Deliverable **D4.2** /

Legal Requirements for AD Piloting and Cyber Security Analysis

Version: 1.2 Final

Dissemination level: PU

Lead contractor: TME

Version date: 10.05.2019

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 723051.

Document information

Authors

Nicolas Vignard – TME

Anastasia Bolovinou – ICCS

Angelos Amditis – ICCS

Gerhard Wallraf – FEV

Obaid Ur-Rehman – FEV

Markus Kremer – FEV

Arshad Moilingal Ziyad – FEV

Al Tariq Sheik – WMG

Ugur-Ilker Atmaca – WMG

Mehrdad Dianati – WMG

Viktoria Mayr – BMW

Pandeli Borodani – CRF

John-Fredrik Grönvall – SAFER

Arjan Van Vliet – RDW

Ashfaqur Rahman, JLR

Yves Page – REN

Tom Gasser – BASt

Coordinator

Aria Etemad

Volkswagen Group Research

Hermann-Münch-Str. 1

38440 Wolfsburg

Germany

Phone: +49-5361-9-13654

Email: aria.etemad@volkswagen.de

Project funding

Horizon 2020

ART-02-2016 – Automation pilots for passenger cars

Contract number 723051

www.L3Pilot.eu

Legal Disclaimer

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The consortium members shall have no liability for damages of any kind including, without limitation, direct, special, indirect, or consequential damages that may result from the use of these materials, subject to any liability which is mandatory due to applicable law. Although efforts have been coordinated, results do not necessarily reflect the opinion of all members of the L3Pilot consortium.

Table of Contents

List of Figures

List of Tables

1 Introduction

1.1 L3 Pilot at a Glance

1.1.1 Motivation for the L3Pilot project

Over the years, numerous projects have paved the way for automated driving (AD). Significant progress has been made, but AD is not yet ready for market introduction. Nonetheless, the technology is rapidly advancing and is currently at a stage that justifies automated driving tests in large-scale pilot programmes.

L3Pilot is taking the final steps before the introduction of automated cars in everyday traffic. Drivers are familiar with Advanced Driver Assistance Systems (ADAS), and numerous vehicles are equipped with ADAS.

The issues of automation will not be resolved simply by integrating more and better technology. This topic needs above all a focus on user behaviour with automated driving systems. The key to the success of AD on the market will depend on user acceptance as well as on an understanding of the legal restrictions, which first need to be discussed and resolved on a broad level.

The idea of a vehicle controlling itself by computer creates fears among the general population, not unlike those in the 1800s when the motor vehicle was first introduced. This lack of acceptance may hinder the introduction of driver assistance systems with automation despite their obvious benefits for safety and efficiency. In order to overcome public concerns, automated vehicles (AV) need to be designed according to user needs, otherwise they will not be accepted.

L3Pilot differs from earlier and ongoing EU-funded projects, in that AD systems will influence societies and peoples' lives far more greatly than all previous automotive innovations since the introduction of the mass-produced automobile more than one hundred years ago.

1.1.2 L3Pilot objectives

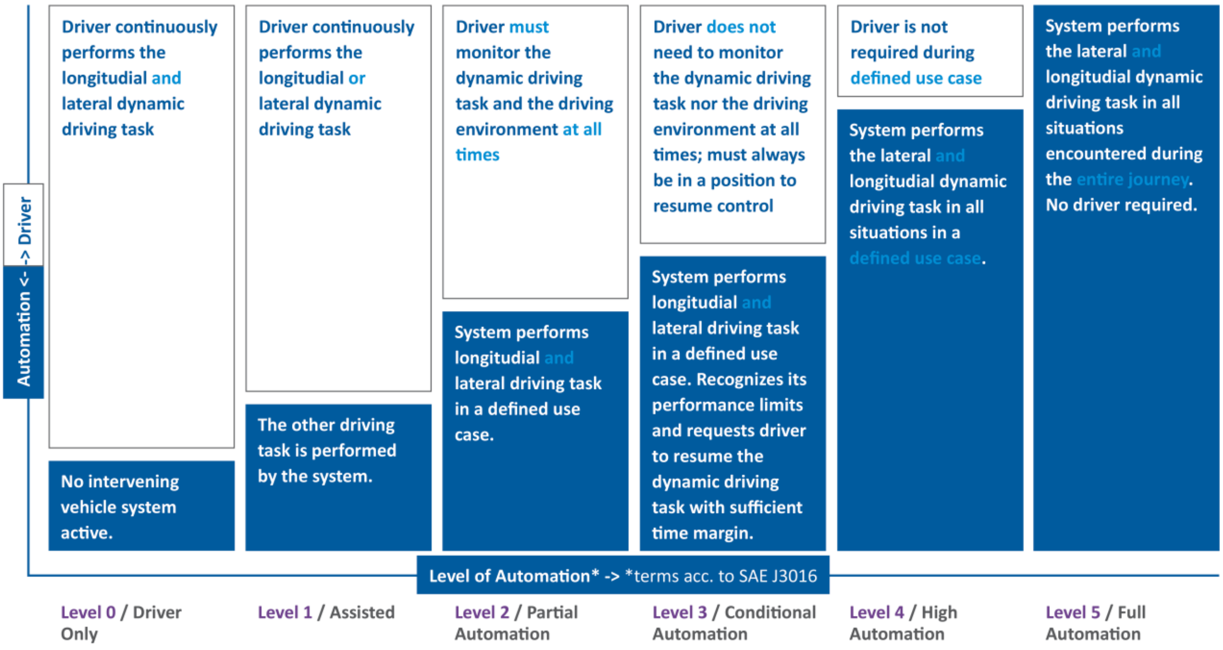
The overall objective of the L3Pilot project is to test and study the viability of automated driving as a safe and efficient means of transportation and to explore and promote new service concepts to provide inclusive mobility.

AD technology has matured to a level that calls for a final phase of road tests to answer the key questions before market introduction. These newly-attained levels of maturity will ensure an appropriate assessment of the impact of AD, the processes both inside and outside the vehicles, the means of ensuring vehicle security, the evaluation of societal impacts, and the emerging business models.

Recent work indicates the means by which driver assistance systems and AD functions can best be validated: by means of extensive road tests, with a sufficiently long operation time, to allow extensive interaction with the driver and testable functions. The project will use large-scale testing and piloting of AD with developed SAE Level 3 (L3) functions (Figure 1.1) exposed to different users and mixed traffic environments, including conventional vehicles and vulnerable road users (VRUs), along different road networks. Level 4 (L4) functions and connected automation will also be assessed.

The data collected in these extensive pilot programmes will support the main aims of the project to:

- Lay the foundation for the design of future, user-accepted, L3 and L4 systems, to ensure their commercial success. This will be achieved by assessing user reactions to, experiences of, and preferences for the AD systems' functionalities.
- Enable non-automotive stakeholders, such as authorities and certification bodies, to prepare measures that will support the uptake of AD, including updated regulations for the certification of vehicle functions with a higher degree of automation, as well as incentives for the user.
- Create unified de-facto standardized methods to ensure further development of AD applications (Code of Practice).
- Create a large database to enable simulation studies of the performance of AD over time that cannot be investigated in road tests, due to the time and effort needed. The data will be one product of the pilots.



Driver continuously performs the longitudinal and lateral dynamic driving task

No intervening vehicle system active.

Level 0 / Driver Only

Driver continuously performs the longitudinal or lateral dynamic driving task

The other driving task is performed by the system.

Level 1 / Assisted

Driver must monitor the dynamic driving task and the driving environment at all times

System performs longitudial and lateral driving task in a defined use case.

Level 2 / Partial Automation

Driver does not need to monitor the dynamic driving task nor the driving environment at all times; must always be in a position to resume control

System performs longitudial and lateral driving task in a defined use case. Recognizes its performance limits and requests driver to resume the dynamic driving task with sufficient time margin.

Level 3 / Conditional Automation

Driver is not required during defined use case

System performs the lateral and longitudial dynamic driving task in all situations in a defined use case.

Level 4 / High Automation

System performs the lateral and longitudial dynamic driving task in all situations encountered during the entire journey. No driver required.

Level 5 / Full Automation

Figure 1.1: SAE Levels of driving automation J3016 (Copyright 2014 SAE International).

The consortium addresses the four major technical and scientific objectives listed below:

1. Create a standardized Europe-wide piloting environment for automated driving.
2. Coordinate activities across the piloting community to acquire the required data.
3. Pilot, test, and evaluate automated driving functions and connected automation.
4. Innovate and promote AD for wider awareness and market introduction.

1.1.3 Approach and scope

The L3Pilot project will focus on large-scale piloting of ADFs, primarily L3 functions, with additional assessment of some L4 functions. The key in testing is to ensure that the functionality of the systems used is exposed to variable conditions and that performance is consistent, reliable, and predictable. This will enhance a successful experience for the users (Figure 1.2). A good experience of using AD will accelerate acceptance and adoption of the technology and improve the business case to deploy AD.

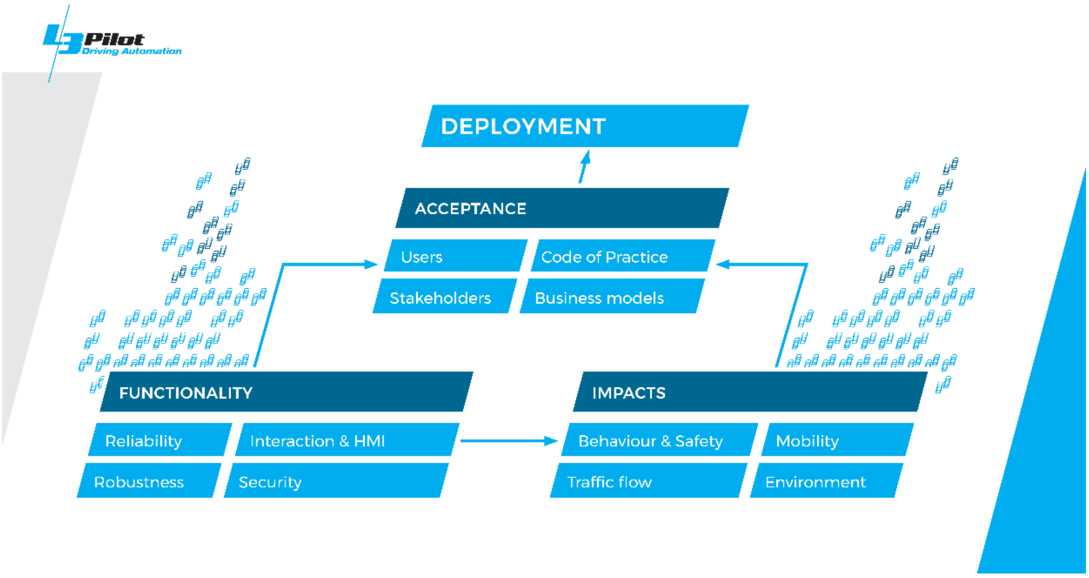
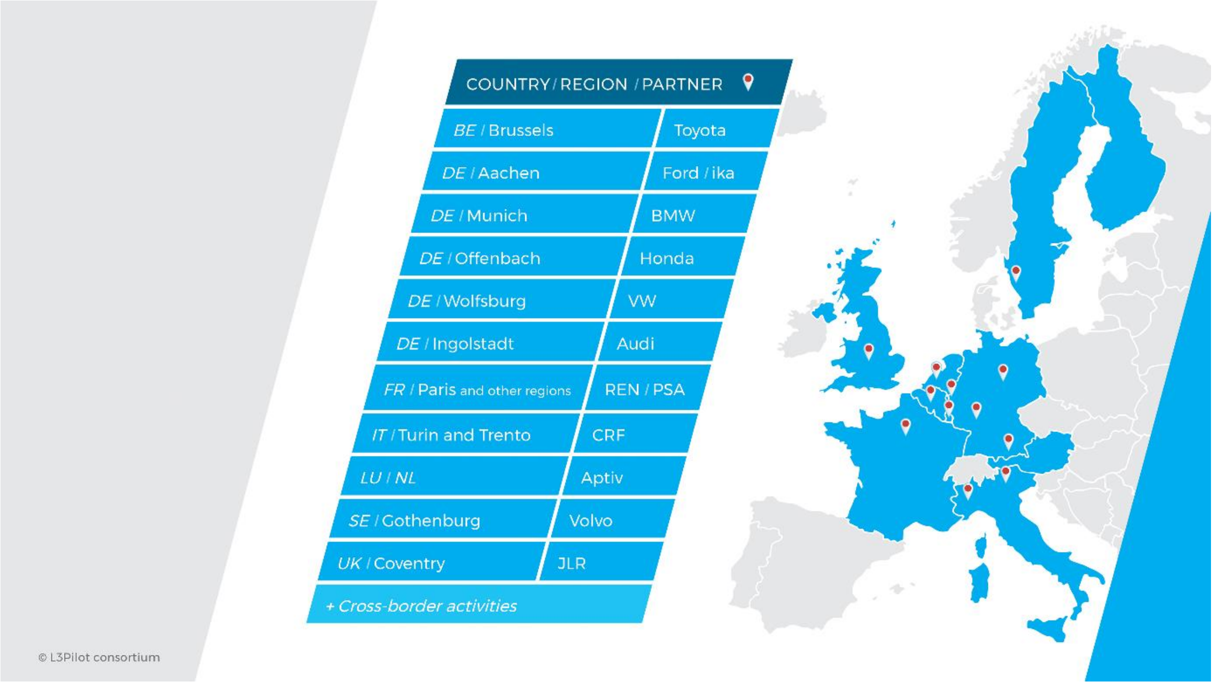


Figure 1.2: L3Pilot approach and the mechanism for deployment.

The L3Pilot consortium brings together stakeholders from the entire value chain, including: OEMs, suppliers, academic institutes, research institutes, infrastructure operators, governmental agencies, the insurance sector, and user groups. More than one thousand users will test approximately one hundred vehicles across Europe with bases in ten European countries, including: Austria, Belgium, Finland, France, Germany, Italy, Luxembourg, the Netherlands, Sweden, Spain, and the United Kingdom, as shown in Figure 1.3. The project will last for 48 months and includes 18 months of road tests.



COUNTRY / REGION	PARTNER
BE / Brussels	Toyota
DE / Aachen	Ford / ika
DE / Munich	BMW
DE / Offenbach	Honda
DE / Wolfsburg	VW
DE / Ingolstadt	Audi
FR / Paris and other regions	REN / PSA
IT / Turin and Trento	CRF
LU / NL	Aptiv
SE / Gothenburg	Volvo
UK / Coventry	JLR
+ Cross-border activities	

© L3Pilot consortium

Figure 1.3: L3Pilot testing areas.

Since the development of ADF, especially at SAE L3, is fairly far advanced, the aim is not only to pilot the functions, but also to study user preferences, reactions, and willingness to use vehicles equipped with AD applications. This information has led the consortium to create plans for the market introduction of AD. The L3Pilot concept can be split into the following two parallel, but intertwined, major activities:

(i) Development of test and evaluation methodologies, and actual testing and evaluation of L3 and L4 ADFs, to answer the call text open questions. In this scientific part, a variety of controlled experiments will be carried out in the three pilot areas shown above.

(ii) Promotion of the project work for maximum impact. This includes dissemination of the project results and communication to the public, through showcases, to accelerate deployment of AD. The planned showcases are:

- Showcase 1: Dynamic pit stop – Software Defined Vehicles (SDV).
- Showcase 2: L4V2X – connected automated vehicles.
- Showcase 3: Urban driving + automated parking.
- Showcase 4: Cross-border driving – highway automation.

1.1.4 Methodology and evaluation

The project follows the FESTA V process methodology of setting up and implementing tests, and adapting the methodology to suit L3Pilot needs, with the four main pillars as follows: (i) prepare, (ii) drive, (iii) evaluate, and (iv) address legal and cyber security aspects. FESTA was originally created as an ADAS testing methodology to be used in FOTs. L3Pilot will adapt it, however, to the piloting of ADFs.

When functions and use cases have been determined, research questions (RQs) and hypotheses (HYPs) will be formulated. The piloting will mainly focus on RQs and HYPs in four impact areas: (i) safety (ii) mobility (iii) efficiency, and (iv) environment. Additional evaluation areas will be carried out separately to address issues such as legal aspects and cyber security, as well as user evaluation and acceptance.

In the evaluation stage, a holistic approach will be used by analysing different aspects of AD based on real-world driving data. As such, the approach will follow FESTA evaluation domains: technical, user acceptance, driving and travel behaviour, impact on traffic, and societal impacts (Figure 1.4).

However, in addition to different evaluation aspects, a third dimension is needed. For instance, the analysis of driving situations is locally limited to the surrounding traffic. Hence, this is an analysis on single vehicle and fleet levels, whereas a European level is required, using aggregated data. The holistic evaluation approach of L3Pilot will consider aspects in all three dimensions. Investigating different fleets will allow L3Pilot to analyse intercultural differences in the interaction with AD applications. The evaluation will also take into account that the test vehicles are not market-ready products.

Technical analysis will focus on the situations in which AD functions operate outside their specifications, as well as their misuse and operational limits due to environmental conditions. Transition of control from the vehicle to the driver will focus on timing and causes of transition.

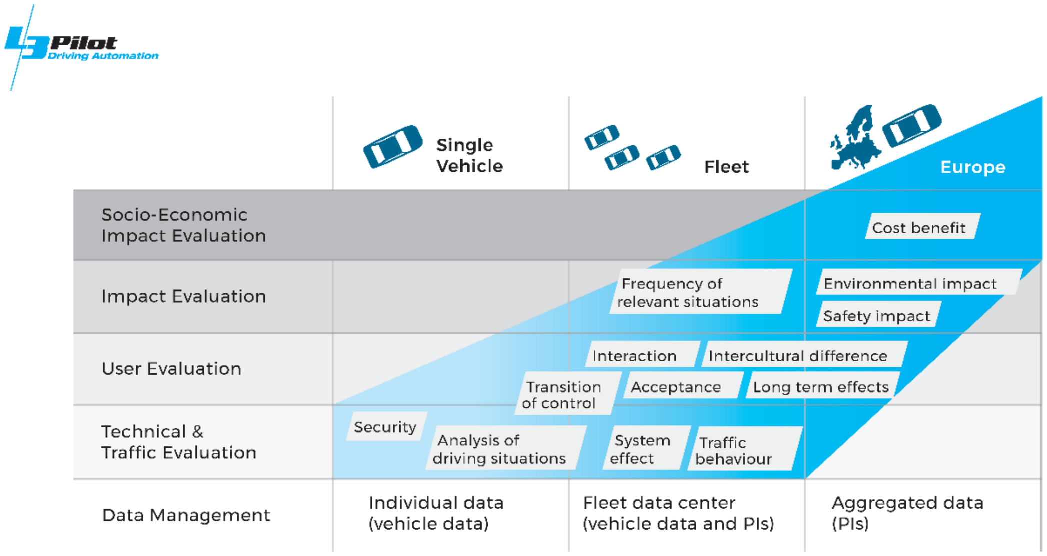


Figure 1.4: Considered evaluation aspects depending on the level of traffic and evaluation domain.

1.2 Objectives of Legal Aspects and Cyber Security Tasks in L3Pilot and Structure of the Deliverable

This section introduces the key activities performed in subproject SP4 – Pilot Preparation and Support, with regard to two main objectives:

- To provide information on national legislation addressing AD testing, so that the project teams involved in the pilots can operate safely, follow the necessary procedures, and obtain suitable permission from the authorities;
- To indicate the best strategies to prevent possible cyber security attacks on the functions under test, with a view to generating a set of design guidelines.

Introductory outline: Context

An important aspect of the EU strategy for the “mobility of the future” consists in supporting the experimentation of automated driving on public roads, by means of ad hoc testing regulations. Based on the framework established by the EU and indications by member states, several cities in Belgium, France, Italy, and the UK[1] are planning to allow the operation of automated cars and trucks under certain conditions. Germany, the Netherlands, Spain, and other countries have regulated the testing procedures for AD vehicles in ordinary

[1] BBC News. (2014). *UK to allow driverless cars on roads*. [online] Available at: https://www.bbc.com/news/technology-28551069 [Accessed 18 Oct. 2018].

traffic [25]. As a further example regarding a manufacturer, in 2017 the Swedish company Volvo began testing one hundred automated cars driven in normal traffic by regular clients. All these initiatives are intended as a means to support and facilitate the introduction of AD to the road. L3Pilot partners recognize the importance of operating in conformity with these rules and beyond, in order to guarantee quality and maintain safety during the tests.

Another concern to be thoroughly addressed in order to assure the safety of AD piloting is cyber security. This is well summarized by researchers at the advanced mobility centre of the University of Michigan in a recent report [26]: "As cars progress from a few automated functions – such as self-parking and lane monitoring – to become fully automated vehicles without any driver controls, the cyber security issue will become increasingly complex. Even fail-safe solutions that seem sensible under certain conditions could be problematic, meaning that, with each added piece of automation, all the previous components will need to be re-assessed."

The approach of L3Pilot regarding these issues is based on the following considerations:

The progress towards substantial security will be facilitated by the deployment of widely adopted systems, the focus on new standards, and efforts on common platforms, based on harmonized work by all stakeholders. Moreover, the use of several suppliers providing just one or two vehicle components to a single manufacturer could limit the potential severity of a cyber-attack. As a matter of fact, while each component may not have robust protection, the effects at system level could be more easily controlled. Hackers wanting to create a large-scale attack on automated vehicles would need to understand and be able to foil many different security approaches. It remains true that further developments are needed in this domain, since any successful attack that breaks through will have the potential to hit a large amount of vehicles. This is especially true for functions based on vehicle communication, which are more prone to attacks by hackers.

Legal aspects

The work on legal aspects is focused on the needs of each Pilot Centre, considering the specific regulations of the nation where the respective tests are planned, and also possible cross-border operations. A detailed survey has been conducted on the legislation to be applied. All vehicle owners, following a set of defined guidelines, will ensure that they hold suitable permission for experimenting with cars equipped with AD functions. Furthermore, a common approach has been taken to ensure that data privacy requirements at the European and national level are completely fulfilled (see L3Pilot Deliverable 8.1). Section 2 of the present deliverable covers this work in detail.

Cyber security

The work on cyber security has been focused on three generic functions under development in the project, which are important representative use cases. The study has produced an analysis of the current state of the art and a methodology for identifying relevant cyber attacks, while assessing their criticality. In turn, this has allowed the development of strategic and technical recommendations for vehicle owners. The employed methodology was a "Threat Analysis and Risk Assessment" (TARA), tailored to the objectives of level L3 functions with respect to cyber attacks. As part of this method, the probable points of intrusion were identified for each use case and a risk assessment was computed, considering the probability and the impact of each attack. The AD functions implemented in the project fleets will be verified to be cyber secure before the pilot phase.

After a general description of some relevant technologies in Section 3, the adopted methodology is described in Section 4, the work on the assessments in Section 5, and the practical recommendations for cyber security in Section 6.

2 Regulations Concerning Automated Driving Experiments on Public Roads

2.1 Introduction

In most countries, legislation or regulation requires specific authorization for experimenting with automated cars on public roads. A review of these requirements has been conducted for each country where experiments will take place during the course of the project (2018–2021).

This section presents the review for the seven countries where experiments are planned thus far: Belgium, France, Germany, Italy, Sweden, the Netherlands, and the United Kingdom. During the project, additional countries might be added: Austria, Finland, and Luxembourg. The review consists of a presentation of requirements in each country, using a standard template to allow comparisons between countries. It is worth highlighting that requirements are set by rule or law in all countries but the UK (where only recommendations are provided).

All car owners in the L3Pilot project will comply with the regulations in the countries where they conduct experiments, including cross-border experiments. The procedures reported in this section can also be used by any car owner who would like to apply for permission in any of the countries, thereby facilitating access to national procedures.

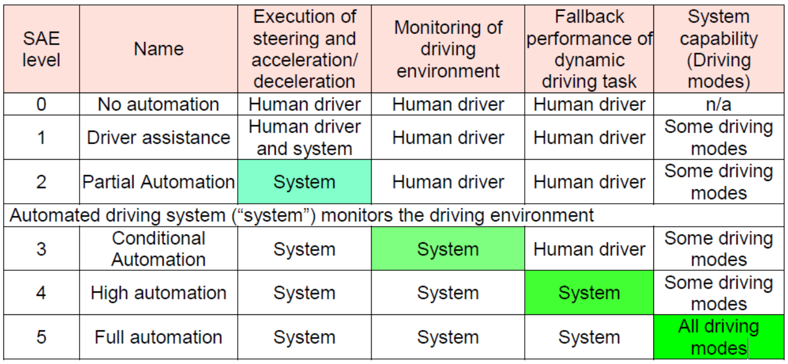
2.2 Disclaimer

The information contained in Sections 2.3.1 to 2.3.7 is intended for reference and information purposes only. The information is given on an as-is basis, is designed solely to provide guidance to vehicle owners, and is not intended to be a substitute for vehicle owners seeking personalized professional advice. The working group makes no claims as to accuracy, completeness, suitability, or validity of any information and will not be liable for any errors, omissions, or delays. As such, the information presented below does NOT constitute legal advice and should not be interpreted as such.

Although the working group has made every reasonable effort to ensure that the information is accurate, there are no guarantees, expressed or implied, on the information provided below. Vehicle owners accept the information “as is” and assume all responsibility for the use of such information.

2.3 Countries

2.3.1 Belgium

<table>
<tr><th>Country: BELGIUM</th><th>September 2018</th></tr>
<tr><td>Regulation – Reference</td><td>Code of practice for testing in Belgium
Arrêté (act of 19 April 2018) related to AD experiments on public roads (Belgium can now allow the testing of fully automated vehicles on public roads without a driver, but the test must be supervised by an operator acting from a control room outside the car)</td></tr>
<tr><td>Scope</td><td>The testing of partial driver assistance or even fully automated vehicle technologies on public roads or in other public places in Belgium (see below: as of SAE level 1).
The testing of a wide range of vehicles, from smaller automated pods and shuttles, through to more conventional road vehicles such as cars, vans, buses, or lorries.</td></tr>
<tr><td>Definitions</td><td>Automated vehicle (see categories 1 to 4 in the table below with specification as to the level of automation)
Fully automated vehicle (see category 5 in the table below with specification as to the level of automation)

<table>
<tr><th>SAE level</th><th>Name</th><th>Execution of steering and acceleration/ deceleration</th><th>Monitoring of driving environment</th><th>Fallback performance of dynamic driving task</th><th>System capability (Driving modes)</th></tr>
<tr><td>0</td><td>No automation</td><td>Human driver</td><td>Human driver</td><td>Human driver</td><td>n/a</td></tr>
<tr><td>1</td><td>Driver assistance</td><td>Human driver and system</td><td>Human driver</td><td>Human driver</td><td>Some driving modes</td></tr>
<tr><td>2</td><td>Partial Automation</td><td>System</td><td>Human driver</td><td>Human driver</td><td>Some driving modes</td></tr>
<tr><td colspan="6">Automated driving system (“system”) monitors the driving environment</td></tr>
<tr><td>3</td><td>Conditional Automation</td><td>System</td><td>System</td><td>Human driver</td><td>Some driving modes</td></tr>
<tr><td>4</td><td>High automation</td><td>System</td><td>System</td><td>System</td><td>Some driving modes</td></tr>
<tr><td>5</td><td>Full automation</td><td>System</td><td>System</td><td>System</td><td>All driving modes</td></tr>
</table>
Source: SAE International and J3016, 2014</td></tr>
<tr><td>Potential restrictions</td><td>The testing of fully automated vehicles on public roads is allowed without a driver, but the test must be supervised by an operator acting from a control room outside the car, with the vehicle’s speed limited to a maximum of 30 km/h.</td></tr>
<tr><td>Procedure description</td><td>Any applicant who wishes to conduct an experiment with automated vehicles on Belgian public roads must obey the following procedure:
1. The applicant has to fill out one application form and answer 37 questions (based on the code of practice).
2. The applicant has to provide the following documents:
• Copy of the appropriate driving licence for every test driver</td></tr>
</table>

Country: BELGIUM	September 2018
	• Copy of an appropriate insurance policy for the test vehicle (after registration if not available during the application) • Risk analysis • Training plan for test drivers • Copy of the roadworthiness test certificate/vehicle inspection (where appropriate) • Auditing record kept by the organizer of the test, showing that internal tests have given sufficient results to allow tests to be conducted on the public road network without creating additional risks for road users • A photo of the automated vehicle 3. The experiment is presented to the Federal Authorities during a meeting. 4. The application form is submitted to the Federal Authorities (Federal Public Services, FPS Mobility, and Transport) 5. FPS Mobility and Transport examine the application form and approve or deny the application. Occasionally, they can raise new questions and the applicant must produce the information requested 6. When everything is agreed, the FPS Mobility and Transport issues an authorization for the vehicle in Belgium. 7. With this authorization the applicant can request an experiment in one region (Brussels, Flanders, Wallonia). Each region can authorize the applicant to drive on its roads. If the experiment uses city roads, the applicant is welcome to ask the city as well. The delay between submission and authorization can vary between 1 month (rarely shorter) and 4 months.
Authorization	When the authorization is granted, the applicant (generally the vehicle owner or someone connected with the vehicle owner) receives an authorization.
General conditions	When the AD mode is switched on, a driver (e.g. subject driver or supervisor) is always able to take control of the vehicle. This driver must have been specially trained to drive AD vehicles beforehand.
Bodies in charge of examining the application for exemption	FPS Mobility and Transport Each region (Brussels, Flanders, Wallonia) for road authorization
Special requirements	The authorization might be accompanied by conditions with the objective of guaranteeing the safety of experiments (risk analysis)
Duration	The authorization mentions the test period of the experiment.
Language	English, French, and/or Flemish

Country: BELGIUM	September 2018
Contact information	FPS Mobility and Transport; DG Transport is the main contact to which the application for authorization is submitted
Web link	Véhicules (semi-)autonomes code_of_practice_en_2016_09 An application form can be requested from FPS Mobility
Miscellaneous	Vehicles must be equipped with data recorders that register whether the vehicle was under driver control or in AD mode at any given moment. The applicant must inform the police and emergency services. The applicant must inform other road users of the test (if necessary). The applicant must provide FPS Mobility with summaries of incidents/accidents. The applicant must provide FPS Mobility with a test summary.

2.3.2 France

Country: FRANCE	August 2018
Regulation – Reference	Décret N° 2018-211 (28 March 2018) related to AD experiments on public roads Arrêté (act of 17 April 2018) related to AD experiments on public roads
Scope	Conditions and application for automated driving experiments in France, e.g.: • Technical experiments • Performance tests for the intended use of vehicles • Public demonstrations and showcases The tested vehicle (so-called “DPTC”) may be allocated to passenger transport or freight transport
Definitions	A “DPTC” (Délégation Partielle ou Totale de Conduite, or Partial or Full Driving Delegation [our translation]) vehicle is a vehicle (international categories M, N, L, T, C or other national category) that is equipped with functions allowing the driver to delegate some or all of the driving tasks during part or all of the trip.
Potential restrictions	Any technology can be tested on any infrastructure as long as the authorization is given by the public authorities. There is no a-priori restriction. However, DPTC technologies of passenger cars cannot be tested on roads/lanes for public transport (bus lanes for example). Only DPTC technologies for public transport can be tested on these roads/lanes.
Procedure description	Any applicant who wishes to conduct an experiment with DPTC technologies on French public roads must obey the following procedure: 1. The applicant has to produce four documents: a dossier explaining what the experiment consists of (objectives, experimental design, etc.), a dossier describing the prototype(s) that will be tested and how its (their) safety has been taken into consideration, a questionnaire (about 90 questions) summarizing the main issues of the experiment, and finally a document from the Ministries providing advice from the road operators on conducting the experiments on their road network. 2. The experiment is presented to the public authorities during a meeting in which questions are raised and responses are recorded in the above dossiers. 3. The dossiers are submitted to the public authorities. 4. Two ministries (Ministry for Ecological and Solidarity Transition/Ministry of the Interior) examine the dossiers and

Country: FRANCE	August 2018
	approve or deny the application. Sometimes, they can raise new questions and the applicant must produce the information requested. When everything is agreed, the Ministry of Ecology issues an authorization for special experimental DPTC registration for the prototype(s) that can be driven strictly in the conditions specified in the dossiers (especially only on the routes declared as tested routes). The authorization runs for at most two years. Delay between submission and authorization can vary between 2 months (rarely shorter) and 4 months.
Authorization	When the authorization is granted, the applicant (generally the vehicle owner or someone connected with the vehicle owner) receives a certificate “WW DPTC”, which is a specific certificate for prototypes for AD experimentation (the certificate for usual prototypes is WW only).
General conditions	When the DPTC mode is switched on, a driver (e.g. subject driver or supervisor) is always able to take control of the vehicle. This driver must have been specially trained in DPTC systems beforehand.
Bodies in charge of examining the application for exemption	Ministry for Ecological and Solidarity Transition (in charge of transport) Ministry of Interior (in charge of traffic safety)
Special requirements	The exemption may be accompanied by conditions with the objective of guaranteeing the safety of experiments.
Duration	The authorization mentions start date and end date of the experiment. Maximum duration is two years.
Language	French
Contact information	Ministry of Ecological and Solidarity Transition – General Directorate for Energy and Climate (DGEC) is the main contact to which the application for authorization is submitted.
Web link	www.demarches-simplifiees.fr/commencer/autorisation-experimentation-vdptc No template available
Miscellaneous	The public authorities also require that an assessment is done quarterly and yearly. The public authorities maintain a register to record all experiments that are authorized. Vehicles must be equipped with data recorders that register whether the vehicle was under driver control or in DPTC mode at any given

Country: FRANCE	August 2018
	moment. Data is automatically and periodically erased. In the event of a crash, recorded data (5 minutes before crash) is stored by the authorization holder for a period of one year.

2.3.3 Germany

Country: GERMANY	December 2018
Regulation – Reference	There is no specific regulation or procedure for AD experiments on public roads yet. General exceptional provisions apply, e.g. • StVZO (“Straßenverkehrs-Zulassungs-Ordnung”; Engl. Road Traffic Licensing Regulations) ▪ Sec. 19 para. 6 StVZO (“registration of test vehicles” required whenever the type-approval-relevant series production condition is altered). ▪ Sec. 70 StVZO (exemption approval for vehicles that do not comply with the StVZO, e.g. AD functionalities which are not approved under current law). • StVO (“Straßenverkehrs-Ordnung”; Engl. Road Traffic Regulations). Exemptions are possible, cp. Sec. 46 StVO. Expert report by technical service is usually required in the process of approval. • StVG (“Straßenverkehrsgesetz”, Engl. “Road Traffic Act”) allows the application of L3 Automation as described in Sec. 1a and 1b StVG on a regular basis – not limited to experimental conditions. However, the prerequisite is type approval of the whole vehicle according to Art. 6 in conjunction with Annexe IV of 2007/46/EG that lists requirements of EC type approval and inter alia refers to UN-Regulations as equivalent (part II). The respective UN Regulation on automatically commanded steering functions is not yet in place for L3 (status: Dec. 2018). L3-Automation would therefore need to be considered an exemption for new technology according to Art. 20 of 2007/46/EG which has not happened so far. Nonetheless, these national automation-relevant provisions can support exemption approval in terms of argumentation as the general concept of Level 3 automation in traffic has passed parliament in Germany and is thus accepted. • Exemption approval for operation of automated vehicles on public roads might be necessary.
Scope	Conditions and application for automated driving experiments in Germany.
Definitions	--
Potential restrictions	There is no restriction for automated driving experiments on open roads in general. However, technologies that do not comply with the StVZO

Country: GERMANY	December 2018
	and StVO need a special authorization (permit) from the public authorities for individual assessment.
Procedure description	1) Any (test) car needs technical approval if used on public roads. The relevant regulation document is the “Straßenverkehrs-Zulassungs-Ordnung” (StVZO, Engl. Road Traffic Licensing Regulations). A vehicle that is subject to dynamic driving tests can have an individual operating permit, granted under Sec. 19 para. 6 StVZO (“registration of test vehicles”). Legal wording, translated (Sec. 19 para. 6 StVZO): If parts of vehicles are modified by the vehicle manufacturer bearing the operating license (acc. to German law) for the respective vehicle, the operating license will remain valid as long as the vehicle is used for the purpose of testing. No additional notification to the vehicle registration office on technical modifications is then required. The first sentence is only valid if the vehicle registration office has confirmed in the vehicle registration document [Registration Certificate Part I] that the vehicle has been registered as a test vehicle. According to Sec. 19 para. 7 StVZO the above translated para. 6 applies accordingly to exemptions from EU-based type approvals. In the event that the vehicle will be testing aspects that are not approved by current law (such as AD functionalities), an exemption approval is required (Sec. 70 StVZO). The exemption will usually be granted by the federal state where the applicant is located. In the event that other federal states are affected by testing, the local authority of the federal state will need to reach mutual agreement. An expert report from a technical service will usually be required during the process of granting approval. 2) For the operation of vehicles on German public roads another regulation is of high relevance: the Straßenverkehrs-Ordnung (StVO, engl. Road Traffic Regulations). Thus, the law may require the approval of a special permit regarding the rules of the road (German “Verhaltensrecht”) (StVO). The holistic issue of safety can likewise be subject to expert review by a technical service. As a basis for the application for a special permit, the applicant will usually be required to deliver a dossier describing the scope of the study (objectives, experimental design, etc.) and the prototype in detail, including a safety assessment (which, however, can be made subject to the technical expert report by the technical service). The experiment and the vehicle may need to be presented to the relevant public authorities and any questions answered. If everything is approved, the applicant receives a permit that describes the conditions under which the experiment can be conducted. The duration of the permit may be limited, e.g. to the duration of the study.

Country: GERMANY	December 2018
Authorization	The responsible body granting permission differs according to the location of the applicant. Contact the local registration office responsible to identify the competent body at the federal state level.
General conditions	Not applicable
Bodies in charge of examining the application for exemption	See above "Authorization". The technical service supporting the evaluation of safety is the technical service of the respective federal state.
Special requirements	Depending on the individual assessment, the public authorities can limit the permit with regard to: • time and duration of usage (e.g. daytime) • area of usage (e.g. defined test track, excluding sections such as motorway access) • other limitations
Duration	Duration depends on the individual approval and can usually be prolonged upon application if necessary.
Language	German
Contact Information	Contact the local registration office for information on the responsible body within the federal state of the applicant.
Web link	StVZO StVO Directive 2007/46/EC UN/ECE R79, rev.2 (2006) Vienna Convention on Road Traffic (1968) Amendment to the Vienna Convention (2016)

2.3.4 Italy

Country: ITALY	December 2018
Regulation – Reference	Tests related to automated driving vehicles on Italian public roads are regulated by the “Smart Road Decree” (Feb. 2018) of the Italian Ministry of Infrastructure and Transport (MIT). MIT has set up the Technical Observatory (TO) to support Smart Roads and connected and AD vehicles (art. 20 of 70/2018 D.M., 19 June), the operative tasks of which also include: • To promote the adoption of methodological and operational tools to monitor, with appropriate ex ante and ex post analyses, the impact of the experimentation of AD vehicles on the road • To examine and express opinions on requests for the authorization of testing of AD vehicles • To handle ethical and legal issues related to the introduction of AD vehicles The TO is responsible for maintaining and updating the list of road infrastructure, verifying compliance with the functional specifications.
Scope	Conditions and applications for automated driving experiments in Italy include: • Technical experiments • Performance tests for the intended use of vehicles • The repeating/transfer of experiments performed in the pre-test phase on test tracks (proving grounds) – covering technical functional verification and performance assessment – on public roads, in order to validate them in real conditions.
Definitions	MIT – Italian Ministry of Infrastructure and Transport TO – Technical Observatory of the MIT Smart Roads – Italian MIT Decree Supervisor – Professional driver authorized to drive vehicles provided with AD functions
Potential restrictions	The main potential restrictions are listed below: • Pilot test authorization must be requested from Motorway Companies and then the Italian MIT. • The authorization refers to the execution of the tests on one or more road sections and, for each of them, for the specific road infrastructures indicated by the applicant *after having obtained clearance from the owner of the road.* Professional drivers must be in compliance with specific requirements (at least 5 years’

Country: ITALY	December 2018
	licence, safe driving, or specific courses for such vehicles at an accredited body, at least 1000 km of tests with AD in a protected area or on public roads). • Before pilot tests, it is necessary to have already carried out experiments of at least 3000 km with AD vehicles (also vehicles other than those for which authorization is required) with simulations and tests in a protected location or on public roads also abroad, provided that they took place in a state where the testing of vehicles with automatic driving is regulated for all homogeneous vehicles, subject to authorization for at least an additional 3000 km. • The authorizing party (i.e. MIT) may suspend or revoke the authorization if it detects, even as a result of default by the authorized party, that the continuation of the tests could cause a high risk to the safety of traffic.
Procedure description	The manufacturer of a vehicle equipped with AD technologies, as well as university institutes or public and private research bodies conducting experiments on vehicles equipped with AD technologies, submit to the MIT the application for authorization to test the automatic guided vehicle on the road. Any applicant who wishes to conduct an experiment for such vehicles on Italian public roads must obey the following procedures: • Require and obtain clearance (nulla osta) from the owner of the road for one or more road sections indicated by the applicant • Require and obtain authorization at the Italian Ministry of Infrastructure and Transport, under the advisement of the Technical Observatory The application for authorization must contain: • Indication of the owner of the vehicle as the responsible subject pursuant to art. 196 of the highway code • Indication of the road areas required for such testing and for each area, an indication of the infrastructural sections on which the experiment is to be conducted • Documentation demonstrating that clearance to conduct the tests has been obtained from the owner (or management operator) of the road, for each proposed infrastructure section • Indication of external, meteorological, and visibility conditions as well as conditions of the roads and traffic in which the tests are carried out and assurance that the vehicle will manage It is necessary to attach the following documentation, attesting to the responsibility of the applicant:

Country: ITALY	December 2018
	• Evidence of the maturity of the technologies that are the object of experimentation with reference to the road areas for which authorization is requested. • Obligatory: Descriptions of the know-how deriving from the suppliers of the components; of the test process being implemented; and of the tests that have been carried out in simulation, highlighting the coverage of the application scenarios and deviations from real application scenarios. Before pilot tests, it is necessary to have already carried out experiments for at least 3000 km with AD vehicles (also vehicles other than those for which authorization is required), with simulations and tests in a protected location or on public roads, also abroad, provided that they took place in a state where the testing of vehicles with automatic driving is regulated for all homogeneous vehicles, subject to authorization for at least an additional 3000 km. The tests refer to each of the road areas for which authorization is required. Possible accidents or anomalies that occurred during the experimentations must be reported and described. • Documentation that highlights the vehicle's ability to manage predictable situations in typical scenarios of road areas for which authorization is required and methods for managing the particularities of the scenarios • Descriptions of the technology used • Descriptions of the intrinsic safety protections designed to prevent unauthorized access to AD systems • Risk analysis associated with the use of vehicles in AD mode on the road, descriptions of the countermeasures adopted and the safety plans for the tests • The list of drivers and documentation of the training conducted and the list of vehicles to be tested Among other things, the holder of the testing authorization has the obligation to: • Ensure that the data of the tests are correctly recorded (time elapsed since the beginning of the registration, coinciding with the beginning of the experimentation, automatic or manual current operation mode, gear ratio engaged, or other equivalent indicators, dynamic variables in real time, etc.) and held at the disposal of the authorizing party, which will be able to view them for the entire duration of the authorization and for the following twelve months

Country: ITALY	December 2018
	• Inform the manager of the infrastructure sections about the program of tests, to be sent ten days in advance of the beginning of the tests
Authorization	When the authorization is granted, the applicant (generally the vehicle owner or someone connected with the vehicle owner) receives a particular certificate, which is a specific certificate for prototypes for AD experiments.
General conditions	The AD testing system subject to experimentation must: • Be suitable at all times to allow the transition from automatic mode to manual mode • Be equipped with intrinsic security protections to guarantee data integrity and the security of communications that prevent unauthorized access • Be able throughout the test to record detailed data with a frequency of at least 10 Hz These features must cover the most frequently occurring risk scenarios for each road sector for which the authorization is required. It means that the capacity of the vehicle in AD mode to manage predictable situations in typical driving scenarios, road areas, and external conditions for which permission is requested must be ensured. In particular, the documentation must highlight the management methods of the particularities of the scenarios. Any accidents or anomalies that occurred during experiments already carried out, even in the laboratory or protected areas, must be reported and described.
Bodies in charge of examining the application for exemption	Not applicable
Special requirements	Not applicable
Duration	The authorization is valid for one year and can be renewed with a request of the authorization holder. At the request for renewal, to be submitted at least 30 days in advance of the expiry of the authorization, the applicant must attach, among other things, the report on the trials that have been carried out.
Language	Italian
Contact information	Italian Ministry of Infrastructure and Transport is the main contact to which the application for authorization is submitted.
Web link	Main “Smart Roads” link:

Country: ITALY	December 2018
	http://www.mit.gov.it/comunicazione/news/smart-road-infrastrutture-digitali/smart-road-veicoli-connessi-e-mobilita-del Templates for pilot application (4 October, 2018) in: http://www.mit.gov.it/comunicazione/news/smart-road-smart-mobility-mezzi-stradali/mit-operativo-osservatorio-tecnico-di-supporto-per
Miscellaneous	The authorization holder, for the entire duration of the authorization, is required to produce and deliver to the authorizing body: • Punctual reports on events or problems of any nature that involved the system and that may have implications for safety, even if only potential, to be delivered within 15 days of the event, which must contain: a detailed description of the event; the extract of the data obligatorily registered by the vehicle, for a reasonable period before and after the event; any other data recorded by the vehicle, including any video footage, for the same period of time. • The annual report on the trials carried out, to be delivered within 30 days from the end of the authorization, which includes the list of the tests carried out. • Demonstration by the applicant that he/she has concluded the specific liability insurance contract for the automated guided vehicle with a minimum ceiling equal to four times that foreseen for the vehicle used for the experimentation in its version without AD technologies, according to current legislation. The insurance contract expressly indicates that the insurer is aware of the mode of use of the vehicle and that the vehicle is used in automatic operating mode on public roads. • An insurance contract expressly indicating that the insurer is aware of how the vehicle is used and that the vehicle is used in automated operating mode on public roads.
Miscellaneous	--

2.3.5 Sweden

Country: SWEDEN	October 2018
Regulation – Reference	TSFS 2017:92 (2017-11-01), The Swedish Transport Agency Regulation on Permissions for Testing of Automated Vehicles (in Swedish). Based on: SFS 2017:309 (2017-07-01 – 2022-07-01), Decree/Regulation on Testing of Automated Vehicles (in Swedish).
Scope	Applies to road traffic with automated vehicles subject to exemption decisions in accordance with Chapter 8, Section 18 of the Vehicle Regulation (2009:211).
Definitions	Automated vehicle means a vehicle that has a fully or partially automated driving system. Experimental activity refers to activities involving the use of an automated vehicle to test and evaluate automatic functions not included in a type approval, individual approval, or registration survey under the Vehicle Act (2002:574).
Potential restrictions	Experiments with automated vehicles may be carried out only with permission. A licence is valid for a limited period of time with the possibility of renewal. Authorization may only be granted if the applicant shows that traffic safety can be ensured during the attempt and that the attempt does not cause significant disturbance or inconvenience to the environment. A permit decision shall be reviewed if there are special reasons to do so.
Procedure description	Application to the Swedish Transport Agency (Transportstyrelsen), which will decide and supervise the testing. Applications shall include, e.g.: • a description of how the testing will be controlled and how responsibilities are distributed • the purpose and objectives of the testing • a description of the automated functions to be tested • a description of how the testing will be performed and evaluated • the geographic area and the streets and roads where the testing will be conducted • a risk assessment
Authorization	When the authorization is granted, the applicant receives a written exemption.
General conditions	When driving an automated vehicle, there must be a physical driver inside or outside the vehicle. A decision on permission to conduct a trial may be combined with additional conditions.

Country: SWEDEN	October 2018
Bodies in charge of examining the application for exemption	The Swedish Transport Agency (Transportstyrelsen)
Special requirements	The exemption might be accompanied by conditions with the objective of guaranteeing the safety of experiments. Accidents and incidents are to be reported to the Transport Agency. A written evaluation of the testing shall be presented to the Transport Agency once a year.
Duration	Not specified
Language	Swedish
Contact information	The Swedish Transport Agency (Transportstyrelsen) Phone: +46 771-503 503
Web link	The Swedish Transport Agency site for automated vehicles: https://www.transportstyrelsen.se/sv/vagtrafik/Fordon/forsoksverksamhet/sjalvkorande-fordon/
Miscellaneous	--

2.3.6 Netherlands

Country: NETHERLANDS	OCTOBER 2018
Regulation – Reference	JBZ 2017/12252 (17 July 2018) related to AD experiments on public roads LINK to the Staatsblad (Dutch Government Gazette, in Dutch)
Scope	Conditions and application for connected and automated driving (CAD) in the Netherlands: All Dutch roads are open for testing, after an exemption has been obtained from The Netherlands Vehicle Authority (RDW). CAD must have a human driver in the vehicle.
Definitions	CAD vehicles (international categories M, N, L, T, C, or other national category) are vehicles that are equipped with functions allowing all or part of the driving tasks to be delegated during all or part of the trip.
Potential restrictions	Restrictions are mentioned in Annex II of the JBZ 2017/12252. In principle any technology can be tested on any infrastructure as long as authorization is given by the public authorities. There are no a-priori restrictions. No tests are allowed with the transport of, for instance, dangerous goods (as described in Dutch Law).
Procedure description	The Dutch assessment framework has five steps. These steps indicate the various points of the test application during the process. The steps are as follows: • The intake step is focused on the preparatory treatment and pre-assessment of the test application; • The preparation step is focused on the preparation of the assessment of the test application; • The assessment step provides a decision on safety and whether the test can and may be carried out; • The execution step is dedicated to carrying out the test on public roads; • The evaluation step reviews whether the process must be improved and safeguards the knowledge acquired. Each step contains criteria that must be satisfied before proceeding to the next step. The application processing time is approximately three months. The application processing time depends on the type of vehicle, completeness and quality of the documents submitted by the applicant, experience from earlier tests, the cooperation of the relevant applicant and the primary and secondary parties, as well as the observance of the handling time. The costs of the application are based on the fixed rates f the relevant type of exemption and the variable costs. These variable costs depend on, inter alia, the required person-hours, any use of RDW services (such as the test

Country: NETHERLANDS	OCTOBER 2018
	centre), and the amount of preparation by the applicant and the distance to be travelled by RDW to assess the vehicle. The applicant is responsible for the payment of the incurred costs. Understanding the “tailored work and flexibility” factors is important in CAD test applications. The RDW works on the basis of new insights. New insights in this context means that important lessons learned from previous applications can lead to direct changes in the method and the process for new and current applications. These will be clearly communicated. This is a learning process for the RDW and all other stakeholders. This may mean that the policy is regularly adjusted. This entire process falls under ISO-accreditation of the RDW.
Authorization	When the authorization is granted, the applicant (generally the vehicle owner or someone connected with the vehicle owner) receives a written exemption.
General conditions	The Netherlands intends to promote a positive impact with CAD on society. Therefore the Minister of Infrastructure and Water Management informed parliament in October 2018 about the latest ambitions and conditions LINK (in Dutch)
Bodies in charge of examining the application for exemption	LINK GENERAL INFORMATION RDW Smart Mobility Embassy is a general national starting point for ITS testing
Special requirements	All exemptions are accompanied by specific conditions with the objective of guaranteeing the safety of experiments.
Duration	The authorization mentions the start date and end date of the experiment. Maximum duration is one year.
Language	Dutch, with English application and documentation also possible
Contact information	RDW, The Netherlands Vehicle Authority
Web link	LINK to application website
Miscellaneous	An experimental law for self-driving cars without a human driver in the car is in preparation. More details can be found in this LINK (in Dutch)

2.3.7 United Kingdom

Country: UNITED KINGDOM	February 2019
Regulation – Reference	The Pathway to Driverless Cars: A Code of Practice for testing. Moving Britain Ahead – July 2015, Department of Transport
Scope	The Code of Practice is intended to apply whenever highly or fully automated vehicle technologies are being tested on public roads or in other public places in the UK. The Code is not intended to apply to tests carried out on private test tracks or other areas not accessible by the public.
Definitions	--
Potential restrictions	No specified restrictions. A suitably qualified test driver will always have to be present in the vehicle when on public roads and should take responsibility for the safe operation of the vehicle.
Procedure description	No authorization required, however manufacturers have a responsibility to ensure that highly and fully automated vehicle technologies undergo thorough testing and development before being brought to market. Much of this development can be done in test laboratories or on dedicated test tracks and proving grounds. However, to help ensure that these technologies are capable of safely handling the many varied situations that they may encounter throughout their service life, it is expected that controlled “real world” testing will also be necessary. Testing of automated vehicle technologies on public roads or in other public places should therefore be facilitated while ensuring that this testing is carried out with the minimum practicable risk.
Authorization	Explicit authorization is not required, but testing organizations are encouraged to engage with the local authorities and infrastructure authorities prior to testing.
General conditions	Vehicles under test on public roads must obey all relevant road traffic laws. It is the responsibility of testing organizations to satisfy themselves that all tests planned to be undertaken comply with all relevant existing laws and that the vehicles involved are roadworthy, meet all relevant vehicle requirements, and can be used in a way that is compatible with existing UK road traffic law. The relevant road traffic laws include regulation 100 (or regulation 115 in Northern Ireland) of Construction and Use Regulations. Broadly these highlight that it is an offence to use a motor vehicle or trailer in such a way that it would present a danger to other road users. Testing organizations should ensure that test drivers hold the appropriate driving licence, have received appropriate training,

Country: UNITED KINGDOM	February 2019
	conduct risk analysis of proposed tests, and have appropriate risk management strategies. The statutory requirements on the holding of insurance will apply whilst a vehicle is being tested. Anyone conducting tests of automated vehicles on public roads or in other public places must therefore hold appropriate insurance or otherwise comply with the statutory requirements.
Bodies in charge of examining the application for exemption	Department for Transport
Special requirements	N/A
Duration	Indefinite
Language	English
Contact information	Department for Transport Great Minster House 33 Horseferry Road London SW1P 4DR Telephone +44 300 330 3000
Web link	https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/776511/code-of-practice-automated-vehicle-trialling.pdf
Miscellaneous	Responsibility for ensuring that testing of these technologies on public roads or in other public places is conducted safely always rests with those organizing the testing. Compliance with these guidelines alone should not be considered to be sufficient to ensure that all reasonable steps to minimize risk have been taken. Testing organizations should consider the benefits of developing a public relations and media communications strategy to: • Educate the public regarding the potential benefits of automated vehicles. • Explain the general nature of the tests to be undertaken. • Explain the implications for other road users, if any, and what steps are being taken to mitigate any risks. • Provide reassurance and address any concerns that the public may have. Particular consideration should be given to the concerns of more vulnerable road users, including the disabled, those with visual or hearing impairments,

Country: UNITED KINGDOM	February 2019
	pedestrians, cyclists, motorcyclists, children, and horse riders.

2.4 Discussion

The collection of regulations described above is intended to provide a comparative overview in a variety of European countries. Some regulations are more detailed and spell out e.g. the mileage demanded in simulation or test track driving, or they require the names of the street where the experiment takes place. Other codes are less specific and recommend safe practices in more general terms.

Due to the limited available experience regarding AD in mixed traffic, we should expect constant updates of the regulatory scheme. The many safeguards now in place reflect the unknown realm of this technology as used in the many varied situations that can be encountered in ordinary traffic. In particular, they remind us of the concerns regarding full automation, under which the vehicle may suddenly perform completely unexpected manoeuvres.

Nevertheless, L3Pilot partners consider these initiatives to be a key milestone for the deployment of the technology. The framework creates the prerequisites for highly and fully automated systems and also shows the interest of many stakeholders in the potential benefits of AD. At the same time, the different national regulations represent an additional challenge. For this reason, the project partners advocate further work towards an internationally harmonized legal framework for automated driving.

In this context, all vehicle manufacturers in L3Pilot have implemented internal processes regarding how to conduct experiments on public roads. These processes are based on their consolidated experience with prototypes and on the knowledge collected during the development of similar products (e.g. ADAS functionalities), with the objective of maximizing safety for all road users, not forgetting the driver/passengers of the test vehicle. Such processes include driving permits for prototype vehicles, medical tests, and specific training for unexpected behaviour of the vehicle or the environment. In addition, a detailed examination of functional safety has an integral role in the process, and in this respect the system developers have strived to include a large range of use cases, which may at first seem quite remote from everyday operation.

3 Background: Automotive Cyber Security in L3-type Vehicle Systems

This section covers general aspects of the vehicle system that are relevant to the work on cyber security that will follow. The analysis takes a generic perspective with regard to vehicles featuring L3 automation. This includes the vehicle system architecture, an overview of the possible intra-system communication interfaces, as well as the communication with an external digital infrastructure privately owned by the OEM and remotely located on the cloud (e.g. in use for secure over-the-air software updates).

3.1 System Architecture

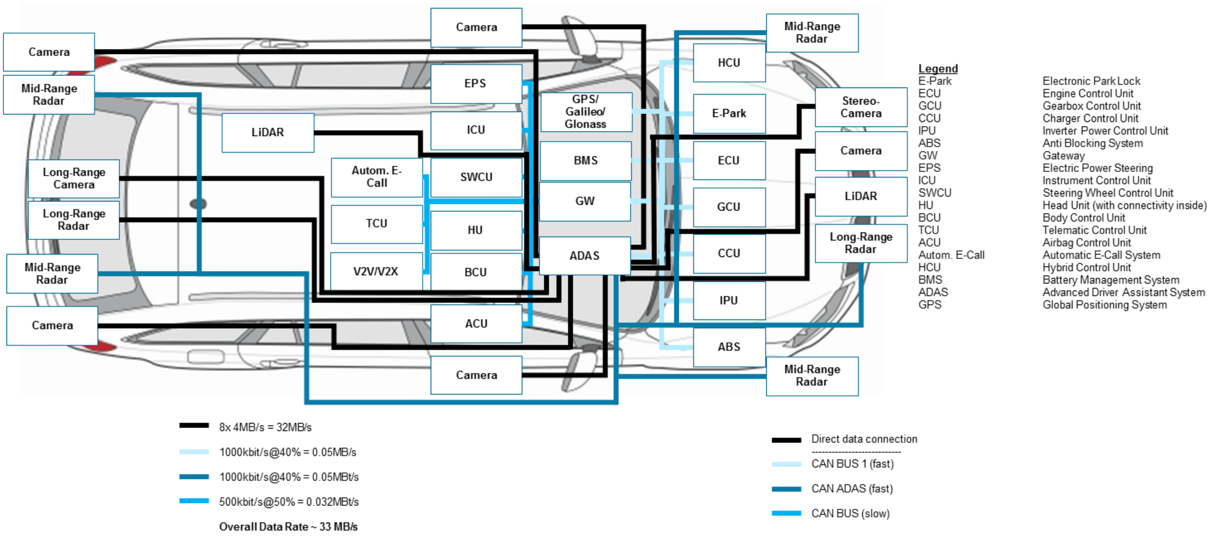


Figure 3.1: Generic system architecture of a typical vehicle based on inputs from the L3Pilot vehicle owners.

A modern vehicle contains a large volume of electronics to meet the highly diversified requirements of drivers, passengers, and regulations. Today's vehicles provide safety systems, dynamic control systems, engine controls, and wireless connectivity, to name just a few. Such functions are normally accomplished by using an electronic control unit (ECU) for each major task. The ECUs are connected to each other over different underlying networks such as CAN bus, FlexRay, or Ethernet. The ECU networks are segregated according to the desired functionalities, such as safety critical and non-safety critical networks or high speed and low speed networks. As an example, a high-speed bus may be used to interconnect powertrain components that generate real-time telemetry, whereas a separate low-speed bus might be used to control binary actuators like lights and doors. In the case of multiple networks, there might still be a need for interaction between the individual networks. These (sub-) networks are then interconnected through a gateway.

3.2 Intra-system Communication

Nowadays, a wide variety of vehicle communication systems is used in the automotive domain.

In [3], the intra vehicular communication groups are divided into five different types based on their technical properties and application areas as shown in Table 3.1.

Table 3.1: Grouping of automotive bus systems [3]

Sub bus	Event-triggered	Time-triggered	Multimedia	Wireless
LIN	CAN	FlexRay	MOST	Bluetooth
K-line	VAN	TTP	D2B	GSM
I^2C	PLC	TTCAN	GigaStar	Wi-Fi

Local sub networks such as LIN (Local Interconnect Network) control small autonomous networks used for automatic door locking mechanisms, power windows, and mirrors, as well as for communication with miscellaneous smart sensors to detect, for instance, rain or darkness. Event-triggered bus systems such as CAN (Controller Area Network) are used for soft real-time in-car communication between controllers, networking with for example the antilock braking system (ABS) or the engine management system. Time-triggered hard real-time capable bus systems such as FlexRay, TTCAN (Time-Triggered CAN), or TTP (Time-Triggered Protocol) guarantee determined transmission times for controller communication and can therefore be applied in highly safety-relevant areas such as in most drive-by-wire systems. The group of multimedia bus systems including MOST (Media Oriented Systems Transport), D2B (Domestic Digital Bus), and GigaStar arise from the new automotive demands for in-car entertainment that requires high-performance, wide-band communication channels to transmit high-quality audio, voice, and video data streams within the vehicle.

The wireless communication group contains modern wireless data transmission technologies that are increasingly expanding into the automotive area. These enable the internal vehicle network to communicate with other cars nearby and external base stations, as well as enabling the utilization of various location-based services.

Figure 3.2 gives an overview with a short comparison of typical data rates and relative cost per node for each vehicular communication group mentioned [3]. The next section introduces in greater detail the widespread CAN protocol and its security challenges.

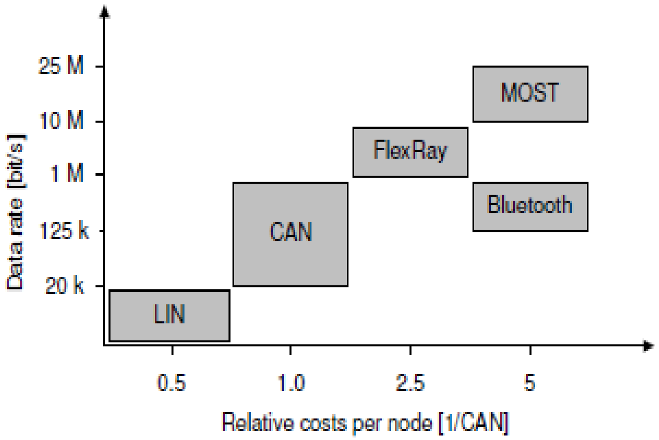


Figure 3.2: Data rates and relative costs of automotive bus systems [3].

3.2.1 CAN

3.2.1.1 CAN introduction

The Controller Area Network (CAN), developed in the 1980s, is an event-based controller network for serial communication. It provides data rates up to 1 Mbit/s. It has a multi-master architecture allowing redundant networks, which are able to operate even if some of their nodes are defective. CAN messages are classified using their respective identifier and do not have a recipient address. CAN controllers broadcast their messages and all receiving nodes decide independently if they will process the message. CAN uses the CSMA/CR (Carrier Sense Multiple Access/Collision Resolution) access control method to guarantee a priority-driven message transmission. Transmission errors are detected using a CRC (Cyclic Redundancy Check) checksum, whereas errors due to collision caused by the transmission of two high priority messages at the same time are safe guarded against through CSMA/CR.

A CAN packet, which does not include addresses in the traditional sense [5], is shown in Figure 3.3. Instead, it supports a publish-and-subscribe communications model. The CAN ID header is used to indicate the packet type. Each packet is broadcast to all nodes, which then decide for themselves whether to process the packets.

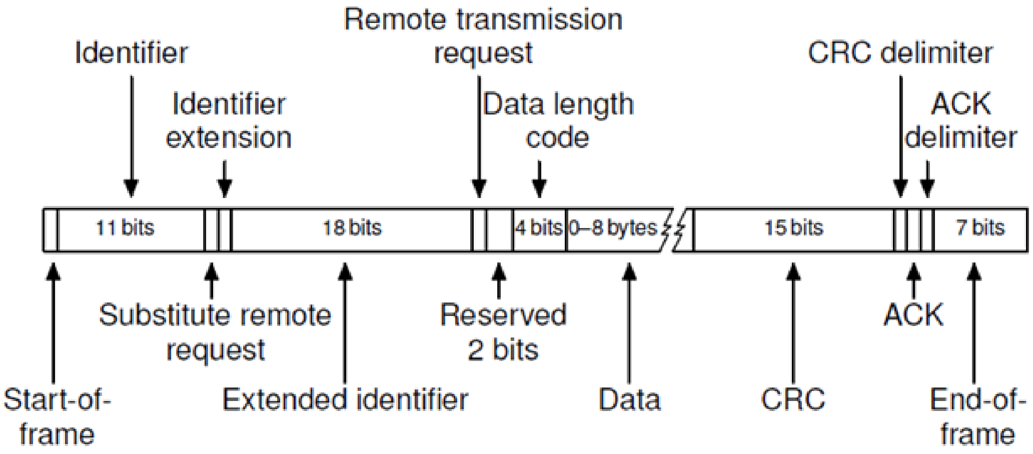


Figure 3.3: Extended frame format of CAN packet [5].

3.2.1.2 CAN security challenges

The underlying CAN protocol has a number of inherent weaknesses that are common to any implementation. Key points among these are:

Broadcast nature

Since CAN packets are broadcast to all the nodes on the network, a malicious component on the network can easily sniff all the communications or even fabricate packets and send packets to any other node on the network.

Vulnerability to Denial of Service (DoS)

The CAN protocol is vulnerable to denial-of-service (DoS) attacks. There are multiple ways to achieve DoS, such as through packet flooding by a malicious node. A node can also assert a dominant state indefinitely, ostensibly sending priority messages, thereby causing all other CAN nodes to stop sending. Moreover, a node can send other nodes into a bus off mode. All of these actions will effectively stop legitimate nodes from transmitting any messages.

Absence of authenticator fields

CAN packets contain no authenticator fields, which allows any component to indistinguishably send packets to any other component. Thus a compromised node can be used to send fabricated messages to other components on the bus.

3.2.1.3 CAN security breach examples

As already mentioned, CAN was not designed with a focus on security and therefore has multiple security shortcomings. Some of these shortcomings are highlighted through the following examples:

1. Unauthorized alteration of ECU software [4]

Software of an ECU can be changed through unauthorized access. Figure 3.4 shows an example of spoofed message transmission by an ECU after its authorized program is replaced by a malicious program. Spoofing is the forging of a message in a way that is not immediately recognized as false.

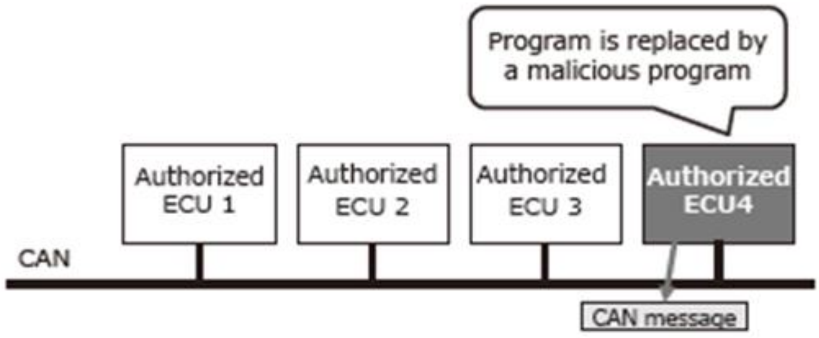


Figure 3.4: Replacement of authorized ECU program by malicious program [4].

2. Connection of unauthorized device [4]

An unauthorized device can be connected to the CAN bus if physical access is possible. Figure 3.5 shows an example of spoofed message transmission by an unauthorized device connected on a CAN bus.

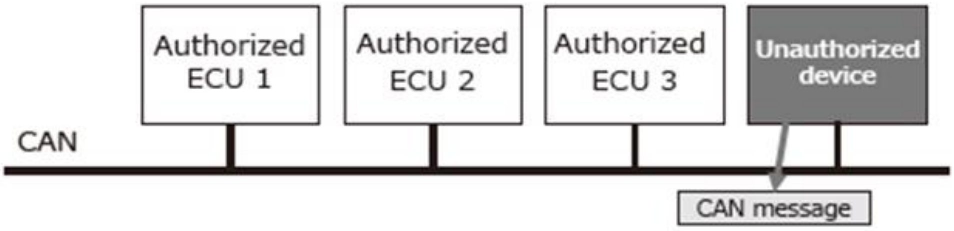


Figure 3.5: Connection of unauthorized device on CAN bus [4].

3. Connection of unauthorized device to OBDII port sending requests/instructions in order to consume available bandwidth and create CAN error codes.

As pointed out in [2], the attacks could cause a denial of service without injecting fake frames but by merely changing one bit at a time from a specific message, creating CAN errors and leading to blockage of the internal component that created the erroneous message.

Security on CAN

If physical integrity of the CAN bus cannot be assured, authentication and integrity protection of sensitive data is necessary to protect correct and safe functionality of the vehicle systems – this ensures that received data comes from the right ECU and has the intended value.

The SecOC [1] module (Secure Onboard Communication specified by AUTOSAR) aims for resource-efficient and practicable authentication mechanisms of sensitive data on the level of protocol data units (PDUs). Figure 3.6 shows the calculation of the MAC tag at the transmitter and verification of the MAC tag (authentication of data) by the receiver. Here, a PDU can be assumed to be data for simplicity and ease of understanding.

The SecOC module provides the functionality necessary to verify the authenticity and freshness of PDU-based communication between ECUs within the vehicle architecture. This approach requires both the sending ECU and the receiving ECU to implement a SecOC module. The two SecOC modules are integrated, providing the upper and lower layer PDU router (PduR) APIs on the sender and receiver side. The SecOC modules on both sides generally interact with the PduR module.

To provide message freshness, the SecOC modules on sending as well as receiving side get freshness from an external Freshness Manager for each uniquely identifiable Secured I-PDU (Interaction Layer – PDU), i.e. for each secured communication link.

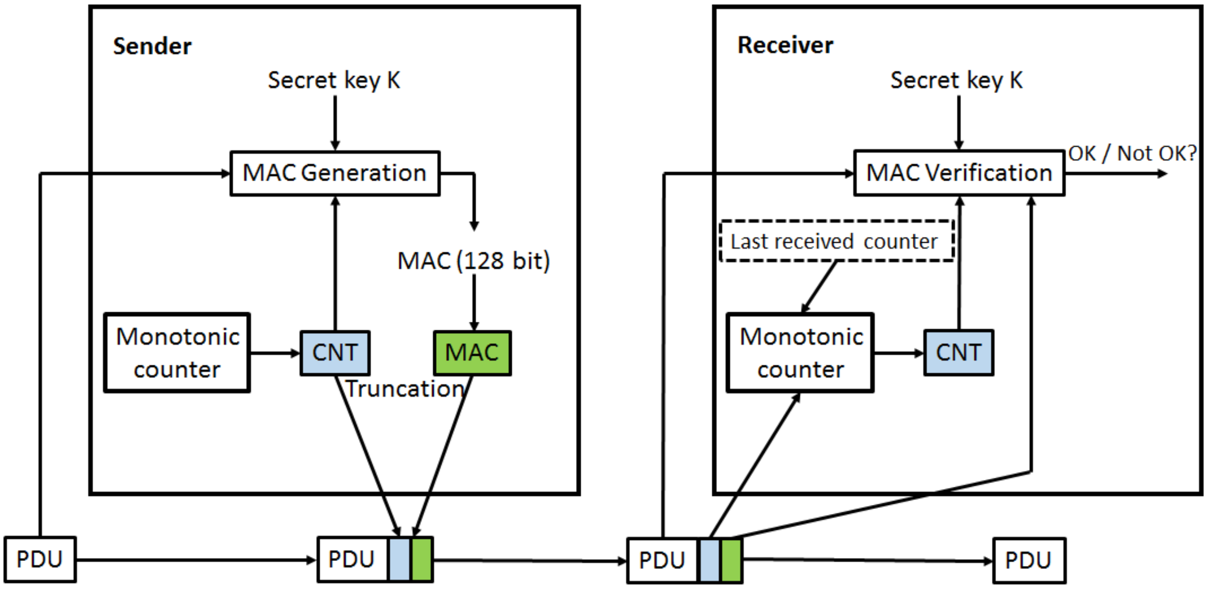


Figure 3.6: Message authentication and freshness verification [1].

3.3 Back End (at OEM)

Connection with the cloud – with the objective of either storing dynamic vehicle data or providing dynamic environment information – is a topic highly relevant for automated vehicles. A good example would be to consider an automated parking service where in-vehicle functionality relies on service provided by the back end. Such connections are vulnerable to malicious manipulation, however. For example, HD maps could be altered by injecting fake data into the service provider database. Thus, a compromised back end should be taken into account as an attack vector.

Another example considers over-the-air firmware updates. During firmware updates, the firmware image delivered by various media (OTA, USB, Bluetooth, mobile app) could be intercepted and decrypted. The attacker could reverse engineer the firmware contents, revealing internal device operation and potentially also stored proprietary information (e.g. keys, commands). In a more sophisticated scenario, an attacker might tamper with the firmware image and use it to reprogram the car's microcontroller to change its operation.

Although pure back end-related topics are considered beyond the scope of L3Pilot, secure OTA updates will be included in the analysis of attack surfaces.

3.4 Attack Surface

Based on the ISACA glossary,[2] an attack vector is a path or route used by the adversary to gain access to the target (asset). There are two types of attack vectors: ingress and egress (also known as data exfiltration). Focusing on the software, "[t]he **attack surface** of a software environment is the sum of the different points (the 'attack vectors') where an unauthorized user (the 'attacker') can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure" [27]. Generalizing the definition above to the operating environment of an L3-type vehicle (SW, HW, and the road context) is the object of this section.

3.4.1 Intro: Possible types of attack

Figure 3.7 highlights the potentially vulnerable xCUs (various control units) and sensors that are of importance to an L3 automated vehicle, featuring functionality similar to the L3Pilot such as Urban Chauffer, Highway Chauffer, and Parking Automation. The vehicle has an ADAS ECU at its heart, which is responsible for the automated driving and control. The ADAS ECU in turn gathers inputs through one or more radars, LiDARs, and cameras in addition to the pre-installed maps and GPS coordinates over the GPS receiver. The ADAS ECU is connected to a gateway, which in turn connects it with other networks in the vehicle. The TCU (telematics control unit for tracking) is also a potential target, as it may be connected to the outside world using wireless external interfaces such as Wi-Fi but also internally to the gateway inside the vehicle. The gateway then provides connectivity from the TCU to the ADAS ECU.

Security attacks on the vehicle can be classified into internal and external attacks. Certain attacks can be launched on an automated vehicle from outside of the vehicle by influencing

[2] https://www.isaca.org/Pages/Glossary.aspx?tid=2049&char=A.

the sensors or by exploiting the external connectivity such as mobile communication, Bluetooth, GPS. These attacks are labelled as **external attacks** in Figure 3.7.

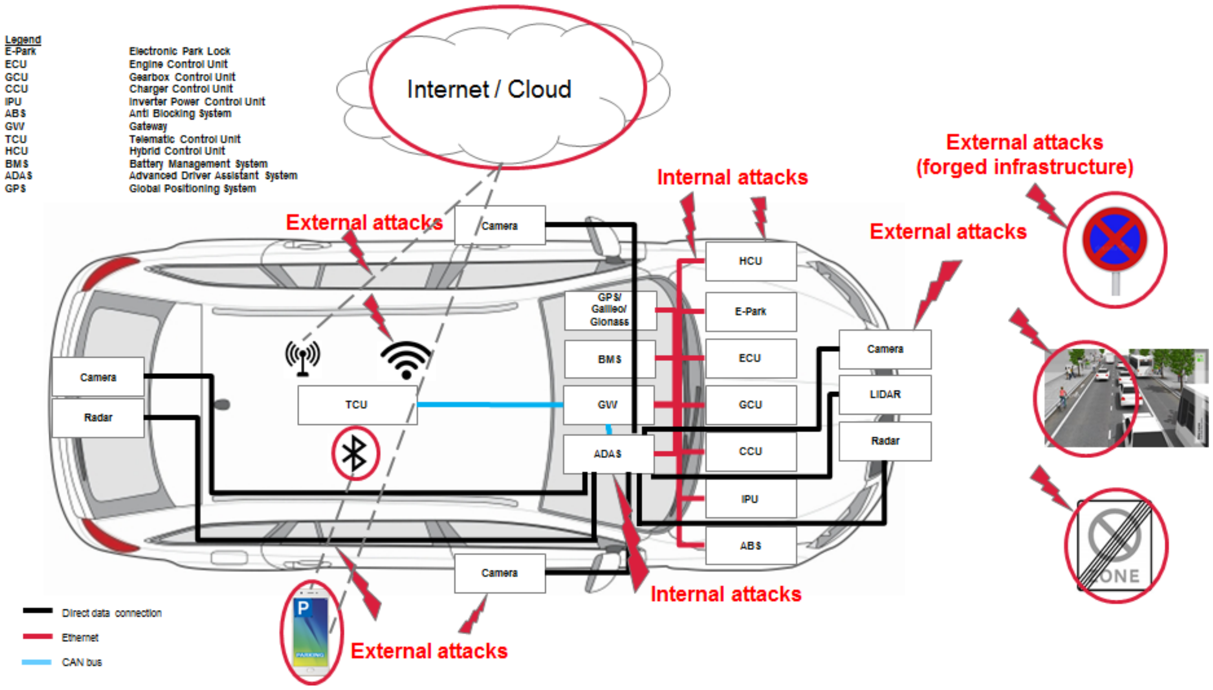


Figure 3.7: Internal attacks vs external attacks for an L3-type vehicle.

Other attacks can be launched from the inside of the vehicle, e.g. through malicious software flashed onto an ECU. This includes attacks performed on vehicular components that are not directly exposed to the outside world, such as the ADAS ECU. These attacks are depicted as **internal attacks** in Figure 3.7.

It is also possible to use external attacks to break into the system and, after gaining access to the internal vehicular components, to install malicious software (malware) on the ECUs/sensors and then use the malware to perform an attack similar to an internal attack. The attack itself can be passive or active and can also be set up to take place at a later point in time, e.g. when the vehicle is at a particular physical location.

According to [31], attackers may focus on different parts of the vehicle's components, such as:

A. *Data:* Attackers could target *stored data* in some ECUs; this data could be cryptographic private keys, digital certificates, or private vehicle and driver activities (e.g. vehicle location, navigation destination, etc.). *Transferred wired/wireless data* within the vehicle could also be threatened. These data include:

   a. In-vehicle exchanged data between different components or one component and its sensors. Spoofing the transferred data between the on-board system and the pressure sensors on the tires is an example of the vulnerability of such data [28].

   b. Transferred data between the vehicle and the external world; such as V2V communication data, V2I communication data, etc. [12].

B. *In-vehicle hardware:* Generally, attacking the hardware infrastructure (ECUs, sensors, and On-Board Units) requires direct access to the target devices. Attacking in-vehicle hardware could occur by replacing a device with a malicious one, or even by installing new hardware that performs mischievously. Sometimes, the attacked hardware may not be a part of the vehicle itself but rather a plugged-in device. The attacker could aim to degrade the performance of the vehicle's components or even lead them to produce misleading results intentionally.

C. *Software and framework:* The massive amount of integrated software on each vehicle and the different levels of security auditing among different vendors make them more susceptible to attacks. The framework that controls the ECU could be a target for various attacks; some attackers could tamper with the framework of the ECU intended to achieve superior performance [30]. A malicious update of one application or of internal parts of the framework could pave the way for the attacker to inflict damage on the vehicle.

3.4.2 Overview of attack vectors

This overview reviews attacks without attempting to discuss their feasibility. Some attacks are quite difficult to perform, others have a remote possibility, while others have already been proven in the field. If an attack is listed it does not necessarily mean that the attack can be exploited in L3Pilot vehicles. With this section we also follow the central rule of security: hiding knowledge does not make it less accessible in the long run (security by obscuration).

Security attacks on modern automobiles with electronic components and external connectivity have been analysed and documented in the literature; see [6]–[15].

In [6], one of the earliest analyses of cyber-attacks in the automotive field, the authors discuss attacks on automated vehicles and connected automated vehicles. In [7] the authors have demonstrated that an attacker who is able to infiltrate any ECU can leverage this ability to completely circumvent a broad array of safety-critical systems. The authors assume that it is possible to access an ECU and examine the consequences but do not study how such an access could be possible. They demonstrate how one can control a wide range of automotive functions and ignore driver inputs, by disabling brakes, selectively braking individual wheels, and stopping the engine completely. The attackers also claim to have been successful in embedding malicious code in the telematics unit of a car by bypassing the challenge-response based authentication. In [7], the authors have presented feasible attacks on different bus systems used in modern vehicles, including CAN, LIN, and FlexRay. The most commonly used network for in-vehicular communications is the CAN bus. Vulnerabilities of the CAN bus and the attacks on it are documented in [8]. Attacks on Ethernet-based networks have also been well studied and documented, e.g. in [9], as Ethernet is one of the most widely deployed protocols. Lately, the topic of security in vehicle-to-infrastructure and vehicle-to-vehicle communication has also been quite extensively researched [10]–[12].

The remainder of this Section investigates and discusses the attack vectors in L3 automated vehicles. Keeping as a reference the generic architecture diagram introduced in Section 3.4.1 (see Figure 3.7) and clustering the attack vectors by the attacker's distance to the attack surface under attack, the **attack surface** can be divided into **three major types**.

The first type is the zero-distance attack and involves (direct or indirect) **physical access** to the vehicle or to infrastructure often visited by the vehicle. In the first case, such access can be obtained, for example, by a mechanic or by someone using the vehicle and manipulating it. Regarding the second case, the possibility of (temporarily) altering the environment, e.g. by erasing a lane or adding a new one in order to mislead the perception sensors, is one example of a potential new attack related in particular with the increase in computer vision algorithms used to provide robust automated vehicle perception.

The second type is an attack on the vehicle from a **short-range distance**, using attack paths such as Bluetooth or short-range wireless access or else attacking the reception of vehicle sensors through e.g. LiDAR, radar spoofing, or camera blinding.

The third type consists of attacking an automated vehicle from a **long-range distance** through its long-range wireless communication interfaces such as GPS, GSM/GPRS, cellular, or Internet connectivity.

These three categories are analysed further in the subsections that follow.

3.4.2.1 Zero-distance attacks (physical access)

If the attackers gain physical access to the targeted vehicle and its system, even for a short time, they can perform many different attacks to compromise the security of the automated driving. Physical access can occur if the attacker is someone trusted by the owner of the vehicle, e.g. a mechanic or a friend who borrowed the car. The attacker can also gain physical access to a parked vehicle by first attacking the keyless entry system and opening the doors, e.g. by using the attacking methods discussed in [14] and [15]. If possible, the attacker might also rent an automated vehicle to gain physical access, then install the devices or the malicious software to carry out the attack at a later point in time.

OBDII CAN interface

Injecting arbitrary CAN packets or changing a bit in a CAN frame – creating error codes leading to the blockage of a specific in-vehicle component – has been proven to be possible through the common OBDII port of all modern vehicles [2]. Research [32] has revealed susceptibility to a type of attack in which an OBD-II aftermarket device can potentially receive arbitrary CAN traffic from outside the vehicle via its wireless radio interface and pass it unfiltered to the internal CAN bus through the OBD-II port.

Advanced Driver Assistance System (ADAS) ECU

It would be very appealing for an attacker to connect to the ADAS ECU by plugging into the gateway and send spoofed messages on behalf of the ADAS ECU to other ECUs. This is possible since the ADAS ECU is connected to the gateway and other ECUs using an Ethernet network, as shown in the architecture of Figure 3.1. In some cases, the communication occurs over a CAN bus instead of the Ethernet network. It is also possible to sniff over the network and listen to the packets from the ADAS ECU to observe the request and response messages. Once enough information is gathered, the attacker can spoof messages to carry out the desired attack. The attackers might also be able to read the firmware of the ECU or even replace it with their own malicious firmware. It is also important to note that an attacker might be able to physically replace the ADAS ECU if adequate security measures are not in place. This would enable the attacker to spoof messages on behalf of the ADAS ECU.

This category of attack can be avoided by using an authentication mechanism, such as by using digital signatures or message authentication codes. The communication can also be secured using a network security protocol, such as transport layer security (TLS) or IP security (IPSec). It is important to note that if instead of Ethernet, another underlying communication networking protocol, such as CAN bus is used, then the corresponding security protocols, e.g. secured/authenticated CAN, should be used.

Firmware access

With physical access to the target vehicle (or a similar vehicle from the same OEM) and the communication network or the ECUs, it is possible to read the firmware either by reading the flash memory of the ECU over the CAN bus or by completely de-soldering the flash memory out of the ECU and reading it out through a flash memory reader. This memory content can be used by the attacker to reverse-engineer the firmware, in order to find security loopholes and seek to exploit them. Afterwards, the identified loopholes of the firmware can be used for exploitation at run time, once the attacker has gained access to the in-vehicular network via other means, such as through Wi-Fi, Bluetooth, or other types of external connections.

One potential solution could be to store the firmware encrypted in a protected memory area, such as on a hardware security module. Similarly the cryptographic key material should be protected using additional mechanisms.

Sensor replacement

Through physical access, an attacker might replace a sensor with a malicious one to report false measurements, or disconnect a legitimate sensor and spoof signals on behalf of the sensor by directly feeding desired signals/inputs, in order to perform an attack. This attack is substantially more realistic as some sensors are accessible from the outside of the vehicle.

As a remedy, the communication between a sensor and the corresponding ECU responsible for the sensor should be secured, e.g. through the use of cryptography (authentication and/or encryption). However, this solution works only for digital sensors. For other types of sensors, other modern research solutions should be investigated, such as the concept of a data aggregator or homomorphic encryption.

Side channel attacks

Side channel attacks have been demonstrated for embedded systems, where an attacker is able to observe and exploit the information gathered from a particular implementation. A side channel attack typically includes gathering information from power analysis [16], timing analysis [17], electromagnetic leaks [18], and cache analysis [19]. The goal of a typical side channel attack is to guess the cryptographic key(s) in use, based on the information gathered from the side channel's statistical analysis. Against a vulnerable system, the attack is computationally inexpensive and often requires only known cipher texts [17].

In the context of the automotive domain, these attacks might be launched on one or more ECUs in the case of physical access. These attacks guess the cryptographic keys being used by the ECUs for secure communications in operations such as encryption and authentication using the above-mentioned techniques [16][19]. Side channel analysis might also be used to guess the cryptographic algorithms, e.g. by guessing the type of processing being done, such as square and multiple operations of the RSA. If static keys are used, a successful attack on one vehicle will compromise multiple vehicles from the same OEM.

USB interface

USB is a pervasive technology that is used quite extensively in modern computing technology. It is used in a wide array of, sometimes lesser known, usage models. In the context of the automotive domain, the USB interface is typically a part of the infotainment system. Due to some of its capabilities, it is a very tempting attack target and has been used for a number of attacks in the past.[3]

An attacker might trick the user into installing malware by simply connecting a USB drive to the USB interface on the car. An attacker might set up an Ethernet network over the USB interface and use it to detect the exposed internal services by running a port scanner. This also opens up the possibility of malicious code execution by performing a software update on services that are expecting an update over the USB interface and are not properly secured.

As a precaution, the auto-run capability should be disabled by default. This will protect against malware installation through the simple insertion of a USB drive. The execution of unsigned code from a USB device should not be allowed. Only signed code from a trusted third party should be executable. The gateway connecting the infotainment system ECU to the safety critical ECU should have security capabilities such as a firewall, as well as some basic intrusion detection capability.

[3] http://illmatics.com/Remote%20Car%20Hacking.pdf.

CD/DVD player

Most modern automobiles include a CD/DVD player to play the media files of the user (driver, passenger). If the media file is infected with malware, this will be loaded and executed by the infotainment system software. Once this code/malware is executed, it may escalate privileges if necessary and send commands to the safety-relevant ECUs. In the absence of any security measures, this can compromise the security of the vehicle and its occupants by spoofing and sending false messages to the safety-critical ECUs.

Only authorized code should be executed on each ECU, including the infotainment system ECU and the TCU. The code should be signed and authenticated on execution. Messages exchanged between the ECUs, especially between the safety-critical ECUs, should be authenticated through an authentication protocol, e.g. using a secured CAN bus. Moreover, the gateway that transfers messages from one network to the other – e.g. from the non-safety-related FlexRay bus to the safety-critical CAN bus – should be hardened against internal and external security attacks. It might also be useful to add some basic intrusion detection and/or prevention capabilities.

(External) Road infrastructure

Cyber security is about more than just the vehicle. The possibility of altering the environment in order to mislead the perception sensors is one example of a potential new attack [6] given the increase in computer vision algorithms used to provide robust automated vehicle perception (recently developed algorithms such as adversarial machine learning constitute proof of concept for cheating on ML data-driven approaches [33]). This is considered in the parking use case analysis (see Sec. 5.3). Such an attack is easier since a vehicle often visits the same road segments, as in the case of parking in a private garage. Such an attack, i.e. by adding a road element that never existed or is not supposed to exist at that place, could be equally effective in parking functions that have learned the parking trajectory a-priori or in more sophisticated parking functions that find the optimum path dynamically using online simultaneous localization and mapping. In [6] on the other hand, highway/urban driving and faked pictures or traffic signs for cheating camera-based perception are considered.

3.4.2.2 Short-range distance attacks

Wireless access provides an attacker the ability to penetrate the in-vehicular network without physically connecting to it. An attacker might be in the proximity of an automated vehicle, such as on the roadside or in a following vehicle, and be able to attack the vehicle with a short-range wireless connection. An example of short-range wireless access is penetrating the system through its Bluetooth or Wi-Fi interface. A possible countermeasure is to use proper authentication and authorization mechanisms as well as calibrating the range of wireless access to a minimum. In the case of automated driving without V2X communications, wireless access is primarily intended for the driver or passengers of the car rather than helping to perform driving tasks.

Bluetooth

Bluetooth is a wireless technology that might be available for connecting a smart phone to the vehicle for user assistance during navigation and parking, or to provide hands-free interface to mobile communication in the vehicle. Bluetooth is not secure by design and can easily be exploited. Bluetooth messages can be sniffed and/or spoofed. The Bluetooth stack itself has been demonstrated to be vulnerable to corruption, resulting in the crashing of relevant components. Additional security measures have to be taken for protection against attacks over the Bluetooth interface. These include switching off Bluetooth when not in use, making Bluetooth undiscoverable, pairing a Bluetooth device only with user permission or multifactor authentication and authorization, using some form of encryption, frequency hopping techniques, and signal range calibration.

Wi-Fi

Wi-Fi (standardized IEEE 802.11) is a wireless technology for local area networking based on the IEEE 802.11 standard. Wi-Fi can connect most of the devices in common use today, such as smart phones, tablets, and laptops, using a wireless connection to form a wireless LAN. The devices can then be connected further to the Internet using a wireless access point connected through the wireless LAN. The same is true for vehicles equipped with a Wi-Fi gateway/router. The passengers of a vehicle might interconnect using Wi-Fi or use the gateway to connect further to the Internet. As the connections are wireless, anyone within the range of the network with a wireless network interface controller can attack the network with less visibility compared to someone with physical access to a wired network. An earlier security method for protecting from attacks on Wi-Fi was introduced as Wired Equivalent Privacy (WEP) in 1997. WEP uses an RC4 stream cipher, with 64- or 128-bit static keys together with a 24-bit initialization vector. In 2001, it was shown by Shamir et al. [16] that an RC4 key can be guessed within minutes. WEP has therefore been abandoned due to its weak security and replaced by the Wi-Fi Protected Access (WPA) series of security protocols..

WPA uses a 128-bit key for each protected packet as compared to the static key used by WEP. WPA also replaced the cyclic redundancy check (CRC) code used in WEP with a message authentication code (MAC) for a higher level of data integrity. WPA’s security was increased through WPA2, which includes mandatory support for an Advanced Encryption Standard (AES) algorithm for data encryption. Recently, in January 2018, a further enhanced version of WPA2 was introduced as WPA3. This is in response to the KRACK [21] attack on the WPA2 protocol, which tricks the victim into reinstalling the key already in use by manipulating the handshake messages.

Wi-Fi access point

Some vehicles feature a Wi-Fi access point as a component of the TCU, providing Wireless LAN to the passengers in the vehicle. This can be very convenient for the vehicle passengers, e.g. for sharing data such as text, files, and photos. However, at the same time it could be a security risk for automated vehicles, especially in the urban case scenario. A determined attacker might have ample opportunity to stay in the vicinity of the vehicle, e.g. due to a traffic jam, and gain access to the in-vehicular network through the Wi-Fi access point.

Some protection mechanisms from external attacks could be to enable network encryption, e.g. WPA2 (IEEE 802.11i-2004) or WPA3 (if applicable), filter MAC addresses, and calibrate the signal range to the necessary maximum.

Telematics Control Unit (TCU)

A telematics control unit is typically connected to the external world using wireless communication interfaces, such as Wi-Fi, Bluetooth, and/or GSM/GPRS. This makes it a tempting target for short-range or even long-range attacks. If an attacker can compromise any of these wireless communication interfaces, they can gain entry to the TCU. Afterwards, the attacker might be able to penetrate further into the vehicle and re-flash the software of the TCU through an unauthorized software update. This would give the attacker the possibility to penetrate further into the ADAS network by connecting to the gateway from the TCU and making their way into the ADAS network if the gateway is not hardened enough to withstand the attack.

The TCU should be hardened against attacks through wireless interfaces. In-bound connections need to be closed. Unnecessary ports and services running on the TCU as well as the gateway should be closed. When necessary, secure communication protocols such as TLS or IPSec, with authentication, should be used.

LiDAR

LiDAR is a sensing method that uses pulsed laser light, as opposed to the radio waves used by radar. It uses the return times and wavelengths to make digital 3D representations and high precision maps of the environment. In automated vehicles, LiDAR is used for control and navigation by understanding the environment and recognizing lanes, license plates, obstacles, and street signs. This is highly useful in the urban use case scenario, where a vehicle must rely on LiDAR, cameras, and radar to understand the environment, such as the traffic situation, obstacles, and availability of lanes, in order to navigate in the urban area.

A LiDAR is however, vulnerable to external interferences due to its exposure to the outside world of a vehicle. Deceiving a LiDAR is analogous to blinding the driver of the vehicle. LiDAR signals can be spoofed [9] to trick an automated vehicle into a false understanding of the environment, resulting in potentially incorrect decisions, especially if sensor redundancy by design is not followed. This includes presenting false objects and obstacles to a vehicle, when they do not exist. Another possible attack scenario would be to jam the sensing ability by incapacitating the LiDAR with false signals (DoS attack) such that it can no longer identify actual obstacles [9].

The number of LiDAR sensors should be kept at an optimum level, so that if one or more of the sensors are spoofed, the remaining can provide correct input. This means an intelligent data analysis system/software must be in place to analyse the input data and to separate the spoofed sensor inputs from the correct ones. Needless to say, this has to be done in real-time, as traffic situations change frequently in the urban driving scenario.

Radar

Radar is used to detect the distance, angle, and speed of objects. It has a transceiver and relies on reflected radio waves to perform these tasks.

Just like LiDAR, radar is also vulnerable to external attacks and interference. Radar jamming and external signal interference are well-known security problems associated with radar.

False input of the velocity and distance of other vehicles and objects on the road might trick a vehicle into changing its lane or merging into the traffic in other lanes when this is not possible. This could result in accidents or at the very least in disruptions to traffic.

Camera

High-resolution cameras are used by automated vehicles for navigation. Camera images and videos are used for lane detection, object detection, object tracking, and traffic sign identification. In order to provide all these features, the application extracts the regions of interest from an image acquired through the camera, performs feature extraction on these regions, and classifies them into different categories.

Potential attacks on the camera include presenting false traffic signs to a car to trick it into performing the desired manoeuvres. As an example, presenting a false red traffic light or a false pedestrian zone sign to a vehicle might make the vehicle unnecessarily apply emergency brakes. Depending on the traffic and speed of the vehicle, this could have undesirable consequences.

3.4.2.3 Long-range distance attacks

Long-range wireless access allows an attacker the possibility to connect to the system from a great distance, virtually anywhere in the world, and perform the attack by controlling the car in real time or by installing malware that then performs the attack at a later point in time. A remote connection is typically possible through a gateway in a vehicle that should be appropriately secured. In general, access from outside should be restricted based on firewalls, multilevel authentication mechanisms should be used for connection establishment, and the connections should be monitored for malicious activities using intrusion detection systems.

Mobile communication

There are many mobile communication standards in use. It is expected that automated driving will use 5G technologies (fifth generation of mobile communications) for potentially numerous applications such as audio, video, and data communication.

From a security point of view it is important that the well-known attacks reported in the literature be mitigated. These include eavesdropping, unauthorized access to the network as well as the data, spoofing, and DoS/DDoS attacks.

Many security solutions exist for data confidentiality and authentication. However, for future use cases, the 5G network is the most promising. A range of solutions has been proposed for 5G networks and can be applied to the automotive domain for security. The interface for connectivity from the outside to the vehicle should typically be closed, unless truly necessary, but then should be properly secured using firewall and/or intrusion detection systems.

Radio

A modern automobile typically includes a radio receiver for receiving broadcasted audio. Typical radio systems include satellite radio (e.g. SiriusXM), digital radio, or the Radio Data System. The range of radio signals depends on such factors as transmission power and modulation mode, as well as environmental factors such as the terrain and interference from other signals.

Typically, a radio receiver is a part of the vehicle’s media system or telematics unit, which also includes a CD/DVD player and a USB interface. This might in turn be connected over the in-vehicular network to the safety-relevant ECUs either directly or through a gateway. Attacking the radio software stack to gain access to the in-vehicular network is a typical attack surface which is common to all media systems including radio, CD/DVD player, and USB interface.

It was recently shown that by simply playing an audio transmitted to the audio player via radio waves, a malware hidden in the audio can be transmitted [52]. This malware can then be used to infect the internal network and ultimately attack the safety-critical ECUs.

Normally the software components of a radio should be hardened against such attacks. In order to provide additional security, the gateway connecting different networks inside a vehicle should be hardened such that only an authorized and valid message is transferred from one network to the other, so that, for example, a message from the media ECU is not forwarded by the gateway to the engine control unit.

Internet

A vehicle might be connected to the Internet using Wi-Fi or cellular connections. Most often these are found in the telematics units and infotainment systems.

The Internet has a wide range of known vulnerabilities and attacks. There are many solutions to address those vulnerabilities and provide security. These include the security protocols at the appropriate layer, such as Transport Layer Security (TLS), IP Security (IPSec), and MAC Security (MACsec). Additionally, other well-established mechanisms for security should be integrated as appropriate, such as access control, firewalls with black and white lists, intrusion detection systems, authentication and authorization, multifactor authentication, and malware detection software.

Cloud connectivity

A vehicle might be connected to a back-end cloud for various reasons including data storage, sensor data analysis, and financial transactions. Regardless of whether this connectivity is provided through Wi-Fi access or a mobile network, it opens up the vehicle to attacks from the Internet. Cloud connectivity should therefore be secured through the same mechanisms as proposed in the section above on the Internet.

Over-the-air (OTA) updates

Unauthorized software updates, as well as data updates including digital maps, pose a great security risk. However, OTA is a greater threat because of its exposure to remote connection exploitation. This could include a whole range of attacks such as man-in-the-middle attacks, spoofing, and session hijacking, if proper security measures are not in place. In the absence of the right set of security measures, an attacker might update the e-maps to show false routes, replace the software on an xCU, or infect the software with malicious code.

The communication channel for software download should be secured through confidentiality, integrity, and authentication mechanisms. It might be possible to use a standard security protocol such as TLS or IPSec, depending on the communication architecture. The code, or data, should be digitally signed and authenticated at the receiver before being installed on the vehicle.

GPS

Global Positioning System (GPS) – the generic term is GNSS for Global Navigation Satellite System; other systems are GLONASS, Beidou, and Galileo – is used by semi-autonomous vehicles for geofencing to limit automation to e.g. highways and by future autonomous vehicles for navigation. It has been extensively used in the aerospace and naval domains for navigation for decades. GPS spoofing has been studied extensively in the literature, e.g. [22] and [23]. GPS jamming attacks are also very common. A review of GPS jamming and anti-jamming techniques can be found in [24].

3.4.2.4 Checklist of attack vectors vs countermeasures proposed in the literature

Based on the foregoing analysis of vehicle-related attack vectors and countermeasures in the literature as well as from L3Pilot technical questionnaires discussed with L3Pilot prototype owners, we summarize below the list of possible attack vectors and possible countermeasures identified for the three L3Pilot AD functions: Highway Chauffeur, Urban Chauffeur, and Parking Chauffeur. Please note that the following tables, Table 3.2 to Table 3.4, do not include the non-vehicle related attack on external infrastructure added at the end of Sec. 3.4.2.1 (which will be part of the parking application analysis).

Table 3.2: Summary of L3-type vehicle attack vectors for physical access to vehicle entry points and countermeasures

Vehicle entry points and types of attack	Countermeasures
OBD-II	
Unauthorized access Spoofing (e.g. ejecting frame)	Separate CAN communication from the network stack

Vehicle entry points and types of attack	Countermeasures
DoS attack	Allow an application to send a request only from a list of pre-chosen OBD-II commands
ADAS ECU	
Malicious software update Message spoofing over the network DoS attack	Intrusion detection system Secure communication using authentication or encryption mechanisms Secure booting of ECU Signed code Secure software execution on xCU
Infotainment system, CD, USB devices	
Malware injection Malicious code execution DoS attack (e.g. CAN bus attack) (includes a whole range of USB devices such as USB-to-Ethernet adaptor)	CD/USB secure software coding and recognition of trusted CD and USB formats according to standards Intrusion detection system Disable auto run Hardened USB interface software stack Code signing Secure in-vehicular gateway (firewall, IDS)
Sensors	
Fake sensor data (by replacing sensors) Sensor damage Compromised sensor	Sensor level security: • Secure communications • Sensor authentication Sensor integrity checks and anomaly detection
Side channel attacks	
Guessing the keys in use through side information	Correlation of leaked information to the secret key must be minimized, e.g. by inserting dummy operations or dummy memory access.

Table 3.3: Summary of L3-type vehicle attack vectors for short-range access to vehicle entry points and countermeasures

Vehicle entry points and types of attack	Countermeasures
Bluetooth	
Eavesdropping	Switch off Bluetooth when not in use

Vehicle entry points and types of attack	Countermeasures
DoS attack	Make Bluetooth undiscoverable Pairing with user authorization using a secure and long passkeys/PINs Unpair the devices immediately after use Encryption using E0 has its weaknesses but still better than not using it Frequency hopping is used as one solution Calibrate signal range to the necessary maximum as Bluetooth can have a range up to 100m
Wi-Fi/IEEE 802.11 (Vehicle Hotspot)	
Eavesdropping/Sniffing Spoofing Man-in-the-middle DoS	Enable network encryption, e.g. WPA2 (IEEE 802.11i-2004) or WPA3 if applicable Filter MAC addresses; however, the authorized addressed can be spoofed too Calibrate signal range to the necessary maximum
LiDAR	
Blinding Spoofing attack by causing illusions in the sensing Spoofing to make obstacles appear much closer than they actually are, to activate emergency braking DoS attack by incapacitating the LiDAR from sensing a certain direction Relay attack Replay attack	Heuristic, machine learning, and AI-based solutions for attack detection Redundant sensors Regular sensor calibration and logging of the check
Radar	
Jamming Spoofing Blinding	Heuristic, machine learning, and AI-based solutions for attack detection Redundant sensors
Camera	
Spoofing	Heuristic, machine learning, and AI-based solutions for attack detection

Vehicle entry points and types of attack	Countermeasures
Blinding	Redundant cameras that overlap either fully or at least partially
TCU Telematic control unit mobile connection	
Malicious software update DoS attack Viruses Privilege escalation Port opening for follow-up attacks from the Internet	Secure software boot Code signing Authorized and authentic software execution on the TCU and in general any xCU

Table 3.4: Summary of L3-type vehicle attack vectors for long-range access to vehicle entry points and countermeasures

Vehicle entry points and types of attack	Countermeasures
Cellular connection	
Eavesdropping Unauthorized Access Spoofing Dos/DDoS Attacks	Service-oriented security (Diversified) Identity management Authentication by network and service providers Privacy protection using cryptographic services and security protocols Block (all unnecessary) incoming traffic
Over-the-Air updates of software and maps	
Spoofing Elevation of Privilege Tampering DoS attack	Trusted source authority Authentication Integrity checks Intrusion detection system Secure booting
GPS	
Spoofing (incorrect coordinates) Jamming Note: The attack could also happen over short range	Intelligent algorithms for GPS data verification Other simultaneous localization techniques based on perception
Internet	

Vehicle entry points and types of attack	Countermeasures
Sniffing Spoofing DoS Malware injection Viruses Worms	Secure software coding and restricted access to OBU functioning Regular updating and patching of system software and firmware Many solutions exist to provide security over TCP/IP Appropriate solutions, depending on the scenario, should be applied, such as: • TLS • IPSec • MACsec • Multilevel security • Dual encryption • Access control • Authentication • Multifactor authentication
Cloud connectivity	
Back end data storage and processing Hack connections/sessions Introduce malicious data Introduce malicious code	Restricted access Secure firmware booting Digital signature Trusted software execution and update on the TCU
Radio receiver	
A radio receiver can be infected with malware by simply letting it receive an audio including the malware	Hardened media player software stack Code signing Secure in-vehicular gateway (firewall, IDS)

3.5 Discussion

When security experts hear about a new cyber security issue in the automotive domain, they tend to dismiss it quickly because car hacks often require either some form of local access or a remotely exploitable vulnerability, which can be patched to solve the problem. Direct access is considered highly improbable, yet current trends in transportation challenge such beliefs, as it is now much more common for different people to gain access to someone’s car. Consider car sharing, ride sharing, automated vehicles – these are becoming commonplace scenarios where many users can access the same vehicle. This change in paradigm calls for an appropriate change in the threat model, which should encompass a local attacker. Although there is agreement that a paradigm shift as argued above is needed, for the purpose of this project, local access of the attacker during piloting activity is considered to be very unlikely and hence other types of attack surfaces are highlighted within this study.

Please note that in the application-oriented part of the analysis that follows (see Section 5), the focus is primarily on attack surfaces introduced by the L3Pilot AD functions, and not on attack vectors for vehicles featuring Level 1–2 automation such as OBD-II, GPS, DAB-Radio, or telematics/infotainment modules, which have already been covered by the literature and are only mentioned as background.

Other underlying assumptions in this deliverable are:

1. The focus of attention for this report is on L3 (and higher) automation systems. This means that the driver's attention is likely to be focused on other subjects while the vehicle is being automatically driven, so that a certain amount of time (at least several seconds) is likely to pass before the driver is able to re-engage to take any corrective actions that may be needed. Therefore, the driver cannot be assumed to be constantly available as the ultimate fallback to ensure safety, in contrast to the assumptions underlying the ISO 26262 [34] functional safety standards, which assume that the driver is indeed the final guardian of safety. This fact contributes to the effect that the ability of the driver to observe an attack can be significantly reduced and hence controllability, which will be introduced later as a factor in our methodology, is reduced. It is also assumed that the driver is not required to have any special training or licensing to operate a vehicle equipped with an L3Pilot AD function, so that driver behaviour should be assumed to be typical of current drivers.
2. The main automated driving functions in this project do not include V2V or V2I communications to support their control functions; thus, the attacks based on communications from external sources apply only in the case of a remote control AD function via the user smartphone, as in the parking application.

For L3-equipped vehicles in the urban and highway environment, an attacker would be more inclined and tempted to attack the vehicle remotely over its external wireless interfaces as compared to gaining physical access. One of the reasons is that the chances of the attacker being caught are lower, as no physical contact takes place. Another reason for this motivation is that by gaining access by circumventing the wireless communication interfaces, the attacker can remotely control the vehicle while it is being driven. It might also be preferred because physical access of any kind is not possible. However, this does not rule out the possibility of physical access to the vehicular components and to the in-vehicular networks, especially to the ADAS ECU, radio, CD/DVD player, and USB interface, which remain highly compelling targets. Gaining physical access is more tempting in the case of a parking AD function, since the vehicle can be located more easily by an attacker. Connecting via the USB interface opens up further attack possibilities. This is due to the fact that conversion from the USB to almost any other communications interface is highly flexible. It is also very easy to introduce malware or a malicious piece of code through an external medium such as the USB or CD player. In all three cases (urban, highway, and parking), and especially in cases where low velocities apply, such as during traffic jams or parking, an attacker could also focus on the external sensors, such as LiDARs, radars, and external cameras. At the simplest, these sensors could be blinded, but many more advanced attacks have also been demonstrated recently [13]. These include spoofing attacks, such as presenting false objects to the sensors and deleting actually existing objects from the scene. The sensors could also be jammed altogether, leading to denial of service attacks. Such attacks would make automated driving extremely difficult, especially in the case of the urban environment, due to the presence of pedestrians and of other vehicles, the majority of which might be not automated driving vehicles (as is the case at the time of writing).

With respect to the impact of an attack, potential safety-critical risks may include:

1. Driver distraction (volume, windscreen wipers, etc.)
2. Engine shutoff or degradation
3. Steering changes (in drive-by-wire vehicles)
4. Acceleration, braking.

There are other, less safety-critical risks, some of which are fairly unique to AD vehicles, as identified in [32]:

5. Theft of the car or its contents
6. Enabling physical crimes against the occupants
7. Insurance or lease fraud
8. Eavesdropping on the occupants
9. Theft of information (e.g. phone list)
10. Vector for attacking mobile devices in the car
11. Theft of personally identifiable information (PII)
12. Tracking the vehicle's location.

4 Threat Analysis and Risk Assessment Framework

4.1 Introduction

A threat model helps a threat analyst to understand different ways in which software, applications, or system architecture could malfunction or be attacked. The process helps identify weaknesses that could be tackled by categorizing and mitigating them with respective countermeasures. Our challenge in this work has been that the threat analysis and risk assessment are based on a generic automated driving function (ADF) description and the limited system information of the HW/SW architecture available during preparation of this report. For this reason, a reference system architecture has been created for use by the L3Pilot cyber security team (see Section 4.1) throughout the SP4-T6.4 work. In addition to the generic reference architecture discussed in Section 4, the actual cyber security analysis is performed on a per-function basis with the aid of a per-function functional diagram that can be found in the application-dedicated Sections, i.e. 5.1.1, 5.2.1 and 5.3.1.

This choice is also supported by the fact that AD implementations can differ by manufacturer and new applications may be developed in the future. As technology improves and expertise becomes accessible, more threats become viable and initial threat identification becomes obsolete. We address these challenges by developing an *application-based approach* as opposed to a component-based one. As AD systems progress to production stage and new applications are developed, our framework may need to be re-applied to account for new information.

In order to select the methodology and define an appropriate threat model, the following considerations were taken into account:

1. Information about the system architecture and hardware/software elements may change, particularly during the concept phase. Focusing on the difficulty of executing an attack instead of vulnerabilities allows a first estimation of risk. This consideration guided us to adopt an attack potential factor, which is estimated based on the difficulty of executing an identified attack scenario as proposed in [35].
2. A formal risk assessment framework is preferred in order to prioritize the risks. Note that the purpose of the assessment is not to calculate exact numeric values of attack probability, but to generate relative values to aid OEMs in clustering and ranking the associated risks in a subsequent step.
3. For the purposes of the risk assessment in this work (refer to Section 6), we limit our focus to attacks that exploit AD and, in particular, the targeted application. We do not assume that any security solutions have been appropriated, although it may be possible that resiliency may come directly from the system architecture (e.g. through redundancy in sensors).
4. TARA – SAE J 3061 [44] vs HARA – ISO26262 [34]: In general, the scope of TARA is wider than HARA. HARA focuses on deviations from the intended functionality that are

caused by failures and may lead to hazards. TARA focuses not only on functionality, but also on the data and extends the scope from safety-related losses to impacts on confidentiality or financial losses. For this reason, TARA will be adopted in this report.

4.2 Relation to Recent Literature

The work most related to ours is that of MCity researchers, who proposed a customizable TARA threat model based on existing approaches [36]. This was created by combining the strengths of threat models from the National Highway Traffic Safety Administration (NHTSA) [41] and the European Commission's E-safety Vehicle Intrusion Protected Applications (EVITA) automotive threat models [44] and expanding on them. These existing models are good, comprehensive examinations that look at automotive applications and their vulnerabilities, but omit considerations about specific sources and actors behind security threats and how they weigh the risks involved in considering an attack. In this deliverable, the following apply:

- Threat agents are reviewed according to their motivations and capabilities to determine the potential likelihood of an attack. While two different attackers might focus on a vehicle's self-parking capabilities, for example, the threat of a lone car thief trying to steal a single vehicle would be significantly different from that of an organized group of dedicated hacktivists looking to harm a manufacturer by disabling a huge number of vehicles.
- Potentially vulnerable components of automated driving applications – such as sensors, GPS systems, or databases that receive over-the-air updates – are analysed according to their characteristics and potential for attack. Combined with the attack method and the targeted application, this allows researchers to estimate the resources required for the threat agent to make an attack successful.
- The attack methods used in the researchers' analysis follow the STRIDE classifications developed by Microsoft [45]: Spoofing Identity, Tampering with Data, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
- Attack potential examines the difference between the threat agent's ability to execute a successful attack and the system's ability to withstand the attack, taking into account such factors as financial requirements, time needed to create and execute an attack, technical expertise of the attackers, and other factors.
- Impact looks at the potential level of loss to the stakeholders, including financial loss, privacy, and safety.

Petit and Shladover [6] offered one of the earliest analyses of security in automated and connected vehicles in their identification of threats in high and full AD. That work made use of the SAE J1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA). The authors assessed potential attacks on AD sensors and infrastructure, using a threat matrix to categorize and prioritize risks by likelihood and impact. In this early threat analysis work of Petit and Shladover, they also include two meta-attack attributes: the **ease of detection** by the driver or by the system and the **controllability**, both of which are potentially useful when determining attack potential and impact but are not present in any of the TARA-inspired methods of the recent literature (with the exception of the very recent SARA model [38]). Hence, we propose in this deliverable an extension of the popular TARA model and argue that these two attributes can be part of a TARA impact calculation, as they directly affect safety and operational impact. While in the recent (2016) paper of [35] they argue that these factors should be part of the after-TARA analysis, we considered them an important addition when defining the System Withstand Potential (currently part of the TARA attack potential model of the state-of-the-art work of [36]) and hence we have included them as a new independent TARA impact-mitigating factor. This approach essentially enhances the SAE J3061 TARA model with ISO 26262 notions. “Controllability” is one of the three parameters adopted by ISO 26262 during HARA impact calculation: when the hazards and all possible hazardous events have been identified, their impact must be estimated by considering the three parameters *severity*, *probability of exposure*, and *controllability*. This was the reason SAE J3061, although suggesting different methods for the rating of risks, includes controllability as an additional parameter only for threats that may impact safety. Note that according to the agenda of ISO 26262, the relation between the two standards and a way of better aligning J3061 with ISO 26262 will be included in new versions of ISO 26262. A similar approach to ours has appeared during the writing of this report in [38], while in [43] an opposite path has been taken to extend the ISO 26262 HARA method.

4.3 Proposed Model: TARA +

To sum up the above analysis, our work borrows elements from the work of both Chalmers University researchers [37] and MCity researchers [36] (being application-oriented and combining NHTSA, EVITA, and STRIDE) and combines these with the more recent work of Montenuuis et al. [38]. The proposed method is called TARA+ and features:

- A simplified attacker profile matrix based on [37];
- An attack surface analysis that also incorporates attack surfaces outside of the vehicle (such as faulty road signage); [NEW]
- An attack potential calculation based on a simplified version of the one proposed in [37] (System Withstand Profile no longer used in calculating the potential of an attack, since it will be replaced by the new “controllability” factor, see below);
- An attack impact calculation that integrates “controllability” and “observability” of an attack (by modifying the controllability definition proposed in SARA [38]) as mitigating factors of the impact. It also adds “Operational Impact” in the Impact assessment (in alignment with [35] and [38]).[NEW]
- A 2D risk matrix based on attack potential and impact as proposed in [37].

Note: We are more interested in the technical feasibility of the attack and less on the role of the adversary (who in most cases can be considered a professional with high motivation). We consider the **2D risk matrix** from [35] easier to understand than the 3D matrix of [36] and so we remove motivation, which was the third dimension, as we consider it redundant.

The different steps of the methodology, including essentially the definition of all intermediate matrices that are utilized and the method of deriving the resulting risk vector, can be explained through the following steps that are visualized in the diagram of Figure 4.1:

- Attack scenario description template
- Threat model parameters (incl. attack **controllability** definition – new factor inspired by ([6], [38])
- Attack **Potential** calculation
- Modified Attack **Impact** calculation (safety and operational effects but also financial and privacy/legislative) taking into account “Controllability” value
- 2D Risk matrix as a linear weighting of Likelihood and Impact.

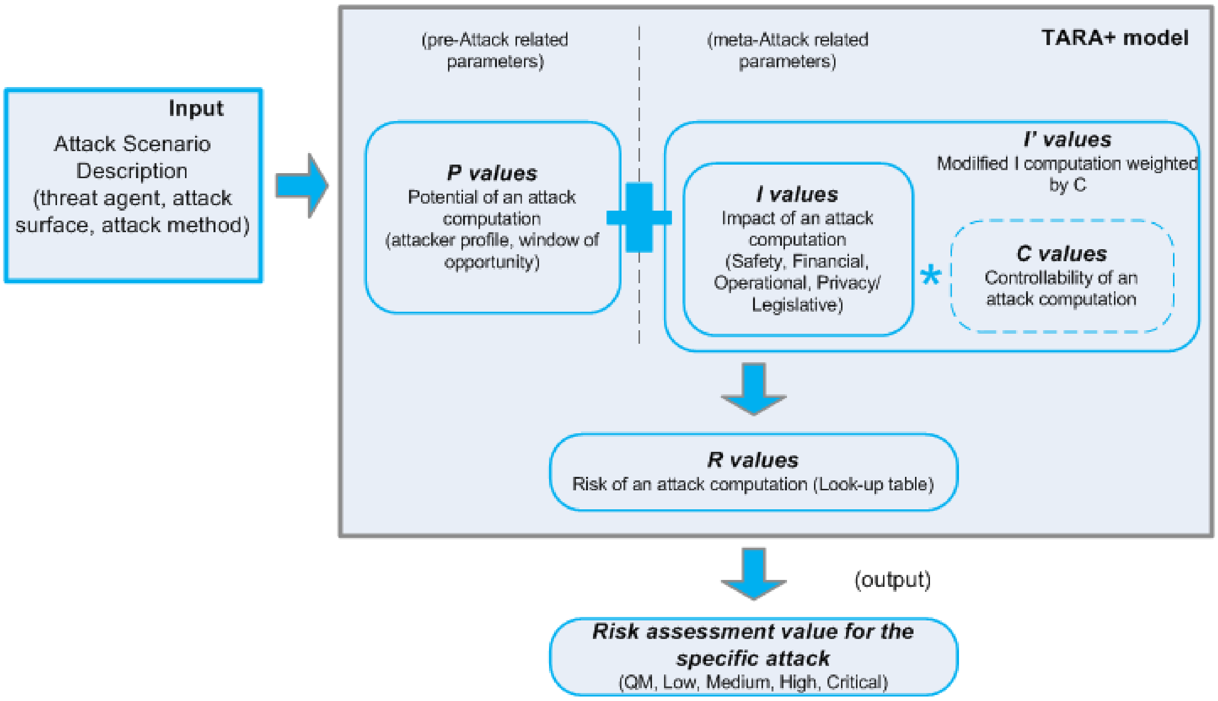

Input
Attack Scenario Description (threat agent, attack surface, attack method)
(pre-Attack related parameters)
(meta-Attack related parameters)
TARA+ model
P values
Potential of an attack computation (attacker profile, window of opportunity)
I' values
Modified I computation weighted by C
I values
Impact of an attack computation (Safety, Financial, Operational, Privacy/ Legislative)
*
C values
Controllability of an attack computation
R values
Risk of an attack computation (Look-up table)
(output)
Risk assessment value for the specific attack
(QM, Low, Medium, High, Critical)

Figure 4.1: TARA+ methodology overview schema.

4.3.1 Attack scenario description template

The attack scenario is described by the parameters shown in Table 4.1 below. For examples of attack scenario descriptions the reader is referred to Sections 5.1.3, 5.2.3 and 5.3.3.

Table 4.1: Scenario description template

Attack Scenario
Attack Name
Threat Agent
Attack Surface
Attack Method
Description

Note 1: The “Attack Method” that appears in the attack scenario table follows the STRIDE model. STRIDE is a threat classification model developed by Microsoft for thinking about computer security threats [45]. It provides a mnemonic for security threats in six categories.

The threat categories are:

- **S**poofing of user identity
- **T**ampering
- **R**epudiation
- **I**nformation disclosure (privacy breach or data leak)
- **D**enial of service (DoS)
- **E**levation of privilege

Note 2: The “threat agent” that appears in the attack scenario table corresponds to specific attackers and attack profiles. Attackers identified for this report are listed in Table 4.3.

4.3.2 Threat model parameters

The threat model attributes for the TARA+ model are classified into two categories that are described as follows:

A) The “potential of an attack” parameters

In order to estimate the likelihood of an attack, hereafter referred to as “potential of an attack”, we use four parameters similar to those used in the calculation of attack potential in the vulnerability assessment of the Common Criteria [5]. The four parameters are:

1. (attacker profile: 1-3) Expertise (E)
2. (attacker profile: 1-3) Knowledge about target (K)
3. (attacker profile: 1-3) Equipment (Eq)
4. (attack profile: 4) Window of opportunity (W) (incl. attack time constraints)

Each of the potential-related parameters has four levels with an associated value, as shown in Table 4.2. The lower the value of the parameter, the more likely the occurrence of the threat. Unlike similar frameworks, we apply a linear scale for each parameter, which facilitates consistent reasoning about the different parameters while deriving the threat level for a particular asset/threat pair. However, the scales can easily be adjusted according to particular needs. Annex 3 includes an explanation of all these parameters, which were first defined in the European research project HEAVENS.

Table 4.2: Threat model attributes: The “potential of an attack” parameters

“Potential of an attack” threat model attributes						
…the attacker profile	**Expertise (E)**		**Available knowledge about the target (K)**		**Equipment required (Eq)**	
	Layman	0	Public	0	Standard	0
	Proficient	1	Restricted	1	Specialized	1
	Expert	2	Sensitive	2	Bespoke	2
	Mult. experts	3	Critical	3	Multiple bespoke	3
…the attack profile	**Window of opportunity[4] (W)**					
	Unlimited	0				
	Large	1				
	Medium	2				
	Small	3				

Determining the parameters considered for the attacker profile (i.e. E, K, and Eq) for specific types of threat agents (profiles are per ISO/IEC 15408; E, K, and Eq values are quantized as in [37]), the following attacker profiles are considered:

[4] As defined in the HEAVENS project, which combines notions of accessibility and time (thus “elapsed time” as in Dominic et al. [36] could be removed from the attacker potential attributes).

Table 4.3: Attacker profiles based on the "potential of an attack" parameters

Attacker profiles	Expertise (E)	Available knowledge about the target (K)	Equipment (Eq)	Classification ranging from [0,9]
Thief (Mr Nobody)	Layman (0)	Public (0)	Standard (0)	0
Owner (unlimited access to vehicle)	Layman (0)	Public (0)	Standard (0)	0
Researchers	Multiple Experts (3)	Public (0)	Specialized (4)	7
Mechanic	Expert (2)	Restricted (1)	Specialized (4)	7
Organized crime	Proficient (2)	Sensitive (2)	Specialized (4)	8
Hacktivist	Multiple experts (3)	Sensitive (2)	Multiple bespoke (3)	8
Competitors	Multiple experts (3)	Restricted (1)	Multiple bespoke (3)	7

B) The "impact of an attack" parameters.

Impact (I) captures the loss to the stakeholders and is modelled via the four following factors as in [37]:

1. Safety (I_S) – to ensure the functional safety of the vehicle occupants and other road users

2. Financial (I_F) – to prevent fraudulent commercial transactions, theft of vehicles, damage to stakeholder reputation, and insurance and warranty fraud

3. Operational (I_O) – to maintain the intended operational performance of all vehicle and ITS functions

4. Privacy and legislation (I_P) – to protect the privacy of vehicle drivers and the intellectual property of manufacturers.

In Table 4.4 below, the numerical scale for each impact factor is provided (which is an integer from 0 to 4 corresponding to the quantization levels “None”, “Low”, “Medium”, “High” and “Critical”).

Table 4.4: Threat model attributes: The “impact of an attack” parameters

Impact factors/ value (I)	**Safety (I_S)**	**Privacy (I_P)**	**Financial (I_F)**	**Operational (I_O)**
0 (None)	No injuries	No unauthorized access to data	No financial loss	No impact on operational performance
1 (Low)	Light or moderate injuries	Configuration data only	Low-level loss	Impact not discernible to operator
2 (Medium)	Severe injuries or moderate injuries for multiple vehicles	Partial data (access to a single update or one application)	Moderate loss	Low losses for multiple vehicles Operator aware of performance degradation Indiscernible impacts for multiple vehicles
3 (High)	Life threatening or fatal injuries Severe injuries for multiple vehicles	Access to complete data	Heavy loss Moderate losses for multiple vehicles	Significant impact on performance Noticeable impact for multiple vehicles
4 (Critical)	Life threatening or fatal injuries for multiple vehicles	Access to data from multiple ECUs in the vehicle	Heavy losses for multiple vehicles	Significant impact on multiple vehicles

NOTE: During final TARA+ assessment per application (see Sections 5.1.3, 5.2.3 and 5.3.3), the impact factors were filled in by the cyber security team based on each expert experience (no dedicated interviews with L3Pilot OEMs have been performed).

In Sec. 5.3.4, the normalized value of the modified impact value that takes into account the “controllability” value will be provided. This “controllability” factor is defined below in Table 4.5.

Table 4.5: Threat model attributes: The “modified impact of an attack” parameters

“Modified Impact of an attack (I’)” threat model attributes					
	Classification of (attack) observability[5] (O)		**Classification of (attack) controllability[6] (C)**		
			Obser-vability	Controllability	Value
…the system withstand profile	Negative – cannot be detected	0	0	Attack cannot be detected by the system or the driver; driver is unavailable[7]	0
	Positive – can be detected by the system (assumes that diagnostics and IDS are in place) or the driver (assumes that driver is familiar with the system)	1	0	Attack cannot be detected by the system or the driver; driver in position to react	1
			1	Attack can be detected by the system or the driver and driver has to take corrective action	2
			1	Attack can be detected by the system and system goes into fail-safe mode	3
			1	Attack can be detected by the system and system goes into fail-operational mode	4

NOTE on how to derive the value of parameter C (controllability):

[5] This is inspired by the “ease of detection” notion considered in the analysis of Petit and Shladover [6]. “Detection” means that the driver is able to recognize an unexpected behaviour of the system and hence should have some prior experience with the AD system.

[6] A “high” level of controllability requires at minimum a 2-channel redundancy design approach that also permits function re-allocation, as well as sensor redundancy and availability through the network as a service [39].

[7] In the L3-level of automation (conditional automation), the driver is expected to be able to resume control of the vehicle’s motion within a few seconds of an adverse event.

The notion of controllability appears also in the ISO 26262 and will be used in this work as a factor influencing the calculation of impact. Estimating it requires knowledge about the AD application, the driver's availability during its operation, and the system's fail-safe or fail-operational design. The value of this parameter needs to be determined for each application and each attack scenario, using available knowledge about the attack surface characteristics and the attack method from Table 5.1, the AD application model under attack (see Sections 5.1.1, 5.2.1 and 5.3.1), as well as the L3Pilot available knowledge of the system's fail-safe or fail-operational design w.r.t a specific AD function and a specific threat. These matters have been discussed in detail in Sections 5.1.4, 5.2.4 and 5.3.4, which follow the application-based risk assessment.

4.3.3 Attack potential calculation (P)

Attack potential is calculated as a linear combination of the attacker profile and the "Window of Opportunity" parameter as proposed in [37], which is similar to the Common Criteria vulnerability assessment [51]:

$$P = E + K + Eq + 2 * W \text{ (Eq. 1)}$$

where E, K, Eq, and W are defined in Table 4.2 "Potential of an attack" parameters and W is weighted by a factor of 2 since it is considered important for the L3 piloting phase under analysis.

As described in Table 4.2, the numerical scale for each P constituent is an integer from 0 to 3 where 0 corresponds to the highest potential for an attack to occur and 3 corresponds to the lowest potential, leading to an overall **P range from 0 (very likely) to 15 (very unlikely)**.

The P values are then quantized to a normalized (inverse) P value, the P*, with a range of 0 (very low probability) to 4 (high probability) according to Table 4.6.

*Table 4.6: Normalized P value derivation: P**

P (Eq.1)	Threat Level	P*
value	(TL)	value
>11	None	0
9−11	Low	1
5−8	Medium	2
2−4	High	3
0−1	Critical	4

Note that the first three P parameters can be determined directly from the choice of the threat agent for a specific scenario (see Table 4.3) and hence only W should be empirically defined for a given scenario.

As proposed in [37], in contrast to the attack potential calculation in the familiar Common Criteria [46], we do not consider the elapsed time required to mount a particular attack as a separate parameter, because it can be derived from other parameters. For example, depending on the attacker's skill level and the availability of the required equipment to mount the attack, the elapsed time may vary significantly – from less than an hour to several months. Similarly, we do not consider the motivation of the attacker as a separate parameter, since it is implicitly defined in the other parameters. For example, a highly motivated attacker may spend a lot of time gaining the necessary expertise to exploit a vulnerability, or spend a lot of money on the equipment needed.

4.3.4 Attack impact calculation (I)

The impact of an attack is formed as a weighted sum of the four "impact of an attack" parameters (see Table 4.4) as proposed in [37]:

$$I = 3I_S + I_F + 2I_O + I_P \quad \text{(Eq. 2)}$$

where I, I_S, I_F, I_O, and I_P are defined in Table 4.3. The weight for privacy and financial impact is set at 1.0 while the weight for operational loss is set to 2.0 and for safety impact to 3.0, to highlight the increasing consequences in the operational and safety areas respectively, resulting in an impact value I in the range of [0, 28].

Since risk is often defined by the two dimensions of likelihood and impact, we used the controllability parameter (stemming from knowledge of the L3Pilot system) in order to influence the impact calculation. Hence, in order to integrate the "controllability" factor, we modify the final impact value, resulting in a modified impact value, denoted as **I'**, that also ranges from [0, 28]:

$$\boldsymbol{I'} = I * (1 - w * C/C_{MAX}) \quad \textit{(Eq. 3)}$$

where C_{MAX} is the maximum quantized *C* value (according to Table 4.5 this is equal to 4) and *w* a constant weight set to 0.5 in order to limit the influence of C in the formula.

Finally the modified impact value I' is quantized to an integer range of 0 to 4 according to Table 4.7. **Quantized modified impact value is denoted with I'***.

Table 4.7: Modified impact value normalization

Modified Impact I'	(I')* quantized
0–4	0 (no)
5–10	1 (low)
11–18	2 (med.)
19–24	3 (high)

Modified Impact I’	(I’)* quantized
25–28	4 (critical)

4.3.5 Risk output (R)

A simple linear combination of the normalized *Attack Potential* (*P* *) and *Modified Impact* (*I’**) values give the final Risk value as proposed in [37] and described in Table 4.8.

Since P* ranges from [0,4] and I’* ranges from [0,4], R ranges from 0 to 8, but it is also quantized to 5 possible values based on Table 4.8, in which “QM” stands for “Quality Management” and denotes the lowest risk level. Final quantized risk value is denoted with R*.

Table 4.8: Risk value quantization

Risk value calculation (R*)		Attack potential quantized (P*)				
		0	1	2	3	4
Modified Impact value quantized (I’)*	0	QM	QM	QM	QM	Low
	1	QM	Low	Low	Low	Medium
	2	QM	Low	Medium	Medium	High
	3	QM	Low	Medium	High	High
	4	Low	Medium	High	High	Critical

For examples of risk value calculations in various application-based attack scenarios the reader is referred to Sections 5.1.3, 5.2.3 and 5.3.3.

5 Application-Centric Threat Analysis and Risk Assessment

Three main application areas are covered in L3Pilot and these include urban driving, highway driving (with or without traffic jams), and parking. High-level descriptions of these three automated driving (AD) functions as implemented by each L3Pilot prototype vehicle can be found in project Deliverable D4.1, classified by the SAE level, various operational design domain (ODD) parameters (per SAE J 3016-2016), HMI-related parameters, take-over characteristics, and system setup configurations.

The adapted process for the application-centric threat analysis and risk assessment incorporates the following main steps:

1. Describe the subject AD function and build an application-oriented system architecture, focusing on functional blocks that model that specific function (Sections 5.1.1, 5.2.1 and 5.3.1).
2. Identify possible attack vectors and their characteristics (Sections 5.1.2, 5.2.2 and 5.3.2).
3. Apply the proposed risk assessment framework to each L3Pilot AD application and discuss the results, providing security insights (Sections 5.1.3, 5.2.3, 5.3.3, as well as Sections 5.1.4, 5.2.4 and 5.3.4).

Before focusing the cyber security analysis work on the AD applications that have been considered by the L3Pilot project (Sections 5.1, 5.2, and 5.3), a more general analysis applying to all L3-type systems is produced in this introduction.

Based on the information from the attack vector analysis provided in Sec. 3.4.2 and the considerations of Sec. 4.3.2 (definition of system withstand factors), as well as information gathered from the project's prototype owners through questionnaires (the questionnaires are not of a public nature but the template used can be found in Annex 2), we have derived a combined matrix of possible attack vectors and corresponding attack profiles, versus system withstand characteristics. Following the TARA+ proposed framework, we extend the attack scenario analysis through the inclusion of attack "observability" and "controllability" by the system or the driver as introduced in [6] and defined by us in Table 4.5 under "system withstand profile". Please note that all the considerations with respect to the system withstand profile (redundancy, observability, controllability) are closely related to the system design and hence the assumptions made here reflect the authors' current knowledge of the systems to be used within the L3Pilot project and may be applied differently for a different L3 vehicle setting.

In Table 5.1, "system reachability" as defined by SAE J3061 is also reported in a way similar to the "remote access required" attribute of [36]. This information is very important, as it will help in the choice of an appropriate attacker profile as well as the "Potential" and "Impact" parameter values of an attack when applying the TARA+ model for each application. More details on which impact factors are considered for each type of attack scenario is provided in the "Discussion" section after the risk assessment table in the Sections 5.1.3, 5.2.3 and

5.3.3. Application-specific considerations complementing Table 5.1 are taken into account in the application-dedicated sections.

Table 5.1: Combined matrix of possible attack vectors vs attacker profile and system withstand characteristics for L3 vehicles

Attack factors (TARA)					Additional factors introduced (TARA+)		
Attack Vector	**Relevant Attack Methods (classified as in STRIDE)**	**Remote Access**	**Expertise Required**		**Redundancy**	**Observability**	**Controllability**
Inertial/ odometric sensors	Spoofing, tampering (providing false sensor data), denial of service (jamming of sensor data channel)	None (internal)	Proficient (understanding of inertial sensors, ability to infiltrate vehicle sensor data channels)		Other inertial/ odometric sensors; range sensors; dynamic localization in a-priori map	Cannot be observed (Log, detect, and flag anomalous sensor output for analysis and warn of need to improve level of sensor security)	Difficult to control since redundancy is not commonly used in such systems
Range sensors (radar, ultrasonic, LiDAR)	Spoofing, tampering (providing false sensor data), denial of service (blinding or jamming from a distance)	Partial (when in range and field of view) (in highway/urban cases it would require specific equipment installed in the vicinity of the test vehicle [e.g. in the rear bumper of a leading vehicle] and hence is not considered very probable)	Proficient (understanding of range sensor)		Other range/vision sensors	Could be observed by the driver if unusual behaviour of the system (braking) or the HMI gives a representation of the outside world and something important is missing or a ghost image appears.	Can be fairly well controlled assuming redundancy and familiarity of the driver with the system
Vision sensors (external)	Spoofing, tampering (providing false sensor data), denial of service (jamming sensor data channel)	Partial (when in range and field of view) (in highway/urban cases it would require specific equipment installed in the vicinity of the test vehicle [e.g. in the rear bumper of	Layman (blinding a camera with extreme white light not very difficult)		Radar, ultrasonic	Could be observed by the driver if HMI gives a representation of the scene captured by the camera.	Can be fairly well controlled assuming redundancy and familiarity of the driver with the system

Attack factors (TARA)				Additional factors introduced (TARA+)		
		a leading vehicle] and hence is not considered probable)				
Vision sensors (internal) [if driver monitoring is performed with use of video]	Tampering	No	Layman	Haptic feedback from steering, pedals	Could be observed by the driver only if ADF HMI shows driver status info.	Very difficult to control but blinding internal camera not considered probable during driving
GPS	Denial of service (jamming), spoofing	Yes (within GPS range)	Layman (understanding of GPS, aided by commercially available jamming tools)	Inertial/odometric sensors; range sensors; stored a-priori map; dynamic localization in a-priori map	Cannot be observed	Relatively difficult to control even assuming redundancy
Remote key/control (e.g. via smartphone inputs to OBU)	Denial of service (jamming), spoofing; stepstone attack to get access to ADAS ECU	Yes (within Bluetooth, DCMA range)	Proficient	Manual inputs by the driver though vehicle HMI	Could be observed (requires IDS)	Not so difficult to control assuming an appropriate IDS system and system segregation
V2X communication	Tampering (providing false data), denial of service	Yes (within Bluetooth, DSRC range)	Proficient (familiar with CAM messages)	n/a	Difficult to be observed (requires IDS)	Can lead to wrong decisions of the function; difficult to control where V2V data are necessary (e.g. intersections – still not relevant for L3Pilot)

Attack factors (TARA)					Additional factors introduced (TARA+)		
Vehicle Wi-Fi	Data eavesdropping; stepstone attack to ADAS ECU?	Yes (within Wi-Fi range)	Proficient		Wired connection	Difficult to be observed (requires IDS)	Here assumed not to lead to system compromise since not directly connected to ADAS ECU
OTA (e.g. firmware updates, map updates)	Spoofing, elevation of privilege (posing as map server), tampering (modifying update messages), denial of service (jamming update channel)	Yes (within wireless range)	Expert (understanding of map localization and encoding, ability to craft and transmit adversarial map updates)		W.r.t map updates: range sensors for environment perception	Difficult to be observed (requires IDS)	Relatively difficult to control even assuming an appropriate IDS system
“Misbehaving” external road/topology element (e.g. traffic sign, traffic light)	Tampering (modifying outside visual landmark)	n/a	Layman (familiar with AD perception)		Range sensors for environment perception, HD maps	Could be observed by the driver if HMI gives a representation of the outside world and something important is missing/not correct	Very difficult to control since HD maps of the environment not usually available, while dynamic localization and matching is a run-time intensive process.

5.1 Highway Chauffeur Function Assessment

5.1.1 AD application model

The Highway Chauffeur (HC), one of the key applications for automated vehicles, encompasses a safe and secure integration of numerous sensors and actuators to operate seamlessly. The application manoeuvres a vehicle on motorways in a partially or fully automated manner, where the former requires the driver's attention and the latter does not.

HC aids vehicles in travelling on various highways with multiple lanes and various road conditions. In general, these roads have good lane markings with diverse curvatures and inclinations connecting cities, towns, and villages with physical cut-offs, guardrails, deer fences, and emergency lanes, with a low probability of pedestrians and bicyclists due to limited crosswalks, junctions, and traffic lights. Also included is travel on motorways, which do not have emergency lanes but rather hard shoulders and slip roads without deer fences, as well as a low probability of pedestrians and bicyclists, and where the vehicle travels at a maximum speed of 130 km/h. The HC application thus requires vehicles to adapt to various traffic conditions. In L3Pilot, both low-velocity traffic jam conditions (0–60 km/h) and free driving conditions (60–130 km/h) are taken into account.

HC utilizes an integrated vehicular interconnected systems technology, dynamically adjusting to the virtually sensed and analysed environment, helping vehicles to manoeuvre at high speed while aiming for complete autonomy. Such applications leverage the use of automation with guidance systems for route planning using GPS. This could enable vehicles to determine optimal pathways based on the traffic by speed adaptation as well as sensing the surroundings.

According to the Society of Automotive Engineers (SAE), Level 3 (conditional automation) targets vehicular systems that assist driving with a combination of cruise control and lane assist functionalities, whereas Level 4 (high automation) aims to achieve complete manoeuvring of vehicles on motorways between junctions. L3Pilot implements both Level 3, where the driver's attention is required for HC application, and Level 4 functions, both of which ideally support the following types of manoeuvres: lane following, lane change, emergency braking, obstacle avoidance, management of entering vehicles.

In general, the L3 HC perception and control functionality may include the following:

- Tracking of surrounding objects (distance and heading as well as potentially class of object)
- Assessment and prediction of lead vehicle condition
- (optionally) Traffic sign/light/speed limit sign recognition
- Function/ODD limit detection, such as sudden braking of lead object, non-motorized road users, unexpected road conditions, etc.

- Speed control
- Lane change (optional)
- Traffic jam automated driving (stop-and-go function)
- Handover of control to the driver within system/function limits

The longitudinal control operates based on functions such as Adaptive Cruise Control (ACC), speed limit information, intelligent speed adaptation, traffic sign/light violation warning, brake assist, and automatic emergency brake [50]. The lateral control includes blind spot detection, lane departure warning, lane keeping support, and lane change support. Moreover, these functions can leverage data from the cockpit, such as monitoring the driver's state, passenger seat observation, navigation, and fuel consumption optimization in order to make decisions such as an emergency stop, etc. Depending on the HC automation level, the need to monitor the driver's state and prepare take-over requests to the driver are also a very important functionality when operating in Level 3.

HC functionality as well as operational design domain (ODD) based on the initial L3Pilot testing plans is outlined below:

- Straight and curved road geometry in good road conditions with steep roads and slippery or bumpy surface.
- Both uncrowded highways and highways with traffic jams are considered.
- Non-motorized traffic participants are generally not part of the HC application but ideally can be detected.
- Management of cut-in vehicles, obstacle avoidance, and emergency braking may be part of the function.
- Response to dynamic changes of the driving environment for special cases (e.g. missing lane markers) is part of the function design.
- Give-back-control functionality initiated by the system should be available in all L3 level functions in two cases: end of the scenario (e.g. highway exit) and unforeseen failure/reaching of system limits.
- Conditional activation of the function based on driver status can be included.
- HD digital map information is required.

The HC application receives multiple data inputs from perception sensors such as cameras, LiDAR, and radar to model and predict object movements and produce a desirable speed/path. Figure 5.1 presents an example of the logical architecture. Table 5.2 and Figure 5.2 are representative examples of the sensor setup used in the L3Pilot fleet.

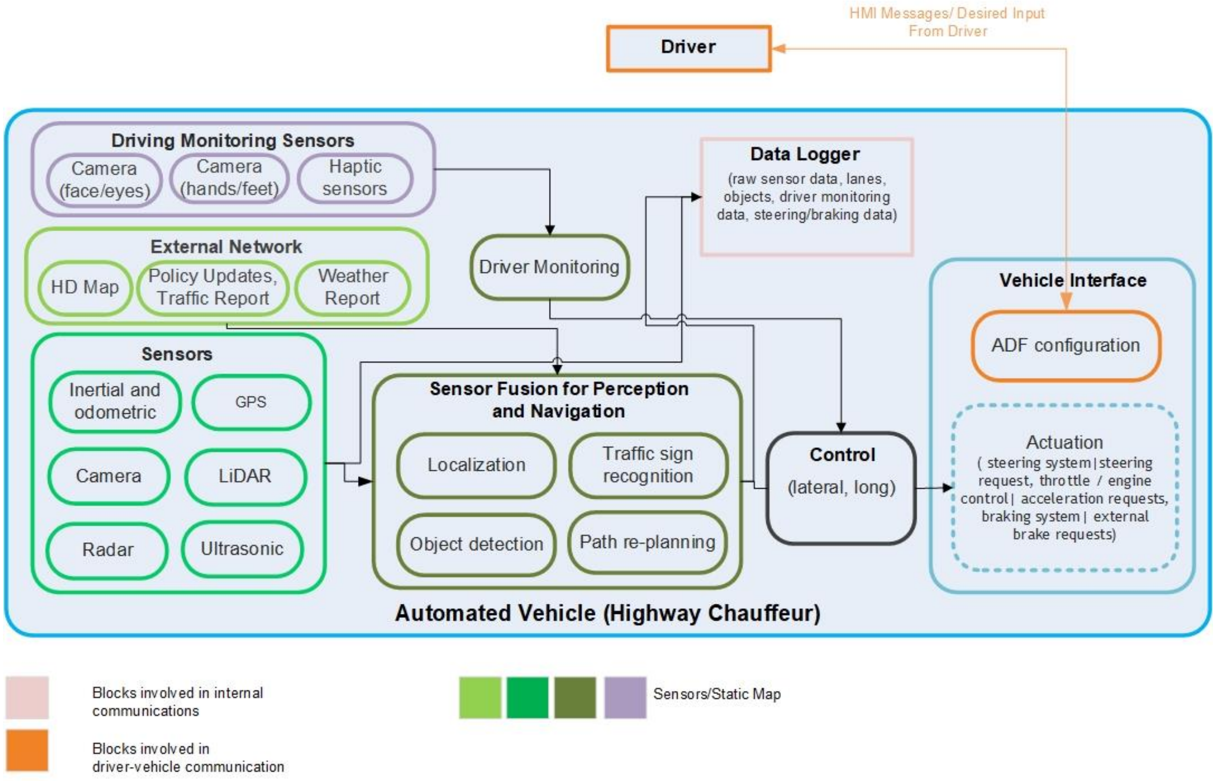

HMI Messages/ Desired Input From Driver
Driver
Driving Monitoring Sensors
Camera (face/eyes)
Camera (hands/feet)
Haptic sensors
Data Logger
(raw sensor data, lanes, objects, driver monitoring data, steering/braking data)
External Network
HD Map
Policy Updates, Traffic Report
Weather Report
Driver Monitoring
Vehicle Interface
ADF configuration
Sensors
Inertial and odometric
GPS
Camera
LiDAR
Radar
Ultrasonic
Sensor Fusion for Perception and Navigation
Localization
Traffic sign recognition
Object detection
Path re-planning
Control
(lateral, long)
Actuation
(steering system|steering request, throttle / engine control| acceleration requests, braking system| external brake requests)
Automated Vehicle (Highway Chauffeur)
Blocks involved in internal communications
Blocks involved in driver-vehicle communication
Sensors/Static Map

Figure 5.1: Highway Chauffeur logical architecture.

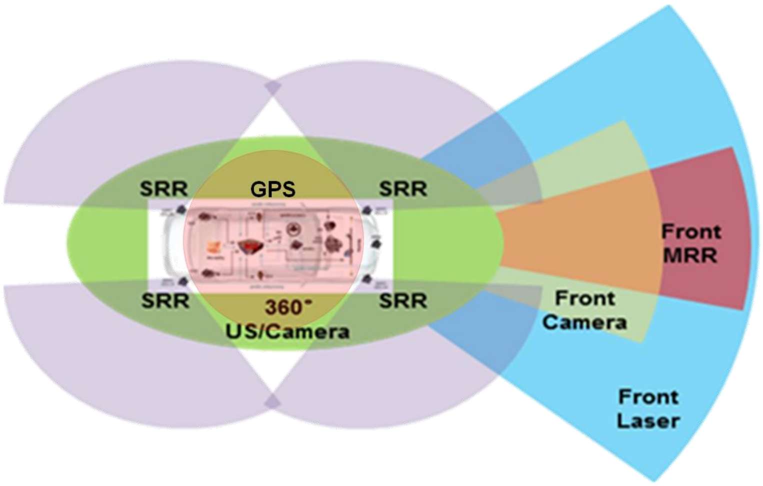


Figure 5.2: A typical sensor set-up for Highway Chauffeur.

Table 5.2: Example of technologies and functions for the Highway Chauffeur application

Technology	Function
Camera	Lanes + objects + traffic signs
Surround-view camera	Lanes + objects
Long-range radar	Front objects
Short-range radar	Side/rear objects
LiDAR	Surrounding objects
Ultrasonic sensor	Objects
GPS	Vehicle position
Steering	Driver monitoring

5.1.2 Attack vectors cross-checking

Complementing the work described in Table 5.1 we include below considerations for the HC application based on information from the previous section.

Table 5.3: HC considerations with respect to Table 4.7

Attack Surface	Highway Chauffeur Considerations
Inertial/odometric sensors	--
Range sensors (radar, ultrasonic, LiDAR)	Challenging because adversary may be capable of reverse engineering, learning, and executing hardware or firmware/software attacks by injecting or relaying malicious data when vehicles are travelling at high speed, also for multiple vehicles. An adversary can exploit the sensors in advance when vehicles are stationary.
Vision sensors (ext.)	The relatively simple blinding of the camera can influence the vehicle to make decisions accordingly, which can affect multiple vehicles. Influencing the system integrity is challenging, as it requires equipment and working knowledge of camera operations for vehicles.
Vision sensors (int.)	Although challenging, such an attack has a crucial impact once exploited, if driver monitoring and interaction with the driver is performed with the use of video. This can influence the vehicle to change lanes or stop, overriding the driver’s actual response.
GPS	The capability to exploit the GPS coordinates can vary from the use of jamming devices to sophisticated wireless communication systems to tamper with the vehicular system’s coordinates. GPS redundancy checks in HC are important for self-navigation of automated vehicles to prevent erroneous manoeuvring.

Attack Surface	Highway Chauffeur Considerations
Remote key/control (OBU)	--
V2X communication	--
Vehicle Wi-Fi	Might not lead to direct attack on ADAS ECU (elevation of privilege attack); however, an adversary can exploit the infotainment system or TCU though Wi-Fi.
OTA (e.g. firmware updates, map updates)	Sophisticated adversarial attacks can exploit the automotive system though OTA updates such as gaining physical access and elevating privileges to update the system. These attacks can also be remote, provided an adversary gains access to the vehicle's identity and operation for further exploitation.
"Misbehaving" external road/topology element (e.g. traffic sign, traffic light)	--

Based on the table above, a subset of possible attack vectors is considered based on TARA+ analysis. The attack types considered most relevant for the Highway Chauffeur case are: sensor blinding, sensor tampering, GPS jamming, OTA tampering.

5.1.3 Risk assessment

The results of TARA+ analysis are summarized in Table 5.5. The choice of the numerical values and a discussion of the results of the analysis are discussed in the next section.

Please note that in this AD application analysis, custom threat agent profiles have been used instead of those proposed in Table 4.3 in order to fine-tune the analysis to the specific attack vectors. Table 5.4 below denotes the values for the adversary profiles in this case (note that apart from the first one, combinations of E, K, Eq, and W did not fall under the static profiles of Table *4.3*).

Table 5.4: Highway Chauffeur custom threat agents adopted

Attack Name	Expertise (E)	Available knowledge about the target (K)	Equipment required (Eq)	Window of opportunity (W)
Blinding Camera	Layman (0)	Public (0)	Standard (0)	Unlimited (0)
Tampering with perception sensors	Expert (2)	Sensitive (2)	Specialized (1)	Medium (2)
Jamming GPS	Proficient (1)	Restricted (1)	Specialized (1)	Large (1)

Attack Name	Expertise (E)	Available knowledge about the target (K)	Equipment required (Eq)	Window of opportunity (W)
Modifying updates	Expert or multiple experts (2 or 3)	Critical (3)	Multiple bespoke (3)	Small (3)

Table 5.5: TARA+ results for the Highway Chauffeur application

<table>
<tr><th colspan="9">Highway Chauffeur ADF TARA +</th></tr>
<tr><td colspan="9"><b>Attack scenario</b></td></tr>
<tr><td>Attack name</td><td colspan="2">Blinding camera</td><td colspan="2">Tampering with perception sensors</td><td colspan="2">Jamming GPS</td><td colspan="2">Modifying updates</td></tr>
<tr><td>Attacker expertise[8]
(from Table 4.2)</td><td colspan="2">Layman</td><td colspan="2">Expert</td><td colspan="2">Proficient</td><td colspan="2">Expert or multiple experts</td></tr>
<tr><td>Attack surface</td><td colspan="2">Vision sensors (external)</td><td colspan="2">Vision sensors (external)</td><td colspan="2">GPS</td><td colspan="2">Over-the-Air (OTA)</td></tr>
<tr><td>Attack method</td><td colspan="2">DoS – blinding camera with extreme white light</td><td colspan="2">Tampering – inaccurate or erroneous calibration of sensors by an adversary</td><td colspan="2">DoS – jamming</td><td colspan="2">Tampering – compromising integrity of the updates</td></tr>
<tr><td>Description</td><td colspan="2">An adversary can blind the nearby vehicle's external camera using an extreme white light projector. The blinding of the camera can influence the vehicle to make decisions accordingly, which can affect multiple vehicles.</td><td colspan="2">An adversary with a working knowledge of the range sensors can exploit the sensors in advance of the HC application while the vehicle is stationary.</td><td colspan="2">An adversary can exploit the GPS coordinates of vehicles in range by using different range jamming devices, which may be commercially available.</td><td colspan="2">Sophisticated adversarial attacks can exploit the automotive system though OTA updates.
An adversary who has gained access to a vehicle's identity and operation for further exploitation can also remotely realize an attack.</td></tr>
<tr><td colspan="9"><b>Attack potential (attacker profile) value</b> $P = E + K + Eq + 2 * W$ <i>(Eq. 1)</i></td></tr>
<tr><td></td><td>0</td><td>0</td><td>2</td><td>2</td><td>1</td><td>1</td><td>2 or 3</td><td>3</td></tr>
</table>

[8] In contrast with Table 4.3, in this use-case analysis custom threat agent profiles have been used instead of the fixed profiles proposed in Table 4.3 and the "attacker profiles" value has been replaced by the "attacker's expertise".

Highway Chauffeur ADF TARA +				
First row: attacker expertise (E)/window of opportunity (W) Second row, P= E+K+Eq+2*W based on Table 4.2	0+0+0+2*0=0	2+2+1+2*2=9	1+1+1+2*1=5	2+3+3+2*3=14 Or 3+3+3+2*3=15
P* (Table 4.6**)**	4 – CRITICAL	1 – LOW	2 – MEDIUM	0 – NONE
System withstand value (C)				
See Table 4.5	2	2	2	1
Impact value I=$(3I_S + I_F + 2I_O + I_P)$				
See Table 4.4	3*4+4+2*4+0	3*4+4+2*4+3	3*1+1+2*2+0	3*4+4+2*4+4
Weighted sum	24	27	7	28
Modified impact I * (1 – w*C/CMAX),CMAX=4	24*(1-0.5*2/4)=18	27*(1-0.5*2/4)=20.25	7*(1-0.5*2/4)=5.25	28*(1-0.5*1/4)=24.5
I’	18	20.25	5.25	24.5
I’* according to Table 4.7	2 – MEDIUM	3 – HIGH	1 – LOW	3 – HIGH
Resulting risk factor				
R = P* + (I’) *	4+2	1+3	2+1	0+3
Total	**6**	**4**	**3**	**3**
According to Table 4.8	**(HIGH)**	**(LOW)**	**(LOW)**	**(QM)**

5.1.4 Discussion

Blinding camera

Attack description:

Blinding camera attacks expose the camera to bright light so that the camera is not able to adjust the auto exposure to attain stability [45].

Attack potential:

Blinding a camera does not require high skills or knowledge for an adversary to carry out the attack. The type of equipment required to blind a camera can be simply reflected sunlight, directed laser beams, or the projection of a bright light onto the camera lens. The window of opportunity for conducting an attack is unlimited, as cameras installed on board are exposed to changing environmental conditions, and physical access is not required by adversaries. Such an attack could undermine the subject vehicle's perception system.

Controllability:

This attack can potentially be detected by the driver and passenger when the attacked vehicle behaves abnormally. It can be controlled by using redundant systems such as surrounding cameras and LiDAR, as it is a major challenge to blind multiple cameras on a vehicle simultaneously. The system should be able to detect the attack and notify the driver about the abnormal situation.

Impact:

Blinding camera attacks can directly impact the attacked vehicle's control algorithms, as the camera takes time to adjust to different lighting conditions, leaving the system unable to detect objects. This may have a high impact on the vehicle's safety and its passengers as the system may make erroneous control decisions. Moreover, such an attack could affect other road users by causing accidents leading to injuries or loss of life, and could also inflict reputational damage on the manufacturer, thereby having a financial impact. The Modified Impact value is 18, which is normalized to 2 (MEDIUM).

Risk:

The normalized attack potential is 4 and normalized impact is 2, thus resulting in a risk factor of 6 (HIGH).

Tampering with perception sensors

Attack description:

Tampering with a sensor causes erroneous readings. The vehicular perception sensors include cameras, LiDAR, radar, and ultrasonic sensors. This attack considers tampering with vehicular cameras with video recording, thereby preventing the vehicle's perception system from observing the actual surroundings of the vehicle.

Attack potential:

Tampering with perception sensors requires specialized equipment, some level of expertise, and knowledge about the target and about the functioning of the vehicular perception system. The window of opportunity is not large since the adversary might need physical access to exploit the perception sensors. It is not easy to physically access the vehicle when it is in HC mode. However, the attack can be prepared in advance to be executed later when the HC application is in use.

Note: While in Table 5.1 we have considered 3 types of potential attacks on visual sensors, in the risk assessment work here, the “tampering” attack has been chosen since a wide range of spoofing attacks are analysed in the Urban Chauffeur application. Moreover, the equipment used to manoeuvre a vehicle is the use of ADAS sensors, which include cameras, LiDAR, radar, etc. As a vehicle relies on the data retrieved from these sensors, ensuring data integrity is one of the active research areas for implementing HC. As a result, it is important to consider various measures to deal with tampering of sensors.

Controllability:

Once an attack has taken place, it hinders the safety functions of the perception system. Redundant systems may be able to identify attacks and notify the driver to take corrective actions. It is therefore estimated that a controllability value of 2 is appropriate for this threat.

Impact:

The attack might have significant impacts on the subject vehicle and its occupants, including potential physical damage, injuries, or death. Once an adversary gains access to perception sensors and is able to tamper with them, the real sensor data can be collected, violating the privacy of the vehicle and drivers/passengers. Nonetheless, vehicles are safety critical systems that rely on redundant systems that are capable of ensuring a fallback mechanism to the driver before informed decisions must be made. Considering the potential impacts, the modified impact value is calculated as 20.25, which is normalized to 3 (HIGH).

Risk:

The normalized attack potential is 1 and normalized impact is 3, resulting in a risk factor of 4 (LOW).

Jamming GPS

Attack description:

An adversary may carry out a cyber attack to influence the availability of the GPS system, in order to cause malfunction of navigation. The jamming attack includes the transmission of high and/or low power noise signals to disrupt the function of the GPS receiver. GPS jamming is a relatively simple attack, compared to GPS spoofing. The attacker need only transmit a sufficiently strong jamming signal at the same frequency band of GPS (e.g. 1575.42 MHz) to disrupt the reception from GPS satellites [46]. This can undermine the vehicular navigation functions in the attacked zone.

Attack potential:

Jamming GPS receivers requires specialized equipment, some level of expertise, and knowledge of the target and the functioning of GPS. An adversary can find the required equipment of various transmitting power on the market. Moreover, there is a large window of opportunity since vehicles are usually easily exposed to a jamming attack. Under this consideration, the attack potential is calculated as 5 and normalized to 2 (MEDIUM).

Controllability:

The system and the driver can detect such attacks by exploiting the data from other sensors (e.g. IMU) to help address this type of attacks. According to the adopted methodology, the controllability value is estimated to be 2.

Impact:

A GPS jamming attack can lead to unexpected outcomes with safety, operational, and financial implications; however, it can be controlled by the driver. Therefore, considering the controllability potentials, the modified impact value is calculated as 5.25, which is normalized to 1 (LOW).

Risk:

The normalized attack potential is 2 and normalized impact is 1, resulting in a risk factor of 3 (LOW).

Modifying updates

Attack description:

Vehicles have more than 100 ECUs with diverse software architecture and a variety of applications. With such complexity, updating automobile software over-the-air (OTA) is important for updating security patches for recently discovered vulnerabilities, to maintain quality and ensure customer satisfaction. It is very critical for updates to have a robust cyber security mechanism ensuring a secure connection with the service provider to preserve the integrity of the OTA update. This would prevent packages from being modified by an adversary. If the OTA update packages are altered by an adversary, it could compromise cyber security and safety requirements, which could expose the vehicle's identity and on-board functions to further exploitation through physical and remote cyber attacks.

Attack potential:

Modifying OTA updates requires highly skilled adversaries who have critical knowledge of the target system. The required tools are also not easily available, and multiple bespoke equipment may be needed to discover a vulnerability and conduct an attack. Under this consideration, the attack potential is calculated in this project as 15 and normalized to 0 (NONE).

Controllability:

An attack that modifies an OTA update can be difficult to detect when it is conducted. The anomaly detection mechanism can be potentially deactivated by the attackers. However, in the case of the L3Pilot project, the "safety driver" is expected to monitor the actions of the vehicle. In that sense, the driver can correct some of the abnormalities the vehicle might make such as navigation route re-planning. Therefore, it is assumed that the driver can react when the vehicle behaves differently than normally expected. According to the adopted methodology in this project, the controllability value is 1.

Impact:

Once an adversary succeeds in maliciously modifying the OTA updates, the impacts might be severe in terms of users' safety, privacy disclosure, and financial and operational impacts since the adversary can gain the privilege of the system. According to these potential impacts, the modified impact value is calculated as 24.5, which is normalized to 3 (HIGH).

Risk:

The normalized attack potential is 0 and normalized impact is 3, resulting in a risk factor of 3 (QM).

5.2 Urban Chauffeur Function Assessment

5.2.1 AD application model

Urban Chauffeur (UC) is an ADAS application that manoeuvres vehicles through the urban area without the need for user intervention at all times. Typically, an urban area includes many obstacles, both stationary and moving, including motorized and non-motorized transport, pedestrians, buildings, and intersecting roads with traffic flowing in both directions. Moreover, the traffic signs must be obeyed at all times. Some of these variables can also change dynamically, which can be quite challenging. In order to perform these tasks, the vehicle makes use of external sensors such as LiDAR, radar, and cameras.

Manoeuvring inside urban areas is quite different than other automated transportation systems such as the autopilot in flight control systems, naval ships, and highway chauffeur. Urban driving can be quite challenging at times due to the presence of a potentially large volume of congested traffic and numerous road intersections. In addition, there are many traffic control signs as well as speed control signs, some of which might also potentially change dynamically. All of this must be respected by the Urban Chauffeur ADAS system when driving within the limits of an urban area.

As long as the vehicle remains inside the urban area, it is guided by the Urban Chauffeur. It is assumed that when such a vehicle leaves the limits of an urban area, control is returned to the driver or the Highway Chauffeur takes over.

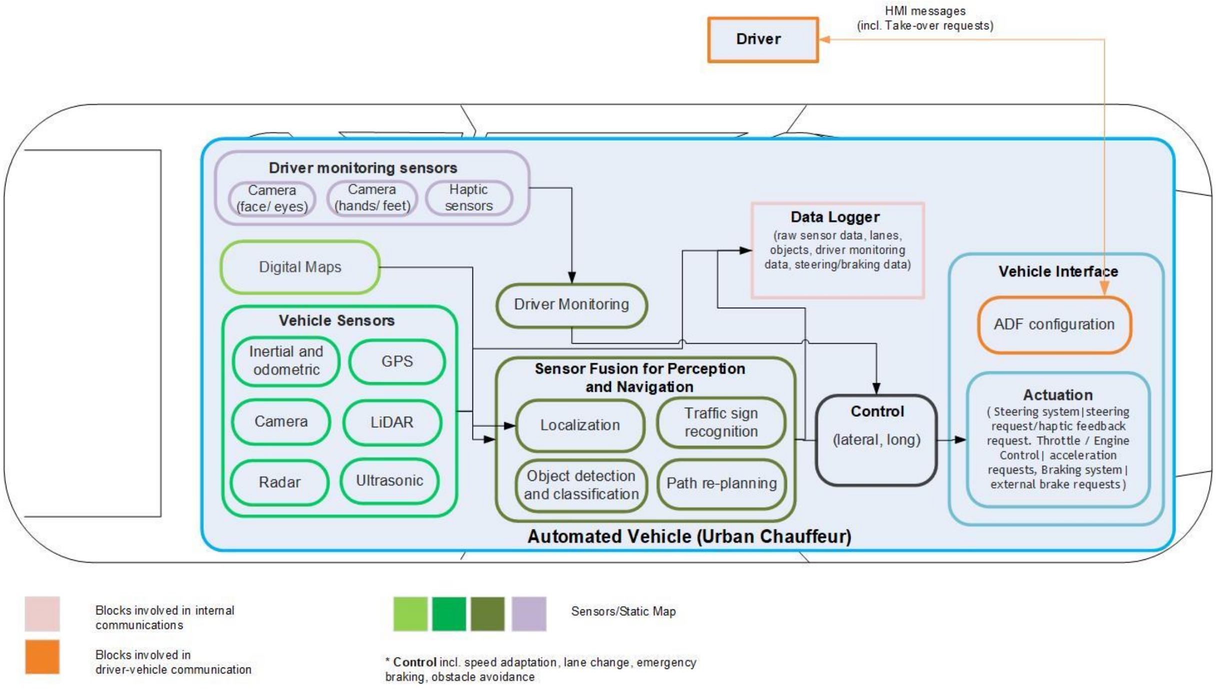

Driver
HMI messages
(incl. Take-over requests)
Driver monitoring sensors
Camera (face/ eyes)
Camera (hands/ feet)
Haptic sensors
Digital Maps
Vehicle Sensors
Inertial and odometric
GPS
Camera
LiDAR
Radar
Ultrasonic
Driver Monitoring
Data Logger
(raw sensor data, lanes, objects, driver monitoring data, steering/braking data)
Sensor Fusion for Perception and Navigation
Localization
Traffic sign recognition
Object detection and classification
Path re-planning
Control
(lateral, long)
Vehicle Interface
ADF configuration
Actuation
(Steering system|steering request/haptic feedback request. Throttle / Engine Control| acceleration requests, Braking system| external brake requests)
Automated Vehicle (Urban Chauffeur)
Blocks involved in internal communications
Blocks involved in driver-vehicle communication
Sensors/Static Map
* Control incl. speed adaptation, lane change, emergency braking, obstacle avoidance

Figure 5.3: Urban Chauffeur logical architecture.

Manoeuvres and functionalities that are typical for the Urban Chauffeur during its operation include:

- **Adaptive cruise control (ACC)**

  While travelling in urban traffic, adaptive cruise control can be helpful for an automated vehicle as it helps to maintain constant speed in the urban area. It is also helpful for keeping a safe distance from the vehicle in front. However, depending on the objects and traffic signs, the speed will need to be readjusted. The speed limits have to be observed at all times to know when there is a need to accelerate or decelerate.

- **Pedestrian and obstacle detection**

  An automated vehicle should be able to recognize stationary and moving obstacles, as well as pedestrians, in order to ensure safe driving.

- **Collision avoidance**

  Collision avoidance uses the help of radar, LiDAR, and/or cameras to identify obstacles and pedestrians and either brake or steer away or do both. Steering away, in turn, requires the car to be able to identify lanes and avoid the traffic in other lanes.

- **Lane departure warning and lane correction**

  Although more useful on highways and motorways, a lane departure system might also be helpful on the main roads of an urban area with higher speed limits. Especially an automated vehicle should not steer too far away from the centre of a lane.

- **Driving inside a tunnel**

  Driving inside a tunnel might result in the loss of GPS signals and therefore the automated vehicle will need to rely on the vision and ranging sensors or IMU for navigation within the tunnel.

- **Emergency braking**

  An automated vehicle might apply emergency brakes on detecting an unavoidable object in front or coming from the side. This could be another vehicle changing its lane without maintaining an appropriate distance or a pedestrian or child suddenly entering the road.

- **Lane change**

  Choosing a lane inside the limits of an urban area is typically a free choice. However, changing a lane might sometimes be necessitated depending on the traffic situation. A lane must be changed by the vehicle if there is a stationary object in front of it or if the vehicle in front stops for more than a certain length of time, e.g. due to an accident.

- **Overtaking**

  Overtaking manoeuvres involve overtaking moving vehicles, stationary vehicles, and non-motorized vehicles such as cycles and pedestrians. Special care is needed regarding speed and distance from the pedestrians.

- **Pedestrian zone management**

  A pedestrian zone might look similar at first to any speed limit zone; however, the vehicle might have to behave differently depending on the situation. The vehicle might have to slow down and come to a halt or apply emergency brakes on detecting the sudden appearance of a pedestrian. While changing direction, e.g. at a traffic signal, the traffic in front as well as the traffic behind has to be carefully observed. This is especially true with regard to pedestrians, cyclists, and motorcyclists, who should be allowed to pass by before the vehicle makes its turn.

- **Traffic signal management**

  - Stop on red light.
  - A vehicle must be able to slow down and stop before the red light on a traffic signal.
  - Go on green light.
  - A vehicle must be able to start and go by carefully observing the status of the traffic light.
  - Turn right or left (change street).

With regard to the L3Pilot functions operating as Urban Chauffeurs, the following set of sensors is utilized:

Table 5.6: Sensor set for Urban Chauffeur application in L3Pilot

Sensing Technology **(superset of what is declared by each OEM)**	**Function**
Camera	Lanes + objects + traffic signs
Surround-view camera	Lanes + objects
Long-range radar	Front objects
Short-range radar	Side/rear objects
LiDAR	Surrounding objects
Ultrasonic	Objects
GPS	Vehicle position
Steering	Driver monitoring

Based on the general description of the L3 Urban Chauffeur application given above, the functional architecture sketch of Figure 5.3 has been created to help understand the system under assessment.

5.2.2 Attack vectors cross-checking

Based on the analysis performed in Sec. 3.4, we highlight in Figure 5.3 and discuss below the potential attack vectors considered relevant for the Urban Chauffeur case.

In urban driving, an adversary may be inclined to attack the vehicle remotely over its external wireless interfaces rather than gaining physical access. One of the reasons is that the chances of the attacker being caught are lower, as no physical contact occurs. Another reason for this motivation is that by gaining access by circumventing the wireless communication interfaces, the attacker can remotely control the vehicle while it is being driven. Such an approach might also be tempting if physical access is impossible. In the case of automated vehicles driving within an urban area, an attacker could also focus on the external sensors, such as LiDAR, radar, and external cameras.

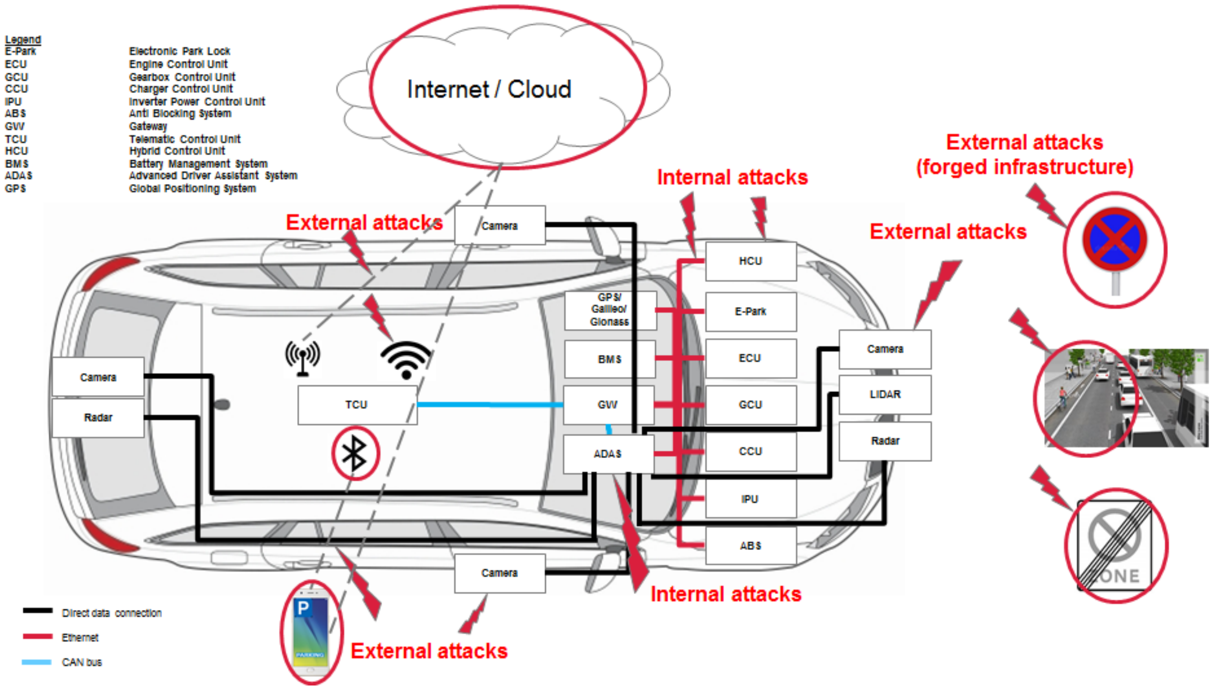


Figure 5.4: Highlighted potential attack vectors for the urban use case.

The attack vectors relevant to the Urban Chauffeur use case are reported in Table 5.1, which summarizes all attack vectors considered for all three AD applications. The features of the attack vectors and the relevant information such as redundancy, observability, and controllability are also given in [6] in the form of notes.

Complementing the work described in Table 5.1, we add below, in Table 5.7, a few considerations for the Urban Chauffer application based also on the information from the previous section. From this table, a subset of the attack vectors is selected for further TARA+ analysis. The considered attacks represent a good subset of the overall set of attacks, as they include the attacks on the sensors (LiDAR, radar, and cameras) as well as on the possibility of penetration via remote access to the TCU, which might be used further to penetrate to the ADAS ECU through the gateway.

Table 5.7: Urban Chauffeur considerations with respect to Table 4.7

Attack Surface	Urban Chauffeur Considerations
Inertial/odometric sensors	--
Range sensors (radar, ultrasonic, LiDAR)	Highly probable in urban use case depending on the attacker's motivation. An attacker can set up equipment to target not just one car but multiple cars within range.
Vision sensors (ext.)	Very critical in the urban use case.

Attack Surface	Urban Chauffeur Considerations
	The example of cheating the camera with an external element planted in the scene is considered more probable since it does not require specific equipment present at the same time as the testing; hence we will include camera tampering as an external attack surface scenario.
Vision sensors (int.)	Not probable. Needs physical access to the vehicle's interior (blinding internal camera not considered probable during driving).
GPS	GPS spoofing is important in the urban use case as on narrow streets it might make self-navigation of an automated vehicle impossible. It might also make the vehicle take paths that are otherwise not allowed.
Remote key/control (OBU)	--
V2X communication	--
Vehicle Wi-Fi	ADAS ECU is assumed to be not directly connected to Wi-Fi, however, a TCU is connected to some kind of wireless interfaces such as Wi-Fi, and an attack is still possible.
OTA (e.g. firmware updates, map updates)	Map updates are considered crucial in the urban use case. The same is true for firmware updates. Unauthenticated firmware can be prevented from running through secure boot and code signing and authentication mechanisms.
"Misbehaving" external road/topology element (e.g. traffic sign, traffic light)	--

5.2.3 Risk Assessment

The results of the TARA+ analysis are summarized in Table 5.8The choice of the numerical values and a discussion of the results of the analysis follow in the next section.

Table 5.8: TARA+ analysis of Urban Chauffeur use case

Urban AD TARA+				
Attack scenario				
Attack name	LiDAR sensor spoofing	Radar sensor spoofing (object removal)	Camera sensor spoofing (object insertion)	Remote TCU penetration and control

<table>
<tr><th colspan="9">Urban AD TARA+</th></tr>
<tr><td>Attacker</td><td colspan="2">Hacktivist</td><td colspan="2">Researcher</td><td colspan="2">Organized crime</td><td colspan="2">Researcher/state</td></tr>
<tr><td>Attack vector</td><td colspan="2">LiDAR</td><td colspan="2">Radar</td><td colspan="2">Camera</td><td colspan="2">Remote access and control through Internet or other external interfaces</td></tr>
<tr><td>Attack method</td><td colspan="2">Induce illusions in LiDAR output.
Make objects appear closer than they are.
Denial of service by saturating signals.</td><td colspan="2">Through radar interference, remove an object, such as a lead vehicle, from the scene.</td><td colspan="2">Insert an object, such as a stop sign or a speed limit sign, in the scene.</td><td colspan="2">Remotely penetrate to the TCU over the mobile interface and control the vehicle remotely.
Furthermore, escalate access to the ADAS ECU.</td></tr>
<tr><td>Description</td><td colspan="2">Spoof or blind a LiDAR sensor from nearby via optical means.
The aim might be to induce a crash, such as with the surrounding elements, or result in emergency braking, leading to a crash or traffic disturbance at the least.</td><td colspan="2">Spoof radar by generating signals such that an object is made to disappear from the scene.
This might result in an accident or crash if a vehicle is made to believe that an obstacle does not exist, although it actually does.</td><td colspan="2">Show a spoofed object, which actually does not exist.
An example would be a spoofed stop sign resulting in vehicle applying unnecessary brakes.
Another example would be a spoofed speed limit sign with higher speed than actually allowed, making the vehicle unnecessarily accelerate and pose danger to other traffic and more importantly to pedestrians.</td><td colspan="2">Connect to the TCU through its mobile interface, e.g. by establishing an illegitimate connection or by hijacking a legitimate session.
Once connected, spread further to the ADAS ECU through the gateway if adequate security measures are lacking.
Control the vehicle remotely and pursue all possible attacks.</td></tr>
<tr><td colspan="9"><b>Attack potential (attacker profile) value (P)</b> $P = E + K + Eq + 2 * W$ <i>(Eq. 1</i><b>)</b></td></tr>
<tr><td>Threat agent (See Table</td><td>3 + 2 + 3</td><td>1</td><td>3 + 0 + 4</td><td>1</td><td>2 + 2 + 4</td><td>1</td><td>3 + 0 + 4</td><td>0</td></tr>
</table>

Urban AD TARA+				
4.2)/window of opportunity / P = E + K + Eq + 2*W	10 = 8 + 2*1	9 = 7 + 2*1	10 = 8 + 2*1	7 = 7 + 2*0
P* (according to Table 4.6**)**	1 – LOW	1 – LOW	1 – LOW	2 – MEDIUM
System withstand value (C)				
See Table 4.5	2	1	2	2
Impact value (3*S+F+2*O+P)				
See Table 4.4	3*2 + 2 + 2*1 + 0	3*2 + 3 + 2*1 + 0	3*3 + 3 + 2*1 + 0	3*4 + 4 + 2*3 + 4
Weighted sum	10	11	14	26
Modified I' = I * (1 – w* C/C_{MAX}),C_{MAX}=4	10 * (1 - 0.5*2/4)	11 * (1 - 0.5*1/4)	14 * (1 - 0.5*2/4)	26 * (1 - 0.5*2/4)
I'	7.5	9.625	10.5	19.5
I' * (according to Table 4.7)	1 – LOW	1 – LOW	1 – LOW	3 – HIGH
Resulting risk factor R = P* + (I') *	1 + 1	1 + 1	2 + 1	2 + 3
Total	**2**	**2**	**2**	**5**
According to Table 4.8	**(LOW)**	**(LOW)**	**(LOW)**	**(MEDIUM)**

5.2.4 Discussion

On LiDAR sensor spoofing

Attack description:

LiDAR sensor spoofing attacks include inducing illusions in the LiDAR output, making objects appear closer than they actually are, and/or performing a DoS attack by saturating the LiDAR signals. This could force Urban Chauffeur to apply emergency brakes, potentially leading to serious accidents. This could also trick the urban chauffeur into diverting from its path, in an attempt to avoid the perceived obstacle, resulting in further collisions or at least in traffic disruption and unnecessary hindrances to the surrounding traffic.

Attack potential:

Performing a LiDAR spoofing attack does not require a high level of expertise and knowledge of the target, provided that the highly specialized equipment needed for the attack is available to the attacker. Additionally, the window of opportunity required to perform the spoofing attack should be large enough for the attacker to establish a position in the vicinity of the victim vehicle so as to influence its LiDAR signals. In consideration of these factors, the attack potential is numerically calculated as 10, which is then normalized to 1 (LOW) according to Table 4.6.

Controllability:

The above-mentioned LiDAR spoofing attacks can be recognized by the driver by observing the unusual behaviour of the vehicle (e.g. by observing that the vehicle is braking even in the absence of obstacles or vehicles in front). The driver must then take the necessary corrective measures such as taking back control of the vehicle and driving it out of the attackers' range. The controllability value is thus 2.

Impact:

A successful attack has the potential for moderate safety impacts. It can result in injuries for the passengers of the target vehicle and/or passengers of the neighbouring vehicles. The operational and financial impacts are expected to be moderate, depending on the severity of the accident and the number of vehicles involved. However, at least a moderate operational and financial impact is expected. The modified impact value, I', is calculated as 7.5, which is normalized to 1 (LOW) according to Table 4.7.

Risk:

The normalized attack potential is 1 (LOW) and the normalized impact of the attack is 1 (LOW), resulting in an overall risk factor of 2, or LOW according to Table 4.8.

On radar sensor spoofing

Attack description:

The radar sensor spoofing attack considered in this analysis involves object removal, thereby fooling the system to believe that there is no vehicle or obstacle in front, though there is one. This would result in the Urban Chauffeur maintaining its speed or even increasing its speed, which might lead to a crash.

Attack potential:

Performing the radar spoofing attacks requires good expertise and some basic knowledge of the target. Dedicated equipment is needed to be able to perform the attack. Additionally, the window of opportunity to perform the spoofing attack must be large enough for the attacker to gain a position in the vicinity of the attacked vehicle. Considering these factors, the attack potential is numerically calculated as 9 and normalized to 1 (LOW) according to Table 4.6.

Controllability:

The driver may not be able to identify the attack, as it will appear to be a random crash. However, an attentive driver can at least get enough time to respond by applying emergency brakes or steering the vehicle away to avoid a collision. The controllability value is therefore chosen as 1.

Impact:

A successful attack on the radar sensor has safety impacts. It might result in severe injuries for the passengers of the vehicle or moderate injuries for the passengers of multiple vehicles involved in a collision. The operational impact will be moderate and not very high since it is expected that not a large number of cars will be simultaneously affected by the attack. The financial impact of the attack can be high for an attacked vehicle. The modified impact value, I', is therefore calculated as 9.6 and the corresponding normalized value is 1 (LOW) according to Table 4.7.

Risk:

The normalized attack potential and the normalized impact are both 1 (LOW, resulting in an overall risk factor of 2, or LOW according to Table 4.8.

On camera sensor spoofing

Attack description:

The camera sensor spoofing attacks considered in this analysis include object insertion and removal. This might include, amongst others, the insertion, modification, or removal of traffic signs. A speed limit might be changed, e.g. increased to 50 km/h, whereas it should have been 10 km/h in the pedestrian zone. This will have an impact on the safety of multiple pedestrians. Alternatively, a stop sign could be removed from the scene, resulting in the attacked vehicle not stopping at a critical junction, causing an unsafe situation for multiple vehicles.

Attack potential:

Performing certain camera spoofing attacks requires basic expertise, such as placing a wrong/false traffic sign at the right place. Some fundamental knowledge of the target system, such as how the camera captures the scenes and extracts the traffic signs and how they are interpreted by the system, is sufficient to successfully carry out the attack. The attacker does not need highly sophisticated equipment. However in certain cases, such as modifying the dynamic speed limits, bespoke equipment might be required. The window of opportunity to perform a camera spoofing attack should be large enough for the attacker to position the attack equipment in the path of the vehicle in order to be able to successfully perform the attack. The numerical value of the attack potential (P) is therefore calculated as 10, which is normalized to 1 (LOW) according to Table 4.6.

Controllability:

Camera spoofing attacks can be recognized by the driver of the victim vehicle by observing the abnormal behaviour of the vehicle, e.g. when the vehicle fails to respect certain traffic signs. The driver must then take the necessary corrective measures, such as taking over control in the suspicious area where the attack is taking place. The numerical value of controllability is therefore chosen as 2.

Impact:

A successful camera spoofing attack potentially has a moderate impact on the safety of the targeted vehicle, its passengers, and potentially also on the neighbouring vehicles and/or pedestrians. The operational impact can be low to medium. Depending on how the attack is organized and how many vehicles are affected, the financial impact of the attack can be low to moderate for the victim vehicles. The modified impact value, I’, is calculated as 10.5, which is normalized to 1 (LOW) according to Table 4.7.

Risk:

The normalized attack potential and normalized impact value are both 1 (LOW), resulting in an overall risk factor of 2, or LOW according to Table 4.8.

On remote TCU penetration and control

Attack description:

The transmission control unit of the sample vehicle considered in the analysis of L3Pilot provides connectivity to the outside world. This connectivity includes wireless access to the Internet using Wi-Fi or mobile communication. The TCU might also have a radio receiver and player. Additionally, a Bluetooth connection might also be present in the TCU. An attacker can exploit any of these wireless interfaces to the outside world and penetrate the TCU. These interfaces can be used to help malware enter the TCU and then spread further. This includes spreading via the gateway to the ADAS ECU. Once the attacker has crossed the gateway and especially if the attacker has found a way into the ADAS ECU, many different attacks can be remotely launched on the ADAS system.

Attack potential:

Attacks involving remote connectivity to the TCU require good expertise of Internet technologies and network penetration. A basic attack can be launched by the attacker while relying on publically available information about the target. However for a highly successful attack and access to the ADAS network beyond the gateway, more sensitive information is required. Some of this information can also be obtained by performing penetration and/or fuzz testing. However, the equipment required by the attacker is typically standard, such as a laptop with connection to the Internet or a smart phone or tablet with Internet and/or

Bluetooth connectivity through which the attacker can penetrate the TCU. In certain cases, such as attacking the software stack of the radio player, the attacker might need a bit more dedicated equipment. The window of opportunity should be relatively large for the attacker, as for a successful attack, the attacker must first gather information about the TCU. Once enough information is available about the system – such as the software running on the TCU, external connectivity, and the open ports and services running on the system – the attacker might then try to connect to a service on the TCU stack with the aim of compromising it. The attacker might also prepare malware and try to get it installed in order to perform the required attack. In consideration of these factors, the attack potential (P) is calculated as 7, which is then normalized to 2 (MEDIUM) according to Table 4.6.

Controllability:

The attack on TCU can be detectable in certain cases by the system if sufficient detection mechanisms, such as a firewall or an intrusion detection system, are in place. The driver can also detect the attack when the vehicle performs unexpected activity such as an unusual acceleration or application of emergency brakes when not needed. A driver may be able to take back the control of the vehicle, e.g. by disconnecting the vehicle from the Internet or switching off the Bluetooth and taking control of the driving. However, if sophisticated malware has been transferred to the vehicle and installed in the ADAS ECU, it might no longer be possible for the driver to take back control of the driving. The controllability value is therefore chosen as 2.

Impact:

A successful attack on the TCU and thus a penetration into the ADAS network can have a very high impact on the safety of the vehicle and its surroundings such as neighbouring vehicles and/or pedestrians. The operational and financial impacts of the attack are expected to be quite high for the affected vehicles. If the attacker is able to penetrate the TCU and send acceleration and steering messages remotely on the ADAS network, havoc can be created in the surrounding traffic. A successful attack can also have a substantial effect on the system, the driver’s privacy, and confidentiality. The data, e.g. from the data logger, can be accessed by the attacker. The cryptographic keys can be compromised as well, resulting in the compromise of current and future communication within and outside of the vehicle. GPS data and phone calls might be recorded as well and sent back over the Internet connection to the attacker. The modified impact value, I’, is calculated as 19.5, which is normalized to 3 (HIGH) according to Table 4.7.

Risk:

The normalized attack potential is 2 (MEDIUM) and the normalized impact calculated for this attack vector is 3 (HIGH), resulting in an overall risk factor of 5, or MEDIUM according to Table 4.8. Such an attack is anticipated, as Internet connectivity is expected to increase the likelihood and risks of attack. Attacks from the Internet on computer systems are already quite high and are becoming increasingly specialized. In general, this is also true for the

Internet of things and the devices that are connected. Automated vehicles, when fully connected through the Internet, will thus also carry a very high risk of being attacked through the Internet.

5.3 Parking Chauffeur Function Assessment

5.3.1 AD application model

Two use cases are considered in L3Pilot:

1. Parking assistance and partial automated parking into and out of a parking space on a public parking area; driver inside the vehicle. [Level 2, 3]
2. Conditional automated parking in and out of a parking space in a private garage, provided that the path has been learnt previously and is (re)planned under modified constraints: low velocity manoeuvres/driver inside or outside the vehicle; use of smartphone or key for remote activation of the function. Optional: picking up passengers in their private property. [Level 2, 3]

NOTES on driver involvement:

- Driver either sits inside the vehicle where he or she can monitor the driving directly, or is outside of the vehicle with visual contact with the vehicle and monitors the driving on a smartphone. If the vehicle detects an obstacle and is not able to drive around it, the vehicle halts the function and hands over control back to the driver.
- If the vehicle has determined that it cannot get to the parking spot, the vehicle will inform the driver, who will have to take over the manoeuvre.

  Therefore, the driver even outside of the vehicle is present and monitors the manoeuvre up to its final completion.

Perception and control functionality:

- Detection of obstacles
- Path (re)planning under modified constraints

For the second type of scenario (private garage, driver outside), path tracking for replaying a learnt trajectory should be also supported.

Other features: remote shutdown not available.

Manoeuvres involved: Following learned trajectory, obstacle avoidance.

Environmental conditions supported: Good/bumpy/slippery road surface condition, straight/curved geometry, day and night setting, weather fine, heavy rain, fog (not always supported).

Other road participants involved: Motorized type B/non-motorized

Table 5.9: Sensor set for Parking Chauffeur in L3Pilot

Sensing Technology (superset of what is declared by each OEM)	Function
Camera	Lanes, objects, depth
Surround-view camera	Objects, depth
Surround radar	Side/rear objects
LiDAR	Front and rear objects
Ultrasonic	Objects at close distance
GPS	Vehicle position

Based on the description of L3Pilot Parking Chauffeur (in SP4), the following functional architecture sketch describes the system under assessment.

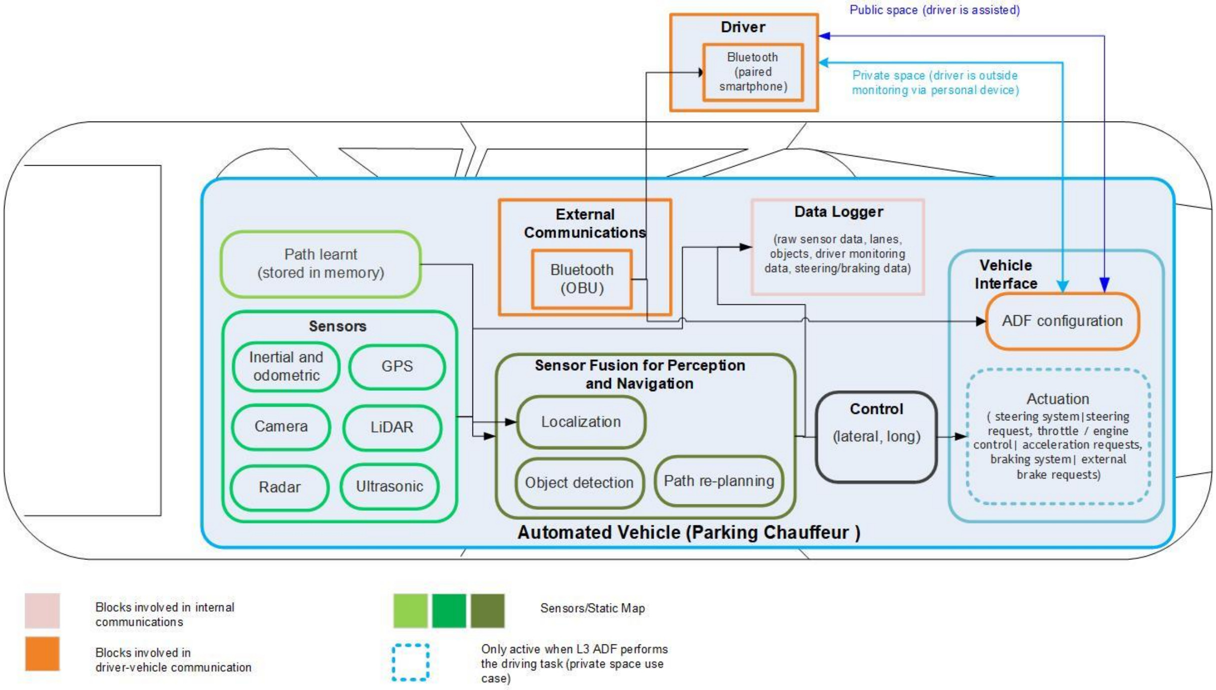

Driver
Bluetooth (paired smartphone)
Public space (driver is assisted)
Private space (driver is outside monitoring via personal device)
Path learnt (stored in memory)
External Communications
Bluetooth (OBU)
Data Logger
(raw sensor data, lanes, objects, driver monitoring data, steering/braking data)
Vehicle Interface
ADF configuration
Sensors
Inertial and odometric
GPS
Camera
LiDAR
Radar
Ultrasonic
Sensor Fusion for Perception and Navigation
Localization
Object detection
Path re-planning
Control
(lateral, long)
Actuation
(steering system|steering request, throttle / engine control| acceleration requests, braking system| external brake requests)
Automated Vehicle (Parking Chauffeur)
Blocks involved in internal communications
Blocks involved in driver-vehicle communication
Sensors/Static Map
Only active when L3 ADF performs the driving task (private space use case)

Figure 5.5: Parking Chauffeur logical architecture.

5.3.2 Attack vectors cross-checking

For the L3Pilot Parking Chauffeur and according to the architecture diagram of the previous section and the filtering of Table 3.2 to Table 3.4, the following attack vectors of interest have been identified:

- (ADF-related) Telematics: short-range wireless communication for remote control (e.g. via synched user's smartphone) (3G, BT, CDMA)/USB [INTERNAL]

- Wired or short-range wireless communication for data logging (affects mainly privacy but could be used as a stepping stone for intrusion if connected with critical ECUs) [INTERNAL]
- Sensors and static map memory [INTERNAL]
- Static environment alteration (e.g. vanishing of a line or new line drawn) [EXTERNAL]
- (out of the L3Pilot scope) Over-the-Air Application: SW updates & remote diagnostics [INTERNAL]

Complementing the work described in Table 5.1 we include below, in Table 5.10: Parking Chauffeur considerations with respect to Table 4.7Table 5.10 a number of considerations for the Parking Chauffeur application based also on the information from the previous section. From this table, a subset of the attack vectors is selected for further TARA+ analysis, namely radar sensor jamming, remote control “replaying”, reading the vehicle Wi-Fi used for AD function data logging, and the external attack surface of changing a road element (highlighted in blue background in the table below):

Table 5.10: Parking Chauffeur considerations with respect to Table 4.7

Attack Surface	Parking Chauffeur Considerations
Inertial/odometric sensors	We exclude these attack surfaces as they require physical access to the internal vehicle sensors and the vehicle during the piloting will be under supervision.
Range sensors (radar, ultrasonic, LiDAR)	Cannot be ignored. In the parking case, the possibility of such an attack is higher as the environment of the testing is more constrained and with velocities that allow for identification of the target more easily. Hence an attacker could more easily set up static equipment for attacking. IMPACT: safety (false detection of surroundings), operational (driver disturbance in case take-over request is issued)
Vision sensors (ext.)	Cannot be ignored either. Similar to the above but easier for the attacker. The situation with cheating the camera with an external element planted in the scene is considered more probable since it does not require specific equipment present at the same time as the testing and hence we will include camera tampering as a scenario of an external attack surface.
Vision sensors (int.)	Not crucial. Not used in parking.
GPS	GPS spoofing will be excluded as it is a common attack studied in the literature and does not greatly affect the parking scenarios where the vehicle performs self-localization with other means (with the aid of stored static map and sensors).
Remote key/control	Very important scenario since this is one of the vehicle’s interfaces that is open and can be jammed. IMPACT: safety (remote control of the vehicle); financial (theft)

Attack Surface	Parking Chauffeur Considerations
(e.g. via smartphone inputs to OBU)	
V2X communication	No V2X, covered by “remote key/control” attack surface in our case.
Vehicle Wi-Fi	ADAS ECU is assumed isolated and protected and hence attacking the logger will not affect driving behaviour but only privacy. IMPACT: privacy (driver data eavesdropping), financial (vehicle’s data eavesdropping).
OTA (e.g. firmware updates, map updates)	Map updates not considered crucial in parking app. For firmware updates, work in progress. Unauthenticated firmware is prevented from running through boot checks and signature code.
“Misbehaving” external road/topology element (e.g. traffic sign, traffic light)	Very possible scenario and easy to execute for the attacker since it can be done offline. Drawing a new line or deleting a line in order to confuse perception from self-localization would be a problem if: i) the perception module uses dynamic information of the parking spot limits with a higher weight than the pre-defined map; ii) if an obstacle is detected and the vehicle has to re-plan its path. For L3Pilot, due to the fact that the tests will be in specific places for specific timeslots and the environment will be monitored by a crew that will be familiar with it, this is not so important. IMPACT: safety (wrong manoeuvre leading to crash); financial (false detection of surroundings leading to crash with static element).

5.3.3 Risk Assessment

The results of the TARA+ analysis are summarized in Table 5.11. The choice of the numerical values and a discussion of the results of the analysis are discussed in the next section.

Table 5.11: Parking Chauffeur TARA+ results

Parking Chauffeur TARA+					
Attack scenario					
Attack name	Blinding range sensor	Faking remote control for taking control of the vehicle while it is being parked.	Accessing logger data	Altering static environment
Attacker	Hacktivist	Thief	Competitors	Hacktivist

<table>
<tr><th colspan="9">Parking Chauffeur TARA+</th></tr>
<tr><td>Attack surface</td><td colspan="2">Radar</td><td colspan="2">(Bluetooth) remote key/control</td><td colspan="2">Vehicle Wi-Fi</td><td colspan="2">Public parking area</td></tr>
<tr><td>Attack method</td><td colspan="2">Denial of service (blinding or jamming from a distance)</td><td colspan="2">Spoofing</td><td colspan="2">Information disclosure</td><td colspan="2">Tampering</td></tr>
<tr><td>Description</td><td colspan="2">Blind range sensor from a distance via optical means to induce a crash with static element (e.g. wall)</td><td colspan="2">Fake remote control signals for waking up vehicle and taking control of the vehicle while it is being parked.</td><td colspan="2">Data breach attack carried out by competitors to get access to ADF data.</td><td colspan="2">Alter static environment in way that surroundings misperception is induced (e.g. adding/removing a visible parking spot boundary line).</td></tr>
<tr><td colspan="9"><b>Attack potential (attacker profile) value (P)</b> $P = E + K + Eq + 2 * W$ (<i>Eq. 1</i>)</td></tr>
<tr><td rowspan="2">Threat agent (See Table 4.3)/window of opportunity
E+K+Eq+2*W</td><td>9</td><td>1</td><td>0</td><td>2</td><td>8</td><td>2</td><td>9</td><td>3</td></tr>
<tr><td colspan="2">11</td><td colspan="2">4</td><td colspan="2">12</td><td colspan="2">15</td></tr>
<tr><td><b>P*</b>
(according to Table 4.6)</td><td colspan="2">1 – LOW</td><td colspan="2">4 – HIGH</td><td colspan="2">0 – NONE</td><td colspan="2">0 – NONE</td></tr>
<tr><td colspan="9"><b>System withstand value (C)</b></td></tr>
<tr><td>See Table 4.5</td><td colspan="2">2</td><td colspan="2">3</td><td colspan="2">0</td><td colspan="2">2</td></tr>
<tr><td colspan="9"><b>Impact value (3*S+F+2*O+P)</b></td></tr>
<tr><td>See</td><td colspan="2">3*2+2+4*2+0</td><td colspan="2">3*4+2+2*3+0</td><td colspan="2">2*0+3+2*0+3</td><td colspan="2">2*1+1+2*2+0</td></tr>
<tr><td>Weighted sum</td><td colspan="2">16</td><td colspan="2">20</td><td colspan="2">6</td><td colspan="2">7</td></tr>
<tr><td>Modified I' =
I * (1 – w* C/C_{MAX}),C_{MAX}=4</td><td colspan="2">16 * (1-0.5*2/4)</td><td colspan="2">20 * (1-0.5*3/4)</td><td colspan="2">6 * (1-0.5*0)</td><td colspan="2">7 * (1-0.5*2/4)</td></tr>
<tr><td><b>I'</b></td><td colspan="2">12</td><td colspan="2">12.5</td><td colspan="2">6</td><td colspan="2">5.25</td></tr>
<tr><td><b>I' *</b></td><td colspan="2">2 – MED</td><td colspan="2">2 – MED</td><td colspan="2">1 – LOW</td><td colspan="2">1 – LOW</td></tr>
</table>

Parking Chauffeur TARA+				
(according to Table 4.7)				
Resulting risk factor				
$R^* = P^* + (I')^*$	1 + 2	4 + 2	0 + 1	0 + 1
Total (quantized value)	**3**	**6**	**1**	**1**
Resulting risk factor (According to Table 4.8)	**(LOW)**	**(HIGH)**	**(QM)**	**(QM)**

5.3.4 Discussion

Different considerations for the attack scenarios selected can be found in Table 5.10.

- Spoofing remote control signals to wake up vehicle and taking control of the vehicle while it is being parked:

  This is considered one of the attacks with the highest risk mainly due to the low difficulty of executing such an attack (e.g. Bluetooth attacking) and the assumed low level of controllability from the system point of view (no BT dedicated IDS system/no driver on board). Impact of the attack in terms of safety and operational aspects is also considered high despite low operational velocity, mainly due to the potential of hitting a pedestrian. System segregation and Bluetooth IDS systems are thus recommended.

- Blinding range sensor from a distance via optical means to induce a crash with static element (e.g. wall):

  This has been assessed as low risk mainly due to the low potential of attack value (due to the low probability assigned to a hacktivist threat agent, despite the large window of opportunity) and medium controllability. Impact is also assessed as "MEDIUM" as the initial value of 16 for unmodified impact value is compensated for by the controllability value of 2, thus falling to 12. However, this attack cannot be easily ignored since a private parking environment with the frequent presence of the vehicle offers an ideal use case for someone who wants to attempt a sensor jamming experiment.

- Accessing logger data via vehicle Wi-Fi set-up for internal purposes (e.g. logging data during the L3 pilot):

  This has been assessed as very low risk although assessed as not controllable, mainly due to the very low potential of attack value (in the L3Pilot context) and the low impact considered. However, this attack cannot be totally ignored since logging data via wireless interfaces remains an option, given the frequent presence of the vehicle in the OEMs and private parking environment, which offers an ideal use case for someone who wants to attempt a vehicle Wi-Fi interference experiment (although the possibility of such an occurrence in the controlled environment of an OEM premises is considered very low).

- Altering static environment to induce misperception of surroundings (e.g. adding/removing a visible parking spot boundary line):

  This has been assessed as very low risk and of medium controllability (localization and mapping via sensor fusion could alleviate the effects of such an attack and a-priori map is available and stored in the memory of the ADF), mainly due to very low potential of the attack value (in the L3Pilot context someone entering the OEM premises for altering a parking spot setting is considered not probable) and the low impact considered. However, this attack cannot be generally ignored since it requires very little technical knowledge to perform a road infrastructure change that will distort the sensors' perception. Parking areas are likely to be the number one venues for such attacks since they are easily accessed.

6 Practical Cyber Security Recommendations for Piloting and Beyond

SAE J3061 [44] requires the identification of cyber security goals from TARA analysis. The goals describe the highest-level cyber security requirements. These are in the form of a high-level and concise description of what should be avoided, detected, or prevented.

In this section, high-level recommendations for further use by the L3Pilot prototype vehicle owners during the project's pilot preparation phase will be proposed for planning against cyber attacks for the entire L3 vehicle lifecycle. For this purpose, the recommendations are based on the literature review (e.g. [42]), the L3Pilot OEM questionnaires/interviews, and the results of our TARA+ analysis. Technical recommendations in the form of countermeasures per attack vector as described in the literature can be found in the general analysis part of Section 3 and in particular in Table 3.2 to Table 3.4.

6.1 General Guidelines

General cyber security recommendations for L3 pilot prototype owners include:

1. Perform penetration tests or seek confirmation that these tests are performed by your selected suppliers.
2. Based on TARA analysis, produce mitigation plans for the most probable attacks.
3. Make sure that cyber security design takes into account aspects of the entire vehicle lifecycle (attacks by a malicious mechanic or during an OTA update are considered probable).
4. Promote OBDII standard evolution to integrate security requirements, since physical attacks can no longer be ignored.
5. Increase awareness among your users about ADF functions by visualizing what the sensors perceive and by using periodic messages on the TCU. Overall, observability of an attack leads to higher controllability.
6. Make sure all the critical ECU components are physically separated from the rest of the system.
7. Prevent eavesdropping of wireline and wireless communication.
8. Prevent tampering with wireline and wireless communication.
9. Secure sensor-based perception by allowing for sensor redundancy and by developing Intrusion Detection Systems specifically for dynamic sensor data spoofing (taking into account the recent literature on adversarial machine learning).
10. Avoid unauthorized or wrong (unfinished) software updates.
11. Prevent and detect attacks on web server for software updates.

12. Prevent application of unauthorized or wrong ADF configuration data.

13. Prevent exploitation of known vulnerabilities (e.g. Bluetooth communication).

Other general guidelines to take into consideration are provided in the list that follows:

- Implement your system with AUTOSAR

Modelling and generating of secure component communications will be supported by AUTOSAR Adaptive [1]. This new platform aims to support dynamic deployment of customer applications, to provide an environment for applications that require high-end computing power, and to connect deeply embedded and non-AUTOSAR systems in a smooth way while preserving typical features that originated in deeply embedded systems, such as safety, determinism, and real-time capabilities. Built around existing standards such as POSIX, the AUTOSAR Adaptive Platform will complement automotive specific functionalities, enabling the platform to run in an automotive network.

Note 1: AUTOSAR specs documents are public and can be retrieved online.

Note 2: The AUTOSAR standard acknowledges the need for improved security in automotive communications by providing a set of standard modules for encryption and authentication, to ensure confidentiality and integrity. However, these modules are not currently matched by corresponding models for security at the application level, and their use is somewhat in violation of the established AUTOSAR methodology that relies on code generation from high-level specifications for all the communications and scheduling features.

Note 3: One of the major achievements featured in the AUTOSAR Adaptive Platform Release 18-03 is the Update and Configuration Management, which enables vehicles to be updated over-the-air.

- Follow the standards (safety and security go hand-in-hand)

Table 6.1: Recommendations for standards to be followed in L3Pilot

Standard	Summary	Notes
SAE J3061 (security guidelines)	The recently published SAE J3061 guideline establishes a set of high-level guiding principles for cyber security by: • defining a complete lifecycle process framework • providing information on some common existing tools and methods (different TARA methods are included) • supporting basic guiding principles on cyber security	• Cyber security engineering lifecycle process, which is defined analogous to the process framework described in ISO 26262. • No restrictions are given on whether to maintain separate processes for safety and security engineering with appropriate levels of interaction or to attempt

Standard	Summary	Notes
	- summarizing further standard development activities	direct integration of the two processes.
IEC 61508 Ed 2.0 & 3.0	Functional safety of electrical/electronic/programmable electronic safety-related systems (The functional safety standards include IEC 61508 for the general industry and ISO 26262 for road vehicles. These standards define the appropriate safety lifecycle and Safety Integrity Levels (SILs), develop hardware and software, and provide a safety analysis with supporting confirmation measures and processes)	First approach of integrating safety and security; security threats are to be considered during hazard analysis in the form of a security threat analysis. Ed 3.0 is expected to elaborate even further on the topic of security-aware safety.
ISO 26262 Ed 2.0 – Annex F	Road vehicles functional safety standard Addresses possible hazards caused by malfunctioning behaviour of E/E safety-related systems (HARA methods)	- Fail Safe vs Fail Silent vs Fail Tolerant requirements - Does not include nominal operation of such systems - (under development) Likely to include recommendations for fitting security standards and appropriate security measure implementations
SOTIF ISO/PAS 21448 – Public Available Specification	For automated or autonomous vehicles, safety is not only endangered by failures in the classical understanding – e.g. a hardware element fails or a software has a design error – but also by misinterpretations of sensor signals or failure to combine sensor data and processing. SOTIF is a newly developed standard that addresses such issues.	Fail-operational architectures Under development
ISO 15408	Information technology/security techniques/evaluation criteria for IT security	Extending the Common Criteria framework to vehicles would be a positive step in improving vehicle cyber security (currently missing, relevant work in the EU project SaferTEC).

Standard	Summary	Notes
ISO/SAE CD 21434 Road Vehicles – Cyber security engineering	Due to increasing connectivity, V2X communication, and the shift of functionality towards software and more complexity that increases the need for over-the-air (OTA) updates, cyber security is increasingly important for dependable automotive systems. Recently demonstrated hacker attacks on automotive control systems via maintenance or entertainment channels have shown the necessity as well. Therefore SAE, which already created SAE J3061 as a guideline for automotive cyber security engineering, and ISO have joined forces towards an Automotive Cyber Security Standard (ISO/SAE JWG1, ISO TC22 SC32 WG 11).	Under development

- Update your team with knowledge published in the recent literature (look for works that deal with both safety and cyber security engineering in parallel)

Table 6.2: Recommended recent literature

Ref.	Description
[47]	Good overview of TARA methods available for automotive apps split by their applicability in the concept phase (early development phase) vs the system phase of the analysis “A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context”
[48]	Proposal for a joint SAEJ3061/ISO26262 security analysis framework https://www.researchgate.net/publication/315859565_Integrated_Safety_and_Security_Development_in_the_Automotive_Domain
[37]	EVITA inspired TARA model A Risk Assessment Framework for Automotive Embedded Systems
[35]	SAEJ3061 – ISO 26262 link when doing TARA “Using SAE J3061 for Automotive Security Requirement Engineering”
[49]	Security application of failure mode and effect analysis (FMEA)

6.2 Practical Recommendations in Four Directions

Establish and use a sound secure engineering process

- Perform threat analysis of the vehicular environment using standard threat analysis methods such as TARA and others discussed in this deliverable
    - Identify the assets to be protected
    - Identify the threats to those assets
    - Identify the potential of an attack
    - Assess the impact (e.g. financial, operational) of damage to the organization in the event of an attack and of the identified assets being compromised
- Risk assessment
    - Identify the risks, with a high focus on the risks to the safety-critical infrastructure
    - Classify the risks and identify those which are highly undesirable or unacceptable
    - Develop defences against the unacceptable risks
- Security requirements
    - Identify security requirements for the entire system
    - Security requirements should not only be identified and proposed for software development but also for other domains related to the vehicle, such as requirements for network design and communication as well as requirements for any piece of hardware that is running software and/or is part of a communication
- Security by design
    - Prefer security by design rather than security as a patch
    - Follow secure programming and software development guidelines, such as MISRA C or NIST
    - Perform code analysis for compliance with the guidelines used
    - Perform software testing such as integration, unit, functional, and system testing
- Data privacy and confidentiality
    - Develop methods to address the confidentiality, integrity, and availability of the system
    - Use standard and well-tested protocols for the provision of confidentiality and integrity, such as transport layer security for TCP/IP-based communication or secured CAN for CAN communications
    - Avoid using proprietary cryptographic methods, which are not as thoroughly tested as their publically available and standardized counterparts
    - Avoid implementing cryptographic methods yourself, but use publicly available, well tested and standardized libraries

  - Use well-tested and preferred methods for cryptographic functionality, such as the hardware security modules (HSM)/tamper-proof modules (TPM)
  - Key material should be highly protected, also preferably using HSMs/TPMs
  - A preferable option might be to aim for a decentralized architecture so that a single point of failure can be minimized and availability of the system can be increased

Internal and external connectivity/communications

- Close the debugging access to the electronic devices in the production vehicles
  - Debug access to the ECUs should be closed
  - Flashing interfaces such as JTAG should be permanently shut down after initial flash
- Segregate the safety critical infrastructure from the non-safety critical infrastructure
  - Connect the safety critical and non-safety critical sub-systems to different networks or sub-networks
  - Message exchanges between safety critical and non-safety critical components should be avoided as far as possible
  - Integrate an explicit security gateway between the safety critical and non-safety critical parts of your vehicle architecture
- Only provide external or internal connectivity to the vehicle when absolutely needed or important from a business point of view
  - Properly secure the connection points such as USB, radio, audio player, and OBD ports
  - Network segregation will additionally help in preventing or at least minimizing the spread of malicious access from the non-safety critical sub-system to the safety critical sub-system of the vehicle
- Wireless connectivity methods that can be accessed outside the realm of the vehicle, such as mobile communications, Wi-Fi, GPS, and Bluetooth, should be properly secured
  - Use the latest version of the standard protocols for provision of security for the respective connectivity methods
  - The older versions might already have been broken (found to have vulnerabilities that can be exploited later) and therefore should not be used
- Typically, connections from outside to the vehicle should be kept at a minimum and be properly tested
- Control and limit the possibility of updating firmware
  - Re-flashing of ECUs should only be possible if certain pre-conditions are met

    - A successful challenge-response communication with the ECU must occur before the update is allowed
    - The vehicle should be stationary and the safety critical systems should be deactivated, e.g. the wheels or steering should be stationary
    - ECU should not be programmable from a low-speed bus if the segregation of buses exists, e.g. low- and high-speed buses

Self-Auditing

- Gather information about the policies and procedures currently in place
    - Analyse the policies and procedures in place
    - Identify the missing or outdated ones
    - Fill the gaps by including the missing ones
- Gather information on vulnerabilities
    - Vulnerability detection software tools can be used
    - Rate the vulnerabilities to prioritize them, using a standardized approach such as a numerical rating system
    - Find or develop methods to address the vulnerabilities, and integrate them in the production vehicle, before they can be exploited
- Test the system – more importantly the safety critical systems or sub-systems:
    - Use fuzz testing – mainly for code testing
    - Use penetration testing – mainly for testing the vehicular infrastructure, networked devices, and services on the network components
    - Document the results of testing
    - Review the results and look for new vulnerabilities which were not known before
    - Address the identified vulnerabilities
    - Retest the system to make sure that the vulnerabilities are no longer exploitable and that in fixing the vulnerabilities no new vulnerabilities were introduced

Vulnerability or incident detection and response

- Establish an information sharing and analysis centre (ISAC)
    - Establishment of an ISAC consortium-wide in the scope of L3Pilot is highly encouraged
    - There are also already existing ISAC or related consortiums where membership might be obtained

  - However, if it is not possible to form an L3Pilot wide ISAC or join an international one, at least each OEM should have its own team which assumes the role of an ISAC
  - All vulnerabilities, exploits, and incidents should be reported to ISAC by the involved partners
- Establish a vulnerability disclosure and reporting procedure
  - Reporting of vulnerabilities to the manufacturer should be made possible
  - There should be a clear way, e.g. a form or email address, for an external party such as an independent researcher to report vulnerabilities
- Develop and have a standard operating procedure in place to address the identified or reported vulnerabilities
  - A formal and clear process to address the identified or reported vulnerabilities
  - Focus on containing the incident, remedying the system, and retesting it to make sure the vulnerability is handled
  - Update the vulnerable parts of the system
  - Communicate back to the ISAC for sharing and analysis
- If a protocol is found to be using cryptographic algorithms or mechanisms which are found to be broken, the updated and/or patched version of those protocols should be used as soon as they are available
- Log the incidents, especially those which might have an impact on security (aside from safety)
  - Log the incidents relevant for security purposes
  - Communicate the incidents or (potential) security breaches to the back end for storage and/or further analysis by security experts
  - For back-end connectivity, use standardized IP security protocols, such as TLS or IPSec

7 Conclusions

Legal aspects

Due to the importance of the legal aspects, we have reviewed the regulations applicable to conducting experiments in seven countries, namely: Belgium, France, Germany, Italy, Sweden, the Netherlands, and the United Kingdom. The review produced a presentation of requirements in each nation, using a standard template to allow a direct comparison between countries. It is clear that further updates of these regulations can be expected, due to the limited experience that currently exists with automated driving in the varied situations that can be encountered in the road environment.

All car owners in the L3Pilot project have agreed to comply with the regulations in the countries where they conduct experiments, including cross-border testing. Moreover, these procedures are part of a more general internal process followed by each car company, based on their experience with prototypes and on the knowledge collected during the development of similar products (e.g. ADAS functionalities). The overall objective is to maximize safety for all road users, including the driver/passengers of the test vehicle.

L3Pilot partners consider the regulatory initiatives at the European level as a key milestone for the deployment of the technology. The framework creates the prerequisites for highly and fully automated systems and also shows the interest of many stakeholders in the potential benefits of automated driving. The different national regulations represent an additional challenge. For this reason, the project partners advocate further work towards an internationally harmonized legal framework.

Cyber security

Cyber security is a key aspect that impacts on all intelligent systems. Particularly in the field of automated driving, security becomes critical due to safety implications. Therefore, a robust and coherent approach to address this problem is essential for the future of the automotive industry.

In this project, we have aimed to cover the cyber security aspects for level-3 AD vehicles in the context of the project use cases, namely Urban Chauffeur, Highway Chauffeur, and Parking Chauffeur. Our methodology was based on a customized framework, derived from the state-of-the-art method for cyber security analysis known as Threat Analysis and Risk Assessment (TARA). This method estimates the potential and the impact of an attack and derives the associated risk value.

The present deliverable has described our enhanced Threat Analysis and Risk Assessment Framework called “TARA+”, which incorporates the notions of controllability and observability of an attack. The TARA+ was applied to the relevant use cases, providing a comprehensive cyber security analysis based on the most prominent attack scenarios for each application. Our analysis covered various attack surfaces and adversaries with different levels of expertise. The likelihood, controllability, impacts, and risk factors were formally calculated, and the most risky situations were identified. In addition, a generic approach was taken to the investigation with the aim of generalizing the results to all functions at level 3 for automated vehicles.

The conclusions of the TARA+ analysis, together with a literature survey and interviews with the automotive partners, allowed a list of high-level cyber security recommendations to be compiled. These recommendations are intended for further use by the L3Pilot vehicle owners during the design and execution of the pilot studies.

References

[1] AUTOSAR (2017). AUTOSAR_SWS_SecureOnboardCommunication, 4.3.1. Available at: https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SWS_SecureOnboardCommunication.pdf [12.10.2018].

[2] Federico Maggi., Trend Micro, Inc. TrendLabs Security Intelligence Blog. A Vulnerability in Modern Automotive Standards and How We Exploited It (August 2017).

[3] M. Wolf, A. Weimerskirch and C. Paar, "Security in automotive bus systems", in proceedings of the Workshop on Embedded Security in Cars (ESCAR), 2004.

[4] H. Ueda, R. Kurachi, H. Takada, T. Mizutani, M. Inoue, and S. Horihata, "Security Authentication System for In-Vehicle Network", SEI technical review, number 81, October 2015.

[5] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile", 2010 IEEE Symposium on Security and Privacy, Berkeley/Oakland, CA, 2010, pp. 447–462.

[6] J. Petit and S. E. Shladover, "Potential Cyberattacks on Automated Vehicles", IEEE Transactions on Intelligent Transportation Systems, 16(2):546–556, April 2015.

[7] Wolf M., Weimerskirch A., Paar C. (2006) Secure In-Vehicle Communication. In: Lemke K., Paar C., Wolf M. (eds) Embedded Security in Cars. Springer, Berlin, Heidelberg.

[8] O. Avatefipour, H. Malik, "State-of-the-Art Survey on In-Vehicle Network Communication 'CAN-Bus' Security and Vulnerabilities", IJCSN – International Journal of Computer Science and Network 6 (6).

[9] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, 2017, Pearson.

[10] I. Ivanov, C. Maple, T. Watson, and S. Lee, "Cyber security standards and issues in V2X communications for Internet of Vehicles", Living in the Internet of Things: Cyber security of the IoT, pp. 1–6, London, 28–29 March 2018.

[11] M. Villarreal-Vasquez, B. Bhargava, and P. Angin, "Adaptable Safety and Security in V2X Systems", IEEE International Congress on Internet of Things (ICIOT), pp. 17–24, Honolulu, HI, 25–30 June 2017.

[12] K. Bian, G. Zhang and L. Song, "Security in Use Cases of Vehicle-to-Everything Communications", IEEE 86th Vehicular Technology Conference, pp. 1–5, Sydney, Australia, 4–7June 2017.

[13] H. Shin, D. Kim, Y. Kwon, Y. Kim, “Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications”, In: Fischer W., Homma N. (eds) Cryptographic Hardware and Embedded Systems – CHES 2017, Taipei, Taiwan, 25–28 September, 2017.

[14] A. Alrabady and S. Mahmud, “Some attacks against vehicles’ passive entry security systems and their solutions”, IEEE Transactions on Vehicular Technology, 52(2):431–439, March 2003.

[15] A. Alrabady and S. Mahmud. “Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs”, IEEE Transactions on Vehicular Technology, 54(1):41–50, January 2005.

[16] P. Kocher et al., “Introduction to differential power analysis”, Journal of Cryptographic Engineering, 1(5):5–27, April 2011.

[17] P.C. Kocher, “Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems”, Koblitz N. (eds) Advances in Cryptology — CRYPTO ’96, 16th Annual International Cryptology Conference Santa Barbara, California, USA, 18–22 August 1996.

[18] Longo, Jake, et al., “SoC it to EM: Electromagnetic side-channel attacks on a complex system-on-chip”, Cryptographic Hardware and Embedded Systems – CHES 2015, Springer Saint-Malo, France, 13–16 September 2015.

[19] Dag Arne Osvik, Adi Shamir, Eran Tromer, Cache attacks and countermeasures: The case of AES, proc. RSA Conference Cryptographers Track (CT-RSA) 2006, Lecture Notes in Computer Science 3860, pp. 1–20, Springer-Verlag, 2006.

[20] S. R. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4”, in Serge Vaudenay and Amr M. Youssef, editors, Selected Areas in Cryptography 2001, Springer, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, 16–17 August 2001.

[21] M. Vanhoef and F. Piessens, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, CCS’17, Dallas, TX, USA, 30 October–3 November 2017.

[22] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O. Hanlon, and P. M. Kintner, “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer”, in Proceedings of the Institute of Navigation GNSS (ION GNSS 2008), 2008.

[23] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller, “An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers”, in Proceedings of the Institute of Navigation International Technical Meeting (ION ITM 2009), January 2009.

[24] H. Hu and N. Wei, “A study of GPS jamming and anti-jamming”, 2nd International Conference on Power Electronics and Intelligent Transportation System (PEITS), pp. 388–391, Shenzhen, China, 19–20 December 2009.

[25] CORDIS | European Commission. (2013). Driverless cars take to the road | Result In Brief | CORDIS | European Commission. [online] Available at: https://cordis.europa.eu/result/rcn/90263_en.html [Accessed 18 Oct. 2018].

[26] Weimerskirch, A. and Dominic, D. (2018). Assessing Risk: Identifying and Analyzing Cyber security Threats to Automated Vehicles. [online] Mcity.umich.edu. Available at: https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf [Accessed 18 Oct. 2018].

[27] Manadhata, P.K.: An attack surface metric. Ph.D. thesis, Carnegie Mellon University (2008).

[28] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu,M. Gruteser, W. Trappe, and I. Seskar. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In I. Goldberg, editor, USENIX Security 2010, pp. 323–338. USENIX Association, Aug. 2010.

[29] V. Izosimov, A. Asvestopoulos, O. Blomkvist, and M. Torngren, “Security-aware development of cyber-physical systems illustrated with automotive case study”, in 2016 Design, Automation & Test in Europe Conference & Exhibition, DATE 2016, Dresden, Germany, 2016.

[30] A. Wasicek and W. Andre, “Recognizing manipulated electronic control units”, in SAE 2015 World Congress & Exhibition, April 2015.

[31] M. Hamad, M. Nolte, and V. Prevelakis, Towards Comprehensive Threat Modeling for Vehicles. 1st Workshop on Security and Dependability of Critical Embedded Real-Time Systems (CERTS 2016).

[32] Dan J. Klinedinst, Christopher King, White Paper, On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle, CERT/Carnegie Mellon University’s Software Engineering Institute, April 2016.

[33] Tuncali, Cumhur Erkan et al. “Simulation-based Adversarial Test Generation for Autonomous Vehicles with Machine Learning Components.” CoRR abs/1804.06760 (2018).

[34] ISO 26262 Road Vehicles – Functional Safety. November, 2011. ISO, Geneva, Switzerland.http://www.iso.org.

[35] Schmittner, Christoph et al. “Using SAE J3061 for Automotive Security Requirement Engineering.” SAFECOMP Workshops (2016).

[36] Derrick Dominic, Sumeet Chhawri, Ryan M. Eustice, Di Ma, and André Weimerskirch. 2016. Risk Assessment for Cooperative automated driving. In Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy (CPS-SPC ‘16). ACM, New York, NY, USA, 47–58. DOI: https://doi.org/10.1145/2994487.2994499.

[37] M. Islam, A. Lautenbach, C. Sandberg, & T. Olovsson, (2016). A Risk Assessment Framework for Automotive Embedded Systems. 3-14. 10.1145/2899015.2899018.

[38] J-P. Monteuuis, A. Boudguiga, J. Zhang, H. Labiod, A. Servel, & P. Urien, (2018). SARA: Security Automotive Risk Analysis Method. 3-14. 10.1145/3198458.3198465.

[39] R. Grave, Autonomous Driving: From Fail-Safe to Fail-Operational Systems, Elektrobit Automotive GmbH 2015, presentation at TechDay, 3 December, 2015.

[40] Karahasanovic, A. (2017) Automotive Cyber security. Göteborg: Chalmers University of Technology.

[41] McCarthy, C., Harnett, K., and Carter, A. (2014, October). Characterization of potential security threats in modern automobiles: A composite modeling approach. (Report No. DOT HS 812 074) Washington, DC: National Highway Traffic Safety Administration. Available at www.nhtsa.gov/Research/Crash+Avoidance/ci.Office+of+Crash+Avoidance+Research+Technical+Publications.print.

[42] National Highway Traffic Safety Administration. (2016, October). Cyber security best practices for modern vehicles. (Report No. DOT HS 812 333). Washington, DC.

[43] G. Macher, E. Armengaud, E. Brenner, C. Kreiner, Threat and Risk Assessment Methodologies in the Automotive Domain, Procedia Computer Science, Volume 83, 2016, pp. 1288–1294, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2016.04.268.

[44] SAE J3061_201601, Cyber security Guidebook for Cyber-Physical Vehicle Systems, SAE standard, 2016.

[45] A. Shostack. Threat modelling, designing for security. Wiley, 2014.

[46] CCRA Members. Common Criteria for Information Technology Security Evaluation. CCMB-2012-09-00X, Version 3.1, Revision 4.

[47] G. Macher, E. Armengaud, E. Brenner, CJ. Kreiner. (2016). A Review of Threat Analysis and Risk Assessment Methods in the Automotive Context. In International Conference on Computer Safety, Reliability, and Security: SAFECOMP 2016. Lecture Notes in Computer Science, Bd. 9922 2016, Springer International Publishing AG , p. 130. DOI: 10.1007/978-3-319-45477-1_11.

[48] G. Macher, R. Messnarz, E. Armengaud, A. Riel, E. Brenner, C. Kreiner (2017). Integrated Safety and Security Development in the Automotive Domain. 10.4271/2017-01-1661.

[49] C. Schmittner, T. Gruber, P. Puschner, and E. Schoitsch. Security application of failure mode and effect analysis (FMEA). In Computer Safety, Reliability, and Security, pp. 310–325. Springer, 2014.

[50] Zhao M. Advanced driver assistant system, threats, requirements, security solutions. Intel Labs. White paper, 2015.

[51] CCRA Members. Common Methodology for Information Technology Security Evaluation Evaluation Methodology, chapter Vulnerability Assessment (AVA), pp. 404–433. September 2012. CCMB-2012-09-004, Version 3.1, Revision 4.

[52] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX Security Symposium, USENIX Association, (2011).

List of abbreviations and acronyms

Abbreviation	Meaning
ACC	Adaptive Cruise Control
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
ADF	Automated Driving Function
AV	Automated Vehicles
CAN	Controller Area Network
CoP	Code of Practice
D2B	Domestic Digital Bus
DoS	Denial-of-Service
DDoS	Distributed Denial-of-Service
ECU	Electronic control unit
FOT	Field Operational Tests
HC	Highway Chauffeur
HYP	Hypotheses
ISAC	Information Sharing and Analysis Centre
LIN	Local Interconnect Network
MOST	Media Oriented Systems Transport
OBD	On-Board Diagnostics
OBU	On-Board Unit
ODD	Operational Design Domain
OTA	Over-the-Air
RQ	Research Question
SAE	Society of Automotive Engineers
SDV	Software Defined Vehicles
TARA	Threat Analysis and Risk Assessment
TCU	Telematics Control Unit
TTCAN	Time-Triggered CAN
TTP	Time-Triggered Protocol
VRU	Vulnerable Road Users

Term	Description	Source
Attack vector	Entry point of the potential attack, e.g. OBD-II input, USB port, Bluetooth, GPS, audio system, etc.	NHTSA

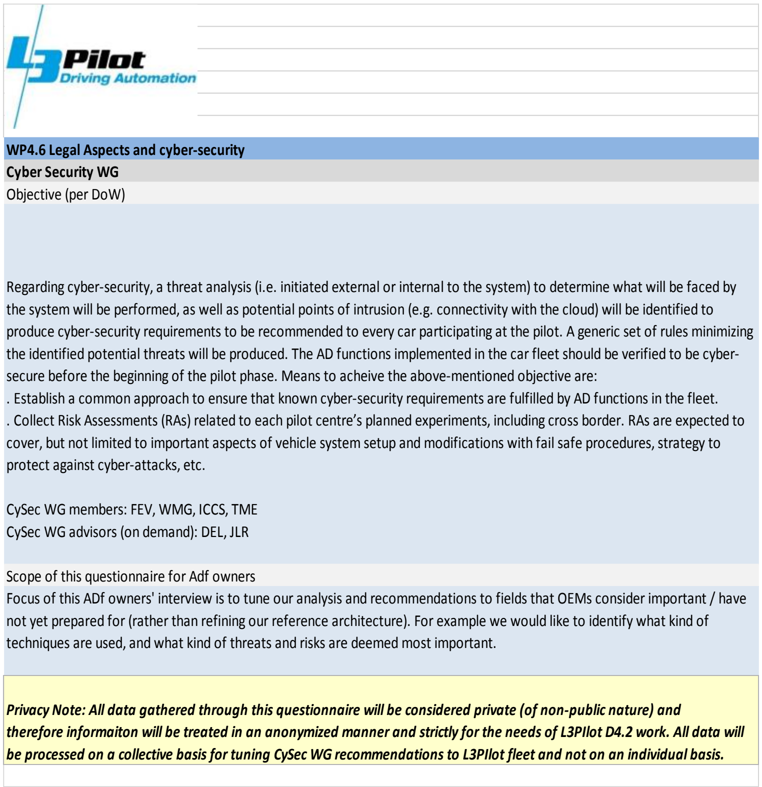
Abbreviation	Meaning	
Attack surface	The different points (the “attack vectors”) where an unauthorized user (the “attacker”) can try to enter data to or extract data from an environment.	SAE J3061
Attack potential	The likelihood that a potential attack can be successfully carried out.	SAE J3061
ASIL - Automotive Safety Integrity Level	A means of classifying hazards in ISO 26262.	ISO 26262
Attack type	Type of attack that could be used • Spoofing identity • Tampering with data • Repudiation • Information disclosure • Denial of service • Elevation of privilege	MS STRIDE model
ECU	Electronic Control Unit: Any embedded system in automotive electronics that controls one or more of the electrical systems or subsystems in a vehicle.	
STRIDE	Threat modelling technique by Microsoft. Stands for Spoofing identity, Tampering with data, Repudiation, Information disclosure, Denial of service, and Elevation of privilege.	[45]
TOE	Target of evaluation	SAE J3061

Annex 1 Legal Aspects Template

Country:	Date
Regulation – Reference	
Scope	
Definitions	
Potential restrictions	
Procedure description	
Authorization	
General conditions	
Bodies in charge of examining the application for exemption	
Special requirements	
Duration	
Language	
Contact information	
Web link	
Miscellaneous	

Annex 2 Cyber Security Questionnaire Template

Click to open the attached file in Excel



WP4.6 Legal Aspects and cyber-security

Cyber Security WG

Objective (per DoW)

Regarding cyber-security, a threat analysis (i.e. initiated external or internal to the system) to determine what will be faced by the system will be performed, as well as potential points of intrusion (e.g. connectivity with the cloud) will be identified to produce cyber-security requirements to be recommended to every car participating at the pilot. A generic set of rules minimizing the identified potential threats will be produced. The AD functions implemented in the car fleet should be verified to be cyber-secure before the beginning of the pilot phase. Means to acheive the above-mentioned objective are:

. Establish a common approach to ensure that known cyber-security requirements are fulfilled by AD functions in the fleet.

. Collect Risk Assessments (RAs) related to each pilot centre’s planned experiments, including cross border. RAs are expected to cover, but not limited to important aspects of vehicle system setup and modifications with fail safe procedures, strategy to protect against cyber-attacks, etc.

CySec WG members: FEV, WMG, ICCS, TME
CySec WG advisors (on demand): DEL, JLR

Scope of this questionnaire for Adf owners

Focus of this ADf owners' interview is to tune our analysis and recommendations to fields that OEMs consider important / have not yet prepared for (rather than refining our reference architecture). For example we would like to identify what kind of techniques are used, and what kind of threats and risks are deemed most important.

Privacy Note: All data gathered through this questionnaire will be considered private (of non-public nature) and therefore informaiton will be treated in an anonymized manner and strictly for the needs of L3PIlot D4.2 work. All data will be processed on a collective basis for tuning CySec WG recommendations to L3PIlot fleet and not on an individual basis.

Annex 3 Threat Model Parameters Referred to in SAE J3061

Based on the work of the HEAVENS project [37] and retrieved from the SAE J3061 SoA overview, the parameters related to the potential of an attack are defined as follows:

- **"Expertise (E)"** refers to the level of generic knowledge of the underlying principles, product type, or attack methods that are required to carry out an attack on the target of interest and can take one of the following values:
  - "Layman" is unknowledgeable compared to experts or proficient persons, with no particular expertise; examples may include persons who can only follow simple instructions that come with the available tools to mount simple attacks, but not capable of making progress themselves if the instructions or the tools do not work as expected.
  - "Proficient" persons have general knowledge about the security field and are involved in the business, such as workshop professionals. Proficient persons know about simple and popular attacks. They are capable of mounting attacks – for example, odometer tuning and installing counterfeit parts – by using available tools and if required, are capable of improvising to achieve the desired results.
  - "Experts" are familiar with the underlying algorithms, protocols, hardware, structures, security behaviour, principles, and concepts of security employed, as well as techniques and tools for the definition of new attacks, cryptography, classic attacks for the product type, attack methods, etc. implemented in the product or system type.
  - The level "Multiple experts" is introduced to allow for a situation in which different fields of expertise are required at an Expert level for the distinct steps of an attack.
- **"Available knowledge about the target (K)"**, also known as "Knowledge about TOE" in HEAVENS, refers to the availability of information about the TOE and the community size that possesses knowledge about the TOE from an attacker perspective. This parameter points to the sources from which attackers can gain knowledge about the TOE and indicates how easy or difficult it can be for an attacker to acquire knowledge about the TOE. It can take one of the following values:
  - "Public" information concerning the TOE (e.g. as gained from the Internet, bookstore, information shared without non-disclosure agreements).
  - "Restricted" information concerning the TOE (e.g. knowledge that is controlled within the developer organization and shared with other organizations, for example, between suppliers and OEMs, under a non-disclosure agreement). Examples include requirements and design specifications, internal documentation.
  - "Sensitive" information about the TOE (e.g. knowledge that is shared between discrete teams within the developer organization, access to which is constrained only to members of the specified teams). Examples include restricted ECU configuration

parameters to enable/disable features in vehicles, vehicle configuration database, and software source code.

  - “Critical” information about the TOE (e.g. knowledge that is known by only a few individuals, access to which is very tightly controlled on a strict need to know basis and individual undertaking). An example would be a secret root signing key.

- **“Equipment (Eq)”** refers to the equipment required to identify or exploit a vulnerability and/or mount an attack. It can take one of the following values:
  - “Standard” equipment is readily available to the attacker, either for the identification of vulnerability or for an attack. This equipment may be a part of the TOE itself (e.g. a debugger in an operating system), or can be readily obtained (e.g. Internet downloads, protocol analyser, or simple attack scripts). Examples include simple OBD diagnostic devices and common IT devices such as notebooks.
  - “Specialized” equipment is not readily available to the attacker, but could be acquired without undue effort. This could include purchase of moderate amounts of equipment (e.g. power analysis tools, the use of hundreds of PCs linked across the Internet) or the development of more extensive attack scripts or programs. Examples include in-vehicle communication devices (e.g. CAN cards) and costly workshop diagnosis devices. If clearly different test benches consisting of specialized equipment are required for distinct steps of an attack this would be rated as bespoke.
  - “Bespoke” equipment is not readily available to the public as it may need to be specially produced (e.g. very sophisticated software) or because the equipment is so specialized that its distribution is controlled, possibly even restricted. Alternatively, the equipment may be very expensive.
  - “Multiple bespoke” is introduced to allow for a situation in which different types of bespoke equipment are required for the distinct steps of an attack.
- **“Window of opportunity”** combines the access type (e.g. logical, physical) and access duration (e.g. unlimited, limited) that are required to mount an attack on the TOE by an attacker. It can take one of the following values:
  - “Low”: very low availability of the TOE. Physical access required to perform complex disassembly of vehicle parts to access internals to mount an attack on the TOE.
  - “Medium”: low availability of the TOE. Limited physical and/or logical access to the TOE. Physical access to vehicle interior or exterior without using any special tools (e.g. opening the hood to access wires).
  - “High”: high availability and limited time. Logical or remote access without physical presence.
  - “Critical”: high availability via public/untrusted network without any time limitation (i.e. TOE/asset is always accessible). Logical or remote access without physical presence

and time limitation as well as unlimited physical access to the TOE/asset. Examples include access via wireless connection or Internet (e.g. V2X or cellular interfaces).

*Table Annex 3.1**:** Microsoft's STRIDE methodology [45]*

Threat	Violated Attribute	Explanation
Spoofing	Authenticity	Attackers pretend to be someone or something else
Tampering	Integrity	Attackers change data in transit or in a data store
Repudiation	Non-repudiation	Attackers perform actions that cannot be traced back to them
Information disclosure	Confidentiality/privacy	Attackers gain access to data (e.g. in transit or in a data store)
Denial of service	Availability	Attackers interrupt a system's legitimate operation
Elevation of privilege	Authorization	Attackers perform actions they are not authorized to perform