cases will be an important part of the proof of concept and will be defined in the relevant deliverable (D5.1).

3 Detailed Description of Selected Use Cases

The following use cases have been selected and are described in detail in this document.

1. E-Toll
2. E-Call
3. Parking lot reservation
4. Secure Integration
5. Meta-UC: Hazard Warning between Vehicle
    - Emergency vehicle signal pre-emption (1 & 2)
6. Stolen vehicle tracking
7. Traffic Information between Entities
8. Safety Reaction: Active Brake
9. Personalize the car
10. Car finder (e.g., via mobile phone)
11. Electronic license plate
12. Dynamic Traffic Management
13. Break-Down-Call-Live-Check
14. Remote Car Control (e.g. door opener)
15. Pay As You Drive (Road Safety & Eco)
16. Install applications
17. Remote vehicle rental
18. Parking Sensor System
19. Electronic Driver logbook
20. Web 2.0 for Cars

3.1 E-Toll

Use Case Label & Name	UC-TOLL: e-Toll
Domain	ITS
Category	Mobility
Functional/Technical Category	Application Communication
Originator	Public authority Third party
Operation description	OVERSEE provides a secure and privacy-preserving vehicle authentication and payment mechanism to provide automated, wireless "marking" of vehicles when entering a toll road and corresponding automated, wireless vehicle recognition and payment when leaving the toll road. Toll payment itself can be backend-driven (e.g., by simple provision of a credit card number or similar) or even direct by enabling vehicle-driven payment (e.g.,

	by having a virtual money transfer from vehicle to the toll station).
	• Precondition
	  ○ There exists a mechanism to reliably recognize vehicles entering and leaving a toll road section.
	  ○ There exists an secure external communication channel to the corresponding vehicle recognition and toll payment system

Roles, Stakeholders, Actors	• Driver / Passenger • Toll road operator
Benefits	Driver / passenger: Fast, easy, more safe(!) and seamless tolling Toll road operator: Efficient, reliable and very flexible (e.g., reg. costs, location) tolling Toll booth personal: No extremely stupid and bleakly toll booth employments anymore

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN)
	  ○ Positioning services (PS)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Secure Memory (SMem)
	• Provider's System
	• Road Side Units (RSUs)
	• (Public Key Infrastructure (PKI))
	• Human Machine Interface (HMI)

Security aspect	• Potential misuses (vs. security objectives)
	  ○ Unauthorized interception of communication to toll system (vs. privacy)
	  ○ Unauthorized manipulation of communication to toll system (vs. integrity/authenticity)
	  ○ Denial of service of communication to toll system (vs. availability)
	  ○ Unauthorized read-out of storage associated to the e-toll system (vs. privacy)
	  ○ Unauthorized manipulation of storage associated to the e-toll system (vs. integrity/authenticity)
	  ○ Unauthorized deletion of storage associated to the e-toll system (vs. availability)

Table 2 UC-TOLL

3.2 **E-Call**

Use Case Label & Name	UC-eC: e-Call
Domain	ITS
Category	Other
Functional/Technical Category	Application
Originator	OEM & Public Authorities

Operation description	• Precondition:
	  ○ Airbag deployed OR
	  ○ Detection of a rollover OR
	  ○ Sense of life-threatening emergency
	• Scenario
	  ○ After an accident car C sends an emergency message to the nearest local emergency authority, ideally including:
	  ○ Vehicle location (Where it has been happened?)
	  ○ Vehicle dynamics (What has been happened?)
	  ○ Vehicle info (What car/truck is involved? Any danger goods involved?)
	  ○ Passenger info (Who is involved?)
	  ▪ Further info important to know, e.g., important medical info (e.g., blood type)
	  ○ The route of the message can be many kinds.
	  ▪ The message can be sent directly to a Road Side Unit (RSU).
	  ▪ If no RSU is reachable, then C broadcasts the emergency message to cars in range.
	  ▪ Each of them tries to forward the message to a RSU, or hops the message.
	  ▪ The RSU forwards the message directly to the nearest local authority.
	  ▪ The message can be sent via wide-range communication channel (e.g., GSM or UMTS)
	  ○ Once the message received an emergency authority, the vehicle or the emergency authority try to establish a voice connection into the vehicle to contact the driver for further information, help or important instructions

Roles, Stakeholders, Actors	• Emergency or Road Side Unit (incl. wide-range communication RSUs such as GSM network nodes)

	• Drivers • Manufacturer

Benefits	• Drivers / Passengers:
	  ○ have quick and automated request for assistance and/or emergency care
	• Car manufacturer
	  ○ provide a safer car (selling argument)
	• Emergency or Road Side Unit :
	  ○ Faster reaction and more precise reaction (due to the automated information exchange)

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN) (GSM/GPRS, UMTS)
	  ○ Positioning services (PS) (GPS)
	  ○ In-Vehicle networks (IVN) (CAN, FlexRay)
	  ○ Local wireless networks (LWN) (DSRC)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Provider's System
	• Sensors
	• Electronic Control Units (ECUs)
	• Road Side Units (RSUs)
	• Public Key Infrastructure (PKI)
	• Human Machine Interface (HMI)
	• Navigation or positioning capability

Security aspect	• Threats
	  ○ Joke, Flood Local authority
	• Security requirements
	  ○ ID authentication
	  ○ Location authentication
	  ○ integrity
	  ○ (optional) confidentiality
	  ○ ID Privacy
	  ○ Location Privacy (public authorities or insurance company want to have access to identity or location of node)
	  ○ Auditability (This might also include non-repudiation requirements, where senders or receivers can prove that messages have been received or sent respectively.

Testing Requirements	• Communication: PCO • Check the correctness/validation of routing protocol carrying the message

	• Check the storage of isolated data about the crash

Table 3 UC-eC

3.3 UC-parking lot reservation

Use Case Label & Name	UC-PLR: Parking lot reservation
Domain	Infotainment
Category	Mobility
Functional/Technical Category	Application (involving Communication)
Originator	Third Party
Operation description	Before departure or during a trip, the driver has the possibility to check the availability and to reserve a suitable parking lot near to his destination. For that purpose an application running on the Oversee platform connects via Internet to a parking management system. Additional information (like extra space for big vehicles/trucks, accessibility for handicapped drivers, etc) may be submitted. Alternatively, a parking lot is reserved as soon as a vehicle enters a car park. Precondition: Parking management systems with the possibility of remote parking lot reservation exist, e.g. in a parking deck or basement garage. Post-condition: Parking lot is reserved.
Roles, Stakeholders, Actors	• Driver • Car park operator • Society
Benefits	• Driver: No need to search for a parking lot, saves time and fuel • Car park operator: Efficient lot occupancy, flexible fee models • Society: Reduction of useless traffic and CO2 • Possible disadvantage for other drivers, which cannot use empty but reserved parking lots
Involved components	• Global wireless networks (GWN) • Runtime Environment (RE) • Human Machine Interface (HMI)

	• Provider's System
	• Optional
	  ○ Navigation or positioning capability
	• Alternative (see operation description)
	  ○ Local wireless networks (LWN)
	  ○ Road Side Units (RSUs) at car park entry

Security aspect	Potential misuses • Useless reservation (blocking) of parking lots

Table 4 UC-PL

3.4 UC Secure Integration

Use Case Label & Name	UC-SCoND: Secure Integration of Nomadic devices
Domain	Infotainment
Category	Platform
Functional/Technical Category	Convenience
Originator	OEM and Third party
Operation description	The use case demonstrates the integration of an application installed on mobile device, e.g. a media player on a notebook, within the multimedia function of the car. This use case demonstrates how a notebook could use the audio and video devices of the car to display these data; or access entertainment data stored in the vehicle. Precondition • A stable and secure communication interface for the device. • A stable and secure communication interface within the car. Scenario • Mobile Device make an authentication request • The authentication is provided by the vehicle system, and access is granted • MD request video/audio/storage device access

	• the system establish the connection
Roles, Stakeholders, Actors	• Vehicle manufacturer • Drivers • Mobile device manufacturer

Benefits	• Vehicle manufacturer
	  ○ provide optional functionalities to its products
	  ○ no need to develop specific remote device
	  ○ could easily extend the number of possible devices in its cars
	• Drivers
	  ○ Allow roaming with a mobile device
	  ○ Synchronization of various devices inside and around the vehicle
	  ○ Easily utilization of a mobile device with the capability on the in-vehicle ones.
	• Mobile Device manufacturer
	  ○ New market
	  ○ New application

Involved components	• Communication Unit (CU)
	  ○ User Network (UN)
	  ○ In-Vehicle Network (IVN)
	• Runtime environment (RE) isolated
	• Security Module (SM) : must verified that the device is harmless, and isolate the devices from the network until it was done
	• Nomadic devices
	• HMI : to add/identified a new device for instance

Security aspect	• ID Authentication (User) • Property Authentication (Authorized mobile device) • Confidentiality • ID privacy • Location privacy • Access control • Integrity • MisUC: ○ If the authentication part is not correctly achieved, the system is exposed to unauthorized usage or harmful attack

Table 5 UC-SCoND

3.5 UC Meta UC: Hazard Warning between Vehicle

Use Case Label & Name	UC-LDW: Local Danger Warning to other Cars
Domain	ITS and ADAS
Category	Mobility
Functional/Technical Category	Application / Communication
Originator	OEM
Operation description	Preconditions • Vehicles are equipped with sensors and remote communication capabilities. Description • Tracking of safety critical information. • Recognition of a critical situation • The vehicle sends a warning message to others. • The message is received and processed by other cars according to some road safety policies • Warning message with indication of the critical situation is emit to the drivers Options • Vehicle can forward the warning according a TTL (by geocasting or broadcasting) • Infrastructure could be also contacted (e.g. via a Road Side Unit) to request an emergency vehicle.
Roles, Stakeholders, Actors	Drivers
Benefits	Drivers • More anticipation of possible danger • Reduce risk of an accident (cheaper car insurance)

Involved components	• Communication Unit (CU)
	  ○ Positioning services (PS)
	  ○ In-Vehicle networks (IVN)

	○ Local wireless networks (LWN) • Runtime Environment (RE) • Sensors • Navigation or positioning capability • HMI • Actuator
Security aspect	• Threats ○ Forging of Warnings ○ Suppression of Warnings ○ Modification on Sensors (harder) ○ User/Vehicle tracking • Security requirements ○ Property authentication ○ Location authentication ○ Integrity ○ Privacy ○ Availability

Table 6 UC-LDW1

This use case covers a large number of applications. However, a specific one has to be mentioned as a sub-use case. It concerns Emergency vehicles that need to reach an accident area, or a hospital, in the safer and quicker manner. That implies an emergency vehicle can pre-empt traffic light or other infrastructure elements. In the following subsection, two variants of this use case are described

3.6 UC Emergency Vehicle Signal Pre-emption

Use Case Label & Name	UC-EVSPE: Emergency vehicle signal pre-emption
Domain	ITS
Category	Mobility
Functional/Technical Category	Application/Communication
Originator	OEM and Public authorities
Operation description	Emergency vehicles can control traffic lights, dynamic lane marks or other infrastructure elements to avoid or escape from traffic jams and accelerate the time of arrival at an emergency scene or hospital

	Precondition: • Vehicle is registered as emergency vehicle. • Infrastructure elements are directly or indirectly controlled by emergency vehicle. • Emergency vehicle uses standard emergency flashers and standard traffic rules apply Scenario: • Navigation system or emergency control centre advices optimal route considering signal pre-emption options. • Emergency vehicle (EV) heading to intersection with traffic lights communicate either directly with traffic lights' RSU or indirectly via other vehicles using a Multi-Hop link. • EV is being authorized by RSU and traffic lights are changed.
Roles, Stakeholders, Actors	• Emergency Vehicle • Vehicles (normal) • Infrastructure for traffic light handling

Benefits	• Emergency Vehicle :
	  ○ faster and safer trip to or from emergency scene
	  ○ reduce risk of being trapped in a traffic jam
	
	• Vehicle :
	  ○ Reduce unusual behaviour
	  ○ Warned easily of the special situation

Involved components	• Communication Unit (CU)
	  ○ In-Vehicle networks (IVN)
	  ○ Local wireless networks (LWN)
	  ○ Positioning services (PS)
	• Runtime Environment (RE)
	• Road Side Units (RSUs)
	• Public Key Infrastructure (PKI) -- authentication of the EVU
	• Human Machine Interface (HMI)
	• Navigation or positioning capability

Security aspect	• Threats
	  ○ Forging of Warnings
	  ○ Suppression of Warnings
	
	• Security requirements
	  ○ Property authentication
	  ○ Location authentication
	  ○ Integrity
	  ○ Availability
	  ○ Access control

	○ Auditability

Table 7 UC-EVSPE

This use case has also an alternative version:

Use Case Label & Name	UC-EVSPE2: Emergency vehicle signal pre-emption 2
Domain	ITS
Category	ADAS
Functional/Technical Category	Application/communication
Originator	Public authorities
Operation description	Due to risk of clogging the road and multi-hop communication potential problem (w.r.t. authentication and non-repudiation) this use case is alternative of the UC-EVSPE use case. • Precondition : ○ Emergency vehicle is registered in system. ○ Infrastructure elements are directly or indirectly controlled by emergency vehicle. ○ A Headquarter assigns EV • Authorization for pre-emption (centralized) ○ Emergency control centre received a request for assistance with localisation information ○ Emergency control centre (ECC) compute optimal route considering signal pre-emption options and road traffic information for a selected EV ○ ECC gives authorisation of pre-emption to the EV with timeout ○ ECC gives authorisation with activation token for each signal • Activation of pre-emption (localized) ○ pre-emption accepted against token ○ pre-emption activation limited to one-hop communication (currently around 250 m with Wi-Fi) ○ pre-emption is recorded
Roles, Stakeholders, Actors	• Emergency Vehicle • Vehicles (normal) • Headquarter

	• Infrastructure for traffic light handling

Benefits	• Emergency Vehicle:
	  ○ faster and safer trip to or from emergency scene
	  ○ reduce risk of being trapped in a traffic jam
	• Vehicle:
	  ○ Reduce unusual behaviour
	  ○ Warned easily of the special situation

Involved components	• Communication Unit (CU)
	  ○ In-Vehicle networks (IVN)
	  ○ global wireless networks (GWN)
	  ○ Positioning services (PS)
	• Runtime Environment (RE)
	• Secure Memory (SMem) - to store token
	• Road Side Units (RSUs)
	• Public Key Infrastructure (PKI) -- authentication of the EVU
	• Human Machine Interface (HMI)
	• Navigation or positioning capability

Security aspect	• Threats
	  ○ Forging of Warnings
	  ○ Suppression of Warnings
	  ○ Illegal access to token
	• Security requirements
	  ○ Property authentication
	  ○ Location authentication
	  ○ Integrity
	  ○ Availability
	  ○ Access control
	  ○ Auditability

Table 8 UC-EVPSE2

3.7 UC Stolen Vehicle Tracking

Use Case Label & Name	UC-SVT: Stolen vehicle tracking
Domain	DAS
Category	Security services
Functional/Technical Category	Application

Originator	• OEM • Public authority • Third Party

Operation description	The information about a stolen vehicle is forwarded by several mobile nodes up to the authorities.
	
	Variants
	
	• via identification of the driver
	  ○ may tamper privacy of users
	• clear identification of any intrusion manoeuvres
	  ○ may need far more vehicle sensors than oversee is designed to connect
	• vehicle owner informs a service about the theft and the vehicle verifies this status cyclic
	
	Procedure
	
	• If the vehicle discovers, that it is stolen, it starts to send out beacons with a stolen flag (and the usual timestamp, position, etc.)
	• receiving OBUs and RSUs forward this type of beacon to the corresponding law enforcement officials
	
	Precondition
	
	• a vehicle can detect that it is stolen (see variants)

Roles, Stakeholders, Actors	• Vehicle driver • Vehicle owner • Law enforcement officials
Benefits	• Vehicle driver: none • Vehicle owner: gets a higher level of theft protection • Law enforcement officials: may easier detect that a vehicle is stolen

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN)
	  ○ Positioning services (PS)
	  ○ In-Vehicle networks (IVN)
	  ○ Local wireless networks (LWN)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Provider's System
	• Sensors
	• Electronic Control Units (ECUs)

	• Road Side Units (RSUs)
Security aspect	• Malfunction may lead to false positives and distrust in the system. • Measures to make this secure like engine immobiliser and alarm today. • Misuse of this function can lead to privacy invasion.

Table 9 UC-SVT

3.8 UC Traffic Information between Entities

Use Case Label & Name	UC-TIE: Traffic information between entities
Domain	ITS
Category	Mobility
Functional/Technical Category	Application
Originator	OEM or Third-party

Operation description	Preconditions
	• Vehicles are equipped with sensors, remote communication capabilities and have traffic computation capabilities
	• Vehicle are equipped with localization and navigation capabilities
	
	Description
	• Detection & Emission
	  ○ Recognition of relevant traffic information from sensors.
	  ○ Sending of data to other cars and infrastructures (geocasting, broadcasting – multi-hop)
	• Reception & Processing
	  ○ Reception of multiple traffic data for multiple sources
	  ○ Computing traffic information
	  ○ Update navigation for the Drivers
	  ○ Warning of the update AND/OR of the possible

	problem that occurs
Roles, Stakeholders, Actors	• Drivers • Road Services

Benefits	• Drivers
	  ○ Efficient navigation by combining information of multiple sources
	  ○ Reducing traffic jam
	  ○ Reducing CO^2 emission
	• Road Services
	  ○ Better over watching of traffics
	  ○ Can alert non-equipped vehicle drivers of problems faster
	  ○ faster reaction in case of problem

Involved components	• Sensors
	• Runtime Environment RE (Traffic computation)
	• CU
	  ○ Global Wireless Network (GWN)
	  ○ In-Vehicle Networks (IVN)
	  ○ Positioning services (PS)
	• HMI
	• Navigation or positioning capabilities

Security aspect	• Threats
	  ○ Forging of Warnings
	  ○ Suppression of Warnings
	  ○ Modification on Sensors (harder)
	• Security requirements
	  ○ Property authentication
	  ○ Location authentication
	  ○ Integrity
	  ○ ID Privacy
	  ○ Availability

Table 10 UC-TIE

3.9 UC Safety Reaction: Active Brake

Use Case Label & Name	UC-ABR: Messages lead to safety reaction(V2V) cf. Safety reaction: Active brake (V2V)
Domain	ADAS
Category	ADAS

Functional/Technical Category	Active safety application, V2V Communication
Originator	Third Party
Operation description	Short description • enhances the safety of vehicles in a dense driving environment or with decreased visibility • avoid rear end collisions • The driver will be warned before he is able to realize that the vehicle ahead is breaking hard • The vehicle automatically breaks if the driver remains idle Procedure • vehicles broadcast a self-generated emergency brake event to the surrounding vehicles • detection of emergency braking is based on a deceleration threshold in conjunction with brake assistant, brake light and optional ABS action • Upon receiving such event information, the receiving vehicle determines the relevance of the event and then provides a warning to the driver if appropriate and through the vehicle to the brakes' actuator • the warning may be presented in the HMI by visual, audio or other tactile signals
Roles, Stakeholders, Actors	Driver
Benefits	Driver: Better accident protection
Involved components	• Runtime Environment (RE) • In-Vehicle networks (IVN) • Human Machine Interface (HMI) • Sensors
Security aspect	• False warnings may lead to accidents, so a high level of protection against false positives should be implemented • Latency is critical for all types of active safety applications

Table 11 UC-ABR

3.10 **UC Personalize the car**

Use Case Label & Name	UC-PTC: Personalize the car
Domain	Infotainment
Category	Convenience
Functional/Technical Category	Platform (involving communication)
Originator	OEM

Operation description	• Precondition
	  ○ Application on the OVERSEE platform to control driver individual settings (e.g., seat position, mirrors) is already installed.
	• Scenario
	  ○ The driver registers the nomadic device on which the personal settings should be stored respectively from which they should be loaded. (Only one time)
	  ○ Once the driver enters the vehicle and a nomadic device containing the user settings is available (e.g., via Bluetooth) the user settings will be downloaded to the OVERSEE platform and applied to the vehicle system.
	  ○ If the personal settings are changed the application asks the driver whether he likes to store the personalized settings to the nomadic device or not.

Roles, Stakeholders, Actors	Driver
Benefits	Driver: Improved comfort, especially on frequently changes of the vehicle (e.g., vehicle rental)

Involved components	• Communication Unit (CU)
	  ○ User networks (UN) (USB, Bluetooth)
	  ○ In-Vehicle networks (IVN) (CAN)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Secure Memory (SMem)
	• Actuators
	• Electronic Control Units (ECUs)
	• Nomadic Devices (NDs)
	• Human Machine Interface (HMI)

Security aspect	• Threats and potential misuses ○ Faking of user settings (especially their application while driving) might cause safety risks. • Security requirements

	○ Authentication • Security and Dependability objectives

Table 12 UC-PTC

3.11 **UC Car finder**

Use Case Label & Name	UC-CF: Car finder (e.g. via mobile phone)
	Infotainment
Category	Convenience
Functional/Technical Category	Application (involving communication)
Originator	• OEM • Third Party
Operation description	A user is searching for his car, because he forgot where he has parked or someone else parked the car. The user starts the car finder software on his mobile device (e.g. mobile phone). The software connects through a secure Internet connection to a backend service where the latest position of the car is stored. The coordinates are sent to the user's mobile device, which displays the location on a map. On the car an application running on the Oversee platform connects through a secure Internet connection to a backend service and sends its actual position when the car is parked. The status "car is parked" occurs when clamp 15 is off and the car is closed and locked. Precondition: • Localization software for a mobile device (e.g. mobile phone) exists. • Vehicle is equipped with a positioning system. • A backend service exists where the position of the car can be stored securely. Post-condition: • The user knows the exact location of his vehicle.
Roles, Stakeholders, Actors	• User • Driver

Benefits	• User: Always knows the exact location of his car • Driver: None
Involved components	• Global wireless networks (GWN) • Positioning services (PS)

Security aspect	• Potential misuses
	  ○ Tracking of vehicle
	• Security requirements
	  ○ Privacy
	  ○ Confidentiality
	  ○ Authentication
	  ○ Access Control

Table 13 UC-CF

3.12 **UC Electronic Licence Plate**

Use Case Label & Name	UC-ELP: Electronic Licence plate
Domain	ITS
Category	Mobility
Functional/Technical Category	Application
Originator	OEM or Public authority

Operation description	• Precondition:
	  ○ Assignment of identity and credentials to vehicles
	  ○ Detection of the approaching vehicle, vehicle request to the infrastructure or detected violation of rules
	• Scenario
	  ○ Infrastructure generates an ELP request message (ELP-REQ); message is signed
	  ○ Infrastructure transmits the ELP-REQ, which can be targeted to a specific vehicle or all vehicles receiving the message
	  ○ Vehicle receives and validates ELP-REQ; if successful (authentic, recent), vehicle returns its ELP encrypted

Roles, Stakeholders, Actors	• Corporation or Public Utility that owns the infrastructure • Drivers
Benefits	• Drivers:

	○ easy and personal identification to access services • Corporation or Public Utility : ○ automated identification of vehicles ○ enhance quickness of identification Comments : One consider a benefit would be part of other use cases concerning automatic billing, such as eToll. But automatic access control could be used with any identifier. Could include public authority certificate stickers (e.g., vehicle inspection, emissions stickers etc.) in an electronic manner. But it can lead to some break in privacy laws
Involved components	• Communication Unit (CU) ○ In-Vehicle networks (IVN) ○ Local wireless networks (LWN) • Secure Memory • Road Side Units (RSUs) • Public Key Infrastructure (PKI)
Security aspect	• Threats ○ Forging of ELP ○ impersonation ○ Vehicle/driver tracking • Security requirements ○ ID authentication ○ ID Privacy ○ Location Privacy ○ Access Control
Testing Requirements	• Knowledge of the encryption and signatures • Points of Control and Observation (PCOs) on wireless communication (could be remote ones)

Table 14 UC-ELP

3.13 **UC Dynamic Traffic Management**

Use Case Label & Name	UC-DTM: Dynamic Traffic Management
Domain	ITS
Category	Mobility
Functional/Technical Category	Application (involving communication)
Originator	Public authority

Operation description	• Precondition
	  ○ Traffic management centre must be able to monitor and control traffic lights and signs in a certain area
	• Scenario
	  ○ All vehicles in the area monitored by the traffic management centre transmit their current position, direction and speed to the traffic management centre using RSUs (Road Side Units). (If interaction with a navigation system is possible also the transmission of the planned route is possible)
	  ○ The traffic management centre determines the best traffic flow from the information of all vehicles in the controlled area as well as additional information (e.g., information on construction zones) and controls the traffic lights and signs. (Not in project scope)
	  ○ If interaction with a navigation system is possible, the traffic management centre is also able to provide information for rerouting of single vehicles based on the optimized traffic flow (e.g., for splitting a lot of vehicles driving in the same direction to different routes)

Roles, Stakeholders, Actors	• Driver • Traffic management centre • Society • Public authority
Benefits	• Driver: Faster and safer arrival at destination • Society: Reduced emission of CO2, reduced consumption of fuel, efficient use of road network by the reduction of traffic jams • Public authority: More efficient use of road network (instead of continuous expansion of the road network)

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN) (UMTS, GSM/GPRS)
	  ○ Positioning services (PS)
	  ○ Local wireless networks (LWN) (DSRC)
	  ○ In-Vehicle networks (IVN) (CAN)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Provider's System
	• Sensors (wheel rotation sensor)
	• Road Side Units (RSUs)
	• Human Machine Interface (HMI)
	• Navigation or positioning capability

Security aspect	• Threats & potential misuses
	  ○ Denial of Service Attacks
	  ○ Faking of V2I messages or I2V messages to influence traffic flow
	  ○ Attacks on privacy of the driver
	  ○ Faking of vehicle identities (especially in case of rerouting of single vehicles)
	• Security requirements
	  ○ Confidentiality
	  ○ Authentication
	• Security and Dependability objectives

Table 15 UC-DTM

3.14 **UC Break-Down Call / Live Check**

Use Case Label & Name	UC-BDC: Break-Down-Call / Live-Check
Domain	Car Manufacturer Interest
Category	Operation
Functional/Technical Category	• Application • Communication
Originator	OEM
Operation description	OVERSEE has a secure (mainly regarding authenticity) and privacy-preserving (confidentiality and minimum amount of information collected) logging and -- in case of a break-down -- reporting application that enables the driver to contact the vehicle OEM (or other responsible) in case of a vehicle break-down to identify the problem and give or organize any help required (remote repair,

	repair instructions, calling breakdown service car, inform next capable garage around etc.). In accordance with the driver and owner of the vehicle, the live-check application can also be used to do any kind of anonymous statistics (e.g., failure rate, usage) to enhance efficiency, safety or reliability of next-generation vehicles or to do automated (small) error reporting to detect potentially upcoming failures.
	
	• Precondition
	  ○ There exists a diagnostic service application monitoring the ECU's event memory.
	  ○ There exists an secure logging application
	  ○ There exists a secure external communication channel to the corresponding break-down-service system.

Roles, Stakeholders, Actors	• Driver / Passenger • Breakdown service company / OEM
Benefits	Driver / passenger easy, fast, effective and professional help in case of a vehicle breakdown Breakdown service company fast and precise (due to in additional monitoring info) break-down service business model OEM customer satisfaction, on-line statistics and hence early warnings about (potentially) frequent issues Public authority Easy certificate check (e.g., last vehicle inspection, failure of safety-relevant vehicle components, emission class, etc.)

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN)
	  ○ In-Vehicle networks (IVN)
	• Security Module (SMod)
	• Secure Memory (SMem)
	• Providers System
	• Sensors
	• Actuators
	• Electronic Control Units (ECUs)

Security aspect	• Potential misuses (vs. security objectives) ○ Unauthorized monitoring read-out (vs. privacy)

	○ Unauthorized interception of communication to breakdown service system (vs. privacy) ○ Unauthorized manipulation of communication to breakdown service system (vs. integrity/authenticity) ○ Denial of service of communication to breakdown service system (vs. availability) ○ Unauthorized usage of diagnostic service layer

Table 16 UC-BDC

3.15 **UC Remote Car Control**

Use Case Label & Name	UC-RCC: Remote Car Control
Domain	Car Manufacturer Interest
Category	Convenience
Functional/Technical Category	Application
Originator	OEM
Operation description	Enable a remote control of car functions from both outside and inside the vehicle via mobile devices. Possible application examples are closing and opening of windows, doors or similar units with a smart phone. In this use case we describe unlocking and opening of the convertible top from outside of the car with a smart phone • Precondition ○ A stable and secure software system exists, which when installed on the mobile device will ensure the security and integrity of the connection to the vehicle. ○ The software also guarantees that the remote control function cannot be activated accidentally. • Scenario ○ Mobile Device makes an authentication request by a radio communication (e.g. wifi or Bluetooth) ○ The authentication is provided by the vehicle system, and access is granted ○ MD sends the command (to open the doors, for instance) by its radio communication medium ○ The command is performed by the car relying on the

	in-vehicle network (e.g. CAN)
Roles, Stakeholders, Actors	• Vehicle manufacturer • Drivers • Mobile device manufacturer

Benefits	• Vehicle manufacturer
	  ○ provide optional functionalities to its products
	  ○ no need to develop specific remote device
	• Drivers
	  ○ All-in-one mobile device
	  ○ Easy to use

Involved components	• Communication Unit (CU)
	  ○ User networks (UN) - WLAN capabilities (Bluetooth, Wifi, etc…)
	  ○ In-Vehicle networks (IVN)
	• Actuators(ex: door opener)
	• Nomadic Devices (NDs) with wireless capabilities

Security aspect	• ID Authentication (User)
	• Property Authentication (Authorized mobile device)
	• Integrity
	• MisUC :
	  ○ Forged ID could allow a non-authorized person to enter in the car or worst
	  ○ Non-authorized devices can have flaws in their security system

Table 17 UC-RCC

3.16 **UC Pay as You Drive**

Use Case Label & Name	UC-PAYD: Pay as you drive • Eco (-ECO) • Road Safety (-SAFETY)
Domain	infotainment
Category	-ECO: Operation -SAFETY: Mobility
Functional/Technical Category	Application (involving Communication)

Originator	-ECO: Public authority together with OEM -ROADSAFETY: Third Party together with OEM

Operation description	By secure and non-deniable recording of driving behaviour (e.g., average speed, heavy braking) and data from sensors or systems (e.g., time of use, driven distances) new fair taxes or usage-specific payment insurances.
	
	This can influence the driving behaviour and hence both road safety and CO^2 emission. Moreover these aspects are heavily bonded for fuel engine based car.
	
	• Precondition (ECO)
	  ○ There exist eco tax models supporting the accounting of taxes based on the driving behaviour of the vehicle user.
	
	• Precondition (SAFETY)
	  ○ There exists an underlying business model supporting such usage-specific driving insurances.

Roles, Stakeholders, Actors	• Driver • Owner • Public Authority • Company Business • Society
Benefits	• Society: Improved compliance to road policy • Driver: More transparent, more fair, more reliable and usage-specific payment for insurances or eco taxes. Ensure compliance to road policy • Company Business: More flexible and real cost-driven insurance models, improved compliance to road policy leading to reduced insurances rates • Public Authority: Reliable logging to enable taxes which are able to influence the driving behaviour • Society: Reduced CO2 emissions and fuel consumption

Involved components	• Communication Unit (CU)
	
	  ○ Global wireless networks (GWN) (UMTS, GSM/GPRS)
	  ○ In-Vehicle networks (IVN) (CAN)
	  ○ User networks (UN) (Bluetooth, USB)
	  ○ In-Vehicle networks (IVN) (CAN, FlexRay)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Secure Memory (SMem)

	• Provider's System Sensors (Motor sensors, wheel rotation sensor) • Electronic Control Units (ECUs) (ABS, instrument cluster) Nomadic Devices (NDs) • Navigation or positioning capability • Human Machine Interface (HMI)

Security aspect	• Threats or potential misuses
	  ○ Unauthorized logging manipulation (vs. integrity/authenticity)
	  ○ Unauthorized logging read-out (vs. privacy)
	  ○ Sensor manipulation for input parameter manipulation (vs. integrity/authenticity)
	  ○ Unauthorized interception of log transmissions to external system (vs. privacy)
	  ○ Unauthorized manipulation of log transmissions to external system (vs. integrity/authenticity)
	  ○ Denial of service of logging and log transmissions to external system (vs. availability)
	• Security Requirements
	  ○ Strong process isolation
	  ○ Secure storage
	  ○ Secure authentication
	  ○ Secure external communication
	  ○ Secure sensor data acquisition

Table 18 UC-PAYD

3.17 **UC Install Application**

Use Case Label & Name	UC-IA: Install application
Domain	Infotainment
Category	Operation
Functional/Technical Category	Platform (involving communication)
Originator	OEM

Operation description	• Pre Condition
	  ○ Installation package of OVERSEE application stored in the memory of a nomadic device (e.g., USB-Stick or mobile phone)
	  ○ Installation package is signed by an eligible organization / person.
	  ○ The public key of the signer is verifiable by the

	OVERSEE platform (e.g., by a verifiable certificate or due to the availability of the authentic public key of the signer within the OVERSEE platform or a corresponding certificate chain with trustworthy root certificate)
	
	• Scenario
	  ○ The driver connects the nomadic device to the OVERSEE platform (e.g., by USB or Bluetooth)
	  ○ The driver starts an application on the OVERSEE platform which has the clearance to install new applications on the OVERSEE platform. (Perhaps a user authentication should be necessary)
	  ○ The installation package on the nomadic device is selected by the driver.
	  ○ The digital signature of the installation package and the approval of the application for the OVERSEE platform will be verified.
	  ○ The new application will be installed on the OVERSEE platform.

Roles, Stakeholders, Actors	• Driver • Software developer or distributor
Benefits	• Driver: Easy installation of recent software applications without costs for data transmission (e.g., by mobile phone networks) • Software developer or distributor: Easy and affordable distribution of innovative software

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN) (UMTS, GSM/GPRS)
	  ○ User networks (UN)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Secure Memory (SMem)
	• Nomadic Devices (NDs)
	• Public Key Infrastructure (PKI)
	• Human Machine Interface (HMI)

Security aspect	• Threats and potential misuses
	  ○ Fraud by vehicle driver to install illegal or harmful software packages
	  ○ Fraud by third parties to install applications without awareness of the driver
	
	• Security requirements
	  ○ Authentication / Integrity

	○ Secure Storage • Security and Dependability objectives

Table 19 UC-IA

3.18 **UC Remote Vehicle Rental**

Use Case Label & Name	*UC-VRE: (Remote) Vehicle Rental*
Domain	Infotainmen
Category	Convenience
Functional/Technical Category	*Application (involving Communication)*
Originator	Third Party
Operation description	• Pre Condition ○ The status of the driving license was already checked by the rental company ○ Established contract between user and rental company ○ Mobile phone with short-range communication capability • Scenario ○ User wish to rent a vehicle at a certain time and place for a defined period (extension of the rental period during the rental should be possible if no conflict with other reservations occur). The rental should be feasible without the involvement of the rental company's office stuff, so fully automatically. ○ The User sends his rental request to the rental company. This could happen, e.g., via the website of the rental company delivered to the mobile phone of the user. (This process is out of the project's scope) ○ The rental company checks the request (e.g., the account of the user) and sends a confirmation including the location of the vehicle and a "secure token" (this token acting like a one-time vehicle key) as well as a PIN which is valid for the whole rental period to the user. (This process is out of project's scope) ○ The rental company sends the PIN (in a secure way) to the rental application which is installed on the OVERSEE platform.

	○ The user sends the "secure token" via, e.g., Bluetooth to the rental application which is installed on the OVERSEE platform in the vehicle. (The transfer should be protected by the application of the HSM-based security functions provided by the OVERSEE platform with an appropriate security protocol.) ○ The user starts the vehicle by entering the PIN in the rental application. ○ During the rental period the rental application stores information about driven distance, fuel consumption, etc. inside the secure storage and informs the driver about the expected costs. ○ At the end of the rental period the billing information will be transferred in a secure and reliable way to the rental company. Variations of this scenario are applicable to classical rental companies and innovative mobility projects like car2go.
Roles, Stakeholders, Actors	• User / Driver • Rental Company • Society
Benefits	• User: Flexible (time and place) car rental • Rental Company: Reduced administrative overhead, better utilization of the rental vehicles, improved service for the customer • Society: Reduced amount of vehicles due to better utilization of the vehicles
Involved components	• Communication Unit (CU) ○ Global wireless networks (GWN) (UMTS, GSM/GPRS) ○ Positioning services (PS) ○ User networks (UN) (Bluetooth) ○ In-Vehicle networks (IVN) (CAN) • Runtime Environment (RE) • Security Module (SMod) • Secure Memory (SMem) • Provider's System • Electronic Control Units (ECUs) • Nomadic Devices (NDs) • Human Machine Interface (HMI)
Security aspect	• Threats and potential misuses ○ Vehicle theft by attacking the vehicle access process ○ Manipulation of vehicle systems ○ Charging frauds by vehicle users ○ Charging frauds by rental company

	• Security requirements
	  ○ Confidentiality
	  ○ Non-Repudiation
	  ○ Authentication
	  ○ Secure Storage
	  ○ Access Control
	
	• Security and Dependability objectives

Table 20 UC-VRE

3.19 **UC Parking Sensor System**

Use Case Label & Name	UC-PSS: Parking Sensor System
Domain	ADAS
Category	Convenience
Functional/Technical Category	Application
Originator	OEM or Third Party
Operation description	Motivation : There are simple parking sensor systems available for purchase, building one ourselves would make a simple use case which is not only useful, but also of relatively low complexity with respect to the applications demands, while allowing to demonstrate the abilities of integrating COTS/FLOSS components (i.e. open-source libraries for signal processing). The safety relevance of this use case is very low, since parking sensor systems are used at low speed. From a real-time perspective it should not be too hard either. The worst case latencies have to be fast compared to the reaction capacity of the driver, which in real world situation can be assumed at 1s [1], so a reaction time in the range of some milliseconds is sufficient. Since there will be no need to access this application from the outside, the security relevance is not very high either, making this a suitable showcase to make publicly available. Operation description : Several sensors (e.g. ultra sound) integrated into the bumper of the car can evaluate the distance from obstacle. If an obstacle is detected a message in send through the in-vehicle

	network The measured value is transmitted to the driver via a display and/or a warning signal.
Roles, Stakeholders, Actors	• Manufacturer • Driver

Benefits	• Benefits for us:
	  ○ From the principle capabilities of the OVERSEE ECU this use case would constitute a basis for more challenging (security and safety wise) applications like automatic parking applications.
	• Benefits for third party manufacturer / end user:
	  ○ No extra ECU needed
	  ○ Less collisions

Involved components	• Runtime Environment (RE) • Sensors (ultra sound) • Human Machine Interface (HMI) (display, speaker)
Security aspect	Very Low, since the only necessary interfaces to the outside world are Sensors (e.g. ultra-sound) and a display to tell the driver how much space he has left, but no communication interface is needed for this use case. Therefore the only thinkable security issue would be, if one of the other applications manipulated the data on the parking sensor system. This will not be possible, since the safety standards (ARINC, AUTOSAR) require the operating system to strictly partition the applications in time and memory. Therefore another application could never succeed in manipulating the data of the parking sensor system.
Testing Requirements	We believe that this use case can be tested easily on a real car, without big investments. Ultra-Sound sensors from commercial parking sensor systems could be taken and connected to the OVERSEE ECU. • See Appendix 5.1 Test Environment

Table 21 UC-PSS

3.20 **UC Electronic (Driver) Logbook**

Use Case Label & Name	UC-ELB: Electronic (Driver) Logbook
Domain	Infotainment
Category	Convenience
Functional/Technical Category	Application involving Communication
Originator	Third Party together with Public Authority
Operation description	The capability for secure recording of driving data will be used to store start and end points of journeys and the driven distances together with some information provided by the vehicle driver (e.g., on the purpose of the trip business / private etc.). This will lead to a reliable driver log book which can be used for tax declaration (business car) and settlement purposes (e.g., for a customer or driven distances with a private car on business reasons) • Precondition ○ There exists legitimacy and a business models supporting such electronic log book.
Roles, Stakeholders, Actors	• Driver • Company Business / Public Authority
Benefits	• Driver: More transparent, more reliable and simple logging enables flexible models of vehicle usage and reduce the effort for settlement • Company Business / Public Authority: More transparent, more reliable and simple logging for settlement

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN)
	  ○ Positioning services (PS)
	  ○ User networks (UN)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Secure Memory (SMem)
	• Provider's System
	• Nomadic Devices (NDs)
	• Human Machine Interface (HMI)

Security aspect	• Potential misuses (vs. security objectives)
	  ○ Unauthorized logging manipulation (vs. integrity/authenticity)
	  ○ Unauthorized logging read-out (vs. privacy)

	○ Sensor manipulation for input parameter manipulation (vs. integrity/authenticity) ○ Unauthorized interception of log transmissions to external system (vs. privacy) ○ Unauthorized manipulation of log transmissions to external system (vs. integrity/authenticity) ○ Denial of service of logging and log transmissions to external system (vs. availability)

Table 22 UC-ELB

3.21 **Web 2.0 For Cars**

Use Case Label & Name	UC-WEB: Web 2.0 for Cars
Category	Convenience
Functional/Technical Category	Application involving Communication
Originator	Third Party
Operation description	OVERSEE provides in-vehicle infrastructure to integrate current and upcoming interactive web 2.0 applications to integration "mobile information" such as current location, destination or current picture or thoughts to interactive communities such as flickr, facebook, twitter etc. • Precondition ○ Interactive web application can make reasonable benefits from processing "mobile information" ○ There exists an secure external communication channel to the corresponding web application
Roles, Stakeholders, Actors	• Driver • Company Business / Public Authority • Third Party
Benefits	• Driver / passenger: ○ Extend your social networks into automotive world, inform your "friends" about your "vehicular activities" and get location-based relevant information (e.g., find nearby friends, twitter next speed trap or traffic jam, and all kind of location-based services) ○ Build new automotive networks (“CarBook”) automatically posting your current mileage, visited locations, fuel consumption etc. on a web page like

	Facebook • Company Business: ○ Improve/extend your web application (usability), run LBS/mobile business models, create new LBS/mobile web communities (“Carbook”, “Car Twitter” etc.)

Involved components	• Communication Unit (CU)
	  ○ Global wireless networks (GWN)
	  ○ Positioning services (PS)
	  ○ User networks (UN)
	• Runtime Environment (RE)
	• Security Module (SMod)
	• Secure Memory (SMem)
	• Provider’s System
	• Nomadic Devices (NDs)
	• Human Machine Interface (HMI)

Security aspect	• Potential misuses (vs. security objectives)
	  ○ Unauthorized interception of transmissions between vehicle and web application (vs. privacy)
	  ○ Unauthorized manipulation of transmissions between vehicle and web application (vs. integrity/authenticity)
	  ○ Denial of service of transmissions between vehicle and web application (vs. availability)

Table 23UC-WEB

4 Conclusion

This document described a representative subset of the Use Cases identified by the OVERSEE partners. The identification relied on a collaborative process in different steps.

During this process 72 use cases have been identified from other projects, stakeholder expectations, and recommendations of the EU or exploitation interests. After a consolidation and detailed description phase, the number has been reduced to 57.

In order to provide a more readable deliverable, a subset of 20 use cases has been selected to highlight the versatility of the possible applications as well as to cope with the major expectation of each partner (who represent different point of view). Selection criteria for each one cover security aspect, functional category or automotive stakeholder in-use category as well as taking into account current and future applications.

The use cases identified during this first task, as well as the expertise of the partners is an input for the coming task about functional and non-functional requirements (D1.2/1.4 and D1.3/1.5). The consolidated list of use cases will also be used as basis to define a set of proof-of-concept use cases in WP5.

References

[1] SEVECOM Project. SEVECOM : Secure Vehicle Communication. [Online]. HYPERLINK "http://www.sevecom.org/" http://www.sevecom.org/

[2] EVITA Partners. (2008-2011) EVITA (E-safety Vehicle Intrusion protected Applications) research project. [Online]. HYPERLINK "www.evita-project.org" www.evita-project.org

[3] TECOM Consortium. Tecom Project webpage. [Online]. HYPERLINK "http://www.tecom-itea.org/" http://www.tecom-itea.org/

5 Appendix

5.1 Annex: Test Environment

The selected use cases intend to highlight the specific capabilities of OVERSEE while at the same time serving as a flexible basis for developing other concepts - in this sense the use cases described here should serve as ”templates”. Furthermore, we propose a test environment, which allows implementing all of them with minimum hardware costs, by connecting to the car’s electronic system via the OBD3 interface.

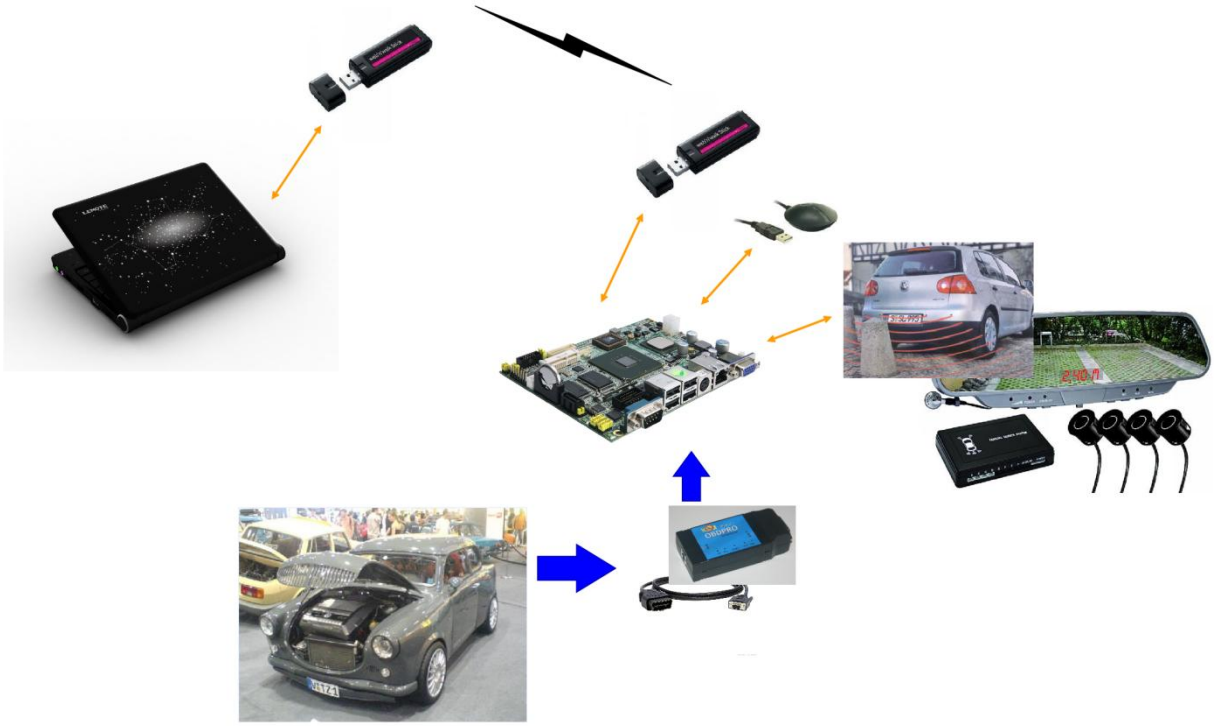

Figure 1 : Test Environment

OBD3 is favoured for regulatory reasons - OBD3 specifies remote connectivity - thus constitutes a good basis for developing such a concept. At the same time it provides a plethora of well-defined data interfaces and a clear data communication protocol that would allow OVERSEE to focus on the core technologies while still being a highly flexible basis to spin-off further development. We tried to identify use cases with small safety relevance but a big demand for security, since it is more realistic to be able to implement those applications than for example a motor control. While safety should not be out of the picture - the clear focus on security issues should also be transported in the respective use cases.

As mentioned above, the test cases proposed by OpenTech, are built on the simple, inexpensive test environment shown in Figure Figure 1. This test environment consists of an OVERSEE ECU that is connected to the car (e.g. via the On-board Diagnosis port - OBD3).

Furthermore, the OVERSEE ECU is equipped with additional hardware (e.g. GPS receiver, some sensors) and a wireless connection adapter (e.g. UMTS, GPRS etc).

By providing a set of open interfaces to the outside world, and to the open- source development community - OVERSEE can ensure safety and security by adequate isolation of internal buses from externally accessible buses. Thus OVERSEE's security- gateway functionality can be demonstrated in an obvious way while at the same time providing a flexible interface to a large set of COTS/FLOSS components potentially of interest.

The wireless connection can be used to access the OVERSEE ECU remotely and access test data, upload new test applications, reset them, and so on - with all the security issues being fully exposed. Some use cases / test applications that we think are possible to implement within the OVERSEE project are shortly described in the following sections. For early stage testing, it might be possible connect the OVERSEE ECU to a PC that replays the recorded information to the OVERSEE ECU, instead of a real car (i.e. based on recorded data sets by VW). This we believe further would allow OVERSEE partners to get hands-on experience with the automotive domain at an early project state, especially for project partners with little experience in automotive domain.

We would like to emphasise that the essence of this use case proposal is not the specific proposed application, but rather the principle setup of a low-cost environment that would allow propagation into an open-source community.

5.2 Annex: Use Cases Process Tables

This annex is composed of the table of the use cases illustrating the different steps of the collaborative process resulting in this document.

- Step 1: First list of use cases - Table 24 Step 1: First List of Use Cases
- Step 2: List of the use cases after a first consolidation pass - Table 25 Step 2: List of the Use Cases after a First Consolidation Pass
- Step 3: List of use cases with additional use cases - Table 26 List of Use Cases with Additional Use Cases
- Step 4: Final consolidated list of use cases - Table 27 Final Consolidated List of Use Cases
- Step 5: Ranking by the partners and the selected 20 use uases - Table 28 Ranking by the Partners and Selected 20 Use Cases

Trialog
Safety reaction: Active brake (V2V)
Local Danger Warning from other Cars (V2V)
Traffic Information from other Entities (V2V)
Messages lead to safety reaction (V2V)
Local Danger Warning to other Cars (V2V)
Traffic Information to other Entities (V2V)
eTolling (V2I)
eCall (V2I)
Remote Car Control (V2I)
Point of Interest (V2I)
Install applications (V2D)
Secure Integration (V2D)
Personalize the car (V2D)
Replacement of Engine ECU (Aftermarket)
Installation Car2x Unit (Aftermarket)
Remote Diagnosis (Diagnosis)
Remote Flashing (Diagnosis)
Flashing per OBD (Diagnosis)
SOS services (1)
Stolen vehicles tracking (2)
Map download/update (3)
Intersection collision warning (4)
Vehicle-based road condition warning (4)
Electronic license plate (5)
Road surface conditions to TOC (6)
Software update/flashing (7)
Emergency vehicle signal pre-emption (8)
Work zone warning (8)
Siegen
Electronic Toll Collection systems (e.g. for influence traffic demand)
ITS applications for journey planning (e.g. dynamic in-vehicle navigation)
Integrating nomadic devices

eCall
“plug and play” integration of future new or upgraded applications, software download (app store)
Electronic vehicle identification
User specific application e.g. application for a fictive cash transport provider (see proposal)
Improvement of road safety by secure and non-deniable recording of driving behaviour and providing this information to insurance companies with special driving behaviour rates (Improving safety)
Reducing of CO2 emissions by secure and non-deniable recording fuel consumption, driving behaviour and data from motor sensor to enable fair eco-taxes (personal environment account see press release)
Remote diagnosis and service support
Remote software updates
Remote door opener
Remote feature activation
Vehicle-to-home communication/synchronization (garage opener, music/map downloads, driving data upload such as driven distance, fuel consumption)
Remote vehicle rental
Extension or replacement of the gateway component in modern vehicles
Digital Rights Management for vehicular applications (e.g. different driving profiles – gas saving versus fast driving, different rights for different drivers)
Theft intervention
Hazard warning between vehicles
Cooperative awareness
Dynamic Traffic Management
Point-to-point connectivity across multiple vehicles
Electronic driver logbook
MisUseCase: Causing accidents, traffic jam and aggro by faking or manipulating messages
MisUseCase: Warn other vehicles concerning speed cameras
MisUseCase: Unauthorized tacking or locating of vehicles
Escrypt
OEM-AppStore for 3rd-Party Infotainment (e.g. navigation, POI, parking lots, tourist info)
Vehicle access control (e.g. on-site parking etc.)

Interactive Web 2.0
Error reporting with online help incl. position finding or "Next-Open-Garage-Around" / Request for Automobile Club Assistance
(Anonymous) live remote check for OEM or component supplier
Anonymous and automated pushing of position and velocity to ITS for traffic reports or active ITS management (traffic lights etc.)
M-Commerce (Access of any kind, gas station, drive-through-X, info's.)
Environmental accounting, CO2-Tracking etc.
Remote access for a technical supervisory association
Pay-As-You-Drive: Assurance, taxes, road charge. (e.g., Pay =f(location, time, velocity, target, loading, number of passengers, emission))
Online-Park ticket (GPS-Position + m-Commerce + WLAN-request/check)
Parking place reservation
Car finder (e.g. via mobile phone)
Active theft management (e.g. remote velocity reduction.)
Car-sharing, Rent-a-car: on-demand activation of available cars

Table 24 Step 1: First List of Use Cases

UC	Similar UC (same concern but different treatment)	Meta-UC (include more than one other use cases)
eTolling (V2I)		
eCall (V2I)		
Remote Car Control (V2I) ex: door opener		
Secure Integration (V2D) (of nomadic devices)		
Stolen vehicles tracking (2)	Active theft management (e.g. remote velocity reduction.)	
Electronic license plate (5)		
Remote Diagnosis (Diagnosis)		
Remote Flashing (Diagnosis) ↔Software update/flashing (7)		
Reducing of CO2 emissions by secure and non-deniable recording fuel consumption, driving behaviour and data from motor sensor to enable fair eco-taxes (personal environment account see press release)		
Local Danger Warning from other Cars (V2V)		
Local Danger Warning to other Cars (V2V)		
Vehicle-based road condition warning		Hazard warning between vehicles
Emergency vehicle signal pre-emption (8)		
Work zone warning (8)		
Intersection collision warning (4)		
Traffic Information to other Entities (V2V)		
Road surface conditions to TOC (6)		Cooperative awareness
Traffic Information from other Entities (V2V)		
Point of Interest (V2I)	OEM-AppStore for 3rd-Party Infotainment (e.g. navigation, POI, parking lots, tourist info)	
Dynamic Traffic Management	Anonymous and automated pushing of position and velocity to ITS for traffic reports or active ITS management (traffic lights etc.)	
Safety reaction: Active brake (V2V)		
Installation Car2x Unit (Aftermarket)		
Flashing per OBD (Diagnosis)		
SOS services (1)		
Map download/update (3)		
Messages lead to safety reaction (V2V)		
Install applications (V2D)		
Personalize the car (V2D)		
Replacement of Engine ECU (Aftermarket)		
Electronic driver logbook		
Remote feature activation		

Vehicle-to-home communication/synchronization (garage opener, music/map downloads, driving data upload such as driven distance, fuel consumption)		
Remote vehicle rental		
Extension or replacement of the gateway component in modern vehicles		
Digital Rights Management for vehicular applications (e.g. different driving profiles – gas saving versus fast driving, different rights for different drivers)		
Point-to-point connectivity across multiple vehicles		
MisUseCase: Causing accidents, traffic jam and aggro by faking or manipulating messages		
MisUseCase: Warn other vehicles concerning speed cameras		
MisUseCase: Unauthorized tacking or locating of vehicles		
Application for cabs (e.g., to handle incoming trips by the cab centre, storing invoices in a reliable manner for tax audit) Proposal		
Application for parcel services (handle the tour data and customer information including updates by the centre for spontaneous pickups) - Siegen		
Pay-As-You-Drive: Assurance, taxes, road charge. (e.g., Pay =f(location, time, velocity, target, loading, number of passengers, emission)) ???		
Vehicle access control (e.g. on-site parking etc.)		
Interactive Web 2.0		
Error reporting with online help incl. position finding or "Next-Open-Garage-Around" / Request for Automobile Club Assistance		
(Anonymous) live remote check for OEM or component supplier		
M-Commerce (Access of any kind, gas station, drive-through-X, info's)		
Remote access for a technical supervisory association		
Online-Park ticket (GPS-Position + m-Commerce + WLAN-request/check)		
Parking place reservation - Heavy Trucks (From Proposal)		
Car finder (e.g. via mobile phone)		

Table 25 Step 2: List of the Use Cases after a First Consolidation Pass

UC	Similar UC (same concern but different treatment)	Meta-UC (include more than one other use cases)
Parking lot reservation		
eTolling (V2I)		
eCall (V2I)		
Remote Car Control (V2I) ex: door opener		
Secure Integration (V2D) (of nomadic devices)		
Stolen vehicles tracking (2)	Active theft management (e.g. remote velocity reduction.)	
Electronic license plate (5)		
Remote Diagnosis (Diagnosis)		
Remote Flashing (Diagnosis) ↔Software update/flashing (7)		
Reducing of CO2 emissions by secure and non-deniable recording fuel consumption, driving behaviour and data from motor sensor to enable fair eco-taxes (personal environment account see press release)		
Local Danger Warning between vehicle Cars (V2V)		
Vehicle-based road condition warning		Hazard warning between vehicles
Emergency vehicle signal pre-emption (8)		
Work zone warning (8)		
Intersection collision warning (4)		
Traffic Information between Entities (V2V)		
Road surface conditions to TOC (6)		Cooperative awareness
Point of Interest (V2I)	OEM-AppStore for 3rd-Party Infotainment (e.g. navigation, POI, parking lots, tourist info)	
Dynamic Traffic Management	Anonymous and automated pushing of position and velocity to ITS for traffic reports or active ITS management (traffic lights etc.)	
Safety reaction: Active brake (V2V)		
Installation Car2x Unit (Aftermarket)		
Flashing per OBD (Diagnosis)		
SOS services (1)		
Map download/update (3)		
Messages lead to safety reaction (V2V)		
Install applications (V2D)		
Personalize the car (V2D)		
Replacement of Engine ECU (Aftermarket)		
Electronic driver logbook		
Remote feature activation		

Vehicle-to-home communication/synchronization (garage opener, music/map downloads, driving data upload such as driven distance, fuel consumption)		
Remote vehicle rental		
Extension or replacement of the gateway component in modern vehicles		
Digital Rights Management for vehicular applications (e.g. different driving profiles – gas saving versus fast driving, different rights for different drivers)		
Point-to-point connectivity across multiple vehicles		
MisUseCase: Causing accidents, traffic jam and aggro by faking or manipulating messages		
MisUseCase: Warn other vehicles concerning speed cameras		
MisUseCase: Unauthorized tacking or locating of vehicles		
Application for cabs (e.g., to handle incoming trips by the cab centre, storing invoices in a reliable manner for tax audit) Proposal		
Application for parcel services (handle the tour data and customer information including updates by the centre for spontaneous pickups) - Siegen		
Pay-As-You-Drive: Assurance, taxes, road charge. (e.g., Pay =f(location, time, velocity, target, loading, number of passengers, emission)) ???		
Vehicle access control (e.g. on-site parking etc.)		
Interactive Web 2.0		
Break-Down-Call		
Error reporting with online help incl. position finding or "Next-Open-Garage-Around" / Request for Automobile Club Assistance		
(Anonymous) live remote check for OEM or component supplier		
M-Commerce (Access of any kind, gas station, drive-through-X, info's)		
Remote access for a technical supervisory association		
Online-Park ticket (GPS-Position + m-Commerce + WLAN-request/check)		
Parking place reservation - Heavy Trucks (From Proposal)		

Car finder (e.g. via mobile phone)		
Software Test Container		
Monitoring System		
Parking Sensor System		

Table 26 List of Use Cases with Additional Use Cases

UC	Similar UC (same concern but different treatment)	Meta-UC (include more than one other use cases)
Parking lot reservation		
eTolling (V2I)		
eCall (V2I)		
Remote Car Control (V2I) ex: door opener		
Secure Integration (V2D) (of nomadic devices)		
Stolen vehicles tracking (2)	Active theft management (e.g. remote velocity reduction.)	
Electronic license plate (5)		
Remote Diagnosis (Diagnosis)		
Remote Flashing (Diagnosis) ↔Software update/flashing (7)		
Reducing of CO2 emissions by secure and non-deniable recording fuel consumption, driving behaviour and data from motor sensor to enable fair eco-taxes (personal environment account see press release)		
Local Danger Warning between vehicle Cars (V2V)		
Vehicle-based road condition warning		Hazard warning between vehicles
Emergency vehicle signal pre-emption (8)		
Work zone warning (8)		
Intersection collision warning (4)		
Traffic Information between Entities (V2V)		
Road surface conditions to TOC (6)		Cooperative awareness
Point of Interest (V2I)	OEM-AppStore for 3rd-Party Infotainment (e.g. navigation, POI, parking lots, tourist info)	
Dynamic Traffic Management	Anonymous and automated pushing of position and velocity to ITS for traffic reports or active ITS management (traffic lights etc.)	
Safety reaction: Active brake (V2V)		
Installation Car2x Unit (Aftermarket)		
Flashing per OBD (Diagnosis)		
SOS services (1)		
Map download/update (3)		
Messages lead to safety reaction (V2V)		
Install applications (V2D)		
Personalize the car (V2D)		

Replacement of Engine ECU (Aftermarket)		
Electronic driver logbook		
Remote feature activation		
Vehicle-to-home communication/synchronization (garage opener, music/map downloads, driving data upload such as driven distance, fuel consumption)		
Remote vehicle rental		
Extension or replacement of the gateway component in modern vehicles		
Digital Rights Management for vehicular applications (e.g. different driving profiles – gas saving versus fast driving, different rights for different drivers)		
Point-to-point connectivity across multiple vehicles		
MisUseCase: Causing accidents, traffic jam and aggro by faking or manipulating messages		
MisUseCase: Warn other vehicles concerning speed cameras		
MisUseCase: Unauthorized tacking or locating of vehicles		
Application for cabs (e.g., to handle incoming trips by the cab centre, storing invoices in a reliable manner for tax audit) Proposal		
Application for parcel services (handle the tour data and customer information including updates by the centre for spontaneous pickups) - Siegen		
Pay-As-You-Drive: Assurance, taxes, road charge. (e.g., Pay =f(location, time, velocity, target, loading, number of passengers, emission)) ???		
Vehicle access control (e.g. on-site parking etc.)		
Interactive Web 2.0		
Break-Down-Call		
Error reporting with online help incl. position finding or "Next-Open-Garage-Around" / Request for Automobile Club Assistance		
(anonymous) live remote check for OEM or component supplier		

M-Commerce (Access of any kind, gas station, drive-through-X, infos..)		
Remote access for a technical supervisory association		
Online-Park ticket (GPS-Position + m-Commerce + WLAN-request/check)		
Parking place reservation - Heavy Trucks (From Proposal)		
Car finder (e.g.. via mobile phone)		
Software Test Container		
Monitoring System		
Parking Sensor System		

Table 27 Final Consolidated List of Use Cases

Use Case Name	Usiegen	Escrypt	FOKUS	TUB	UPV	VW	Otech	Trialog	Total
Parking lot reservation	13	4	10	5	10	7		13	62
e-Toll	14	1			14	2	13	14	58
eCall	15	2			6		15	15	53
Secure Integration (V2D)		9	15	11		8		9	52
Emergency vehicle signal pre-emption -- Emergency vehicle signal pre-emption 2	6		14	13				12	45
Meta UC : Hazard Warning between Vehicle	7	11	45	39	8	12	0	10	132
Stolen vehicles tracking	9				11	10		8	38
Traffic Information between Entities (V2V) *similar to* Extended Floating Car Data	8		7	14				7	36
Safety reaction: Active brake (V2V)	5		1	1		13		11	31
Personalize the car (V2D)		14		2	1	6		4	27
Car finder (e.g., via mobile phone)					13	14			27
Electronic license plate		10	8				8		26
Dynamic Traffic Management	4	3			15			1	23
Break-Down-Call-Live-Check		7			3	11			21
Remote Car Control(V2I)		8	5	7					20
PayAsYouDrive (Road Safety & Eco)	21				19			6	46
Install applications (V2D)		15			2				17
Remote vehicle rental	1					3	11	2	17
Parking Sensor System						1	12	3	16
Electronic driver logbook			2	6			7		15
Map download/update						5	5	5	15
Extended Floating Car Data						15			15
Meta-UC Record Driving Data including		13							13
Meta-UC Cooperative awareness including		12							12
Remote Flashing (Diagnosis) ↔ Software update/flashing							10		10
Vehicle access control		5			5				10

Interactive Web 2.0		6			4				10
Point of Interest (V2I)	3						6		9
Software Test Container							9		9
WiFi hotspot						9			9
M-Commerce (Access of any kind, gas station, drive-through-X, info's)		8							8
Road surface conditions to TOC			4	3					7
MisUseCase: Causing accidents, traffic jam and aggro by faking or manipulating messages			3	4					7
Remote feature activation	2					4			6
Vehicle Blackbox	12				2	-28	14		0
Meta-UC Hazard warning between vehicles including									0
Flashing per OBD (Diagnosis)									0
Replacement of Engine ECU (Aftermarket)									0
Vehicle-to-home-to-business									0
Point-to-point connectivity across multiple vehicles									0
Application for cabs (e.g., to handle incoming trips by the cab centre, storing invoices in a reliable manner for tax audit) Proposal									0
Application for parcel services									0
Monitoring System									0
Request for Automobile Club Assistance									0
Meta-UC System Management									0
Deployment									0
Mode Change									0

Table 28 Ranking by the Partners and Selected 20 Use Cases