



## Deliverable **D2.2 /**

# Draft and results from pilot application of draft CoP

Version: 1.0 Final

Dissemination level: PU

Lead contractor: BMW

Due date: 31.10.2019

Version date: 02.04.2020



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

## Document information

### Authors

Felix Fahrenkrog – BMW

Moritz Schneider – BMW

Frederik Naujoks – BMW

Fabio Tango – CRF

Andreas Knapp – Daimler

Stefan Wolter – Ford

Yu Cao – PSA

Thibault Griffon – PSA

Elias Demirtzis – Aptiv

Jorge Lorente Mallada – Toyota

Giancarlo Caccia Dominiononi – Toyota

Silvia Fabello – Veoneer

Oliver Brunnegard – Veoneer

Adam Kucewicz – Jaguar Land Rover

Stuart Whitehouse – Jaguar Land Rover

Johannes Hiller – RWTH Aachen University (ika)

Frank Bonarens – Opel

Ulrich Eberle – Opel

Roland Schindhelm – BAST

Elisabeth Shi – BAST

Michael Moroff – Audi

### Coordinator

Aria Etemad

Volkswagen Group Research

Hermann-Münch-Str. 1

38440 Wolfsburg

Germany

Phone: +49-5361-9-13654

Email: [aria.etemad@volkswagen.de](mailto:aria.etemad@volkswagen.de)

### Project funding

Horizon 2020

ART-02-2016 – Automation pilots for passenger cars

Contract number 723051

[www.L3Pilot.eu](http://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.

© 2020 by L3Pilot Consortium

## Table of contents

<b>1 Introduction</b>	<b>1</b>
1.1 Motivation for the L3Pilot project	1
1.2 L3Pilot Objectives	1
1.1 Approach and scope	3
<b>2 Introduction to the Code of Practice</b>	<b>5</b>
2.1 History of the Code of Practice	5
2.2 Scope of the Code of Practice for Automated Driving	6
2.3 Application of the Code of Practice for Automated Driving	7
<b>3 Development Process of the Code of Practice for Automated Driving</b>	<b>9</b>
3.1 Description of the Development Process of the CoP for Automated Driving	9
3.2 Development Phases in the CoP-AD	10
3.3 Categories and Topics in the CoP-AD	11
<b>4 Draft Code of Practice for Automated Driving</b>	<b>14</b>
4.1 Overall Guideline and Recommendations	14
4.1.1 Minimal Risk Manoeuvre	15
4.1.2 Documentation	17
4.1.3 Existing Standards	19
4.2 Category “ODD Vehicle Level”	20
4.2.1 Requirements	21
4.2.2 Scenarios and Limits	26
4.2.3 Performance Criteria and Customer Expectations	28
4.2.4 Architecture	31
4.2.5 Testing	36
4.3 Category “ODD Traffic System Level & Behavioural Design”	45
4.3.1 Automated Driving Risks and Coverage Interaction with Mixed Traffic	46
4.3.2 V2X interaction	49
4.3.3 Traffic simulation	52
4.3.4 Ethical & Other Traffic Related Aspects	57
4.4 Category “Safeguarding Automation”	60
4.4.1 Functional Safety	61
4.4.2 Cybersecurity	66
4.4.3 Implementation of Updates	71



4.4.4 Safety of the Intended Functionality (SOTIF)	76
4.4.5 Data Recording, Privacy and Protection	82
<b>4.5 Category “Human-Vehicle Integration”</b>	<b>87</b>
4.5.1 Guidelines for HVI	88
4.5.2 Mode Awareness, Trust & Misuse	92
4.5.3 Driver Monitoring	99
4.5.4 Controllability & Customer Clinics	102
4.5.5 Driver Training & Variability of Users	107
<b>5 Pilot application of draft CoP-AD</b>	<b>110</b>
5.1 Process of information collection	110
5.2 Identification of relevant topics for L3Pilot	110
5.3 Results to pilot application of draft CoP-AD in L3Pilot	112
5.3.1 Overall Guideline and Recommendations	112
5.3.2 Category “ODD Vehicle Level”	113
5.3.3 Category “ODD Traffic System Level & Behavioural Design”	115
5.3.4 Category “Safeguarding Automation”	117
5.3.5 Category “Human-Vehicle Integration”	118
<b>6 Conclusion</b>	<b>121</b>
<b>Annex 1 Report of the L3Pilot SP “Methodology” on test and evaluation of ADF</b>	<b>131</b>
Objective data collection	131
Subjective data collection	140

## List of figures

Figure 1.1: SAE Levels of Driving Automation J3016 (Copyright 2014 SAE International). ....	2
Figure 1.2: L3Pilot approach and the mechanism for deployment. ....	3
Figure 1.3: L3Pilot testing areas and cross-borders. ....	4
Figure 2.1: Scope of the CoP-AD. ....	7
Figure 3.1: Development phases that have been proposed in deliverable D3.1. ....	10
Figure 3.2: Development phase applied in the draft CoP-AD. ....	11
Figure 3.3: Categories used for the draft CoP-AD. ....	12
Figure 4.1: Development phase applied in the draft CoP-AD. ....	14

## List of tables

Table 3.1: Overview of topics of the CoP-AD categories and the corresponding chapters ...	12
Table 5.1: Overview on topics of the CoP-AD that are relevant in L3Pilot. ....	111
Table A1.1: Overview pros and cons for different objective data collection tools by SP3. ....	131
Table A1.2: Rating of the suitability of different objective data collection tools (1 of 3) .....	133
Table A1.3: Rating of the suitability of different objective data collection tools (2 of 3) .....	135
Table A1.4: Rating of the suitability of different objective data collection tools (3 of 3) .....	137
Table A1.5: Overview pros and cons for different subjective data collection tools by SP3. ....	140
Table A1.6: Rating of the suitability of different subjective data collection tools (1 of 2).....	141
Table A1.7: Rating of the suitability of different subjective data collection tools (2 of 2).....	142



## 1 Introduction

### 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. However, the technology is rapidly advancing and today is at a stage that justifies automated driving tests in large-scale pilots.

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

Automation is not solved simply by integrating more and better technology. This topic needs, above all, a focus on user behaviour with automated driving functions. User acceptance is the key to the success of AD on the market as well as an understanding of the legal restrictions which first need to be discussed and solved on a broad level.

The idea of the vehicle controlling itself by a computer can create uneasiness among the global populous akin to the first impression in the 1800s when a motor vehicle was introduced. The 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.

### 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 motivating a final phase of road tests which can answer the key questions before market introduction. These newly-attained levels of maturity will ensure an appropriate assessment of the impact of AD, what is happening both inside and outside the vehicles, how vehicle security can be ensured, evaluating societal impacts and emerging business models.

Recent work indicates how driver assistance systems and AD functions can be best 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, 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.

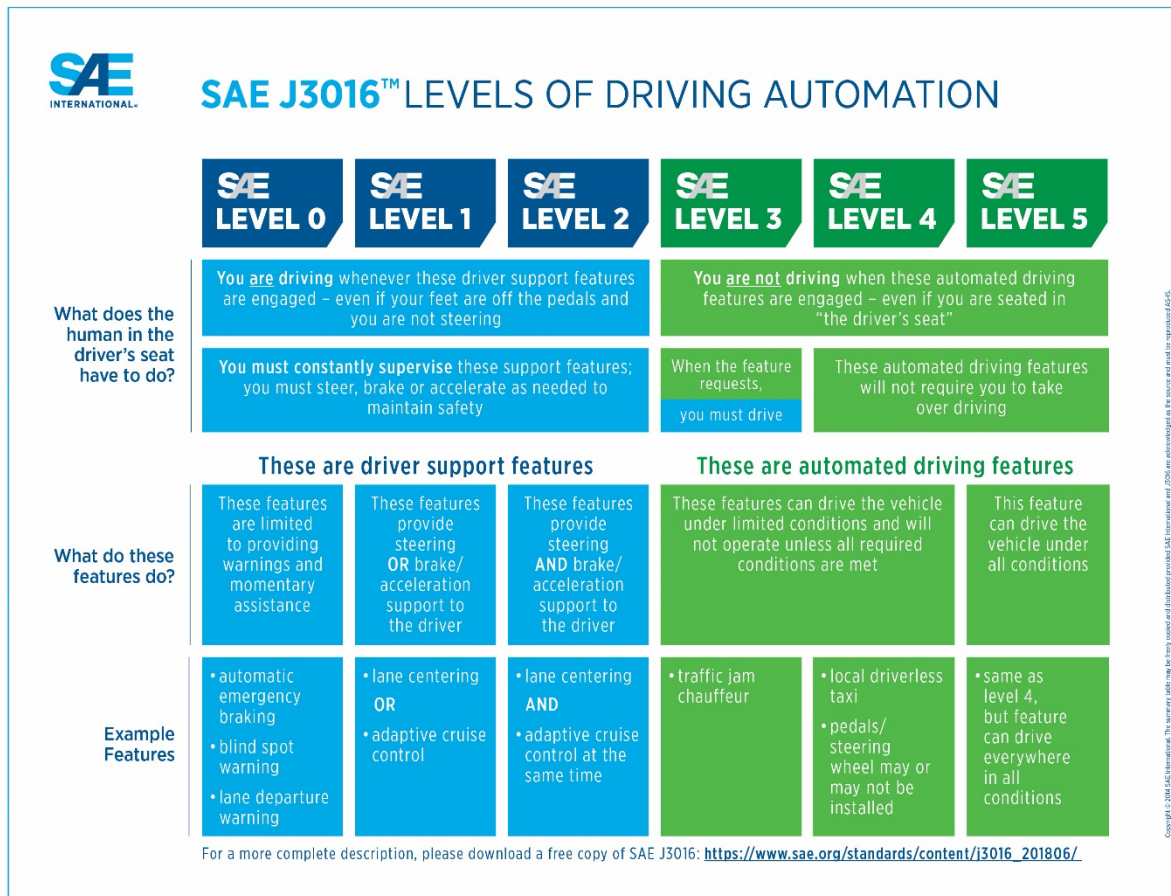


Figure 1.1: SAE Levels of Driving Automation J3016 (Copyright 2014 SAE International).

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

- Lay the foundation for the design of future, user-accepted, L3 and L4 functions, to ensure their commercial success. This will be achieved by assessing user reactions, experiences and preferences of the AD 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 standardised methods to ensure further development of AD applications (Code of Practice).
- Create a large databank to enable simulation studies of the performance of AD over time which can't be investigated in road tests, due to the time and effort needed. The data will be one product of the pilots.



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

1. Create a standardised 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 Approach and scope

The L3Pilot project will focus on large-scale piloting of ADFs (Automated Driving Functions), 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 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.

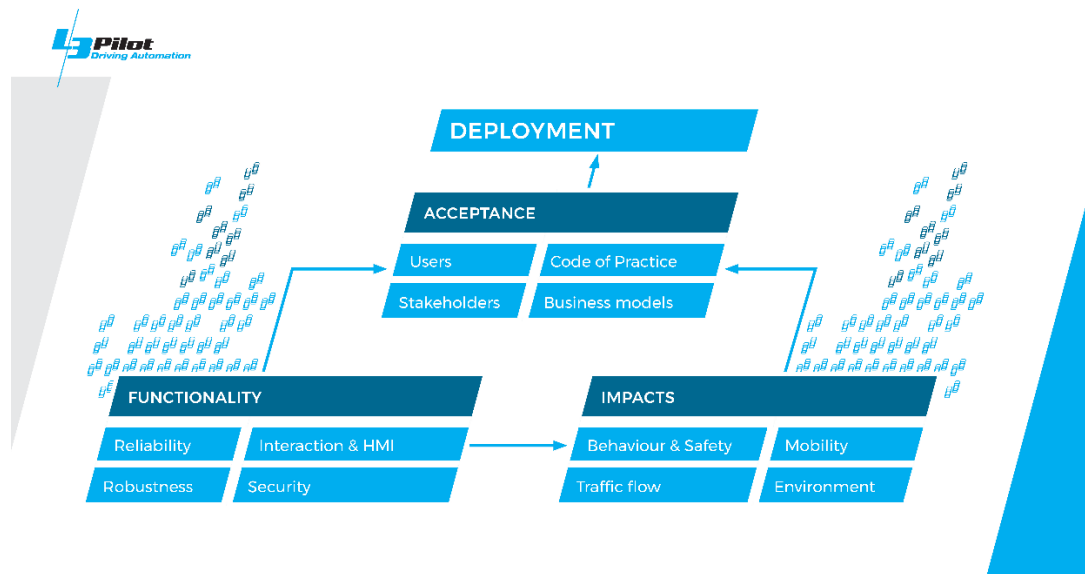


Figure 1.2: L3Pilot approach and the mechanism for deployment.

The L3Pilot consortium brings together stakeholders from the whole value chain, including: OEMs, suppliers, academic institutes, research institutes, infrastructure operators, governmental agencies, the insurance sector and user groups. More than 1,000 users will test approximately 100 vehicles across Europe with bases in 10 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.

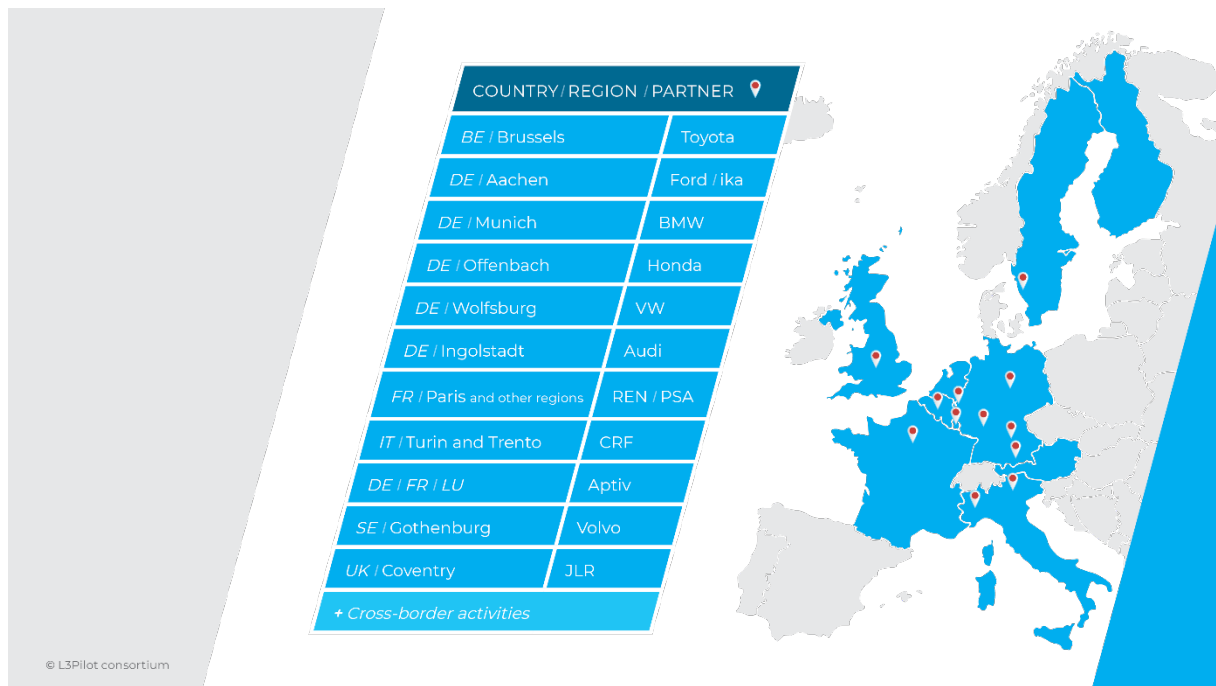


Figure 1.3: L3Pilot testing areas and cross-borders.

Since the development of ADF, especially at SAE L3, is fairly well progressed, 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 leads the consortium to create plans for the market introduction of AD. *The* L3Pilot concept can be split into the following two large parallel, but intertwined, activities:

- (i) Development of test and evaluation methodologies, and actual testing and evaluation of L3 and L4 ADFs. In this scientific part, a variety of controlled experiments will be carried out in the three pilot areas shown above (see Figure 1.3).
- (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.

## 2 Introduction to the Code of Practice

The European research project L3Pilot combines different activities. The main objective of this deliverable is to report on the draft version of the Code of Practice for automated driving (CoP-AD). The CoP-AD is to provide comprehensive guidelines for supporting the automotive industry and relevant stakeholders in the development of automated driving technology. The guidelines are derived from knowledge gained in the industry as well as from collected best practices on this topic. Thus the CoP-AD includes the following aspects:

- Collection of best practices on the topics that have been identified as relevant to L3Pilot;
- A typical process for the development and release of an automated driving function;
- Safety aspects and methods to confirm the safe operation of automated driving functions;
- Hands-on checklists targeting engineers or to support the community.

**It is important to note that this document presents only the draft version of the CoP-AD. The main purpose of this document is to be the basis for discussion and preparation of the final CoP-AD. All of this report's findings are therefore intermediate results that are still under discussion and will be subject to a future review. The final version of the CoP-AD will be published in the upcoming L3Pilot deliverable D2.3.**

The document is structured as follows: After a general introduction to the L3Pilot Project, the history of the Code of Practice is outlined and its scope for automated driving is described. The third chapter presents the approach for the COP-AD and clarifies the adaptations that have been necessary during the compilation of the CoP-AD as compared to the initial plan presented in deliverable D2.1 (Wolter et al., 2018). The draft version of the Code of Practice for automated driving is described in chapter four. The final chapter reports on the application of the CoP-AD within L3Pilot. Note: As a reminder, the L3Pilot project does not cover the entire development process of the vehicle. Thus the description of the application is limited to topics actually covered as part of L3Pilot. A second aspect that must be considered is that the L3Pilot project continues after the publication of this deliverable. Accordingly, this document only contains a snapshot of the current status of the L3Pilot project at the time of its writing and publication.

### 2.1 History of the Code of Practice

The CoP activities started with the rise of advanced driver assistance systems (ADAS) at the end of last century. At that time it became clear that these functions have a great deal of potential, however technical limits as well as liability issues could delay the market introduction of ADAS. Starting from this issue, the Response 1 project (1998–2001) was

conducted. The activity proposed the creation of a Code of Practice for the development and validation of ADAS. These “principles” for the development and evaluation of ADAS were to be established on a voluntary basis as a result of a common agreement between all involved partners and stakeholders.

The requirements for an ADAS Code of Practice were further elaborated within the RESPONSE 2 project (2002–2004). The RESPONSE 3 project (2004–2008) continued along this path in the context of the PReVENT project. The outcome of RESPONSE 3 was the final “Code of Practice for ADAS” (CoP) (Knapp et al., 2009). The CoP provided the vehicle industry with tools and a common understanding for overcoming and managing the issues around ADAS safety and liability.

Since the PReVENT project, the research and development has progressed and has led to technologies that support the driver or even take over the driving task entirely in a wider range of situations. These technologies that take over the lateral as well as the longitudinal driving task are known today as automated driving functions (ADF). Similar to ADAS, ADF faces different challenges that need to be addressed to avoid hindrance to their market introduction.

Therefore the CoP activities were continued in the European research project AdaptIVe (2014–2017), which dealt with the development of automated driving functions. RESPONSE 4 – a subproject of AdaptIVe – focused on the classification (Bartels et al., 2015) and legal aspects of automated driving (Bienzeisler et al., 2017). Furthermore, by identifying the challenges within the development of automated driving (Eberle et al., 2017), it laid out the basis for the development of the Code of Practice for Automated Driving in L3Pilot.

The Code of Practice for automated driving in L3Pilot must be seen in the tradition of the RESPONSE 3 CoP, since it is to support the developers of these technologies in order to overcome main developmental challenges. For L3Pilot, the focus is on automated driving and, because of this, is complementary to the previous CoP documents.

## 2.2 Scope of the Code of Practice for Automated Driving

The Code of Practice for Automated Driving (CoP-AD) is to be used as a guideline for developing and validating automated driving functions. The targeted user group includes engineers and other stakeholders in the field of automated driving. The CoP-AD will serve as a recommendation for a safe development of these functions. It is focused on SAE Level 3 and Level 4 functions for vehicles in which steering wheels and pedals are normally available in the vehicle all the time. In addition, the driver shall be available:

- To take over the driving task upon request by the function (user ready to take over) at any time, given a sufficient lead time for Level 3; at the end of the ODD for Level 4.
- To cover driving scenarios outside the scope of the function (e.g. function limits, outside of the ODD, AD function switched off).

- To retake control from the AD function at any time.

There is consensus that the first automated driving applications for passenger cars will be on motorways and for parking of the vehicle (VDA 2015). Traffic Jam Chauffeur for lane following in traffic jams or Motorway Chauffeur for lane following and lane changes are L3Pilot examples of how to perform the dynamic driving task (SAE 2018) on motorways instead of the driver. There will also be low speed parking functions completed without the driver present (Bosch 2017).

Therefore, the scope for the CoP-AD is set to cover SAE Level 3 and Level 4 functions. Level 0, Level 1 and Level 2 functions are not in the focus of this document. They are covered by the CoP for ADAS – see the RESPONSE 3 project (Knapp et al., 2009). In addition, three areas may be considered as extensions to the initial scope:

1. The extended scope shall cover the application of the CoP-AD to one non-EU market (e.g. China, Japan or the USA) yet to be selected.
2. The content of the CoP-AD will be checked for one robot taxi application. A robot taxi is a driverless vehicle working in a geo-fenced ODD (SAE Level 4 or 5).
3. An example of an application working in an urban or rural traffic area to help understand how to expand future automated driving functions.

The overall scope is summarised in Figure 2.1. In addition, the CoP-AD will provide relevant references to specification documents, legal guidelines or literature. In this context, the CoP for ADAS (Knapp et al., 2009) serves as a starting point for many aspects and is one of the major references for this document.

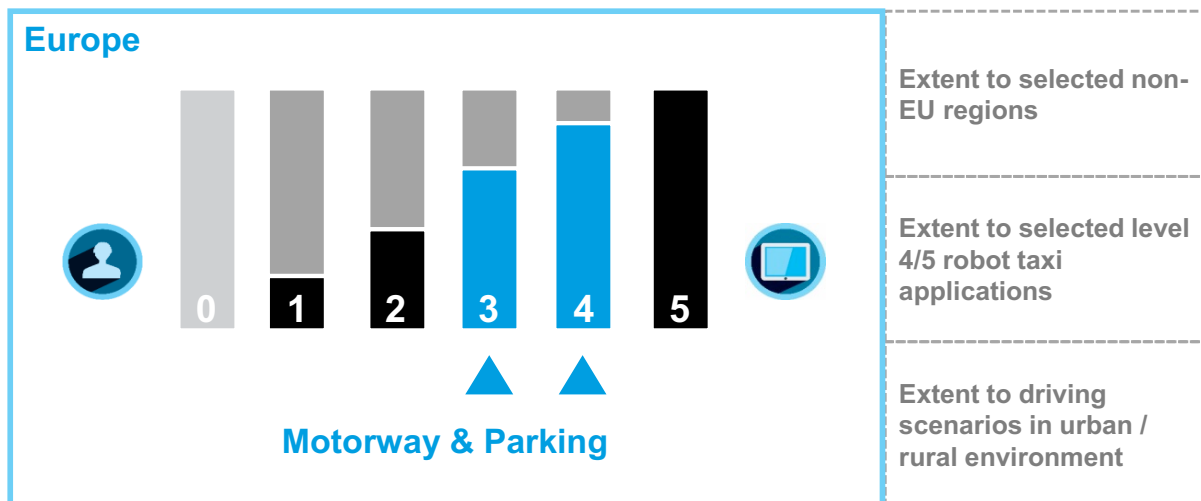


Figure 2.1: Scope of the CoP-AD.

## 2.3 Application of the Code of Practice for Automated Driving

The CoP is intended to support ADF developers by providing several questions that have been defined based on the experience gained in the development process thus far. These

questions should guide the user through different topics that are relevant to developing an ADF. It is important to note that it is not necessarily required to answer all questions with “yes” for developing an ADF. Depending on the question, a “no” might also be an appropriated answer. Some questions might also not be relevant for particular ADFs. Thus the purpose of the question is less to lead to a specific answer, but instead to prod developers into thinking about questions and to report whether and how a certain topic has been addressed in the development process. Furthermore, the questions enable documentation of the decisions and approaches taken in development. In case a question has not been addressed in the development of an ADF, it is strongly recommended that the reason for this decision be documented. This will help lead the CoP-AD to a more comprehensive view of the development of automated driving.

There is no clear recommendation from L3Pilot on how the CoP shall later be used within companies developing ADFs. One option would be to address questions directly in a dedicated process. Another option would be to include the questions in already existing development processes. Thus each company must individually decide which approach will be taken.

This document – the draft CoP-AD – is mainly intended to foster discussions and to prompt feedback for the final CoP-AD (deliverable D2.3 due at the end of February 2021). It is thus possible that the contents, formulations and structure of the CoP-AD may change over the course of the work. Furthermore, the topics and questions of the draft CoP-AD will be elaborated upon in more detail if they are considered relevant. These updates might also include hands-on checklists for certain topics. This aspect has not been covered by the draft CoP-AD.

## 3 Development Process of the Code of Practice for Automated Driving

This chapter describes the development process of the CoP-AD, beginning with a recap on the CoP-AD framework as described in the L3Pilot deliverable D2.1 (Wolter et al., 2018). Over the course of the project, certain updates related to the development phase and categories have been necessary. These updates of the framework are described and combined with an overview about the categories and topics of the CoP-AD.

### 3.1 Description of the Development Process of the CoP for Automated Driving

The development of the CoP-AD was started by defining the CoP-AD framework (Wolter et al., 2018). A survey was initially distributed among the L3Pilot partners to collect the relevant topics and processes for the CoP-AD. Criteria were defined in order to evaluate whether a certain topic was relevant for the CoP-AD. These criteria are as follows:

- The topic/process poses a common challenge in the development process that requires cooperation.
- A wrongly applied approach for the topic/process would lead to serious consequences (e.g. malfunctions in certain traffic situations leading to non-release of the function).
- A frequent misapplication of an approach for a topic/process is highly likely.
- The topic/process has already been identified as relevant by others, for instance the German Ethics commission on AV (Fabio et al., 2017), Whitepaper “Safety first for automated driving” (Wood et al., 2019), the CoP for testing in the UK (DOT 2015), or the AV Guidelines in the US (NHTSA 2017) or in Japan (MILT 2018).
- The topic/process can be described in a general way that does not lead to unreasonable limitations in the development process (company independent).
- And the optional criteria: the topic/process is of relevance for L3Pilot prototype vehicles and can be evaluated in this project.

The identified topics within this CoP-AD deliverable have been clustered into different categories (see chapter 3.3). In addition, the topics have been classified according to the addressed development stages (see chapter 3.2).

With the framework set, the actual work on the CoP-AD was started. The first step was to collect and analyse relevant literature. Based on the literature research, a set of relevant questions for the CoP-AD was defined and then improved and consolidated using an iterative process. The outcome is the draft version of the CoP-AD that is presented in this deliverable.

A major objective of this draft CoP-AD is to initiate the discussion with further stakeholders inside and outside the project. The stakeholders’ feedback is required in order to ensure

broad acceptance of the CoP-AD. The collected feedback will be used to prepare the final version of the CoP-AD that will be published in the L3Pilot deliverable D2.3.

Feedback to the L3Pilot project has also been collected in parallel to all of this. Thus the leaders of the other subprojects of L3Pilot have been asked which topics of the CoP-AD were dealt with in their subproject. Relevant topics were discussed in more detail. An example is the findings of the “Methodology (SP3)” subproject, which prepared an internal report summarising important aspects for evaluation tools related to automated driving (see Annex 1). However, it must be taken into account that the L3Pilot project only focuses on some issues of the testing of automated driving on public roads. For this reason, not all topics outlined in the CoP-AD are covered by L3Pilot. The feedback of the subproject leaders on the different topics has been analysed and reported in chapter 5.

### 3.2 Development Phases in the CoP-AD

When a technology is being developed, different aspects become relevant at different stages of the development. In order to consider this aspect, the CoP-AD is split into different phases along the development process. This decision was made in the CoP-AD framework (Wolter et al., 2018), see Figure 3.1. For the definition of the development phase, the Response 3 CoP for ADAS (Knapp et al., 2009) serves as a baseline. The phases cover the concept (light blue) as well as development phase (dark blue). For the CoP-AD, an additional phase has been added that also considers the time after start of production phase. Although this phase is traditionally not part of the development, this phase has become more relevant in recent times, since it covers topics such as in-market updates and the importance of monitoring the product in field as requested by the ISO 26262 part 2-7 (ISO 26262 -2 2018) and 7-6 (ISO 26262 -7 2018).



Figure 3.1: Development phases that have been proposed in deliverable D3.1 (Wolter et al., 2018).

A consensus was reached over the course of the work that merging two pairs of phases to two single phases would improve the structure and comprehensibility of the CoP document without leading to a loss of content (see Figure 3.2). The main changes are:

- “Concept Selection Phase” and “Proof of Concept Phase” are merged to one phase “Concept Selection”, since the covered time frame of the “proof of concept” is rather short and it can be seen as the final step of the concept selection;
- “Verification” and “Validation & Sign off” are merged to one phase “Validation & Verification”, which still includes the sign-off process; the reason is to avoid confusion between the two phases.



The new phase structure is presented in Figure 3.2.

After the development phases, the CoP-AD categories and related topics are presented. Each question is assigned to a certain topic and development phase. It has been decided that one CoP question can be assigned to multiple development phases.



Figure 3.2: Development phase applied in the draft CoP-AD.

### 3.3 Categories and Topics in the CoP-AD

The categories were derived from the survey amongst L3Pilot partners. Next to the development phases, they represent the second dimension of the CoP-AD. Different topics are grouped within a category. Five different categories were described in the framework (Wolter et al., 2018). These five categories are:

1. Operational Design Domain (ODD) – Vehicle Level: description of the function and scenarios at vehicle level.
2. Operational Design Domain (ODD) – Traffic System Level: description of the function at the level of the overall environment.
3. Safeguarding Automation: how to ensure a safe operation of the function.
4. Human-Machine Interaction: interaction between the driver<sup>1</sup> and the vehicle's displays and control elements.
5. Behavioural Design: how to take into account the behaviour of other road users.

During the work it became clear that Categories 2 and 5 have much overlap, so the two categories were merged into one. Furthermore, certain topics were identified as relevant to more than one category and have therefore been moved to an overall category. The updated structure of the categories is provided in in Figure 3.3.

---

<sup>1</sup> Please note that in this deliverable the term “driver” also covers users outside the vehicle that are operating the vehicle.





Overall Guidelines and Recommendations Minimum Risk Manoeuvre, Documentation, Existing Standards			
<b>ODD Vehicle Level</b>    Function Description, System Limits, Scenarios, Testing etc.	<b>ODD Traffic System &amp; Behavioural Design</b>    Automated Driving Risks, Mixed Traffic Simulation Approach, Ethics, etc.	<b>Safeguarding Automation</b>    Functional Safety, Cybersecurity, SOTIF, Updates etc.	<b>Human-Vehicle Integration</b>    Provide Guidelines for HMI, Mode Awareness/ Confusion, Controllability etc.

Figure 3.3: Categories used for the draft CoP-AD.

The CoP-AD covers 22 different topics overall. The following table provides an overview of the different topics and the related categories.

Table 3.1: Overview of topics of the CoP-AD categories and the corresponding chapters

Category	Topics
Overall Guidelines and Recommendations	<ul style="list-style-type: none"> <li>Minimal Risk Manoeuvre (4.1.1)</li> <li>Documentation (4.1.2)</li> <li>Existing Standards (4.1.3)</li> </ul>
ODD Vehicle Level	<ul style="list-style-type: none"> <li>Requirements (4.2.1)</li> <li>Scenarios and Limitations (4.2.2)</li> <li>Performance Criteria and Customer Expectations (4.2.3)</li> <li>Architecture (4.2.4)</li> <li>Testing (including Simulation) (4.2.5)</li> </ul>
ODD Traffic System & Behavioural Design	<ul style="list-style-type: none"> <li>Automated Driving Risks and Coverage of Interaction with Mixed Traffic (4.3.1)</li> <li>V2X Interaction (4.3.2)</li> <li>Traffic Simulation (4.3.3)</li> <li>Ethics &amp; Other Traffic-Related Aspects (4.3.4)</li> </ul>
Safeguarding Automation	<ul style="list-style-type: none"> <li>Functional Safety (4.4.1)</li> <li>Cybersecurity (4.4.2)</li> <li>Implementation of Updates (4.4.3)</li> <li>Safety of the Intended Functionality (SOTIF) (4.4.4)</li> </ul>

Category	Topics
	<ul style="list-style-type: none"><li>• Data Recording, Privacy and Protection (4.4.5)</li></ul>
Human-Vehicle Integration	<ul style="list-style-type: none"><li>• Guidelines for HVI (4.5.1)</li><li>• Mode Awareness, Trust &amp; Misuse (4.5.2)</li><li>• Driver Monitoring (4.5.3)</li><li>• Controllability &amp; Customer Clinics (4.5.4)</li><li>• Driver Training &amp; Variability of Users (4.5.5)</li></ul>

## 4 Draft Code of Practice for Automated Driving

This chapter presents each question of the draft CoP-AD in the design of a card. The sub-chapters are structured by the CoP-AD categories and topics. All cards follow a template presenting the main question, possible sub-questions and the relevant development phases. Each card is followed by a short explanation of the questions, which can also include hints regarding relevant literature.

The cards with the CoP-AD questions are presented according to this template:

Question X-Y-Z	Relevant Phase(s)	DF	CO	DS	VV	PS
Main question ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Sub-Question 1</li> <li>• Sub-Question 2</li> <li>• Sub-Question 3</li> </ul>				

In the upper left corner question is identified by a three-part ID X-Y-Z. The first “X” denotes the category (0 - 4). The second, “Y” denotes the topic of the category. With the third, “Z”, the number of the questions in the topic is identified. The cells on the upper right hand side are intended to mark the development phase, for which the question is relevant. The colours correspond with the previously defined development phases (see Figure 4.1). An abbreviated title for each development phase has been used for improved readability of the template, e.g. the Definition Phase is abbreviated to DF.



Figure 4.1: Development phase applied in the draft CoP-AD.

The cell on the left side includes the main question, which should be answered by indicating yes or no. In addition to the yes/no answer, there is room to elaborate more on the answers, e.g. to describe why the question has not been considered in the ADF development process. On the right side the cell can include (several) sub-questions that are related to the main question. These sub-questions have two purposes: 1) they should indicate relevant sub topics of the main question 2) they should support you in answering the main questions.

Following each main question you can find – depending on the question – additional explanations on the question and relevant literature references.

### 4.1 Overall Guideline and Recommendations

Before the questions of the dedicated categories are presented, the topics that are relevant to more than one category are discussed. These topics are the minimal risk manoeuvre, the documentation and the compliance with existing standards.

#### 4.1.1 Minimal Risk Manoeuvre

The minimal risk manoeuvre (MRM) is the manoeuvre which is applied in case an ADF can no longer perform the driving task or the driver does not respond to take over requests. The general objective of the vehicle's manoeuvre is to reach the safest possible state in the given situation.

Question 0-1-1	Relevant Phase(s)	DF				
Is there an appropriate mechanism for a fall back solution of the ADF available? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>If there is no appropriate reaction from the driver to take over request, is there an MRM strategy (i.e. process to automatically and safely stop a vehicle)?</li> </ul>				

Different characteristics for initiation and not-initiation of a MRM depending on the TOR status (not issued, issued and noted, issued and not noted), automation level (level 3 or 4) and the driver reaction (no reaction, reaction) are possible. In the following it is focused on characteristics in which a TOR is issued and driver does not react. There could be two different sequences for initiation of a MRM. In the first the ADF initiates a take-over request (TOR) and at the same time MRM. In the second the MRM starts just after TOR fails and the ADF does not detect any driver response. The TOR is a key consideration for a level 3 or level 4 ADF. Information about the design of HMI can be found in chapter 4.5. The take-over request must be carefully considered and designed, thus reducing the likelihood that the MRM will need to be activated. This aspect is also of relevance, when considering SOTIF (see chapter 4.4.4).

For more information please check:

- “Safety first for automated driving” (Wood et al., 2019).

Question 0-1-2	Relevant Phase(s)	DF	CO			
Is an adequate and validated concept for MRM available? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Is a concept for the MRM in the ADF foreseen? (e.g. degradation, take over)</li> <li>Is the concept defined for the different driving situations and conditions?</li> <li>Is the targeted / final minimal risk condition defined?</li> <li>Is the condition(s) clearly defined under which the MRM shall / must be activated?</li> <li>Is a concept for a safe operation during MRM available?</li> <li>Has the concept (e.g. timing, handling) of the MRM been validated in terms of effectiveness and safety?</li> </ul>				

An adequate MRM concept shall be defined in conjunction with the ADF. The concept should consider the option to implement different reactions depending on the given driving situation and condition. The concept should define under which condition the MRM shall be activated and when it should be not. Furthermore, it must be ensured in the concept that the MRM can be operated safely (functional safety, Safety of the intended functionality). The analysis should not only be limited to the ego vehicle but also consider the surrounding traffic.

Question 0-1-3	Relevant Phase(s)	DF	CO	DS		
Are the sensor(s) and the function setup appropriate to perform the MRM in different conditions? ( ) Yes / ( ) No						
						<ul style="list-style-type: none"> <li>Is the ADF capable of performing a MRM in all the various conditions that the vehicle encounters in its ODD - including fault conditions?</li> <li>Is the ADF able to decide for appropriate characteristics of MRM (e.g. stop in lane)?</li> <li>If applicable, has a function redundancy been taken into account for the chosen architecture to support the MRM?</li> </ul>

The MRM only becomes relevant when the ADF reaches its limits. Therefore, it is likely that not all information that the ADF would provide in normal conditions will be available for the MRM to use. It is important to compare exactly what information is available from the sensors at this moment in time and what information is required in order to execute the MRM. If significant gap is detected between available and required information, measures need to be taken to ensure it is minimised.

For more information please check:

- NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2018);
- “Safety first for automated driving” (Wood et al., 2019).

Question 0-1-4	Relevant Phase(s)			DS	VV	
Have appropriate MRM been implemented to cover all the various scenarios and conditions required? ( ) Yes / ( ) No						
						<ul style="list-style-type: none"> <li>Have different characteristics of MRM been considered for different driving scenarios?</li> <li>Has an adequate and appropriate interaction with the driver (and with other road users; e.g. direction indicator) been ensured by the MRM (relevant criteria: safety, driving experience, trust, situation awareness)?</li> <li>Has the MRM been implemented according to the concept and its specification?</li> </ul>

	<ul style="list-style-type: none"> <li>• Has the MRM implementation been tested sufficiently in different conditions (criteria: safety, performance, reliability / robustness)?</li> <li>• Do the MRM test scenarios consider possible reactions of the surrounding road users?</li> </ul>
--	--

Once a concept has been decided on, it must be ensured that the MRM is correctly implemented. For this purpose, different verification steps are required in order to prove completeness and correctness.

For more information please check:

- Thatcham Research Report (Thatcham 2018);
- “Safety first for automated driving” (Wood et al., 2019).

Question 0-1-5	Relevant Phase(s)				VV	PS
Have the test cases considered all the different MRM activation conditions? ( ) Yes / ( ) No		•	Has the ADF reached the safe state after MRM? (also during post start of production)			

In order to perform these verification tests, the test cases for the MRM need to be defined beforehand. When defining the test cases, it must be ensured that they cover the entire operation of the MRM including different traffic and environmental conditions. Furthermore, it must be defined, which test methods (test track, simulation etc.) shall be applied for testing the MRM.

#### 4.1.2 Documentation

This sub-chapter deals with the documentation of results. The main purpose of the documentation is to enable a later comprehension of the ADF’s capabilities, performance as well as decisions made during the development.

Documentation is not only relevant for internal purposes, but can also be relevant for external stakeholders, i.e. for homologation and certification of the ADF and liability issues.

Documentation does not mean explicitly that any kind of information is stored, it means that information that is relevant today or might become relevant at a later stage shall be stored.

The following questions focus on the documentation in the context of test activities. This does not mean that other development related information does not need to be documented. This information is not covered by this document, since it is expected that this is defined by company internal rules, which follow for instance the ISO 9001 (ISO 9001 2015), or external

guidelines. If uncertain whether information for another purpose needs to be documented or not, please consult the responsible individuals in your company.

Question 0-2-1	Relevant Phase(s)				VV	
<p>Is there a documentation and reporting process applied for assessing, testing and validating the ADF capabilities and design decisions? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Has an operating procedure been established to document the performed tests and compliance (fail/pass)?</li> <li>• Has an operating procedure been established to document updates of the test plan?</li> <li>• Does the documentation format comply with requirements of external stakeholders?</li> </ul>				

The first question focuses on whether all test related aspects (test plan, test execution and test result) have been documented properly. The term “test” covers the test and evaluation of the ADF capabilities as well as the general validation & verification of the ADF including the validation of design decisions. In addition to the test activities, the documentation shall cover updates of the test plan, and for comprehensibility, it is also recommended to document the reasons for these changes.

In case documentation of test activities needs to be shared with external stakeholders, i.e. for homologation or certification purposes, it shall be checked, whether the documentation format complies with their requirements.

Question 0-2-2	Relevant Phase(s)	CO	DS	VV	PS
<p>Has a reporting system / procedure been created in which to record the knowledge / lessons learnt during testing and development? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Has a reporting procedure been created in which faulty behaviour can be recorded during testing?</li> <li>• Has a reporting procedure been established to review the results obtained and to address reporting of identified deficiency?</li> <li>• Does the reporting system cover the required steps to handle the identified deficiency?</li> <li>• Has a reporting procedure been established to update test cases based on the experiences of past projects?</li> <li>• Does the reporting system consider data from all test methods (test track, simulation and test on public roads etc.)?</li> <li>• Has a test report been prepared for all detected failures?</li> </ul>			



These questions address how lessons learnt can be collected during testing and development of future ADF(s). Of particular importance is the correct handling of deficiencies that are detected during testing. For each deficiency an adequate reporting procedure needs to be applied that not only covers the reporting of the deficiency, but also how the deficiencies have been handled. The reporting procedure shall cover all test methods.

The knowledge of the test activities cannot only be used for the ADF itself, but also for updates of the tests. These updates can include a change of the tested parameters, the number of tests as well as the methodology.

#### 4.1.3 Existing Standards

A general requirement of technology development is that state-of-the-art is followed. This applies in particular for safety related aspects in order to ensure the safety of users as well as of others, who might be affected by the technology. Therefore, existing standards and best practices must be adhered to in the development.

Question 0-3-1	Relevant Phase(s)	DF	CO	DS	VV	PS
Are (industry) standards and best practices according to their current availability been followed?  ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Have / Are relevant standards and best practices (according to their current availability) been identified and evaluated?</li> </ul>				

A non-complete list of example safety standards that are relevant in the context of ADF development based on (Wood et al., 2019) is given below:

- Endangerment caused by the intended function (e.g. due to sensor performance boundaries), ISO PAS 21448 “SOTIF”(ISO 21448 2019)
- Foreseeable misuse, ISO PAS 21448 “SOTIF”(ISO 21448 2019); ISO 26262 “Functional Safety“ (ISO 26262 2018)
- Malfunctions due to e/e defects and systematic programming- and design errors, ISO 26262 “Functional Safety“(ISO 26262 2018)
- Deliberate manipulation of the system from security point of view, ISO/SAE 21434 „Road Vehicles – Cybersecurity Engineering“ (ISO 21434 20XX)
- Influences from the (traffic) environment, ISO PAS 21448 “SOTIF“(ISO 21448 2019)
- Influences from the humans behaviour, ISO PAS 21448 “SOTIF“ (ISO 21448 2019)

The state of the art is changing over time. Therefore, the compliance with this question requires a constant review and update process.

There are other related topics that are not covered in detail by the CoP-AD. For those topics please have a look at previous CoP deliverables, Response 3 (Knapp et al., 2009) and

AdaptiVe (Bienzeisler et al., 2017). One example are questions related to liability, here the AdaptiVe deliverable D2.3 (Bienzeisler et al., 2017) provides further insights.

## 4.2 Category “ODD Vehicle Level”

The Operational Design Domain describes the specific scenarios and conditions in which the Automated Vehicles (AVs) are designed to function. The scope of the ODD is dependent on the feature of the ADF embedded in the AVs. This chapter focuses on ODD at vehicle level, that is, all the functional aspects of a vehicle are taken into consideration. In particular, the following topics are illustrated:

- Requirements
- Scenarios and Limits
- Performance Criteria and Customer Expectations
- Architecture
- Testing

The first topic is about “*Requirements*”, which can be split into functional and non-functional requirements. The requirements are considered related to the high-level function, to the refinement of the ODD and to its final release of the ADF.

The second topic “*Scenarios and Limits*” depends on the automation level, since each ADF will have certain restrictions as part of the specification. As described below, most of them will be known and defined by intention, but others can occur during the development process.

The third topic is about “*Performance Criteria and Customer Expectations*”, which covers both the performance criteria for the ADF developed and the customer expectations of the ADF. End-users need a correct understanding (and expectations) of the functions behaviour. This topic is strongly related to Category 4 “Human Vehicle Integration”.

The fourth topic deals with “*Architecture*”, which is fundamental since the complexity of the software and hardware integrated in vehicles is continuously growing. Therefore, the function architecture needs to be planned and verified from the early development stages, in order to reduce development risks and costs.

The last topic is about “*Testing*”, which includes the assessment of the ADF at different stages of the development process. The ADF will be verified and validated against the functional and non-functional requirements to ensure it meets the design intent.

All the questions, to be included in the CoP-AD and related to these topics, are considered and presented in the following paragraphs, including possible sub-questions (to specify the main questions further) and indicating the most important stage of development related to each question.

### 4.2.1 Requirements

Right from the definition phase, it is imperative that the requirements are defined clearly. This is essential in order to provide the basis for good testing. The requirements for automated systems describe the system’s desired behaviour under a dynamic environment based on available information. To limit the operational needs of the ADF, it is referred to the ODD which is defined by numerous conditions that may vary within a short period of time. Considering that these conditions need to be fulfilled in order to operate the ADF, the following section discusses the ODD in order to scope the requirements for the ADF. Here, the ADF shall be able to fulfil the requirements of particular driving modes. Therefore, the following chapters focus on the high-level function requirements during the definition, concept, design and validation phases.

The CoP questions described below provide a starting point for specifying the minimum level of ADF requirements needed to define and verify that certain ODD conditions have been met.

Question 1-1-1	Relevant Phase(s)	DF				
<p>Are the different attributes of the requirements considered? (Specific, measurable, relevant, attainable, testable etc.) ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Are target-values defined for all the requirements across the whole project?</li> <li>• Has the controllability been considered?</li> <li>• Have the feasibility and the usage condition of the requirements been considered (i.e. when and in which cases can the requirement be realised)?</li> <li>• Are the expected completion times for these requirements been defined?</li> <li>• Are appropriate metrics and thresholds available?</li> </ul>				

As a starting point for discussing requirements it is useful to have a common understanding between all stakeholders of the rules and terms which are used for these requirements. A requirement needs to meet several criteria to be considered attainable. Therefore, clear technical requirements are required instead of abstract goals in order to be able to properly trace component functionality. The following characteristics are generally accepted as those defining a complete requirement:

- Specific – The requirement is simple and precise. It should not be open to various interpretations.
- Measurable – The requirement should be measured against results. In other words it vague statement like ‘acceptable’ should be avoided, but instead measurement units shall be used.

- Relevant – The requirements meets the actual ODD need.
- Attainable – The requirement can be implemented within the ODD constraints and the resulting deployment of the release.
- Testable – It can be shown that the requirement has been met by the ADF and can be inspected and verified.

Question 1-1-2	Relevant Phase(s)	DF				
Are the requirements classified as functional and non-functional? ( ) Yes / ( ) No						

Functional requirements identify what the ADF should do. These can be conceptualised with use cases or other specific functionalities that define what an ADF is supposed to accomplish.

Functional requirements include descriptions of the ADF and detail the data to be held in the ADF. Features needed to achieve the required functionality should be as specific as possible including any limitations specific to the ODD.

Non-functional requirements specify how the ADF should work. These can be conceptualized mainly with performance requirements, design constraints and quality attributes.

Non-functional requirements usually detail constraints, targets or control mechanisms related with the qualities of the ADF and its success. They describe how well or to what standard an ADF should be provided. In principle those requirements are difficult to measure and test. Therefore, experience in the look and feel of the ADF as well as safety, security and privacy requirements play an important role.

Question 1-1-3	Relevant Phase(s)	DF				
Does the ADF comply with the key requirements (such as functional stability, performance, reliability)? ( ) Yes / ( ) No						

The core technical requirements for ADF must be addressed. Those requirements should be the basis of operational approval. Meeting the key requirements and achieving operational approval will determine whether the ADF is complying with the specifications and rules. For example in addition to yes/no questions, it is helpful to explain how the requirements are met. This can be done by describing the ADF by design and by providing a brief overview of the system architecture focusing on items maximizing performance, reliability and overall system stability.

Question 1-1-4	Relevant Phase(s)	DF				
Is a means (e.g. graphical representations and state diagrams) provided for comprehensive analysis of the requirements? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Are the requirements been defined using graphical representations and state diagrams?</li> <li>Is there a requirements specification available?</li> </ul>				

The main purpose of the question is to formulate a runtime representation of the operational domain in which the requirements are linked with the ODD elements and the system functionality. To ensure that the complete system is built according to the laid out requirements a design methodology is required. Model Based Systems Engineering (MBSE) is one such engineering technique that exploits the use of models to define and analyse a system. The MBSE approach is highly recommended by ISO 26262.

Modelling is a way to deal with the limitations of document-based approaches while being capable of identifying problems and reducing the risk of having ambiguous requirements. MBSE is utilising a System Modelling Language (SysML) which can use requirements diagrams to efficiently capture functional, performance and interface requirements.

Question 1-1-5	Relevant Phase(s)	DF				
Are the ADF states defined? ( ) Yes / ( ) No		Examples: Not operational, Operational without notifications, Operational with some notifications, Operational with all notifications available.				

Fundamental to AD is the need to be safe even as real-life driving context changes. At the same time operation under certain conditions and states should also be considered. Here, it is assumed that there is redundancy in the system so that the ADF can always perform a fallback. Therefore, any additional information relevant to the safe operation of the vehicle must be effectively communicated to the driver. A simulation-based testing methodology provides a structured approach to evaluate the operation state of the system in a wide variety of operating conditions. Generally accepted operational scenarios may be considered the following:

- Not operational – ADF not available
- Operational without notifications – ADF available but unobservable state
- Operational with some notifications – ADF available with limitations on the state
- Operational with all notifications available – ADF available

Question 1-1-6	Relevant Phase(s)	DF				
Do the function limitations cover the identified / considered risks? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Have the risks been analysed to understand which are acceptable and which unacceptable?</li> <li>Has it been ensured that the ADF can achieve a minimal risk condition?</li> </ul>				

ADFs are limited in the way their algorithms react on sensor and other hardware malfunction. Measures must be provided that ensure that risks are minimised when systems fail to work as intended. The ADF must be robust to uncertainties e.g. when system encounters an exception or other situation for which it was not designed for. Please consider in this context also the Safety of the Intended Functionality (SOTIF) (see chapter 4.4.4).

Question 1-1-7	Relevant Phase(s)	DF				
Is the intended level(s) of driving automation defined? ( ) Yes / ( ) No						

Each level has a specific set of safety requirements that an ADF must meet before it can be considered to operate at that level. The safe state of an ADF heavily relies on the situation in which the state has to be maintained or reached. Low levels of automation rely on the human driver in order to maintain a safe state. Higher levels of automation do not rely on the human driver as fall back solution but they are also limited by ODD. Higher levels of automation need more intelligence in processing, sensing and monitoring requirements. This results to higher computing requirements to execute more complex software. From fully manual to fully automated capabilities, the SAE's approach to automated driving remains the industry's most widely accepted classification system. Please consider in this context also the Safety of the Intended Functionality (SOTIF) (see chapter 4.4.4).

Question 1-1-8	Relevant Phase(s)	DF				
Is a checklist considering ODD requirements for the ADF defined? (Like appendix A of Thorn et al., 2018) ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Is the ODD taxonomy of the ADF been derived from the concept of the AD feature?</li> </ul>				

Such a list is unlikely to be complete, but an attempt to compile a list can be a starting point for listing all possible considerations and help to ensure that ODD requirements do not contain crucial gaps due to missing information. This list can be enhanced based on significant experience and can prove essential for ensuring safe real-world operation.

Question 1-1-9	Relevant Phase(s)	DF				
Is a general verification strategy for the chosen ODD defined? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Has / is the right interaction between the vehicle and its environment been ensured?</li> <li>• Has / is the coverage of the requirements by your V&amp;V tools (e.g. MiL, SiL, HiL, proving ground and real-world driving) been checked?</li> </ul>				

While any such question is unlikely to be answered completely, the question can serve as a starting point to ensure that ODD verification efforts for the ADF do not contain crucial process gaps. A conventional strategy on vehicle level should include:

- Requirements-based verification of function, sub-functions and components.
- Validation of a typical fail-operation function with all redundant components capable of performing safe state transitions.

Whatever verification targets are set, the complexity of vehicles and their environment will make testing challenging at a fundamental level. An essential next step will be finding ways to manage the complexity of verification without missing critical effects that may cause unexpected results. It is important to understand that the automated driving domain is changing rapidly and all actors need to track emerging technology trends. Therefore, by using a verification strategy, we maintain a consistent approach of identifying risks, implementing solutions and verifying their effectiveness.

Question 1-1-10	Relevant Phase(s)	DF				
Have / are safety assurance targets been set? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is there any assurance of the ODD used by other regulated industries</li> <li>• Has / is any evidence been gathered from a wide range of assurance methods?</li> <li>• Has / is safety assurance been complete beyond individual components?</li> </ul>				

An important goal for automated vehicle systems is to reduce the potential of risks occurring during operation. Especially for safety assurance at all levels from individual components and subsystems to the vehicle as a whole, a safety assurance methodology must be introduced. Such methodology could include pre-market testing, design and manufacturing processes, performance criteria and standards conforming to national guidance before system deployment.

Question 1-1-11	Relevant Phase(s)				VV	
Has / is the actual technical performance been verified that it is in line with the defined ODD? ( ) Yes / ( ) No						<ul style="list-style-type: none"> <li>Is the actual performance rated against the ODD requirements? (e.g. not-compliant vs. compliant)</li> </ul>

A typical ODD approach defines a limited number of performance expectation criteria which allow the system designers to assess in terms of the ability to achieve the overall desired operational capability within the ODD. The minimum performance criteria define how the ADS is expected to perform and that all aspects of the ODD have been addressed either by ensuring safe system operation or by ensuring that the system can control and mitigate any exemptions beyond the defined ODD.

Question 1-1-12	Relevant Phase(s)				VV	
Is a general strategy available to monitor released vehicles in the field? ( ) Yes / ( ) No						

Perhaps the most logical way to assess an automated vehicle is to drive it in real traffic and observe its performance. If an ADF system is expected to detect whether it has left the ODD, then it must be able to monitor the ODD at runtime. Even after a vehicle is released a mechanism to monitor performance results or safety trends by collecting the vehicle’s safety data should be included as a next step. Developers of automated vehicles rely upon this approach to evaluate and improve their systems

Question 1-1-13	Relevant Phase(s)				VV	
Is a strategy available to feedback learnings into the development cycle and to release updates for already delivered vehicles? ( ) Yes / ( ) No						

An automated system is not enabled by one single technology or component, but rather by a combination of technologies. Numerous lessons could be learned during the development and deployment of AD systems. A strategy must exist to explore and highlight challenges associated with the deployment of the system in real-world.

#### 4.2.2 Scenarios and Limits

Depending on the automation level (SAE 2018), each ADF will face certain restrictions as part of its specification. These restrictions define the ODD of the ADF. Most of the restrictions will be defined intentionally and are known, but it can be expected that there will be cases where the intended ODD is either “smaller” or “larger” than the implemented ODD. Potential causes for such inconsistencies could be for instance technical limitations of ADF (sensors, logic, and actuators) or unexpected driving scenarios, which have not been considered



during the development. The following questions aim to support in dealing with the scenarios and limits of the ADF.

Question 1-2-1	Relevant Phase(s)	CO	DS		
Are the function limitations known? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No					
					<ul style="list-style-type: none"> <li>• Are function limitations reproducible (e.g. in the same situations/ under the same conditions)?</li> <li>• Have the ADF tasks (dynamic driving task) that the function must cope with been analysed?</li> <li>• Have limitations been considered in the selection of the perception platform?</li> <li>• Are function limitations measurable?</li> </ul>

The ODD summarises operating conditions under which the ADF is specifically designed to function. The ODD is comprised of elements that can be allocated to different categories including, but not limited to, environmental, geographical, time-of-day restrictions, and/or the required presence or absence of certain traffic or roadway characteristics (SAE 2018). In addition, all objects classes which the driving automation function shall respond to must be defined in the ODD.

Defining a consistent ODD is one of the key success factors for an ADF. For every element in the ODD, the possible values or parameter ranges must be defined, e.g. the illumination can be limited to values greater than 500 lx, to ensure that the driving automation function (or feature) only operates during day time. The ODD might however change during the development due to newly discovered limitations or changes in the development. In this case, it is not feasible to cover the originally defined ODD any longer. Therefore a constant review of the function limits in relation to the ODD is necessary. One indicator is an inconsistent behaviour of the vehicle function while driving with an activated ADF.

Question 1-2-2	Relevant Phase(s)	DF	CO		
Is the function operating under the ODD limit? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No					
					<ul style="list-style-type: none"> <li>• Can each inherent ODD limitation be detected by the function once it is reached</li> </ul>

An ADF that operates outside of the ODD can instil false customer trust and overconfidence.

The function shall be able to identify whether it is operating within or outside the ODD, which implies:

- recognising all defined ODD elements and their parameter ranges;
- recognising the ODD boundaries before leaving them, with enough time to warn the driver and/or to take necessary actions (depending on the feature itself, e.g. a safe stop on the hard shoulder).

To secure that the function operates only inside the ODD limits, scenarios must be defined to verify and validate the ADF at its ODD borders (see also next two questions and question 1-5-7).

Question 1-2-3	Relevant Phase(s)	CO			
Has / is a structured-approach based on test tools (e.g. simulation, X-in-the-Loop) been used to identify critical scenarios? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is a test catalogue utilised in order to guide the verification and validation activities?</li> <li>• Are functional, logical and concrete test scenarios been considered for verification?</li> </ul>			

In order to identify limits and update the specification accordingly the identification of relevant driving scenarios is required. Apart from “black box testing” of an integrated function, which involves real world testing to try to find potential issues based on real world traffic in a representative environment, there are several other approaches that can be applied to test for such limitations at an early stage of development. One approach is to identify corner and edge cases combined with robustness tests (e.g. by introducing noise). The underlying assumption is that if the ADF can deal with these, it will also be capable of dealing with less critical scenarios. Thus, it is necessary to expose the ADF to a repeatable set of driving scenarios, an activity for which a simulation environment is most suitable.

In addition to the approach in 1-2-6 the application of a test catalogue supports reuse of past experiences and company / vehicle specific test sets. A test catalogue will also be needed for regression testing to re-run past tests for a system after a modification has been introduced during development.

The tests should be defined in a way that they address all definition layers of test – ranging from functional via logical up to concrete test scenarios. Additional information regarding this topic is provided by the PEGASUS project (PEGASUS 2019).

#### 4.2.3 Performance Criteria and Customer Expectations

This topic covers the performance criteria for the ADF developed as well as the customer expectations of the ADF. The link between both aspects is required since the customer will need to be supported in order to have an understanding about the ADF’s performance and his or her role and responsibilities during automated driving (ITF 2018).

Question 1-3-1	Relevant Phase(s)	DF				
Has a concept been defined to identify customer requirements? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Have / are customer abilities and limitations been considered?</li> <li>• Have / are customer preferences and expectations of the ADF that is being designed been considered?</li> <li>• Has / is customer feedback in previous projects been considered?</li> </ul>				

This question addresses the importance of considering customer expectations, which can be translated to requirements when setting performance criteria for the ADF to be developed. Customer expectations may cover a wide spectrum, not considering only comfort but also safety, usability, controllability, acceptance etc. Additionally, customer’s abilities and limitations shall be identified, considering different learning curves. In order to identify these aspects, it may be relevant to segment the customers / users groups identified. Finally, reflecting customer feedback refers to the information which can be obtained after deployment and which can be fed into the next development or ADF update. These factors shall be addressed at the definition phase.

Additional information regarding this topic is provided by:

- International Transport Forum “Safer Roads with Automated Vehicles” (ITF 2018).

Question 1-3-2	Relevant Phase(s)	DF				
Has a concept been defined to set realistic and objective performance criteria? ( ) Yes / ( ) No						

On top of customer expectations, it is important to consider which other performance criteria the ADF should meet. This shall be addressed based on objective and realistic data and shall address aspects such as safety, comfort, and drivability. This is something which is particularly complex due to the lack of historic data and the wide diversity of technologies, therefore appropriate testing activities including customer clinics shall be performed during development. Additional information regarding this topic is provided by:

- International Transport Forum “Safer Roads with Automated Vehicles” (ITF 2018).

Question 1-3-3	Relevant Phase(s)		DS			
Have / are forms of cooperative control between the ADF and the driver been defined? (the driver may be inside or outside the vehicle) ( ) Yes / ( ) No			<ul style="list-style-type: none"> <li>• Is the specific performance of the ADF (including performance boundaries) been clearly defined for the user?</li> </ul>			

	<ul style="list-style-type: none"> <li>• Has / is a concept been developed to validate each of the performance criteria which has been set?</li> <li>• Is a concept been developed for identifying variable user requirements while driving and adapting ADF driving characteristics accordingly?"</li> </ul>
--	---

Transport systems can be improved in terms of efficiency and safety of systems by cooperative behaviour among different traffic participants (Bartels et al., 2015). The CoP-AD focuses on ADFs in which the driver needs to be ready to take control of the vehicle and so it is essential that it is defined how the cooperation between the user and the ADF is established. This should be defined in the design phase of the development process. This cooperation can happen at either strategical level (e.g. navigation), tactical level (e.g. guidance) and / or operational level (e.g. control) (Flemisch et al., 2016).

Additionally, it is necessary to identify the performance boundaries between the ADF and the user. Shared control should communicate the proximity to task boundaries, environmental constraints, or function limits to facilitate a need for adaptation in control strategy or adaptation in the cooperation balance (Abbink et al., 2018).

Since this question shall be addressed at the design phase, it is also relevant to define a concept to validate the defined performance criteria, although the validation concept will be implemented in a later phase.

Additional information regarding this topic is provided by:

- A Topology of Shared Control Systems – Finding Common Ground in Diversity (Abbink et al., 2018);
- Shared control is the sharp end of cooperation: Towards a common framework of joint action, shared control and human machine cooperation (Flemisch et al., 2016);
- System Classification and Glossary, AdaptIVe Deliverable D2.1, 2015 (Bartels et al., 2015).

Question 1-3-4	Relevant Phase(s)			VV	
Has / is a method been implemented to validate the target performance and the customer requirements? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Have / are performance boundaries been validated?</li> </ul>			

A validation and verification concept is required to ensure that the targets that were defined in the design phase can be met. Therefore, the validation and verification concept must be implemented. This validation and verification shall include not only the performance criteria

and customer requirements but also the identified boundaries which affect the cooperative control. The applied method shall include different test tools depending on criteria or customer requirements that are being tested (see chapter 4.2.5).

Additional information regarding this topic is provided by:

- Recent release of NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2018)

Question 1-3-5	Relevant Phase(s)				VV	
Has / is a process been established to understand how customer expectations can be satisfied? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Does the process consider how customer expectations evolve based on their driving experience in automated driving mode?</li> <li>• Does the process consider how customer expectations evolve based on their driving experience in manual driving?</li> </ul>				

As part of the validation phase, it is necessary to review whether the customer requirements are in line with their expectations. Those expectations can evolve over time alongside with the user’s driving experience. A higher level of driving experience might lead to evolving capabilities of the user based on different learning curves (Abbink et al., 2018).

Additional information regarding this topic is provided by:

- A Topology of Shared Control Systems – Finding Common Ground in Diversity (Abbink et al., 2018).

#### 4.2.4 Architecture

An architecture framework for an ADF is made by several standardised viewpoints, among which typically a functional, a logical and physical architecture. As the complexity of software and hardware integrated in vehicles grows, there is an increasing need to plan and verify the architecture starting from the early development stages, to ensure safety and to reduced development risks and costs. The questions in this section aim at highlighting fundamental steps in the development and validation of the architecture at vehicle level, with a focus on assuring safety when the ADF finds itself outside its ODD a detailed example of a testing architecture and a scenario-based test framework for ADF features can be found in Thorn et al., 2018.

However, the process of choosing an architecture includes going through different views, and finally identifying the physical function elements capable of performing the desired AD functions and identifying the physical interfaces capable of carrying the required data flows. One of the critical aspects of developing an ADF is the interaction with its user, as the function must be developed to be easily and safely operated by the user, and therefore one of its critical elements is the HVI. Because of its relevance, a section of this CoP is devoted to display and control concepts, i.e. the human-vehicle-integration (HVI – Section 4.5). In

particular, the first subsection covers the general guidelines on how to design the HVI, and we refer the reader there for more information.

Question 1-4-1	Relevant Phase(s)	DF	CO			
Has / is a rationale for the chosen physical architecture been put in place? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Has / is a rationale for the chosen sensor set been put in place?</li> <li>Has / is a rationale for the chosen actuator(s) been put in place?</li> <li>Has / is a rationale for the chosen ECU been put in place?</li> </ul>				

According to ISO 15288:2015 (ISO15288 2015), ‘the purpose of the Architecture Definition process is to generate function architecture alternatives, to select one or more alternative(s) that frame stakeholder concerns and meet function requirements, and to express this in a set of consistent views’. At the end of the process, the optimal physical architecture should be selected that implements all the stakeholder and function requirements. To select the final architecture, criteria to compare the produced candidates should be defined and the selection criteria should also be documented. A more detailed elaboration on architecture selection activities can be found in (INCOSE 2015), where possible criteria for selection are listed, together with additional activities like assessments, risks analysis, prototypes, etc. which are generally performed in parallel to obtain “proven” requirements.

Purpose of this question is to ensure that the rationale for the final architecture, i.e. not only requirements but also decision activities and steps, is recorded for later steps and to ensure traceability. This allows design validation of the architecture against its specification. In later iterations architectural decisions can still be understood and can be maintained or changed based on the defined target.

Question 1-4-2	Relevant Phase(s)	DF	CO			
Has / is a verification/analysis been undertaken to ensure that the selected architecture can detect, recognise and classify any object within the ODD? ( ) Yes / ( ) No						

Once the ODD is defined, the Object and Event Detection Response (OEDR) capabilities must be specified. OEDR refers to ‘the subtasks of the DDT that include monitoring the driving environment (detecting, recognizing, and classifying objects and events and preparing to respond as needed) and executing an appropriate response to such objects and events (i.e., as needed to complete the DDT and/or DDT fallback’ (SAE 2018)).

The OEDR capabilities are derived from two inputs. First the objects defined in the ODD must be analyzed regarding possible events that can be triggered by them, e.g. a pedestrian (object) crossing the road (event). Second the tactical manoeuvres that the driving automation function can implement must be analyzed, as they indicate which capabilities the driving automation function has, to respond to the event, triggered by the object. Examples for tactical manoeuvres are changing lanes, driving at constant speed, braking, etc. In case of the example stated above (pedestrian crossing the road), a possible response is braking.

As one object can trigger multiple events that can lead to multiple possible responses by the driving automation function, the task of defining the OEDR capabilities can become very complex. A possible tool to handle the complexity is to define logical rules for the combination of object-event-response, e.g. Object A cannot trigger Event B, etc. Thus, the theoretical number of combinations ( $\#O \times \#E \times \#R$ ) is reduced to the number of feasible combinations.

Question 1-4-3	Relevant Phase(s)	DF	CO			
Has / is a verification/analysis been completed to ensure that the selected architecture responds to any (relevant) object when the ADF is operating under the ODD limit <sup>2</sup> ? ( ) Yes / ( ) No						

ODD and OEDR allow the derivation of logical scenarios. Logical scenarios, in combination with requirements, form the input for testing the architecture response. Thorn et al., (Thorn 2018) suggests three testing techniques, i.e. modelling and simulation, closed-track testing and open-road testing, which constitute a three-pillar approach becoming a standard in validating complex ADF features. Test procedures can vary depending also on the selected tools, but should always aim at “achieving repeatability, reliability, and practicality” (Thorn 2018).

Question 1-4-4	Relevant Phase(s)		CO			
Does the chosen function architecture satisfy the defined SAE level and requirements? ( ) Yes / ( ) No						

The SAE J3016 standard (see end of the Section) describes the classification for road-bound vehicles with autonomous driving functions. Each of the six defined levels is classified by the (minimum) requirements on how much the driver has to be involved in the Dynamic Driving

<sup>2</sup> ODD limit includes here also the continued operation during a take-over request until the driver has taken over the control or a minimum risk manoeuvres start. Operation during the minimum risk manoeuvre shall be also be covered in an appropriated way.

Task (DDT), i.e. how alert they need to be while in the vehicle and how much they are supposed to remain in the loop.

The purpose of this question is therefore to ensure that the designed function has not only a defined SAE level, but also that it will behave as expected within its ODD. Moreover, it is fundamental to ensure that specific measurements are taken in case the ODD is exceeded. For level 3, the DDT fall back strategy relies either upon the attentive driver to respond by resuming manual driving or by achieving a minimal risk condition. For a level 4 or 5 ADF, the function shall perform the fall back by automatically achieving a minimal risk condition (for more information see chapter 4.1.1).

Question 1-4-5	Relevant Phase(s)	CO			
Are the architectural aspects between function and other elements outside vehicles (V2X, Backend etc.) been considered? <input type="checkbox"/> Yes / <input type="checkbox"/> No					

Ensure that the required interfaces of the function(s) to backend solutions are considered. By doing this, the function(s) integrity is ensured for a specific context. An interface Control Document should be available. Additionally, relevant documentation for functional safety and cybersecurity (item definition, safety case, safety manuals, cybersecurity case, ...) can support safety and cybersecurity analyses. The functional safety concept and the cybersecurity concept of the different involved systems, if safety and/or security relevant, should be analyzed for consistency.

Question 1-4-6	Relevant Phase(s)	DF	CO			
Are requirements for safety, security and maintainability been considered for the selection of an appropriate architecture? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>Based on the ADF scope, has a high-level sensor architecture been identified, which can outline the technology to be used for the required perception and functionality?</li> <li>Does ADF's architecture fulfil standard like the SAE architecture (SAE 2012) or other state-of-the-art published architecture (e.g. Wood et al., 2019)?</li> </ul>				

The architecture and the ADF shall be designed to satisfy additional non-functional requirements from different disciplines and standards, of which most relevant are requirements regarding safety, security and maintenance. Since such aspects have a huge impact on the architecture and ADF design, the entire section 4.4 "safeguarding automation" addresses these cross-functional topics.



Some important aspects that shall not be neglected during the design phase, since they could cause drastic harm during function operation, are:

- The function is safe with respect to state-of-the-art safety methods and standard (e.g. ISO 26262);
- The function is secure with respect to state-of-the-art security methods and standards;
- The function achieves maintainability requirements.

Good practice is therefore to check if current architecture standards are available to provide guidelines on designing the ADF architecture. We refer for example to the ISO/IEC/IEEE 42010:2011 standard (and reference inside) which specifies architecture viewpoints, architecture frameworks and architecture description languages for use in architecture descriptions.

Question 1-4-7	Relevant Phase(s)		CO			
Are sensing, perception, world modelling and navigation and planning supported by your software and hardware components? ( ) Yes / ( ) No						

The purpose of this question is to investigate whether the mapping and allocation of the desired functions or sub-functions to physical components is done properly. In addition it checks if the selected ADF elements are reviewed to be capable to satisfy the defined functions.

Question 1-4-8	Relevant Phase(s)				VV	
Do the selected tools satisfy quality and safety standards and requirements? ( ) Yes / ( ) No						

In the case a tool is used in the development of ADF, confidence in the use of the selected tool is required. For software, confidence is achieved if the tool effectively minimises the risk of systematic faults in the developed product, and the development process and the tool complies with the processes of ISO 26262 (ISO 26262 2018). To evaluate the confidence of a software tool in the development, following criteria shall be considered:

- the possibility that a malfunctioning software tool could produce erroneous outputs, which could in turn:
  - introduce errors in the function being developed;
  - prevent errors in the function being developed to be detected; and
- the confidence in preventing or detecting such errors in the output.

The evaluation contemplates two main aspects: the tool usage and the tool qualification. The first one is based on the tool's required functions and properties, considering the appropriate usage in the user environment. The second one is carried out based on given or assumed information regarding the tool usage (e.g. use cases, user requirements, ASIL). Based on these aspects a Tool Confidence Level (TCL) can be determined. Finally, if a certification is required, qualification methods are applied as per ISO 26262 (ISO 26262 2018).

Next to ensuring the quality of the tool, it is necessary to investigate and validate the selected tools for development purpose, e.g. checking, whether the applied model deliver the required level of realism of real world (see question 1-5-5 and 1-5-6).

Unfortunately the ISO 26262 standard does not address evaluation of HW tools, like measurement equipment, reference systems for data collection. Nevertheless, the verification strategy and the test equipment should be checked through a Functional Safety analysis.

#### 4.2.5 Testing

At different stages of the development process the ADF needs to be assessed regarding the technical capabilities, verified with respect to the compliance with the function requirements and to be validated regarding their design. All these steps require testing by means of one or more test tools (field test, test in controlled environments like test tracks, driving simulators, computer simulation etc.).

The following question shall support a safe testing of ADF and cover the entire range from the development of the test concept up to the execution of the tests with the ADF.

Furthermore, they are defined independently of the used test tool. However, not all sub-questions are equally relevant for each test tool.

Question 1-5-1	Relevant Phase(s)	DF				
<p>Is a test concept for the development, certification / homologation, validation and verification of the ADF and its subcomponents available? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Has / is a test concept been defined which verifies / validates the technical maturity of the ADF?</li> <li>• Has / is a test concept been defined that verifies that the requirements for the ADF are met?</li> <li>• Has / is a test concept been defined which proves that the ADF fulfils its intended purpose?</li> <li>• Has / is a test concept been defined which investigates the safe operation of the ADF in the corresponding ODD in conjunction with the driver?</li> </ul>				

	<ul style="list-style-type: none"> <li>• Has / is a test concept been defined that is capable of proofing a positive balance of risks?</li> <li>• Has / is a test concept been defined which investigates additional risks associated with ADF in conjunction with the driver compared to manual driving?</li> <li>• Has / is any (specific) security testing been planned covering not only the function and architecture but also the AD scope (e.g. operation as fleet vehicles)?</li> <li>• Is testing with different penetration rates been considered at every traffic layer (from vehicle infrastructure up to network components)?</li> <li>• Does the concept define appropriate test tools / environments for the tests?</li> <li>• Considering the purpose of test (e.g. homologation /certification of the ADF), has / is the required data be identified?</li> <li>• Does the test concept include an execution plan / time plan for the tests?</li> <li>• Have / are all requested tests been included in the concept?</li> </ul>
--	---

Before the actual tests are performed, a test concept shall be defined which states the respective purpose for the different tests and the various aspects that need to be tested.

First, the technical maturity of the ADF shall be tested at different stages of the development and before the market introduction in order to ensure a safe enough operation of the ADF in its ODD. Depending on the stage (e.g. first test in a closed environment, start of on-road testing, market introduction), different safety thresholds might apply while testing.

Nevertheless, at any time all feasible measures must be taken in order to reduce the potential risk for all involved persons to the technical minimum. The test concept needs to include and detail the safety measures which must be taken while carrying out the test.

The test concept shall define the tests, which are required in order to verify that the function meets its requirements. The requirements can be internal ones as well as external requirements that are relevant for the homologation or certification of the ADF in a market. The homologation / certification of an ADF might require specific tests in certain markets. It must be ensured that these tests are covered by the test concept.

The tests of the test concept shall not only focus on the pure technical aspects of the function, but also the interaction with the user(s) in different driving scenarios.

In the validation phase, it must be assessed, whether the ADF fulfils its purpose and meets the external expectations. The external expectations cover the customer’s expectation as well as societal expectation. One famous example for societal expectation is to reduce the number of accidents compared to human driving. The German ethic commission on automated driving refers here to a positive balance of risks (Fabio et al., 2017). The risk balance implies that not only the situation, for which a positive effect of the ADF is expected, shall be assessed, but also challenging situations, in which the ADF might have negative consequences. The assessment of positive risk balance as part of the validation must therefore also be covered by the test concept. Regarding simulation in the traffic context please see also chapter 4.3.3)

Finally, the test concept can include tests that target specific operation purposes of the ADF (e.g. fleets operating in specific environments) or the effects that might occur at higher penetration rates of the ADF.

The test concept shall define which test tools or test environments should be used in order to assess the ADF in order to get a reasonable level of validation. In addition, the test concept can also include a time plan for the testing.

For more information please check:

- “Safety first for automated driving” (Wood et al., 2019).

Question 1-5-2	Relevant Phase(s)	CO			
<p>Is each single test of the (test) concept been specified properly? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Have / are the test parameters (including among others length, number of tests) been defined for each test (e.g. the number of test repetitions, test duration, test subjects)?</li> <li>• Are the test parameters in line with the situations that the ADF will encounter in its ODD?</li> <li>• Is defined, how many test repetitions / test persons / driven mileage / driving time are required?</li> <li>• Are guidelines for the conduction of tests available?</li> <li>• Have / are success criteria for each test been defined and is this is not met, has it been defined when the test needs to be re-run?</li> </ul>			

	<ul style="list-style-type: none"> <li>• Has / is it been defined which information from the tests needs to be documented?</li> <li>• Has / is it been defined, how the information from the tests should be stored?</li> <li>• Has / is the reference data (ground truth data) for the test been defined?</li> <li>• Are data privacy aspects been considered?</li> <li>• Have / are safety measures for the participants been considered?</li> <li>• Has / is the approach for the training of safety drivers or remote operators been defined / implemented?</li> </ul>
--	--

When the tests are due to be carried out, it becomes necessary to specify the tests in more detail. This automatically leads to the question, whether a certain test has been specified in a proper manner. For this purpose, the specification shall include information about the following items:

- The parameters to be tested must be specified. It is important that the parameters are in line with the scenarios the ADF will encounter in its ODD. Therefore, it must be analysed before the test, which situations and parameters occur in the ADF's ODD.
- Depending on the test, the test amount (e.g. number of repetitions, number of test persons, driven mileage, driven time) needs to be defined. It is important that the amount of testing is chosen in a way that it ensures sufficient data to run a solid analysis. The test amount covers also the duration of each test.
- The success criteria for a test must be defined. This could be a single criterion or multiple criteria. It shall be also defined under which conditions a test needs to be repeated or re-run.
- Guidelines on the test execution shall be defined in order to minimise the risk of false test execution, which typically leads to useless data.
- It shall be defined, which data and information of the test must be documented and how the data are stored (see also chapter 4.1.2).
- If reference data are required for or measured in the test, these reference data shall be clearly defined. This includes information, which data should be used as a reference and how they are collected respectively by which tool they are measured.
- It shall be checked for the different tests, whether privacy aspects are relevant and how these can be ensured during testing.
- In case certain interactions (e.g. interaction with other users, V2X interactions) are simulated in test, since the test environment does not provide the real interaction, the

modelled interactions shall be described (what is used? Is the required model available? etc.).

- Develop training protocols that are used for the training of safety drivers. With no standardised industry requirements, automated driving companies have taken a variety of approaches to training safety drivers. Robust procedures to ensure the competency of safety drivers and operators must be developed.

Question 1-5-3	Relevant Phase(s)	CO			
Has the test space been defined according to the function design and the intended ODD? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are the relevant driving scenarios been defined covering the entire ODD?</li> <li>• Are rare driving scenarios been taken into account?</li> <li>• Have scenarios been taken into account that cover the entire operation of the ADF (not available, ready, activation, active and operating, deactivation)?</li> </ul>			

The tests have to be in line with the driving scenarios that the ADF will encounter while operating in real traffic. Therefore, it is necessary to investigate the driving scenarios as well as their parameters before defining the test parameters. A general concept for determining relevant test cases has been developed for instance by the German research project PEGASUS (PEGASUS 2019).

Since the scenarios to be tested depend strongly on the ODD of the ADF as well as the technical capabilities of the ADF, first a description of the intended ODD and the function are required. In the second step the test space and test cases can be defined.

The selected test cases should not only cover scenarios that occur frequently, it is also necessary to test the ADF in rare scenarios – in particular if these rare scenarios could lead to serious consequences. The test scenarios shall cover all operation conditions of the ADF. These include scenarios, in which the function is not operating (ADF not available, ADF ready to be activated, activation) as well as those in which the function is operating (ADF is operating, ADF is deactivated). Within these conditions different modes or sub-conditions could exist (e.g. deactivation by the user, deactivation by the function). If this is the case, the sub-condition must also be covered by the tests.

Question 1-5-4	Relevant Phase(s)				VV	
Has the test plan been implemented and followed correctly? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Have any deviations from the test concept / plan been documented?</li> <li>• Have / are any reasons for the deviation from test concept / plan been documented?</li> </ul>				

	<ul style="list-style-type: none"> <li>• Are all required data for the sign-off, homologation or certification process available?</li> </ul>
--	--

Once the tests have been executed, the question, whether the test plan is correctly implemented and followed, becomes relevant. While testing, different limitations or constraints can occur that lead to intended or unintended deviations from the test plan. Intended deviation might be necessary to overcome detected issues. In contrast the unintended deviations might not be noticed. Therefore, it is strongly recommended to check during the test execution as well as afterwards, whether the tests have been carried out according to plan. This includes checking whether all relevant information has been documented and stored correctly. If a deviation from the test plan has occurred, it should be documented. The documentation should also cover the reasons for this deviation from the test plan.

In the end it must be ensured that the required data for the sign-off, homologation or certification process are available at required quality. If this is not the case, the tests need to be repeated.

Question 1-5-5	Relevant Phase(s)	DF	CO	DS	VV	PS
Are the tests realistically possible? <input type="checkbox"/> Yes / <input type="checkbox"/> No						<ul style="list-style-type: none"> <li>• Is the ADF mature enough to conduct the planned test?</li> <li>• Have safety and security aspects been investigated before test?</li> <li>• Are the required test tools available?</li> <li>• Have / are the applied test tools been verified and validated before they were used?</li> <li>• Are the required input data available?</li> <li>• Are the interfaces for the test tools been properly defined and implemented?</li> <li>• Are all required licenses (incl. testing and driving licenses) for the test available?</li> </ul>

A test concept and test case description are the basis for the test. In order to prevent that the concept and description do not stay abstract, testability of each test need to be checked and ensured. In case the testability is not fulfilled, the test plan or description needs to be updated or the test needs to be postponed in case of time limitations. It is recommended to check the testability from the beginning in order to address issues as early as possible.

For the testability four primary aspects need to be assessed: test tool status, technical testing requirements, status of ADF and the safety & security aspects.

Regarding the test tool it must be ensured that it is available as well as capable of providing the required quality. It is important that the test tool that the test tool has been validated and verified before the test. A test tool which has not been validated could lead to false results. This aspect needs careful attention in case complete virtual test tools (e.g. computer simulation) or partly virtual test tools (e.g. driving simulator) are applied, since the output of these tools is not necessarily a physical result.

Using test tooling often comes along with additional requirements which need to be considered; certain additional equipment may be required, certain inputs (e.g. data) may be required, the interfaces to other test tools or participants have need to be defined or that certain licenses (incl. testing and driving licenses) for the testing may be required. It shall be checked before the execution of the test, whether these requirements are fulfilled.

It must be assessed whether the function is mature enough to be tested in the target environment. Depending on the test environment this could have different meanings. For tests in a real environment this means the function must be capable of operating at a technical maturity level, which allows safe testing of the function. For tests in a virtual environment this means that an adequate model of the ADF must be available.

Safety and security have to be ensured while performing the tests. In the past the security concerns mainly arose from keeping development information confidential. This does not change with ADFs. Security aspects need to be thought through in a wider sense since new cyber security risks have arisen, especially now communications such as V2X and remote vehicle control are being developed. Examples of the cyber security threats which must be avoided at all costs include signal jamming and hacking. These risks should be taken into account for testing. The next questions investigate the safety aspect in more detail.

For more information please check:

- “Safety first for automated driving” (Wood et al., 2019).

Question 1-5-6	Relevant Phase(s)	DF	CO	DS	VV	PS
<p>Is the testing activity safe?  <input type="checkbox"/> Yes / <input type="checkbox"/> No</p>		<ul style="list-style-type: none"> <li>• Is a risk assessment conducted before the test?</li> <li>• Does the risk assessment consider individuals who are not directly involved (e.g. surrounding traffic)?</li> <li>• If verification and validation is carried out on public roads, are potential effects to other traffic participants considered and safety measures defined?</li> <li>• Have / are safety measures for the testing process been taken?</li> </ul>				



	<ul style="list-style-type: none"> <li>• Has / is it been defined how test engineers should respond in the case of a failure during the testing process?</li> <li>• Has and is the staff (e.g. test and safety driver, V2X-operator) involved in the test been properly trained?</li> <li>• Has / is it been ensured that vehicle operators are allowed to operate a vehicle (following company internal and legal requirements) and have received appropriate training?</li> </ul>
--	---

A key aspect for the testing of ADF is to try to prevent any risk of material damage or personal harm. It is also clear that there is no absolute guarantee that material damages or personal harm can be prevented at all times. However, in the testing individuals involved should take all necessary precautions to ensure the testing process is completed as safely as possible.

These precautions which need to be taken are identified early on in the test planning activities by conducting a risk assessment for the test. This risk assessment must also include individuals that are not directly involved in the testing (e.g. other users of the test track). This becomes even more relevant if tests are conducted on public roads, where other road users (motorised as well as non-motorised road users) might not even be aware of the ongoing tests. Before the testing it must be ensured that the planned safety measures are available and operating successfully.

Furthermore, plans should be established that define how the individuals involved in the test should react in case of a failure or malfunction. The test engineers should receive the necessary training which informs them of the appropriate action to take in the case of an issue during testing. In addition to training, it must also be ensured that the driver(s) have the permission to operate the vehicle with the ADF at all times. Here, company internal rules as well as governmental rules need to be followed.

Question 1-5-7	Relevant Phase(s)	CO	DS	VV	PS
Are the national testing guidelines / regulations being followed? <input type="checkbox"/> Yes / <input type="checkbox"/> No					

During the testing national testing guidelines and regulations must be followed. Ideally, the testing regulations have already been considered in the test concept and the test specification. However, it is also important to double check them once the actual testing is / has been planned, since they can change over time. Example testing guidelines are:

- UK: The pathway to driverless cars: a code of practice for testing (DOT 2015)
- USA-CA: Testing of Autonomous Vehicles with a Driver (DCM 2019)
- AUS: Guidelines for trials of automated vehicles in Australia (NTC 2017)

Due to the high intensity of testing required for automated driving, regardless of whether it is testing during the development or for the final sign-off process, it is expected that the traditional approach will not be sufficient (Winner et al., 2013). It is highly likely that the approach to testing will have to change; different tools may need to be used for certain tests or the application and distribution of tools to individual tests may change. A concrete assumption is that more testing needs to be conducted in a virtual environment, and it is to this topic which the last few questions relate.

Question 1-5-8	Relevant Phase(s)	DF	CO	DS	VV	PS
Are simulations part of the test concept and testing? ( ) Yes / ( ) No						

The application of simulation tools comes with some associated challenges. The challenge of validation and verification is already addressed by the questions 1-5-5. However, there are further aspects that need to be considered for the virtual testing:

- It must be decided in which way the ADF is represented in the simulation tool. The three basis options are software-in-the-loop (SIL), model-in-the-loop (MIL) or hardware-in-the-loop (HIL). For each options it must be ensured that the simulation tool provides the right interface to connect the function to the simulation tool. It must be ensured that the function makes use of the information provided by the simulation tool correctly.
- In addition to the type of simulation, it must be decided whether a test can be performed in an open-loop manner (no feedback loop is required) or whether the test requires close-loop testing. Close-loop testing requires a feedback loop from the environment and vehicle back to the ADF. In simulation where the function is not in control of the lateral and longitudinal movement of the vehicle, this feedback loop is typically the driver behaviour model.
- The final aspect which needs to be considered is the testing and the primary objective of the tests. For example, if learning algorithms are applied for the ADF, it must be clearly distinguished between training data (information used to find the requested parameters), validation data (information to evaluate the model fit) and test data (information used for the evaluation). These data sets must be independent.

For more information please check:

- “Safety first for automated driving” (Wood et al., 2019).

Question 1-5-9	Relevant Phase(s)		DS		
<p>Does the simulation take into account development and testing of AI within the ADF? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No</p>			<ul style="list-style-type: none"> <li>• Has the simulation objective been clearly defined as testing the ADF or developing an ADF using AI?</li> <li>• Is there an end-to-end AI function development in your virtual environment?</li> <li>• Is the quality of the applied simulation models sufficient for the intended use case (development / testing of ADF based on AI methods?)</li> <li>• Is the applied dataset up to date?</li> <li>• Is the applied dataset unbiased?</li> <li>• Does the applied dataset comply with ethical aspects?</li> </ul>		

A challenge with simulation is how to deal with an ADF which has been developed using an AI method. The primary sub-question related to the application of simulations in the context of an AI based ADF is, to make sure the purpose or objective of the simulation has been clearly defined; is the focus on testing or development? Depending on the answer different measures can be taken. If the focus is on the testing activity, the major challenge is to ensure a high coverage of the situation space that the ADF or the component being tested will encounter while driving in its ODD. But if the focus is on the development, it must be further distinguished between the development of the entire system or of single components. The latter case requires modelling of the related components and inclusion of all models which interact with this component. For the entire system this task becomes even more demanding, not only do all components require modelling but also the environment and other traffic participants need to be modelled in a correct and sufficient manner. Following on from this, it must also be noted that the interaction between the ADF and other traffic participants needs to be modelled. Regardless of the simulation objective (development / testing) the integrity of the input data needs to be ensured in all cases.

### 4.3 Category “ODD Traffic System Level & Behavioural Design”

Aspects of the operational design domain (ODD) with the focus on the AV have been described in the previous category (chapter 4.2). Nevertheless, the operation of the AV depend also in its surrounding. Therefore, this chapter deals with the ODD aspects related to traffic system level and behavioural design. This chapter incorporates several key issues, which mainly concern topics such as:

- Safety impacts in the context of mixed traffic system
- Interaction between automated driving cars and environment (V2X)
- Traffic simulations
- Ethical/other traffic related aspects

These topics will be covered in a similar way to the previous category, ODD Vehicle Level, with a main question supported by sub questions and a brief explanation of why the question is important to consider during the development of the ADF.

#### 4.3.1 Automated Driving Risks and Coverage Interaction with Mixed Traffic

For an ADF there are several risks that need to be addressed, most notably, the interaction with mixed traffic. Only if the risks are well understood, can mitigation strategies be developed in order to solve or at least mitigate them. This topic has five questions which focus on ensuring that the risks are understood and that mitigation strategies have been considered.

Question 2-1-1	Relevant Phase(s)	DF	CO	DS	VV	
Have / are the risks of the ADF within its ODD been considered? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are the risks at entry to and exit from the ODD considered?</li> <li>• Are the risks from infrastructure or other road users considered?</li> <li>• Are unspecified or unexpected events identified from studies in real traffic?</li> <li>• Are unspecified or unexpected events considered in the hazard analysis and risk assessment (HARA)?</li> <li>• Are the function limitations within the ODD considered?</li> <li>• Is a recording of ADF accident data or disengagements considered to help identify risks?</li> </ul>				

This question addresses directly, whether all ADF related risks have been considered and identified within the ODD. The sub-questions should assist the analysis of this main question. They target specific risk types, which could occur within the ODD and prompt further thoughts whether the risks have been fully understood. Additional information regarding this topic is provided by:

- Safer Roads for Automated Driving (ITF 2019).

Question 2-1-2	Relevant Phase(s)	DF	CO	DS	VV
<p>Are the ADF capabilities identified and verified in terms of OEDR?</p> <p>( ) Yes / ( ) No</p>					
					<ul style="list-style-type: none"> <li>• Has / is the response of the ADF been considered for road obstructions, lane allocation &amp; re-routing, road etiquette for emergency vehicles and interpreting gestures of other road users?</li> <li>• Does the process consider detection and response to other vehicles (in and out of its travel path), pedestrians, bicyclists, animals, and objects that could affect safe operation of the vehicle?</li> <li>• Has / is it been considered how to negotiate aggressive drivers, jaywalkers, bicyclists, delivery trucks, construction, unprotected left turns, 4-way stop signs and other factors that arise when driving in the city?</li> </ul>

Focusing on the object detection and response capability of the ADF, this question verifies whether the associated risks have been considered. The number of different types of objects which need to be detected in mixed traffic is significant. The sub-questions refer to many different object types that the ADF might encounter. Once an object is detected, it needs to be classified. This step includes further risks. An incorrect classification may lead to an incorrect response by the ADF. Additional information regarding this topic is provided by:

- Recent release of NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2019).

Question 2-1-3	Relevant Phase(s)	DF			VV
<p>Is the interaction of the ADF with surrounding traffic identified, verified and validated?</p> <p>( ) Yes / ( ) No</p>					
					<ul style="list-style-type: none"> <li>• Does the ADF operate with human-like behaviour which is predictable and comfortable?</li> <li>• Have / are the active safety capabilities of the vehicle been validated in normal driving scenarios as well as in corner cases<sup>3</sup>?</li> </ul>

<sup>3</sup> Corner cases are very important to consider when defining and validating an ADF. These are scenarios which are of very rare occurrence within the ODD of the ADF, but the ADF still needs to be able to respond appropriately. Often validation efforts will have a high amount of focus on these corner cases so that the failure modes of the ADF can be assessed. If the ADF performs well in the corner cases, it is also highly likely that it will perform well in the nominal or high occurrence scenarios. It can be very difficult to determine the corner cases for the ADF as they can be very rare scenarios which one may never have experienced. During the validation of the ADF, real world testing is a very good way of validating how the ADF performs in a wide range of these corner scenarios.

The interaction with mixed traffic can be extremely complex as the responses of different road users vary significantly in different scenarios. Dangerous situation can occur if the ADF is unable to interact with surrounding traffic in a human-like way. If the response to certain scenarios is unexpected by other road users, there is the risk that misunderstandings occur or other road users might take advantage of the ADF's behaviour. For example if the ADF has not been designed to be as assertive in junction scenarios as a human driver would be, it may be possible that other road users take advantage of this and the ego vehicle will simply fail to progress at the desired rate.

Active safety functionalities are another key aspect. If these features are too sensitive, false positives might occur, which poses the risk of rear end collisions with the following traffic. If the active safety is not sensitive enough, accidents might not be prevented. The active safety of the ADF must be finely balanced in order to reduce the risks in mixed traffic.

Additional information regarding this topic is provided by:

- Recent release of NHTSA's "Framework for Automated Driving System Testable Cases and Scenarios Final Report" (Thorn et al., 2019).

Question 2-1-4	Relevant Phase(s)	CO	DS	
Have / are risks to the surrounding traffic during transition of control been identified and assessed? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Can the ADF recognise function or driver limits that do not allow a safe driver take-over, and react to minimise the risk?</li> <li>• Has it been considered how to initiate take-over to the driver in a robust, safe and intuitive manner?</li> <li>• Does the overall safety of the ADF consider the effect on the driver even once the automated drive ended?</li> </ul>		

The transfer of control is likely to be associated with risks for the ego vehicle as well as for the surrounding traffic. There will be some scenarios in which a transfer of control is inappropriate and / or a driver take-over should not be allowed until the ADF is well within its limits. The transfer itself must be designed in a robust and intuitive way in order to ensure that the driver has regained situational awareness. The HVI is a key component to communicate, whether the driver is responsible for controlling the vehicle or the ADF. Even if the driver is fully in control of the vehicle, there is still a significant risk that the driver has not completely regained situational awareness and will not respond appropriately to all scenarios. It is important that these risks are considered over the entire for all scenarios. Additional information regarding this topic is provided by:

- Safety first for automated driving (Wood et al., 2019).

Question 2-1-5	Relevant Phase(s)		DS		
<p>Have / Are the potential ADF failure modes been identified within the ODD and have relevant failure mitigation strategies been implemented?</p> <p>( ) Yes / ( ) No</p>					
					<ul style="list-style-type: none"> <li>• Are potential failure mitigation strategies considered including both fail-operational and fail-safe techniques?</li> <li>• Has / is the limited capability of the ADF been considered, based on the mitigation strategies selected?</li> <li>• Has / is setting a hierarchy of mitigation strategies been considered depending on its impact and effectiveness?</li> </ul>

In order to minimise risks it is vital that the failure modes of the ADF are identified and mitigation strategies are put in place. Whenever possible, fail operational strategies should be implemented in a way that the ADF can remain in control of the driving task for at least a certain time without initiating an emergency handover. Significant risks are introduced as soon as such emergency handover manoeuvres are required, since this limits the time period for the driver to regain the necessary situational awareness. There may be several mitigation strategies to handle individual failure modes. These should be considered and prioritised depending on their effectiveness. Additional information regarding this topic is provided by:

- Recent release of NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2019).

#### 4.3.2 V2X interaction

Communication with other vehicles and / or the surrounding environment is an important and complementary technology that is expected to enhance the benefits of automation at all levels (USDOT 2018). V2X or Vehicle-to-X-communications refers to the technology that allows vehicles to communicate with other objects around them; V2X encompasses vehicle to vehicle and vehicle to infrastructure (CATAPULT 2017).

This topic is addressing the V2X interactions that an AD vehicle may have to deal with. It is not in the scope of this section to provide the details of which method may be used to deal with them, such as WiFi-DSRC based systems or cellular network-based systems.

Question 2-2-1	Relevant Phase(s)	DF	CO	DS	VV	PS
<p>Have all the V2X interactions that the AD vehicle may encounter while performing any driving task, from strategic level (e.g. route planning, interaction with infrastructure), down to operational level (e.g. longitudinal and lateral) been identified?</p> <p>( ) Yes / ( ) No</p>						
						<ul style="list-style-type: none"> <li>• Based on the identified V2X interactions, is the high-level architecture planned considering the interactions/relationship between sensors and environment?</li> <li>• Is the ODD defined considering the identified V2X interactions?</li> </ul>

	<ul style="list-style-type: none"> <li>Is the type and density of the required infrastructure defined for the specific ODD?</li> </ul>
--	--

At the concept phase and based on the scope of the ADF to be developed, it is necessary to identify all the interactions that the vehicle may have to deal with. This should be done in a holistic manner, considering any possible interaction that may happen from strategic level down to operational level, and considering any type of road user (vehicles, VRU's...) and infrastructure (buildings, traffic, overhead structure etc.).

Once the interactions have been identified, a high-level system architecture needs to be defined in order to understand how the AD Function will be able to cope with them. This process will support the understanding of the relationship with the external environment and defining the ADF's ODD (Thorn et al., 2018). In this context it is also necessary to understand whether the function is available at any time within the ODD.

Additional information regarding this topic is provided by:

- Recent release of NHTSA's "Framework for Automated Driving System Testable Cases and Scenarios Final Report" (Thorn et al., 2018).

Question 2-2-2	Relevant Phase(s)	DF	CO	DS	VV	PS
Has / is a plan been defined to integrate and validate the V2X interactions within the sensor architecture? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Does the plan include the assessment of potential cyber-security threats that could affect these interactions?</li> <li>Does the plan also consider a back-up solution when a required infrastructure is no longer available?</li> <li>Does the plan include a methodology/toolchain to single out critical V2X scenarios within the ODD of the ADF?</li> </ul>				

It is not in the scope of this question to address the requirements and details of the ADF and sensor architecture, since there are already several related standards. Instead, this question addresses how the identified interactions will be integrated into the sensor architecture. It is expected that a plan drafts how each sensor will be able to deal with the different interactions, including a validation strategy by means of appropriate testing. The plan should also include a reference on how to address potential cyber security threats and consider alternative strategies in case the required infrastructure is not available.

Some of these alternative strategies – like the back-up solutions can be considered as critical scenarios, therefore it is expected that this plan includes a methodology / toolchain to identify all of them.

Additional information regarding this topic is provided by:



- Recent release of NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2018).

Question 2-2-3	Relevant Phase(s)	CO			
Has / Is a validation strategy been defined for the safe operation of a combined V2X sensor architecture (e.g. comprising sensor and communication errors or in case of missing infrastructure)? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are potential failure modes of V2X interactions identified?</li> <li>• Are appropriate countermeasures for each potential failure drafted and planned?</li> </ul>			

After identifying the V2X interactions and developing a plan for its integration into the sensor architecture, it is necessary to have a clearly defined strategy to validate and verify the operation of the sensor architecture. This strategy should consider possible errors or failures that could happen either due to external communications (e.g. network being down, unavailable infrastructure) or internal events (e.g. sensor misdetection, sensor communication delay...). Additionally, the development of appropriate countermeasures shall be included.

At this stage it is important that the validation strategy considers appropriate testing methods to provoke every identified potential failure, including countermeasures. A clear documentation of the tests shall also be part of the validation strategy.

Additional information regarding this topic is provided by:

- Recent release of NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2018).

At the validation and verification stage, it must be ensured that the validation strategy of the concept phase is implemented and followed (see chapter 4.2.5 testing). This testing shall include proper documentation of tests and actions taken when failures happened, showing the countermeasures taken and their effect.

Question 2-2-4	Relevant Phase(s)				VV	
Is the validation strategy for V2X of concept selection phase followed and implemented according to the plan? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is a test report generated for all the V2X interactions use cases that were identified?</li> <li>• Is a test report prepared for all the potential failures identified in the concept?</li> </ul>				

At the validation and verification stage, it must be ensured that the validation strategy of the concept phase is implemented and followed. This testing shall include proper documentation of tests and actions taken when failures happened, showing the countermeasures taken and their effect.

### 4.3.3 Traffic simulation

The traffic simulation is an important method of evaluating ADF in a virtual traffic environment. It is required to ensure the viability and robustness of an ADF via different driving scenarios and traffic flow models, as well as providing an assessment of the safety implications on the traffic flow and the interaction effect between automated vehicles and traffic environment. This topic consists of nine CoP questions from definition phase to validation/verification phase regarding traffic simulation.

Question 2-3-1	Relevant Phase(s)	DF	CO			
Has the technological state-of-the-art of the simulation been addressed and researched? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are the sensor suite and vehicle architecture documented?</li> <li>• Are the appropriate toolchains or models selected for satisfying the needs of traffic simulation and ADF within the chosen ODD?</li> <li>• Does the simulation approach comply with one of the three approaches in ISO 21934-1?</li> <li>• Has a state of the art review (benchmark) been performed covering existing solutions including their strength and weaknesses?</li> <li>• Has / is the hardware and software of the simulation well defined and documented?</li> </ul>				

The technological state-of-the-art should be investigated during the definition phase. The preliminary research is deployed in a wide range, which includes:

1. Studies of present toolchains or models in both research and industry, which may provide the possibility to use exchangeable ADF, evaluation metrics and parameter spaces suitable for the intended identification process, and could be applied in the traffic flow simulation and response to the requirements of the simulation task (Hallerbach et al., 2018).
2. Studies of ISO 21934-1, which provide a prospective safety performance assessment of pre-crash technology by virtual simulation (ISO 21934 20XX).
3. Studies of benchmark activities, which is an action of gathering, analysing, and applying information, measures or practices about the latest technology of simulation in the automobile industry.

In addition to the sensor suite of the vehicle, the vehicle architecture and the potential hardware/software for the simulation process should also be considered and documented

during the early definition phase of the simulation. This will enable a full reference vehicle model to be used in the simulation of the ADF in different traffic and environment scenarios.

Question 2-3-2	Relevant Phase(s)	DF				
Does the applied ADF have an impact on traffic flow simulation? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Does the impact analysis of applied ADF consider the safety, the efficiency and the interaction with infrastructure or other road users?</li> </ul>				

This question provides a preliminary analysis and assessment of the impact of the ADF on the traffic flow simulation. The impact of the applied ADF on traffic flow simulation could be related to the safety aspect, the efficiency aspect and the interaction aspect. The traffic flow simulation can be characterised in several ways, two examples are presented below (Maurer et al., 2016):

1. The microscopic approach describes the relevant characteristics of a single vehicle, like its speed, temporal headway or spatial separation;
2. The macroscopic approach takes several vehicles into account and the relevant properties of a traffic flow, like the traffic volume, traffic density and mean speed.

The impact of the safety aspect focusses on the potential risks that may arise from the limitation of the performance of ADF or the unpredicted behaviour of other road users. The impact on the efficiency aspect is related to the density of the platoon of vehicles and the speed with which the platoon passes through the cross-section. The impact on the interaction aspect takes into account the interaction between ego vehicle and infrastructure or other road users.

Question 2-3-3	Relevant Phase(s)	DF				
Are traffic flow simulations used to evaluate ADF evolution by using different scenarios and traffic models? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Are different scenarios and traffic flows considered and implemented in the simulation?</li> <li>Are emergent, cooperative and interoperability aspects addressed in the simulation?</li> <li>Are there appropriate metrics to identify the critical scenarios in the traffic flow simulation?</li> </ul>				

Several scenarios and traffic flows could be implemented in the simulation approach in order to evaluate the ADF evolution. ADF applied in the traffic flow simulation will surely improve the safety circulation of the ego vehicle, as well as other road users. All scenarios identified as potentially critical, such as hard deceleration or an accident, will be addressed and

studied. Feedback from the simulations will allow the evolution of the ADF and could help ensure it handles real world driving safely.

Different aspects during the implementation of scenarios and traffic flows need to be addressed, such as emergent test case, cooperative behaviour between different other road users (in simulation often called traffic agents), as well as interaction between different sub-models, need to be addressed by the traffic flow simulation in order to achieve a realistic simulation.

The critical scenarios mainly arise from malfunctions of automated vehicles but also from unpredictable manoeuvres from other road-users and the traffic flow. It is clear that the identification of critical scenarios is a key factor in the validation of the ADF. A method to identify critical scenarios in the traffic flow simulation is to canvass expert opinions and use peer reviews (Hallerbach et al., 2018).

Question 2-3-4	Relevant Phase(s)	DF				
Has / is a strategy defined to validate/verify the traffic flow simulation? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are the different test scenarios defined?</li> <li>• Have the main research questions been clarified for traffic flow simulation?</li> <li>• Is there a strategy towards higher levels of realism concerning your simulation approach?</li> </ul>				

During the design phase of the simulation approach, it is recommended to consider a strategy to validate/verify the traffic flow simulation in order to facilitate execution of simulation tests. All test scenarios, especially the critical ones, should be defined, whether the scenario's requirements are functional or non-functional. The main research questions should also be clarified, in order to easily validate/verify the traffic flow simulation (Hallerbach et al., 2018).

Compared with real-world tests, one challenge of the simulation approach is to model the systems as realistically as possible, since the model quality decides how close the simulation is to the real world. Thus, a strategy towards higher levels of realism of the simulation is very important to ensure a high quality of simulation (Ragan et al., 2015).

Question 2-3-5	Relevant Phase(s)		CO	DS		
Is the concept capable of taking multiple simulations into account? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Does the simulation consider separate details of traffic simulation, vehicle dynamic simulation and cooperation simulation?</li> <li>• Can the applied simulations be synchronized?</li> <li>• Can the applied simulations exchange data between them?</li> </ul>				

A global simulation concept should take into account several parallel simulations, which may incorporate mixed elements such as traffic environment, traffic flow, vehicle architecture, sensor data, and communication aspects. It could consist of a coupled traffic simulation, a vehicle dynamics simulation, and a cooperation simulation. The traffic simulation provides the surrounding traffic environment for the automated vehicle, which incorporates different scenarios and traffic models. The vehicle dynamics simulation contains a detailed model of the vehicle and includes the ADF that has to be tested. In order to capture the cooperative aspects of these vehicles in the simulation, a cooperation simulation needs to be considered in which cooperative aspects and communication models can be included (Hallerbach et al., 2018).

In order to guarantee a high quality of the global simulation concept, parallel simulations should be synchronised within the same simulation environment. In the meantime, data generated by different simulations also needs to be shared between simulations.

Question 2-3-6	Relevant Phase(s)	CO			
Are the requirements for the level of fidelity of the Software-in-the-loop (SIL) defined? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is there a right fidelity for specific simulation components?</li> <li>• Is there more hardware-based XIL, which is beyond SIL applied?</li> </ul>			

In a virtual environment, High fidelity is not always necessary or advantageous. The relevant fidelity for specific simulation components has to be considered in order to keep the effectiveness of the simulation as well as a relative low cost of either hardware or software. The relevant fidelity will be based on the requirement and specification for the overall simulation approach and/or for a specific scenario.

Furthermore, the hardware-based XIL approaches use virtualisation of the physical components and the embedded function architectures to allow engineers to test different components in the model. Thus, by using these approaches faster development cycles could be achieved (Riedmaire et al., 2018).

Question 2-3-7	Relevant Phase(s)	CO			
Is there real driving data guiding your simulation approaches? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is the behaviour of the traffic agent in line with the real world behaviour?</li> <li>• Have variations of the parameters been applied in this context?</li> <li>• Are the applied simulations based on NDS database, accident database or records of real-world drives?</li> </ul>			

Simulation of the ADF leads to an enormous amount of simulated miles. In order to ensure these miles are worthwhile and useful having realistic virtual scenarios is extremely important. These driving scenarios can be built up from the real world traffic environment or from different driving databases (e.g. intersections, lanes, kerbs, traffic lights, pedestrians, etc.). This information shall be used to refine existing test manoeuvres or to define new test manoeuvres in a realistic way.

Simulation can explore thousands of varying scenarios, by applying parameter variations, such as speed, trajectory or position of oncoming vehicles and the timing of traffic lights. Even the more complex scenarios need to be taken into account, by adding simulated traffic agents (pedestrians, joggers, motorcycles, vehicles, animals, objects, etc.), with realistic behaviours. However, to utilise real world data, the aspect of traceability of the data source and the influence on the result of the simulation also need to be considered and studied (Waymo 2018).

Question 2-3-8	Relevant Phase(s)	CO			
Is a driver behaviour model used in the simulation? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Does the driver behaviour model appropriately cover driving tasks?</li> <li>Is the driver behaviour model in line with driver behaviour of human drivers?</li> <li>Does the driver behaviour model cover the interaction of non-automated drivers to automated vehicles?</li> </ul>			

A driver model could generate different types of control inputs to the vehicle model, such as steering angle for each time step and braking behaviour as a deceleration value. It should be in line with the real human drivers behaviours. In addition to the input on the stabilisation level, the driver behaviour model must consider decisions on the vehicle guidance level, such as lane keeping, lane change or evasive manoeuvres. At the same time, the potential reaction from non-automated drivers towards automated vehicle also needs to be covered.

A driver behaviour model is typically applied in the simulation in order to predict driver control inputs to the ADF, to decide on the right action in the situation and to accomplish the driving task in the test scenarios. Each traffic participant possesses its own adjustable driver model. Different types of driver behaviour models have been studied and designed, such as control perspective (Prokop 2001), behaviour perspective (Markkula et al., 2012) and cognitive perspective (Wann et al., 2004). Depending on the purpose of the simulation, the right driver behaviour model should be used.

Question 2-3-9	Relevant Phase(s)				VV	
Are internal and external stakeholders involved to approve your simulation approach?		<ul style="list-style-type: none"> <li>Are internal processes of the company followed / complied with and are they</li> </ul>				

<input type="checkbox"/> Yes / <input type="checkbox"/> No	compatible with a community/industry-wide approach? <ul style="list-style-type: none"> <li>• Has the public been informed about your use of the simulation in the validation of ADF, the impact of ADF, as well as the validation process?</li> </ul>
--	---

The designed vehicles need to be capable of complying with federal, state and local laws within their geographic area of operations. The validation process should follow local regulation. Besides the internal processes of the company, it is recommended to follow the framework(s) or the guideline(s) of the automobile community/industry (SAE, NHTSA, ACEA, OICA, etc.).

It is assumed that communication of the validation strategy through immersive simulation will improve the public acceptance of the AV. Therefore it is important that these communications are done carefully in order to produce a positive impression with members of the public.

#### 4.3.4 Ethical & Other Traffic Related Aspects

This topic covers the ethical and legal aspect related to the ADF and its development. Overall, this topic consists of three questions. It should be noted that these questions are quite high level. And therefore the sub questions should be addressed carefully.

Question 2-4-1	Relevant Phase(s)	DF	CO	DS	VV	
Have / are all the laws and regulations associated with the development, testing and sale of the ADF been considered? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Have / are the applicable traffic laws been considered and followed by the ADF?</li> <li>• Have / are country specific laws been considered and followed by the ADF?</li> <li>• Have / are laws &amp; regulations for testing been considered and followed?</li> <li>• Have / are data protection laws / regulations been followed through the entire process?</li> <li>• Have / are anti-trust laws been followed?</li> </ul>				

By means of this question, it should be ensured that the development as well as the function behaviour follows the laws. An important aspect is that laws can differ from country to country. Therefore, it is important to know, in which countries the function is developed, in which countries test drives are conducted and in which countries drivers can use the ADF. Regarding the national laws, it is strongly recommended to consult individuals who are familiar the national regulations and laws.

This question is not only relevant for the homologation but also for any development activity. The design of the function should take the national road traffic laws into account. During the development process it must be ensured that the legislative requirements are always considered. Before any testing activities are undertaken, it must be ensured that testing laws are followed. For the testing on public roads, different countries have established different regulations for operating an ADF on public roads.

In addition to the laws related to the ADF behaviour or testing activities, there are laws that are relevant to the development process itself. Here, for instance the national data protection and antitrust laws must be considered and followed.

Additional information regarding this topic is provided by:

- Adaptive Deliverable D2.3 “Legal aspects on automated driving” (Bienzeisler et al., 2017)
- National road laws;
- National civil liability laws;
- National testing guidelines (see chapter 4.2.5);
- National antitrust laws.

For the all aspects related to data protection please also refer to the topic “Data Recording, Privacy and Protection” (chapter 4.4.5).

Question 2-4-2	Relevant Phase(s)	DF	CO	DS	VV	PS
Have / are research and development activities planned according to the applicable (national) ethical standards? ( ) Yes / ( ) No						
						<ul style="list-style-type: none"> <li>• Have / are mechanisms been established to minimise the risk of harm to people in the development, testing and operation phases?</li> <li>• Are ethical standards been considered during the test planning process and the collection and analysis of data?</li> <li>• Does the ADF consider the protection of human lives as a paramount?</li> </ul>

In addition to the legislation, it is also essential to comply with ethical standards. The ethical standards do not need to be explicit standards but can also be implicit societal agreements. Ethical standards can change over time.

One fundamental principle is to prevent causing physical or mental harm to people. This should be ensured, within the realms of technical possibility, through the entire development process. To achieve this goal tests where human actors are involved need to be planned very carefully and risk assessments need to be completed in order to minimise any harm to the individuals both inside and outside of the vehicle. It is also important that ethical



standards are followed during the test planning process and that reviews are established in order to assess that the standards are being upheld correctly.

For the operation of the ADF the protection of human lives must be the paramount. However, it must also be considered, that according to the German ethic commission “in the event of unavoidable accident situations, any distinction based on personal features (age, gender, physical or mental constitution) is strictly prohibited” and that “it is also prohibited to offset victims against one another” (Fabio et al., 2017). The safety first white paper (Wood et al., 2019) for instance transferred these ethical standards into twelve principles for automated driving. Additional information regarding this topic is provided by:

- Report of German ethic commission (Fabio et al., 2017);
- “Safety first for automated driving” (Wood et al., 2019).

Question 2-4-3	Relevant Phase(s)	DF			VV	
<p>Does the ADF achieve a positive balance of risks compared to risk associated with human driving (e.g. reported in accident statistics)? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Has / is the positive risk balance been considered all the way through the life cycle of the ADF; from concept through to end of use?</li> <li>• Have / are the risks induced by the ADF been minimised?</li> <li>• Does the ADF reach a consistent improvement of the overall safety balance in comparison to human drivers / comparable functions while minimising new risks induced by the automated function?</li> <li>• Is a (validated) method / tool available to investigate the risk balance? (see chapter 4.2.5 and 4.3.3).</li> <li>• Is the baseline (human) and treatment (with ADF) condition correctly defined for assessment?</li> </ul>				

By means of this question it should be investigated, whether the ADF is beneficial in terms of traffic safety compared to human drivers. According to the German Ethic Commission prerequisite for the market introduction of a technology is: “The licensing of automated systems is not justifiable unless it promises to produce at least a diminution in harm compared with human driving, in other words a positive balance of risks” (Fabio et al., 2017)]. For this purpose, a baseline condition (human driving) must be compared to the treatment condition with the ADF in place.

The challenges for investigating the risk balance is that it needs to be performed prospectively, i.e. already before the market introduction of ADF. Therefore, methods that

purely rely on retrospective information (e.g. comparison of accident data for both conditions) cannot be applied at this stage. This method might be applicable at later stage, once a sufficient market penetration rate of the ADF is reached. Therefore, other methods (e.g. simulation based prospective impact assessment, ISO 21934 20XX) shall be applied instead. When applying a method, it must be ensured that it is capable of providing valid results, although it is clear that any assessment before the market introduction is a forecast with different uncertainties.

Next to the method, it is important to describe detailed and explicitly, how the conditions for the assessment are defined and which driving / accidents scenario are analysed. For the baseline, additional data sources, such as accident data or NDS / FOT, might be required. For the treatment condition, the ADF itself must be described. Furthermore, the ODD of ADF must be considered as well as the (expected) penetration rate. Regarding the driving scenarios, it is important to note that for a balance of risk all relevant driving scenarios must be considered and analysed. This means that driving scenarios with potential positive effects in terms of traffic safety as well as with potential negative consequences need to be part of the assessment.

Additional information regarding this topic is provided by:

- P.E.A.R.S. (PEARS 2019);
- PEGASUS (PEGASUS 2019);
- ISO (ISO 21934 20XX);
- Report of the German Ethic commission (Fabio et al., 2017);
- “Safety first for automated driving” (Wood et al., 2019);
- SAKURA project in Japan (SAKURA Project 2019).

#### 4.4 Category “Safeguarding Automation”

The category of “safeguarding automation” addresses cross functional topics that need to be considered to develop an ADF in a way that it behaves in a safe manner for the customer / driver and all other traffic participants who interact with an ADF vehicle. In general, the achievement of a safe product benefits from a seamless integration of safety measures in the overall development. The category covers the following topics of:

- functional safety;
- cybersecurity;
- the implementation of updates;
- safety of the intended functionality;
- data recording, privacy and protection.

Some of the principles that are essential to develop a safe product (e.g. requirements elicitation and management) are not specific to this category and can be addressed from different points of view. Therefore, there are safety related aspects also covered in the other categories (e.g. when defining ODD). In case topics are considered to be of high relevance, they will be repeated in this category to support the reader in (re-)considering a question within the given specific context.

#### 4.4.1 Functional Safety

The work in functional safety is closely linked to the ISO 26262 standard (ISO 26262 2018). ISO 26262 serves as a basis for this subchapter. This subchapter does not necessarily apply the same terms as used in the ISO standard. It rather tries to point out the sense of specific important aspects in this context in the language used throughout the document.

The first main task when starting a functional safety activity based on the function description (item definition) is to identify the hazards that may arise by the functionality to be developed. For hazards that are identified as potential sources of harm for an ADF, the possible risk that might result under specific situational circumstances shall be evaluated. This process will lead to integrity requirements for the development of the ADF.

At the definition phase of the development process, only little details about the implementation of the ADF might be known. This is not necessarily a drawback for the analysis of relevant hazards, since the analysis of the ADF is agnostic to the potential causes of a specific implementation. Causes will be identified later during the development process, if a need for hazard mitigation arises from this first step.

Question 3-1-1	Relevant Phase(s)	DF				
<p>Are possible malfunctioning behaviour and the related hazardous events analysed? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Are the relevant hazards identified for the considered function based on its description (item definition)?</li> <li>• Is inadequate control by a driver or a function identified?</li> <li>• Is a systematic approach used (e.g. HAZOP) for the analysis?</li> <li>• Is malfunctioning behaviour identified for cases where the vehicle is in manual driving mode and in automated driving mode?</li> <li>• Is the potential absence of a take-over ready driver considered that may have an impact on the controllability of the vehicle in case of malfunctioning behaviour?</li> <li>• Is the role of the infrastructure to be considered?</li> </ul>				

	<ul style="list-style-type: none"> <li>Is the vehicle reaction in case of a failure defined to avoid malfunctioning behaviour when no take over ready driver is present"?</li> </ul>
--	--

Specific consideration during this activity has to be given to the driver. The driver and other involved traffic participants play an important role in mitigating a certain hazard by actively reacting to a certain hazardous scenario and taking appropriate action(s) to avoid harm or damage. In this context the infrastructure might also be relevant. ADF specific aspects like an ADF that does not require a take-over ready driver needs to be reflected in the analysis. Based on this the risks are assessed.

Question 3-1-2	Relevant Phase(s)	DF				
Are safety requirements (including safety goals) derived to avoid unsafe functional behaviour? <input type="checkbox"/> Yes / <input type="checkbox"/> No						

Following the identification of hazards and risks, a concept needs to be drafted on a functional level that defines, how an ADF will react to avoid a certain hazard. This may depend on the current state of the vehicle and the ADF, e.g. is automation switched “on” or “off”, is a take-over ready driver available or has the ADF erroneously exceeded its ODD. The definition of a safety concept according ISO 26262 (ISO 26262 2018) includes

- the required reaction to bring the vehicle in a safe state,
- the required time within which the transition needs to be achieved,
- the required involvement of persons (the driver or other traffic participants),
- information about warning strategy and / or applied degradation concepts (an important aspect in this context is the MRM, which is described in detail in chapter 4.1.1).

Note that the definition of the safety concept needs to be consistent with the overall OEDR strategy and other vehicle reactions that may be required, e.g. resulting from security activities, as well as aligned with the cybersecurity concept.

Question 3-1-3	Relevant Phase(s)	CO				
Are there measures to confirm the effectiveness of the safety concept? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>Does a strategy exist to validate the feasibility of the concept?</li> <li>Do criteria exist that allow to define whether a vehicle behaviour can be accepted as safe?</li> </ul>				

Once a safety concept has defined the required reactions to mitigate the potential hazards of an ADF, a confirmation of the effectiveness of the measures is needed. In this sense

effectiveness means that the risk of the original hazardous event is reduced and no unacceptable new risks are introduced. One example is the following case: in case a level 3 ADF loses the ability to further follow the lane, therefore switches itself off and alerts the driver, it has to be confirmed that switching off and alerting the driver is indeed avoiding harm and that the driver will be able to take over within the required time frame.

Question 3-1-4	Relevant Phase(s)		DS		
Are there mechanisms included in the design that collect safety relevant data, which will be needed for documentation purposes (e.g. required by law or for certification)? <input type="checkbox"/> Yes / <input type="checkbox"/> No					

Requirements for data collection may result from several sources and depend on whether the vehicle is a prototype or a series production vehicle. Requirements may also be country or state specific. Before a vehicle is used for development in public areas (e.g. road testing) or introduced to the market, the existing requirements within the specified ODD need to be collected, please see also sub-chapter 4.2.1. The requirements have to be considered already during the design phase as this may have an impact on the overall vehicle architecture and on the required bandwidth of the communication bus and storage size. Examples for such requirements are EDR data for post-crash evaluation or data for disengagement reports as required for automated vehicles by the State of California (DCM 2019).

Question 3-1-5	Relevant Phase(s)		DS		
Are the included safety mechanisms based on accompanying safety analysis? <input type="checkbox"/> Yes / <input type="checkbox"/> No	<ul style="list-style-type: none"> <li>Is there a clear concept how to avoid the propagation of faults through the function and avoid an unsafe function reaction (on which level of the function architecture are failures addressed)?</li> <li>Are child-requirements covering the higher level requirements (correctness and completeness)?"</li> </ul>				

A clear structure of the requirements for an ADF and a systematic approach to requirements elicitation are key to argue safety for any vehicle function. Using safety analyses to support the process of breaking down the requirements from one level of detail to the next and identifying gaps in the requirements structure at the same time, are common practice when deriving and defining requirements.

Question 3-1-6	Relevant Phase(s)		DS		
<p>Are function reactions specified that transition the function to a safe state in the presence of a fault (depending on the kind of fault)?</p> <p>( ) Yes / ( ) No</p>			<ul style="list-style-type: none"> <li>Is degraded operation or transition to a safe state sufficiently safe for the specific failure scenarios?</li> <li>Are the restrictions to the function behaviour specified, which result from the transition to the safe state (e.g. reduction of the ODD while operating in a safe state or operating a function for a limited amount of time before further transitioning to a final safe state)?</li> </ul>		

A fault in an ADF may occur at any time, independent from the current operating mode or the driving scenario of the vehicle. At each possible operating mode an appropriate safety mechanism has to keep the vehicle in a safe state in case of a failure. To achieve this there are several options:

- switch off the function and inform the driver (e.g. when driving in manual mode and a sensor which is required for an ADF fails, meaning the ADF is no longer available for the driver)
- provide a backup with full functionality for a limited amount of time (e.g. if driving in an automated mode provide a backup for sufficient time to transfer the control to the driver)
- Switch to a degraded mode (e.g. if one sensor in a set of sensors fails that results in a reduced resolution of environmental data, then reduce the ODD, e.g. the maximum vehicle speed)

For different operating modes and failure scenarios the ADF's reaction may be different in order to achieve a safe vehicle reaction. Consider operating modes that are generally applicable for all ADF (ADF on/off, inside/outside ODD, handover driver-ADF etc.) but also function specific modes such as diagnostic mode or decommissioning. These modes might be part of a MRM, see section 4.1.1.

Question 3-1-7	Relevant Phase(s)			VV	
<p>Is a verification and validation process defined, which is covering the various integration steps of software, hardware, function, and vehicle?</p> <p>( ) Yes / ( ) No</p>				<ul style="list-style-type: none"> <li>Is the successful mitigation of all findings from the hazard analysis confirmed during verification activities?</li> </ul>	

During the integration of the elements that are needed for an ADF several stakeholders will be involved, e.g. suppliers for hardware elements, software and ECU, and on the OEM side the function and vehicle integration (and most likely also part of the software). To finally

achieve a safe function, the workshare for “who is verifying what, how and why”, i.e. workers, test goals, test methods and test targets need to be defined and described. For functional safety it is essential that there are no gaps in the overall verification. From a more general point of view it is desirable to avoid redundant verification at different stakeholders and perform the required verification steps at the most suitable integration level.

Question 3-1-8	Relevant Phase(s)				VV	
Are risks to equipment and involved persons and equipment resulting from safety verification/validation activities assessed? <input type="checkbox"/> Yes / <input type="checkbox"/> No	<ul style="list-style-type: none"> <li>• If verification and validation is carried out on public roads, are potential effects to other traffic participants considered and safety measures defined?</li> <li>• Is ensured that vehicle operators are allowed to operate a vehicle (following company internal and legal requirements) and have received appropriate training?</li> </ul>					

When verification is based on tests (and not simulation or similar), it needs to be considered that the tests could be either passed or failed. Note ISO 26262 is applied to achieve safe products and does not have a focus on a safe development. Even more, it may be necessary to manipulate the function under development to stimulate a certain faulty behaviour for the verification of safety mechanisms. Before executing any test, assess what the possible outcome would be in the case the test failed, if this may result in material damage or harm to people, and if there are additional measures that should be taken to prevent any damage or harm.

Question 3-1-9	Relevant Phase(s)				VV	
Do the test cases for the safety requirements cover the entire operational design domain? <input type="checkbox"/> Yes / <input type="checkbox"/> No						

Test cases have to cover the entire ODD. This is practically impossible. When designing the test cases, an approach needs to be defined how the relevant test cases will be determined, e.g. choosing representative operating profiles, building equivalence classes for test cases, etc. One approach for testing of the safety requirements is that faults need to be injected to stimulate the safety mechanisms and, as described above, if these mechanisms depend on the operating state, at least all these states need to be tested.

Question 3-1-10	Relevant Phase(s)				VV	
Does the function transit to a safe state when being erroneously operated outside of ODD? <input type="checkbox"/> Yes / <input type="checkbox"/> No						

One specific case that is not considered for functional testing is the violation of the ODD as a fault itself. This has to be included in the testing to sufficiently cover the safety requirements.

Question 3-1-11	Relevant Phase(s)				VV	
Is the vehicle behaviour safe when transitioning to a safe state (behaviour may be evaluated with simulations or testing)? ( ) Yes / ( ) No						

When all the safety requirements are verified and have been successfully implemented there is one final step: it needs to be validated, whether the implemented safety concept with all its safety mechanisms is appropriate and keeps the vehicle safe in the case of a fault. Independent of the automation level it must also be checked whether the safety concept avoids that involved people are harmed in the case of a failure. The involved people may be the driver, passengers or other traffic participants outside the vehicle, depending on the automation level and current operating mode.

#### 4.4.2 Cybersecurity

One of the topics to be addressed within the Category “Safeguarding Automation” is the cybersecurity. As summarized by Mcity researchers in their report Identifying and Analysing Cybersecurity Threats to Automated Vehicles (Mcity2018), automated vehicles will probably have to face all the security threats that nowadays disrupt our computer networks, on top of the ones that could be unique to them. Therefore, one of the first steps towards mass market introduction of automated vehicles is the need of establishing robust and sophisticated cybersecurity measures.

For reference, the information contained in this section is aligned with the L3Pilot D4.2 Legal Requirements to AD piloting and cybersecurity analysis. For more details, refer to this deliverable

Question 3-2-1	Relevant Phase(s)	DF	CO	DS	VV	PS
Are a threat analysis and risk assessment performed based on the ADF scope and the previously defined high level architecture? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Has the threat analysis considered all possible types of attack vectors and their characteristics (e.g. description of attack, likelihood, impact, risk...)?</li> <li>Are external factors considered in the threat analysis? Examples of external factors are remote diagnostics and maintenance operations.</li> <li>In the case of remote operated vehicles, has remote fleet management been considered in the threat analysis?</li> </ul>				



Based on the ADF scope and the defined high level architecture, the first step to address this topic, is the threat analysis. It shall be performed considering all development phases, in order to understand what the function will have to face during its lifetime.

This is done in order to identify function weaknesses which could make the function vulnerable for an attack. To do so, it is also necessary to perform a risk assessment in order to prioritize the risks that the function may be exposed to.

The threat analysis and risk assessment shall consider all possible entry points of the potential attack (so called attack vectors), the likelihood of the attack, the impact, the risk, and more details such as the expertise required to perform such attacks and the possible attack methods.

As addressed by the sub-questions, this threat analysis and risk assessment shall be done considering not only threats during “normal operation” but also considering specific cases where the ADF may have a higher exposure to threats. One example is performing remote function diagnostics or function maintenance operations. Another example is when dealing with remotely operated fleet vehicles. Those vehicles may have remote management functions which could also be specifically vulnerable for any attack.

Additional information regarding this topic is provided by:

- ACEA principles of Automobile Cybersecurity (ACEA 2017);
- Draft Recommendation on Cybersecurity of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA;
- The key principles of vehicle cybersecurity for connected and automated vehicles (HMG 2017);
- L3Pilot D4.2 Legal Requirements to AD piloting and cybersecurity analysis (Vignard et al., 2018);
- Documents that are under preparation, such as SAE J3061 (SAE International 2016) ISO 21434 that is in preparation (ISO 21434 20XX).

Question 3-2-2	Relevant Phase(s)	DF	CO	DS	VV	PS
<p>Is there an established and followed cybersecurity process within your organisation to ensure the security architecture of the overall function?</p> <p>( ) Yes / ( ) No</p>	<ul style="list-style-type: none"> <li>• Is there a similar culture existing at sub-contractors, suppliers and potential 3rd parties directly or indirectly working with your organisation?</li> <li>• Is the use of appropriate control considered based on the principle of least privilege?</li> <li>• Is the management of keys and accesses implemented based on the principle of least privilege?</li> </ul>					

In order to ensure that everyone (dealing directly or indirectly with this topic) can follow the required steps and behaves responsibly, it is necessary to establish a cybersecurity culture within the organisations through self-audit processes, awareness and training programmes. These can be adapted depending on employee’s roles and responsibilities, meaning that those dealing closely with cybersecurity concerns shall have higher awareness, follow appropriate processes with allocated accountabilities and have access to the required resources.

As part of the cybersecurity culture, access control and means of appropriate control shall be established based on the principle of least privilege, to make sure that each function or component has the least authority necessary to perform its duties (ACEA 2017).

Additional information regarding this topic is provided by:

- ACEA principles of Automobile Cybersecurity (ACEA 2017);
- Draft Recommendation on Cybersecurity of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA;
- The key principles of vehicle cybersecurity for connected and automated vehicles (HMG 2017).

Question 3-2-3	Relevant Phase(s)	DF	CO	DS		
<p>Are (cyber-)security requirements identified for the whole function, including not only those related to hardware/software development but also those related to network design and communication? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Are clear methods defined to address confidentiality and data privacy such as by using publicly available and well tested cryptographic methods?</li> <li>• Are standard and publicly available IP security protocols used for back end connectivity functions?</li> <li>• Are recovery measures implemented in case of function outage for back end connectivity functions?</li> </ul>				

Every cybersecurity requirement has to be implemented considering that ADF’s weaknesses and vulnerabilities may happen from the component level (e.g. ECU) up to extended vehicle level (which includes network communication, intra-vehicle communication, function architecture and backend at OEM such as HD maps information or over-the-air updates). This shall be performed at the definition phase.

Additionally, and to ensure robustness of the function, publicly available IP security protocols and cryptographic methods shall be used. Also, it shall be considered that a function downtime may happen and therefore data may not be available. For such cases, recovery measures shall be put in place securely

Additional information regarding this topic is provided by:

- ACEA principles of Automobile Cybersecurity (ACEA 2017);
- Draft Recommendation on Cybersecurity of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA;
- The key principles of vehicle cybersecurity for connected and automated vehicles (HMG 2017).

Question 3-2-4	Relevant Phase(s)	DF	CO	DS	VV	PS
<p>Is a self-audit process established to gather information about the policies and procedures followed?</p> <p>( ) Yes / ( ) No</p>						
						<ul style="list-style-type: none"> <li>• Does the self-audit process include a procedure to log the (hazardous) events (e.g. potential security breach) with impact on security and report eventual vulnerabilities?</li> <li>• Does the self-audit process include a list of the tests performed including the test reports?</li> </ul>

During the whole development cycle, a self-audit process shall be considered. This is part of the cybersecurity culture to ensure that the whole function from a component level up to vehicle level is secure enough. To do so, self-audits shall be put in place not only internally but also at Tier 1's and subcontractors.

The audit shall be able to collect all the information related to the policies and procedures established by the company. Additionally, it should also contain logging of hazardous events, report eventual vulnerabilities and include a documentation with the test reports.

- ACEA principles of Automobile Cybersecurity (ACEA 2017);
- Draft Recommendation on Cybersecurity of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA;
- L3Pilot D4.2 Legal Requirements to AD piloting and cybersecurity analysis (Vignard et al., 2018)

Question 3-2-5	Relevant Phase(s)	CO			
<p>Is an update of the high-level sensor architecture - defined in the concept phase - based on the threat analysis performed and the identified requirements considered?</p> <p>( ) Yes / ( ) No</p>					
					<ul style="list-style-type: none"> <li>• Has the separation of safety critical from non-safety critical infrastructure been considered?</li> <li>• Has a decentralised architecture been considered in order to increase the difficulty of attacks succeeding?</li> </ul>

During the concept selection phase, and once the threat analysis has been performed, some vulnerabilities may have been identified and the sensor architecture may need to be revised.

This question focuses on how the outcome of the threat analysis is reflected in the development, prior to the design phase.

It is important that at this stage and knowing the threats that the ADF will face, the ADF architecture is structured in a way that a separation exists between safety critical and non-safety critical infrastructure. The background is that a decentralised architecture is more challenging for possible attacks.

Additional information regarding this topic is provided by:

- Recent release of NHTSA’s “Framework for Automated Driving System Testable Cases and Scenarios Final Report” (Thorn et al., 2018);
- L3Pilot D4.2 Legal Requirements to AD piloting and cybersecurity analysis (Vignard et al., 2018).

Question 3-2-6	Relevant Phase(s)		DS		
<p>Is security by design considered in order to minimise the risks/threats and responding appropriately to them once identified? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Are secure programming and software development guidelines followed?</li> <li>• Are methods related to protection against new and developing security risks considered?</li> <li>• Are methods related to ensuring software updates fixing security risks considered?</li> </ul>			

At the design phase, cybersecurity by design means that from the beginning the design shall be secure. In order to comply with this principle, secure programming and software development guidelines need to be followed.

Also, as the development process evolves, new and developing risks may appear and therefore appropriate protection mechanisms shall be put in place. One example is the software update, which may have not been considered at the beginning of the development but that will take place in time based on the existing architecture. Therefore, those new potential risks have to be identified and appropriate actions have to be taken by for example performing an additional threat analysis and risk assessment, which as shown in the first question, has to be addressed along the whole development process.

- ACEA principles of Automobile Cybersecurity (ACEA 2017);
- Draft Recommendation on Cybersecurity of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA;
- L3Pilot D4.2 Legal Requirements to AD piloting and cybersecurity analysis (Vignard et al., 2018).

Question 3-2-7	Relevant Phase(s)					PS
<p>Is an information sharing and analysis centre (ISAC) to report incidents / exploits / vulnerabilities established? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>Is a procedure established to tackle the identified incidents/vulnerabilities? (Including threat analysis and validation through appropriate testing?)</li> <li>Is a procedure established to properly inform the user when system security support is no longer available?</li> <li>Is a procedure established to properly inform the user when a security breach happens?</li> <li>Has a clear strategy for OTA updates been defined based on cybersecurity requirements?</li> </ul>				

The last step to be covered within cybersecurity refers to the importance of sharing with others the concerns identified such as threats and vulnerabilities. Some consortiums already exist to share such information within the industry such as Auto-ISAC established in 2015 with the aim of sharing within global automakers the emerging cybersecurity risks. The sub-questions show examples of possible risks that may happen after sign-off and which have to be addressed.

- Auto-ISAC Best practices (2016) (AUTO-ISAC 2016);
- ACEA principles of Automobile Cybersecurity (AECA 2017);
- L3Pilot D4.2 Legal Requirements to AD piloting and cybersecurity analysis (Vignard et al., 2018).

#### 4.4.3 Implementation of Updates

This topic addresses the implementation of updates using traditional forms, as well as those completed over the air (OTA). The following questions are to be used as prompts for consideration at the different development stages.

Question 3-3-1	Relevant Phase(s)	DF		DS		
<p>Are international regulations and standards being followed where appropriate during the development of the software update processes? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>Are the relevant type approval organisations informed of any updates and foreseen changes? (i.e. in cases where the performance of an ECU / vehicle component is modified in such a way that the type approval or regulatory standards compliance are affected)</li> </ul>				

	<ul style="list-style-type: none"> <li>Is compliance with the existing type approval ensured?</li> </ul>
--	--

When developing the update life cycle and future updates for a function it is essential to consider and follow both international and national laws, as well as obtaining the relevant type approvals. These should be reviewed and resubmitted where necessary for any updates or modifications to the vehicle.

As this is a fast developing field in the automotive sector, it is important to continuously check for new legislative standards that are required in the relevant markets. See section 4.1.3 for more information on existing standards. Also, the following documents provide current information as of the day of publication:

- 24. UNECE WP29 GRVA Draft Recommendation on Software Updates (UNTF 2018).
- Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-2	Relevant Phase(s)	DF	CO	VV
<p>Is hardware / software compatibility for the lifetime of a vehicle and future updates considered? ( ) Yes / ( ) No</p>	<ul style="list-style-type: none"> <li>Does the update enable new/ additional functionality?</li> <li>Will any other vehicle functionality be altered due to the software update?</li> <li>Is the possibility of performing an OTA update on the ADF considered?</li> <li>During vehicle design, is the future compatibility of ECUs on-board known?</li> </ul>			

When defining/ developing the update strategy it is essential to consider both the vehicle's hardware and functional capability as well as its lifecycle. Considering the short development cycles – in particular for software – it is inevitable that there will be a necessity to make updates throughout the lifetime of the vehicle. The vehicle and the ADF should be designed in such a way as to allow for a safe and seamless update process for the user. These documents provide initial guidance to consider:

- A System-Theoretic Safety Engineering Approach for Software-Intensive Systems (Abdulkhaleq 2017);
- Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-3	Relevant Phase(s)	DF		DS	VV	
<p>Is a clearly defined OTA and software update strategy developed to manage the end to end process? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No</p>		<ul style="list-style-type: none"> <li>• Location - are certain updates only available at predefined locations, such as the registered address of the vehicle?</li> <li>• Status of network connectivity - do updates require local wireless networks, or can some be installed using a cellular network connection?</li> <li>• Vehicle state - Is a robust strategy put in place to manage updates when the vehicle is required to be stationary?</li> <li>• Is there a clear strategy to notify users about the updates?</li> <li>• Has due consideration been given to ensure the software update is conducted in a safe and secure manner?</li> <li>• Is there an appropriate verification and validation strategy to check software updates before they are sent out?</li> </ul>				

The vehicle is a complex collection of interconnected ECUs that must endure extreme variations in environment, as well as having a lifetime far exceeding that of any ordinary electronic consumer device. It is therefore essential that a clear update strategy is developed during the design of the vehicle to ensure that future updates are compatible with the hardware on the vehicle. Furthermore, it is essential that sufficient V&V testing is done before releasing updates to the customer. Additional information can be found here:

- A System-Theoretic Safety Engineering Approach for Software-Intensive Systems (Abdulkhaleq 2017);
- Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-4	Relevant Phase(s)	DF				
<p>Are software safety requirements identified at a function level? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No</p>		<ul style="list-style-type: none"> <li>• Where applicable, are relevant standards (ISO 26262, ISO 21434 etc.) followed during the definition of OTA processes and software updates?</li> </ul>				

It is essential that both holistically and on a function by function basis the relevant software safety requirements are identified and incorporated into the design. As safety standards develop, the system's functional safety should be modified to comply.

For more information, see these documents:

- Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015);
- ISO 26262 (ISO 26262 2018);
- ISO/PAS 21448:2019 Road vehicles - Safety of the intended functionality (ISO 21448 2019);
- ISO 21434 (ISO 21434 20XX).

Question 3-3-5	Relevant Phase(s)	DF	DS	PS
Is there a clear strategy for improving the OTA update process based on cybersecurity developments and lessons learnt from vehicles already in the field? ( ) Yes / ( ) No				

Previous development and project experience, as well as lessons learnt (both in and out of the field) are an invaluable improvement tool. It is recommended to establish a process for implementing this learning back into the development phases and even update the current OTA update process.

Question 3-3-6	Relevant Phase(s)	CO	PS
Is the function being updated safety critical? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Has a robust V&amp;V procedure been developed to ensure OTA updates on safety critical functions are sufficiently tested prior to release?</li> </ul>	

A vehicle contains both safety and non-safety critical functions. Depending on the safety criticality of the effected function, the requirements for the update might differ. A failure in the vehicle infotainment introduced by a bug in a software update might lead to user frustration. On the other hand a failure caused by an update to a safety critical component might lead to serious consequences and must be prevented.

For more information, see Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-7	Relevant Phase(s)	CO	VV
Is a method implemented to notify the user and OEM of each successful update installation? ( ) Yes / ( ) No			



It is important that users are informed when updates are successfully installed and the vehicle is ready to use. In failure cases it is important that the user is notified to enable him / her to take further actions (e.g. contact the manufacturer/ dealership). The manufacturer should also be aware of successful or failed updates to enable it to react promptly in cases of failure and to provide an updated software version.

Additional information regarding this topic is provided in the document see Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-8	Relevant Phase(s)			DS		PS
Is a process for managing failed updates implemented? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>As part of the update process is there a method for identifying the reason for a failed update?</li> <li>As part of the process is there a clearly defined method for pushing updates to the customer vehicle?</li> <li>Is a method for reverting back to the previous software version until a bug fix has been developed implemented into the update process?</li> </ul>				

Any updates sent out to customers should have been sufficiently tested beforehand to ensure the updates are bug free. However, there are always factors that may be overlooked. In these cases, there should be a “failsafe strategy”, which ensures that the vehicle is still operational by for example reverting back to a former software version. Combined with this there should be some form of warning and information on how the user can resolve the issue. In extreme failure cases the response might be to stop the user from being able to use the vehicle. In this case the manufacturer must be informed to resolve the issue.

For more information see Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-9	Relevant Phase(s)	DF				
Is a clear strategy developed to ensure the user knows the update is authentic? ( ) Yes / ( ) No						

With the introduction of OTA updates manufacturers will move – at least partly – away from the traditional customers visiting a dealership approach for servicing to a remote service approach used by software companies. This approach has risks, which are potentially safety critical. This means that the customer has to have confidence that updates are from a trusted

source and not a malicious attack. Typically, software and phone companies use certifications to show software updates authenticity.

For further information see Secure Over-the-Air Vehicle Software Updates - Operational and Functional Requirements (Sena 2015).

Question 3-3-10	Relevant Phase(s)	DF				
Is a (robust) method for the authorised owner of the vehicle developed to accept or reject updates? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Does this method consider the fact that the owner is not necessarily the driver of the vehicle?</li> </ul>				

Just as it is important for the manufacturer to provide proof of the authenticity of the update, it is also important that only authorised people can accept or decline provided updates. This is to stop interference from individuals who may seek to install malicious software or may try to stop new updates from being installed for some benefit to themselves or a third party.

#### 4.4.4 Safety of the Intended Functionality (SOTIF)

Unlike functional safety of automated vehicles, the safety of the intended functionality (SOTIF) mainly focuses on systems that rely on sensing the external or internal environment. The potential hazardous behaviour related to the intended functionality or performance limitation of a system are in the scope of SOTIF (ISO/PAS 21448).

The cause of hazardous event in the scope of SOTIF could incorporate the source with system aspect, as well as external factor aspect, for instance:

- Performance limitations, insufficient situational awareness with or without conjunction with a foreseeable user misuse;
- Reasonably foreseeable misuse, incorrect HVI (user confusion, user overload);
- Impact from car surroundings (other users, “passive” infrastructure, environmental conditions, weather, electromagnetic interference, etc.) (ISO/PAS 21448, 2019).

The following definitions shall support the interpretation of relevant terms:

- **Intended use:** Any use of the product consistent with the manner in which it is promoted/advertised and described by the manufacturer and which can be justifiably expected in accordance with the knowledge and skills of the intended user.
- **Foreseeable misuse/reasonably foreseeable misuse:** Usage of a product in a way not intended by the manufacturer and in a manner inconsistent with the user manual, but which may result from foreseeable human behaviour.
- **Misuse:** Describes an improper and inappropriate usage of the product, which in a particular circumstance can be deemed irresponsible and in complete contradiction to the intended purpose or function of the product

In this topic, we will discuss the issue of the SOTIF during definition, conception, design phase as well as verification/validation phase regarding the development of ADF.

Question 3-4-1	Relevant Phase	DF	CO	DS	VV	PS
Is the development of SOTIF compliant with the latest international standards and regulations? ( ) Yes / ( ) No						

The development of SOTIF should comply with the latest international standards, such as the homologation of state-of-the-art ISO/PAS 21448. The first version of ISO/PAS 21448, which refers to the safety of the intended functionality (SOTIF) and provides guidance on the design, verification and validation measures, will be published around 2020. It aims to avoid a malfunctioning behaviour in the system in the absence of technical faults, which might result from technological and definitional shortcomings.

Additionally, the latest guidelines or regulations of the development of SOTIF should also be taken into account. Such as the latest guidelines of NHTSA and SAE for the US. The organizations OICA and ACEA work to modify and update the Geneva Convention and provide advice on the regulation regarding the development and deployment of automated vehicles to European Union.

Question 3-4-2	Relevant Phase	DF				
Is there a definition regarding a functional and system specification about ADF? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Does the functionality, its dependencies on, and interaction with the environment be defined and described?</li> </ul>				

A definition and description of the functionality, its dependencies on and interaction with the environment and other functionalities can help to elaborate a functional and system specification. This functional and system specification can be the beginning for the improvement regarding the safety of intended functionalities. Similar to the functionality and system definition of ISO 26262-3, Clause 5, an appropriate description of the functionality and system is developed to serve as an input to the development of SOTIF.

The description of the functionality provided by the system to the vehicle mainly including:

1. The use cases in which it is activated;
2. The sensing and arbitration concept and technologies;
3. The level of authority over the vehicle dynamics;
4. The interfaces with the other systems and functionalities of the vehicle and the road infrastructure.

Besides, system related description, such as the system and elements implementing the intended functionality, the limitations and their countermeasures, need to be taken into

account in this case. The description of ADF regarding both functionality and system specification could elaborate and serve as the first step of SOTIF activities. (ISO/PAS 21448 2019)

Question 3-4-3	Relevant Phase(s)	DF				
Is there a hazard analysis in order to conduct the identification of necessary SOTIF activities/ measures? ( ) Yes / ( ) No						

A hazard analysis is employed to identify the different hazards that may arise from a function or its environment. A hazard represents a “condition, event, or circumstance that could lead to or contribute to an unplanned or undesirable event, like an accident, a functional failure, performance limitations or misuse” (ISO 26262-3:2018).

The SOTIF activities/ measures should be derived from the hazard analysis, which can help to identify all the potential hazards that may occur during a driving task of automated vehicles. The identification of SOTIF activities/ measures of an ADF shall be conducted in an earlier phase of development of SOTIF. Later, the SOTIF risk identification and evaluation shall be conducted, which represent a consistency check of functional safety concept in chapter 4.4.1.

Question 3-4-4	Relevant Phase	DF				
Is there a systematic identification and evaluation for the SOTIF risks such that the possible hazardous events arise from system or external environment? ( ) Yes / ( ) No	<ul style="list-style-type: none"> <li>• Is there an assumption of the risk of how the intended functionality makes use of inputs from other vehicle elements, and vice versa?</li> <li>• Is there an assessment of severity and controllability to determine whether a credible harm can result of the SOTIF risk?</li> <li>• Has the assessment of safety impact looked at not only the direct intended effects of ADF but also the indirect and unintended effects?</li> </ul>					

Based on the identification of hazard events caused by the system or external environment, the systematic identification and evaluation for the SOTIF risks can be executed in order to ensure the safety and reliability of intended functionalities. This process can be achieved by applying the methods proposed in ISO 26262-3:2018. For this purpose the same items such as the severity, exposure and controllability of the hazardous events need to be derived by the method as proposed by ISO 26262 (ISO 26262 2018).

In the context of SOTIF, severity and controllability are considered to determine the scenario for which a credible harm can result from functional insufficiencies of the intended functionality or foreseeable misuse. The definition of the severity and controllability classes are the same as ISO 26262, but their determination for a given hazardous event can be specific for SOTIF hazards.

Here, the assessment of safety impact of SOTIF risks should be taken into account. Not only the direct and intended effects within the scope of ADF's limits (e.g. limit of detection and perception of objects in road by sensor suite); but also indirect and unintended effects beyond the scope of detection and perception limits are in the scope of assessment (such as behavioural adaptations or car surroundings, after a long-term automated driving task).

Question 3-4-5	Relevant Phase(s)	DF				
Is there an appropriate mechanism to address SOTIF risks related to the take-over request? ( ) Yes / ( ) No						

A take-over request (TOR) of ADF is a key issue for the level 3 or level 4 of automated vehicles, which can transfer the driving control from vehicle to human within some situation that is beyond the ADF's capabilities. This mechanism is intended to remind the driver to take over the control of vehicle within an appropriate reaction time, as well as support him / her in order to reduce the risk via human-vehicle-interface (HVI) system. Thus, an appropriate HVI can significantly avoid the occurrence of misuse and mitigate the risks under hazardous events. For the aspects regarding HVI, please see also topic "Mode awareness, Trust & Misuse" (chapter 4.5.2).

Additionally, a MRM will be performed by the system in case the driver does not respond to take-over request. The MRM leads to a MRC (such as limited/ end of ADF operation) to minimize the risk and ensuring the safety of the driver (Resende et al., 2010). For the aspects related to MRM, please see also topic "Minimal Risk Manoeuvre" (chapter 4.1.1).

Question 3-4-6	Relevant Phase(s)	DF				
Does the ADF monitor the driver in order to ensure his / her controllability of the ADF? ( ) Yes / ( ) No						

A possibility to ensure the controllability of the ADF is to use a driver monitoring system that can detect distractions or drowsiness of a driver during automated mode. This system could also invoke action to remind and maintain driver's attention in both manual and automated driving. The monitoring allows several functionalities such as: identification of the driver in order to allow the vehicle to automatically restore its preferences and settings; monitor driver fatigue and alert the driver when potential drowsiness situation is detected, etc.

An appropriate driver monitoring function can help automated vehicle to make better decisions to improve its comfort and safety. Especially it can ensure the controllability of the intended function of vehicle from drivers. For the aspects related to driver monitoring, please see also topic “Driver Monitoring” (chapter 4.1.1).

Question 3-4-7	Relevant Phase	DF			VV	
Is there a validation and verification (V&V) strategy to prove the compliance of SOTIF aspects? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Does V&amp;V strategy make sure that the test goals and V&amp;V targets (such as acceptance criteria) are sufficiently covered?</li> <li>Is there an appropriate testing environment that matches your validation strategy?</li> </ul>				

A V&V strategy can support the process of ensuring an appropriate performances and safety capabilities of the ADF. This strategy should support the argumentation for the safety of the intended functionalities. Additionally, V&V activities of the intended functionalities with regard to the risk of safety violations without system faults include integration-testing activities to address the following scope:

1. The ability of sensors and the sensor processing algorithms to model the encountered driving environment;
2. The ability of the decision algorithm to recognize both known and unknown situations and make the appropriate decision according to the environment model and the system architecture;
3. The robustness of the system or function.
4. The ability of the HVI to prevent reasonably foreseeable misuse; and
5. The manageability of the handover scenario by the driver.

In order to achieve this strategy, several information, which is based on the driving test cases should be addressed, especially the test goals and V&V targets. The test goals and V&V targets can be derived from the specifications and safety requirements of vehicle design architecture. These goals and targets should consider known unsafe use cases but should also aim at discovering unknown unsafe use cases. The different test environment should also be specified to match the validation strategy (ISO/PAS 21448 2019).

Question 3-4-8	Relevant Phase	DF				
Are users of the ADF informed about the functional limitations? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Are users of the ADF informed about their responsibilities?</li> <li>Are users of the ADF informed about their correct / appropriate interaction with the ADF? (→ avoid misuse)</li> </ul>				

Before the usage of the automated vehicles in real-life conditions, the users need to be informed about the functionalities in order to improve the knowledge of the ADF. The taken approach to deliver the information, how to use the ADF safely within the scope of ODD, to the users (e.g. instructions, training) need to be decided in accordance with the technical capabilities of the ADF.

The right information about the functional limitations can support users to comprehend the limit of the ADF during a driving task so that they can use the automated vehicle safely and appropriately. Additionally, the notification about the consequences of system misuses can significantly reduce the misuses of functionalities by users (MILT 2018).

Question 3-4-9	Relevant Phase	CO			
<p>Are there functional improvements to avoid or mitigate SOTIF risks?</p> <p>( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>Are there triggering events related to sensors, algorithms and actuators identified?</li> <li>Is there an assessment whether the system appropriately responds to triggering events?</li> </ul>			

Triggering events<sup>4</sup> represent specific conditions of a driving scenario that serve as an initiator for a subsequent system reaction possibly leading to a hazardous event.

The analysis of triggering events could help to identify the system weaknesses (related to sensors, algorithms and actuators) and the related scenarios that could result in an identified hazard. Once the triggering events are identified that could trigger a hazardous event with credible harms, we need functional improvements of ADF to appropriately respond to triggering events and reduce SOTIF risks.

Functional improvements could incorporate several aspects, for instance sufficient performance /accuracy of sensor, sufficient performance of detection and decision algorithms, as well as appropriate Human-Machine Interface regarding the controllability of vehicle and avoidance of misuse, etc. (ISO/PAS 21448 2019).

Question 3-4-10	Relevant Phase	DS	VV		
<p>Is the ADF performance verified in hazardous events and foreseeable misuse case by conducting appropriate testing (XIL, real world and test track test)?</p> <p>( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>Is the ADF validated regarding aspect that it does not cause any unreasonable level of risk in real-life use cases?</li> </ul>			

<sup>4</sup> Triggering event means a scenarios that serves as an initiator for automated action. E.g. while operating on a highway, a vehicle's autonomous emergency braking (AEB) system misidentifies a road sign as a lead vehicle resulting in braking.



Several methods of the V&V of system performance, such as model-in-the-loop (MIL), software-in-the-loop (SIL), hardware-in-the-loop (HIL), test track experiments and long-term endurance test (real world test) with the injection of potential triggering events, could be addressed in order to ensure the safety of intended functionalities. Besides, various conditions such as parts characters, process, phenomenon, and environment condition could affect the system performance; these influencing factors need to be considered during the testing process.

Additionally, according to the ISO/PAS 21448, the ADF should be validated to ensure that it causes the minimum risks, especially the unreasonable level of risks, in real-life use cases. Therefore, two different approaches could be applied as below (ISO/PAS 21448):

1. Minimize the SOTIF risks caused by known scenarios to an acceptable level by SOTIF by means of technical measures, such as function improvement, limitation of use, limitation of the performance of the intended functionality, etc.
2. Minimize the SOTIF risks caused by unknown scenarios as possible by the SOTIF V&V measures, such as endurance testing, test track of the ADF or industry best practice, etc.

These two solutions can significantly help to achieve SOTIF safety goals

#### 4.4.5 Data Recording, Privacy and Protection

The realization of ADF will enable the collection of massive amounts of data. In order to protect the customers' data recorded, this process needs to be done in accordance with international laws.

The vast amount of data needs to be stored off-board of the vehicle in large data clouds. It must be ensured that only those parties with a rightful and reasonable justification have access to the personal data gathered from the customers. Following established procedures, misuse will be minimised and the benefits of the data collection highlighted. Especially the advantages offered by data harvesting such as driving data and accident analysis justify its collection, if done in an adequate and proper way. Customers need to be furthermore aware of how their data is handled and processed. This topic provides the guidelines on how to handle these issues.

Question 3-5-1	Relevant Phase(s)	DF	DS	PS
<p>Is the purpose of the data collected made clear to the customer / user? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No</p>		<ul style="list-style-type: none"> <li>Is the customer informed about the information considered as personal data, and in which categories it is divided?</li> <li>Is the customer informed about the purpose, third parties (categories of third parties) the data is shared with and the identity of the company (group of companies) that governs data processing?</li> </ul>		



	<ul style="list-style-type: none"> <li>• Is this information made available clearly and easily accessible (contract, website, manual etc.)?</li> <li>• Are contact points for the customer maintained?</li> <li>• Is the customer given the choice to share or not share data where possible?</li> <li>• Is the data securely stored</li> <li>• Can data be provided to relevant authorities upon request?</li> </ul>
--	---

The customer requires an understanding of why personal data is collected. There shall be information material available explaining the reasons. There must be a clear communication which data is supposed to be regarded as personal information and which is not. If applicable, the customer should also be informed about different data categories. It also includes information about other organisations accessing the data and the reasons for it. Information about data sharing must be available via different means, such as manuals or websites. Contact points for the customer shall be provided. Ideally, the customer has the choice to decide to share data or not, depending on the purpose. The data must be stored securely. In case requested by authorities, the data shall be made available in an appropriate manner and in accordance with the law.

Additional information regarding this topic is provided by:

- FESTA Handbook (Barnard et al., 2017);
- ACEA principles of data protection in relation to connected vehicles and services (ACEA 2015);
- The pathway to driverless cars: a code of practice for testing (DOT 2015).

Question 3-5-2	Relevant Phase(s)	DF		DS		
Is it defined who owns the data? ( ) Yes / ( ) No						<ul style="list-style-type: none"> <li>• Is it authorized if third parties may access the data?</li> <li>• Is it clear where the data will be stored?</li> <li>• Is it clear who is responsible for maintaining the data?</li> <li>• Is there a process to ask for the deletion of data?</li> <li>• Is personal data accurate and kept up-to-date if necessary?</li> </ul>

There needs to be a clear definition on who owns the data that is generated by the ADF. This includes information about who is responsible for maintaining the data, and who may be allowed to access it for which reason. The place of data storage shall be well defined. In case a data retention deadline is reached, there must be a known and easy process that establish to ask for the deletion of data. This process shall also be available in case data deletion is requested by a customer at any time. In case it is necessary to keep personal data, it must be accurate and up to date. Additional information regarding this topic is provided by:

- FOT-Net Data - Data Sharing Framework (Gellerman et al., 2017);
- FESTA Handbook (Barnard et al., 2017);
- GDPR Guide to the general data protection regulation (ICO 2018).

Question 3-5-3	Relevant Phase(s)	DF				
Is necessary data collected which is related to the occurrence of malfunctions or failures to establish the cause of any crash? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Does data contain the status of the ADF and whether the driver or ADF was in control at the time leading up to, during and following an incident or crash?</li> <li>• Is relevant information shared with the government authorities for crash reconstruction?</li> </ul>				

In order to help with the analysis of crashes and the improvement of ADFs, pertaining data will be collected. This data shall include the status of the ADF, the occurrence of malfunctions and the arbitration of control between the driver and the ADF before and during an accident or incident. The data shall be shared with relevant authorities to enable crash reconstruction up on request. Additional information regarding this topic is provided by:

- Automated driving systems 2.0: a vision for safety (NHTSA 2017).

Question 3-5-4	Relevant Phase(s)		DS			
Is data protection impact assessment carried out? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is the societal impact as of customer rejection assessed?</li> <li>• Is the impact assessed as data is used as evidence of ADF operation in accident cases?</li> </ul>				

There must be an assessment conducted analysing the impact of the data protection measures employed. This includes the impact on the societal level such as customer acceptance and rejection. In addition, the safety impact is of interest, as data protection might make it harder to use data in case of accident investigations involving ADFs. Additional information regarding this topic is provided by:

- ACEA principles of data protection in relation to connected vehicles and services (ACEA 2015).

Question 3-5-5	Relevant Phase(s)		DS		
<p>Are appropriate measures (technical, security, organizational) to protect customer data implemented?</p> <p>( ) Yes / ( ) No</p>			<ul style="list-style-type: none"> <li>• Are contractual safeguards to protect personal data in case of outsourcing imposed?</li> <li>• Is anonymization, pseudonymization and de-identification applied where appropriate?</li> <li>• Is the data processed based on a contract, with consent of customers, to comply with legal obligation?</li> <li>• Is the data processed lawfully, fairly and in a transparent manner in relation to individuals?</li> <li>• Are data collected for specified, explicit and legitimate purposes only?</li> <li>• Is personal data adequate, relevant and limited to what is necessary in relation to purposes for which they are processed?</li> <li>• Is personal data kept in a form that permits identification of data subjects for no longer than it is necessary for the purposes for which it is stored?</li> <li>• Is the user enabled to erase sensible data on functions and connected functions?</li> <li>• Is personally identifiable data managed appropriately (what is stored/transmitted, usage, control of data owner)?</li> <li>• Is personal data retained only as long as necessary?</li> </ul>		

The measures implemented to protect customer data must be appropriate. This includes the technical, security and organisational levels. It is especially problematic in the case of outsourcing personal data. Only relevant and adequate personal data shall be processed, including means to anonymise them. The data must furthermore only be processed with permission of the customers. Personal data shall be analysed according to the applicable laws in a transparent way. Data may only be collected for legitimate and explicitly specified purposes. In case personal data are stored, it must be limited to what is necessary, given the reason for which it is processed. Personal data shall be kept in a form allowing to identify an individual only when and not longer than necessary.

Additional information regarding this topic is provided by:

- ACEA principles of data protection in relation to connected vehicles and services (ACEA 2015);
- GDPR Guide to the general data protection regulation (ICO 2018).

Question 3-5-6	Relevant Phase(s)		DS		
Is responsibility for complying with the GDPR taken, at the highest management level and throughout the organisation? ( ) Yes / ( ) No					<ul style="list-style-type: none"> <li>• Is evidence of the steps taken to comply with the GDPR available?</li> </ul>

It has to be ensured that the developed ADFs are compliant with the data protection regulation that apply in the respective countries. For the European Union, the General Data Protection Regulation (GDPR) has to be considered. Most important, evidence of the steps taken to comply with the GDPR is necessary. Additional information regarding this topic is provided by:

- GDPR Guide to the general data protection regulation (IOC 2018).

Question 3-5-7	Relevant Phase(s)		DS		
Are (security) risk assessment and management procedures in place? ( ) Yes / ( ) No					<ul style="list-style-type: none"> <li>• Are security risks identified and managed by secure coding practices including supply chain, contractors etc.?</li> <li>• Is authenticity and origin of all supplies ascertained?</li> <li>• Is data privacy addressed by using publicly available and well tested cryptographic methods?</li> </ul>

As vehicles get smarter, cybersecurity is becoming an increasing concern in the automotive industry (further information is provided in chapter 4.4.2). As a consequence, measures need to be put into place in order to protect personally identifiable data. This includes the definition of risk assessment and management procedures as well as the development of secure coding practices. Besides, authenticity and origin of all supplies needs to be ascertained.

Additional information regarding this topic is provided by:

- The key principles of vehicle cybersecurity for connected and automated vehicles (HMG 2017)

Question 3-5-8	Relevant Phase(s)		DS		
Are back-end-functions protected appropriately? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No					<ul style="list-style-type: none"> <li>Is a process established that treats data from incoming sources as unsecure until validated?</li> </ul>

A key enabling technology for road vehicle automation is V2X-communication requiring back-end functions (please consider also chapter 4.3.2). However, back-end functions might provide access to personal data on other functions. In consequence, remote and back-end functions, including cloud based servers, should have appropriate levels of protection and monitoring in place to prevent unauthorised access. Additional information regarding this topic is provided by:

- The key principles of vehicle cybersecurity for connected and automated vehicles (HMG 2017).

Question 3-5-9	Relevant Phase(s)		DS		
Is the function able to withstand reception of corrupt, invalid or malicious data or commands (internally and externally received) and remain available for primary use (link to functional safety)? ( <input type="checkbox"/> ) Yes / ( <input type="checkbox"/> ) No					<ul style="list-style-type: none"> <li>Is the function designed resilient and fail-safe if safety critical functions are compromised (link to functional safety)?</li> </ul>

Nevertheless, principles of functional safety have to be considered for cyber-security issues as well. Thus, the function must be designed to be resilient to attacks and should respond appropriately when its defences or sensors fail. Additional information regarding this topic is provided by:

- The key principles of vehicle cybersecurity for connected and automated vehicles (HMG 2017).

## 4.5 Category “Human-Vehicle Integration”

The human-vehicle integration (HVI) category comprises all factors related to the interaction between the vehicle and the user. This ranges across a broad area covering user experience, usability, human factors and cognitive ergonomics.

Display and control concepts, i.e. the Human-Machine Interface (HMI), must be developed in a way that they are easily and safely operated by the user of an ADF. Whereas the HVI is about the harmonious interaction between the user and the vehicle in a broader sense, the HMI is more specifically about the hardware and software interface between them. In order to streamline the various aspects related to HVI, this category is subdivided into five different topics: The first topic covers the general guidelines on how to design the HVI. This includes

the acceptance of the ADF as well as usability and user experience related aspects. The mode awareness, trust and misuse topic is about the awareness of the ADF's current driving mode. This also relates to the users' trust in the ADF and their potential for misuse. Driver monitoring is about assessing the user's state when operating an ADF. This is closely related to the users' mental models and their workload. An important aspect of this is the impact of non-driving related activities (in the following referred to as secondary tasks) operated while driving with a highly automated function. On the one hand controllability and customer clinics refer to the question of an ADF's controllability from the user's perspective. On the other hand, this is related to the question on how to conduct a study to test the controllability of such a function and other properties of an ADF under development. Driver training and variability of users is the final topic. It covers the area of user training required for an ADF. Furthermore, it also relates to the variability of users to be taken into account. Together these topics form a comprehensive overview on the overall category of Human-Vehicle Integration.

#### 4.5.1 Guidelines for HVI

Guidelines for the ADF's HVI are proposed within this topic. A clear and well-designed HVI is a key factor in gaining the user's acceptance of the ADF. The impact of the HVI on user experience, usability and the underlying safety of the ADF are very important and should not be underestimated.

There are six main questions within this topic, and it is important that the sub-questions are also considered carefully to ensure the HVI meets the customer expectations.

Question 4-1-1	Relevant Phase(s)	DF	CO	VV
Are design guidelines followed when defining, assessing & validating the HMI concept? ( ) Yes / ( ) No				
				<ul style="list-style-type: none"> <li>Are user requirements collected based on market research or based on other sources of data?</li> </ul>

Design guidelines should be followed during the development of the HVI. This ensures that all aspects of the HVI are considered. A point to note is that there are many different HVI guidelines (e.g., TRL, 2011; Campbell et al., 1996) and the guidelines used during the ADF development should be selected carefully to ensure they are suitable for the application. Guidelines adapted to HVIs for conditionally automated vehicles were presented by Naujoks et al., (2019-1) and validated in empirical studies (Forster et al., 2019; Naujoks et al., 2019-2) Guidelines may differ for certain demographics as different groups of people may prefer different communication methods such as, symbols or colour coding. However, HVI should be standardised where possible following industry standards that are consistent with user's mental models. This will minimise the time required to familiarise oneself with the HVI, therefore improving the experience of first time users.

Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1).

Question 4-1-2	Relevant Phase(s)	CO			
Are unintentional activations and deactivations of the ADF prevented? <input type="checkbox"/> Yes / <input type="checkbox"/> No					

Unintentional deactivation of an ADF by the user is an event which needs to be avoided at all costs. The driver may be concentrating on a non-driving task and will not be ready to take control of the driving task immediately. The HVI concept should be designed so that it is not possible for the driver to inadvertently initiate a transfer of control – in particular not if the driver has not regained situational awareness yet. Similarly it is important to prevent unintentional activations of the ADF by the user. Unexpected longitudinal or lateral input from the ADF may have a detrimental effect on the user’s trust in the ADF and even the vehicle guidance as a whole.

There are many possible concepts for activating and deactivating the ADF, but the safety of the transition of control should not be overlooked while designing this part of the HVI. Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);
- Guidelines for In-vehicle Display Systems — Version 3.0 (JAMA 2004);
- Adaptive D3.3 (Kelsch et al., 2017).

Question 4-1-3	Relevant Phase(s)	CO			
Is the visual interface designed to be easy to read and interpret? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Do the text size, aspect ratio and contrast designed follow the standards?</li> <li>• Are commonly accepted or standardised symbols used?</li> <li>• Are non-standard symbols supplemented by additional text explanations?</li> <li>• Are the texts and symbols designed to be easily readable and understandable from the user's seating position?</li> <li>• Is the visual interface designed to have a sufficient contrast in luminance and/or colour between foreground and background?</li> <li>• Are the messages designed to convey the correct information in the language of the users?</li> </ul>			

	<ul style="list-style-type: none"> <li>• Are text messages designed to be as short as possible?</li> <li>• Are HVI elements grouped together based upon their function?</li> </ul>
--	--

This question focuses on the importance of having a clear strategy for the visual HVI. Guidelines and standards need to be followed to ensure that the visual feedback is easy and intuitive to understand. Icons can be designed to be interpreted quickly if standard symbols and colours are used where possible. Where icons cannot be used, text messages shall be used. However, it is important that the text can be understood in short glances, so that the driver is not forced to remove the eyes from the road for extended periods of time. Finally, it is important to cluster relevant HVI elements in similar locations so that the driver can intuitively understand where a HVI should appear. It can be confusing if the HVI is spread across different locations as the driver may then have to check in multiple locations for the HVI feedback, leading to a longer period of time where the driver is distracted from the road. Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);
- Guidelines for In-vehicle Display Systems — Version 3.0 (JAMA 2004);
- AdaptIVe D3.3 (Kelsch et al., 2017).

Question 4-1-4	Relevant Phase(s)	CO			
<p>Is the HVI designed to portray the urgency of the message?</p> <p>( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Are the semantics and tone of a message designed to be in accordance with its urgency?</li> <li>• Are high priority messages presented in a multimodal way?</li> <li>• Are communications of sensor failures, their consequences and required user steps considered? Are warning messages designed to orient the user towards the source of danger?</li> <li>• Are messages containing high priority information positioned close enough to the user's line of sight?</li> </ul>			

During the use of an ADF the user may be subject to many types of HVI feedback with various levels of urgency. It is important that the driver understands which HVI elements are high priority and are conveying urgent feedback to the driver. Equally, it is important that the driver understands that other messages are provided primarily for informational purposes



and therefore do not require immediate action. The urgency of the message can be portrayed in numerous ways and when choosing the most appropriate way it is useful to consider the scenario in which the urgent feedback will be provided. A simple example is an urgent transfer of control where the driver needs to re-gain situational awareness in a very short period of time. In this situation visual feedback will not be sufficient. A multi-modal feedback approach would be much more effective.

Feedback can be designed to help orient the driver to the source of danger using directional audio or strategically placed visual or haptic feedback. In other scenarios, in which the driver is engaged in the driving task, it might be more effective to position the visual feedback in a position closer to the line of sight to minimise eyes off the road time.

Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);
- Guidelines for In-vehicle Display Systems — Version 3.0 (JAMA 2004);
- AdaptIVe D3.3 (Kelsch et al., 2017).

Question 4-1-5	Relevant Phase(s)				VV	
Is the user acceptance of ADF assessed? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is the user acceptance assessed as part of a customer clinic?</li> <li>• Is the user acceptance assessed based upon the guidelines in the CpP questions?</li> <li>• Is it determined that users are willing to use the ADF?</li> </ul>				

The impact of the HVI on the user acceptance of the ADF has previously been eluded to, but assessing the user acceptance of the ADF should not be overlooked. Customer clinics, heuristic expert assessments and various other user trials can be carried out to gain both subjective and objective data on user acceptance. Having a clear and high quality HVI which meets all the guidelines outlined in this CoP and the additional material is a good first step to ensuring user acceptance. It is crucial that this exercise is completed before the ADF is introduced to the market to ensure that customers are able to trust the ADF and are willing to use it. It is worth noting that even if the HVI meets the correct standard, the user acceptance is also heavily influenced by many other factors.

Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- L3 HMI Test protocol (Naujoks et al.,, 2019-3).

#### 4.5.2 Mode Awareness, Trust & Misuse

This topic addresses the correct understanding of the role shared between the user and the ADF, as well as the correct usage of the ADF. Alongside the main question, the sub-questions shall also be carefully addressed.

Question 4-2-1	Relevant Phase(s)	DF				
Are all possible automated driving modes explicitly defined in terms of how the driver should acknowledge them? ( ) Yes / ( ) No						

The goal of this question is to ensure that the possible AD modes are clearly defined not only from an engineering viewpoint but also from a user's perspective. It is important that a user is aware of the possible automated driving modes of the ADF to avoid misunderstandings. This is the first step which provides the users with an overview of the ADF, to grasp its capabilities as well as the driver's roles. The driver's role may vary depending on the automated driving mode. Additional information regarding this topic is provided by:

- Ford Safety report (Ford 2018).

Question 4-2-2	Relevant Phase(s)	DF				
Are the modalities to communicate the relevant active (automated) driving modes described? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are the communication ways to the driver about the relevant active (automated) driving modes described?</li> </ul>				

This question focuses on how the currently active automated driving modes are communicated to both the driver and the other road users, in terms of modalities (visual, auditory, haptic, and so on). It is important that these communication ways are considered from the definition phase because the chosen modality will impact both the hardware and the software of the vehicle.

Additional information regarding this topic is provided by:

- Ford Safety report (Ford 2018);
- GM Safety report (GM 2018).

Question 4-2-3	Relevant Phase(s)	DF				
Are all the reasonably foreseeable mistakes and misuse cases of the ADF in relation to the HVI described? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are all of the possible driver mistakes related to the HVI considered?</li> <li>• Are all of the possible driver failures related to the HVI considered?</li> </ul>				

	<ul style="list-style-type: none"> <li>Are all of the possible intentional misuse cases considered?</li> </ul>
--	--

The purpose of this question is to ensure that possible driver mistakes, failures and misuses have been addressed in the best possible way, in order to be able to define countermeasures for them. Additional information regarding this topic is provided by:

- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);
- CoP ADAS (Knapp et al., 2009).

Question 4-2-4	Relevant Phase(s)	DF				
Is the impact of HVI on relevant driver indicators (e.g. eyes-on-road time) described? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Are possible HVI countermeasures to mitigate driver distraction considered?</li> </ul>				

This question is related to the negative and positive impacts that a HVI has on important indicators. The purpose is to trigger a definition of important indicators, related to driver distraction, situational awareness and “in-the-loop” level, and to study the impact and the countermeasures that should be implemented.

Additional information regarding this topic is provided by:

- Human Factors Design Guidance for Driver-Vehicle Interfaces (Campbell et al., 2016).

Question 4-2-5	Relevant Phase(s)	DF	CO	DS	VV	
Is an appropriate and clear way to communicate the automated driving modes to the driver investigated and confirmed? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Are the appropriate number of different automated driving modes communicated to the driver investigated and confirmed?</li> <li>Is the necessity, to permanently display to the driver the active automated driving mode, investigated and confirmed?</li> <li>Is the necessity, to communicate to the driver the automated driving mode changes, investigated and confirmed?</li> <li>Is the appropriate recognition by the driver of automated driving mode changes investigated and confirmed?</li> <li>Is the appropriate recognition by other road users of the active automated driving mode investigated and confirmed?</li> <li>Is the current function mode designed to display continuously to the user?</li> </ul>				

	<ul style="list-style-type: none"> <li>• Is communication of mode changes easily and quickly recognised by the users?</li> <li>• Are colours used to communicate function states in accordance with common conventions and stereotypes?</li> </ul>
--	--

For ADF, a clear communication of the mode is crucial. The driver must understand when he / she is in control of the vehicle and when a transfer of control occurs. If the mode is not clearly understood by the driver, the results could lead to an incident. There are many ways to communicate the mode to the driver and these should be considered when defining the HVI.

This question focuses on the HVI to communicate the AD modes, the consideration of a permanent display of the modes, how to communicate the mode changes, and how well these HVI are recognised by both the driver and other road users. This question focuses on more details in comparison to question 4-2-2, which focuses on the modalities (visual, auditory, haptic etc.).

In the later stages of development, the clarity of mode should also be assessed with a high level of scrutiny to ensure that there is no ambiguity. A test procedure to assess that basic mode indicators are capable of informing the driver about relevant modes and transitions has been proposed by Naujoks et al., (2019-3). Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- L3 HMI Test protocol (Naujoks et al., 2019-4)
- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);
- Guidelines for In-vehicle Display Systems — Version 3.0 (JAMA 2004);
- AdaptIVe D3.3 (Kelsch et al., 2017).

Question 4-2-6	Relevant Phase(s)	CO			
Is a multimodal HVI to improve driver alertness and time to get back in-the-loop investigated? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are different HVI modality combinations investigated?</li> <li>• Is speech being considered for a TOR?</li> </ul>			

The purpose of this question is to draw the attention on the crucial topic related to whether the driver is “in-the-loop”, and how to help the driver to get back “in-the-loop”.

Of course, the necessary uninterrupted time span of the driver being “in-the-loop” can vary depending on the situation and on the capability of the function, among others. Nevertheless, it is important to recognise this necessary level, and to ensure it, because it is strongly related to safety.

The driver is supposed to be kept “in-the-loop” as much as possible during stretches of automated driving, not only during and after a TOR. In case of an unplanned take over event, this would be needed (until Level 3) in order to shorten the time that drivers would need to gain back the necessary alertness / awareness.

On the other hand, it shall not be forgotten that the HVI is assumed to be not more intrusive than necessary. It should not be a burden, but rather an aid to the users. It is therefore necessary to find a (good) balance between the effectiveness of the HVI, and the level of annoyance that it may cause the users, including the passengers. Speech is another possibility to communicate a TOR.

Additional information regarding this topic is provided by:

- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);
- A method to improve driver's situation awareness in automated driving (Yan et al., 2017).

Question 4-2-7	Relevant Phase(s)	CO			
Is the ODD information provided to the driver considered? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is the information provided to the driver about the vehicle currently being in the ODD investigated?</li> <li>• Is the information provided to the driver about the start of the next ODD investigated?</li> <li>• Is the information provided to the driver about the end of the current ODD investigated?</li> </ul>			

The purpose of this question is to consider how and to what extent the ODD information should be displayed to the driver. Three major kinds of information are especially relevant:

1. The vehicle is currently in the ODD: the function should inform the driver so that the driver can decide whether to activate the function.
2. The vehicle is not yet in the ODD but will soon get into the next one: the function should inform the driver so that the driver can get ready for it and possibly decide to activate the function.
3. The vehicle is currently in the ODD, and the end of the current ODD is known: the function should inform the driver so that the driver can prepare for taking over the controls.

Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- L3 HMI Test protocol (Naujoks et al., 2019-3).

Question 4-2-8	Relevant Phase(s)		CO			
Is the information provided to the driver about an ADF-initiated MRM being considered? ( ) Yes / ( ) No						

A MRM typically happens if the driver fails to appropriately take over the controls, or if the function does not have enough time to make a proper TOR (for example due to a sudden unexpected situation). This question aims to consider how to inform the driver in case the function has initiated the MRM in order to provide the driver with the necessary information, such as what is going on, why, and what the driver could do after that.

Question 4-2-9	Relevant Phase(s)		CO	DS	VV	
Is the communication to the driver, of the driver's responsibilities in each defined automated driving mode(s) investigated and confirmed? ( ) Yes / ( ) No						

One of the crucial aspects of HVI is to make sure that the driver fully understands her / his responsibilities during each of the defined AD modes, and therefore to understand the function's capabilities under these modes. Drivers may be informed by several means, including advertisement and owner's manual written explanations. Drivers may get explicit information by the in-vehicle HVI, during the AD activation itself, just before and just after it. Drivers may of course also learn by experience. Additionally, a simple and intuitive HVI can help the drivers understand the situation and take the correct actions with respect to it. This concept complements the above mentioned concept of situational awareness and "in-the-loop" (4.2.6). Additional information regarding this topic is provided by:

- A method to improve driver's situation awareness in automated driving (Yan et al., 2017);
- Ford Safety Report (Ford 2018).

Question 4-2-10	Relevant Phase(s)	CO			
Is the impact that driving scenarios have on driver's understanding of the automated driving modes communication being investigated? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is there different feedback information to the driver depending on the driving scenarios investigated?</li> </ul>			

The purpose of this question is that the driving scenarios may impact the way and the level drivers understand the communication provided by the ADF. Typically, a more critical situation would require more attention and – if necessary – a faster reaction from the driver. In order to ensure these, the displayed feedback information needs to be appropriate and according to the situation.

Additional information regarding this topic is provided by:

- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016).

Question 4-2-11	Relevant Phase(s)	CO			
Is driver awareness of automated driving modes being investigated? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>•</li> </ul>			

Driver awareness is a very important topic. Other than “situational awareness” treated by questions 4-2-6 and 4-2-10 , it is extremely important to ensure driver “mode awareness”, as previous addressed by questions 4-2-1, 4-2-2, 4-2-5, 4-2-11. Question 4-2-13 focuses on the resulting awareness, and the need to confirm, for example by clinics and/or by experts, what has been previously assumed.

Question 4-2-12	Relevant Phase(s)			VV	
Are driver expectations regarding the ADF's features considered? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Does the function provide the information the driver is expecting?</li> <li>• Can the driver easily find the necessary information?</li> <li>• Is the information presented in such a way as to not annoy or distract the driver?</li> </ul>			

During the Validation and Verification Phase, it is important to confirm whether users' expectations are met. This is a very broad subject that would need to be narrowed down to precise specifications, and this question is there to make sure that the process will be

considered. In terms of Human-Vehicle Integration, for example the balance between the amount of information and its conciseness or simplicity can be considered. Additional information regarding this topic is provided by:

- SP3 Input to CoP (see Annex 1).

Question 4-2-13	Relevant Phase(s)				VV	
Are the drivers' trust in the ADF being investigated? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is the ADF trusted by the driver?</li> <li>• Is the ADF not over-trusted?</li> </ul>				

Trust is also a very crucial aspect. It is necessary that the users trust the function, so that they will use it. On the other hand, it is necessary to avoid over-trust, as this may lead to unintended misuse of the function. Again, a good balance must be targeted in order to ensure the correct amount of trust. Additional information regarding this topic is provided by:

- Ford Safety Report (Ford 2018).

Question 4-2-14	Relevant Phase(s)				VV	
Is the appropriate usage of the ADF by customers confirmed? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is the appropriate usage of the system sufficiently described in the user manual?</li> <li>• Are other methods of conveying the appropriate usage to the customer considered?</li> <li>• Is there a way to give immediate feedback to the driver when using the ADF in an inappropriate way (e.g. HMI message)?</li> <li>• Is there a feedback loop to the OEM in case the ADF is used in an inappropriate manner?</li> </ul>				

This question is a general summary confirming that customers would appropriately use the ADF. Also, they shall not misuse the system. In order to make sure the appropriate usage is known, the user manual shall contain a description of how to appropriately use the ADF. In the event the customers do not read the manual, we need to ensure that other methods are available to ensure that customers use the ADF appropriately. There must be direct and immediate feedback, for instance via the vehicle HMI to the driver, in case the ADF is misused. Statistics shall be gathered via the vehicle to inform the OEM about the about the occurrence of misuse. The measures can be taken to prevent further misuse.



Question 4-2-15	Relevant Phase(s)					PS
Are long-term effects of the ADF on the customers investigated? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>Are all the appropriate metrics to evaluate the long-term effects of the ADF considered?                ...in terms of driving skill degradation?                ...in terms of trust in the function?                ...in terms of misuse of the function?</li> </ul>				

Long-term effects of the AD function need to be fully understood. Every opportunity shall be used to continuously improve the functions, by understanding these effects and applying appropriate countermeasures. Designers, developers and evaluators do the utmost to release a mature function to the market, minimising the negative effects of ADF as much as possible. Nevertheless, the actual impact on real customers shall be continuously monitored, and measures need to be applied in order to do so. Typically, the main risks of long-term effects are skill degradation and building over-trust in the function.

Additional information regarding this topic is provided by:

- CoP ADAS (Knapp et al., 2009).

Question 4-2-16	Relevant Phase(s)					PS
Is the HVI impact on driver workload over long journeys being investigated? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li></li> </ul>				

This question is addressing the impact of the HVI over long journeys. It could be investigated by taking advantage of dedicated fleets with typically long travel times, for example.

Additional information regarding this topic is provided by:

- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016).

### 4.5.3 Driver Monitoring

This topic addresses the correct understanding of driver monitoring, specifically the identification and classification of the cognitive status of the driver and the recognition of the actions made inside the vehicle. This consists of several questions; however, the sub-questions shall be carefully addressed as well.

Real time monitoring of a driver's intention / attention is a crucial topic, especially when discussing automated driving. In fact, not only is driver distraction one of the main causes of accidents on the roads, but also the knowledge of driver status is fundamental before a TOR is issued. Since driving is a complex phenomenon, involving the performance of various tasks (including simultaneous quick and accurate decision making), fatigue, workload and

distraction drastically increase human response time, which results in an inability to drive correctly and – above all – to respond properly to a TOR.

Question 4-3-1	Relevant Phase(s)	DF				
Are all relevant secondary tasks considered? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Are plausible secondary tasks possible today and in the near future taken into account?</li> <li>• Which secondary tasks are legal and in what timeframe will they become legal?</li> <li>• Which metrics shall be measured via a driver monitoring function?</li> <li>• Are the metrics appropriate for the automated driving function defined?</li> <li>• Which apps/secondary tasks can be integrated into the vehicle HVI?</li> </ul>				

This question (and related sub-questions) addresses which secondary tasks are allowed during automated driving (at least from SAE level 3). The idea is to consider what is currently available and what will become available in the future. In addition, one sub-question focuses on metrics that shall be considered, when a driver monitoring function is on-board. It is important to address these items from the beginning of the function development (definition phase). Moreover, the possibility to add additional apps/secondary tasks to the vehicle HVI in the future should be considered as well.

Question 4-3-2	Relevant Phase(s)	CO	VV			
Is the HVI connected with the driver monitoring function? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Does it give feedback to the driver?</li> <li>• Are unusual driver states (e.g. drowsiness) communicated to the driver?</li> </ul>				

It is essential to provide crucial information on driver's state directly to the driver – for example drowsiness – because driver impairment (even if only temporarily) can compromise the safety of the ego-vehicle and other traffic participants (e.g. driver is sleeping when a TOR is issued by the ADF). These unusual driver states (e.g. drowsiness) need to be communicated effectively to the driver.

Question 4-3-3	Relevant Phase(s)	CO				
Is it possible to mirror the customers' devices on the vehicle HVI? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is it possible to restrict certain apps or certain activities altogether (e.g. laptop) in general due to their potential distraction level?</li> </ul>				

	<ul style="list-style-type: none"> <li>• In cases where mirroring is possible, is the content restricted according to the driving mode?</li> <li>• Is it possible to show warning messages despite the mirroring?</li> </ul>
--	--

This question focuses on the problem of mirroring contents / apps from user's own mobile device directly on to the vehicle's display(s), especially if some mobile content can create a strong potential distraction level. This issue has to be considered when a TOR is provided by the ADF with particular attention (e.g. in a situation, when the ADF leaves its ODD). The crucial questions are: can the mirroring be limited? If allowed, how can the driver be taken back into the control loop?

Question 4-3-4	Relevant Phase(s)				VV	
Is the impact of typical secondary tasks on take-over time(s) and quality identified? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Is a customer clinic or expert assessment data available on this?</li> <li>• Can this be simulated?</li> </ul>				

Strongly related to the previous question, we need to measure and to understand the impact of secondary tasks on the TOR provided by the function in the validation phase. From here, an answer to the previous point can be given: if the impact is high (i.e. affecting the vehicle safety) some secondary tasks (e.g. mirroring) shall be forbidden.

Question 4-3-5	Relevant Phase(s)					PS
Can data be measured after the start of production to assess the usage of secondary tasks and their impact on driving behaviour, traffic safety, etc.? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Is there consideration for which types of data should be measured after the start of production?</li> </ul>				

The last question of the driver monitoring section is related to measuring the long term effects of secondary tasks on driver behaviour, considering data if available. The selection of appropriate data for this long-term evaluation aims at continuously monitoring the actual impact on real customers.

As aforementioned, long-term effects (at every automation level, including allowed secondary tasks) of the ADF have to be fully understood, in order to continuously improve the functions, by understanding these effects and applying appropriate countermeasures.

Additional information regarding the topic mentioned in the questions is provided by:

- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016);

- A method to improve driver's situation awareness in automated driving (Yan et al., 2017);
- SIP-adus HMI 2017 report (SIP-adus 2017);
- Effects of system information on drivers' behaviour (Makoto 2017);
- Evaluation of driver's condition and keeping driver's state by HMI (Sato 2017);
- Driver distraction and inattention in the realm of automated driving (Cunningham 2018);
- Real-time Driver Drowsiness Detection for Embedded System Using Model Compression of Deep Neural Networks (Reddy et al., 2017);
- Real-time detection of driver distraction: random projections for pseudo-inversion-based neural training (Botta et al., 2019);
- MIT Advanced Vehicle Technology Study: Large-Scale Naturalistic Driving Study of Driver Behavior and Interaction with Automation (Fridman et al., 2019);
- Driver Fatigue Detection based on Eye State Recognition (Zhang et al 2017).

#### 4.5.4 Controllability & Customer Clinics

Level 3 automated driving will still require the driver to take over the driving task in case of system failures and malfunctions. Thus, it has to be ensured that drivers are able to control transitions to manual or assisted driving and avoid safety critical consequences with regards to themselves, passengers and other road users. Driver-initiated transitions should also be considered from this perspective. This chapter outlines measures to support the controllability of Level 3 ADF in different levels of the development cycle.

Question 4-4-1	Relevant Phase(s)	DF				
Are user needs regarding controllability taken into account in the definition phase? ( ) Yes / ( ) No		<ul style="list-style-type: none"> <li>• Is controllability of function limits / failures from L3 to lower levels of automation considered in the design phase?</li> <li>• Are human factors design guidelines followed when defining user needs regarding these transitions?</li> <li>• Are potential users of the ADF and samples for customer clinics selected based on adequate data (e.g. market research)?</li> </ul>				

During the definition phase, it should be ensured that user needs regarding controllability are taken into account. For example, the design of the HVI should consider the transition from automated driving to lower levels of automations with respect to function failures / limits as well as driver-initiated transition. Relevant and applicable guidelines for the design of the HVI should be considered in the design phase in order to ensure that they are in line with

generally accepted standards and best practices in view of the targeted user population. Additional information regarding this topic is provided by:

- Procedure to define use cases (Naujoks et al., 2018-1);
- Ko-HAF Procedure to define test cases (Gold et al., 2017);
- L3 HMI Checklist (Naujoks et al., 2019-1);
- CoP ADAS (Knapp et al., 2009).

Question 4-4-2	Relevant Phase(s)	CO			
<p>Are the limitations of the human driver taken into account based on available guidelines? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Is colour blindness considered by avoiding non-suitable colour combinations?</li> <li>• Is visual impairment considered by choosing sufficiently large enough text and icons for visually impaired drivers?</li> <li>• Is it ensured that the flash rate of icons does not cause epilepsy or similar conditions?</li> <li>• Is it ensured that the audio tones can be perceived by individuals without a full hearing range?</li> <li>• Is the controllability in the case of a function failure also ensured for a driver with impaired capability (e.g. elderly person, acute medical conditions or motion sickness)?</li> </ul>			

The concept selection should be based on a careful consideration of the driver's sensory and motor limitations. The concept selection should thus consider topics like colour-blindness, general vision, sensory-motor and hearing impairments. Additional information regarding this topic is provided by:

- L3 HMI Checklist (Naujoks et al., 2019-1);
- CoP ADAS (Knapp et al., 2009).

Question 4-4-3	Relevant Phase(s)	CO			
<p>Is the driver informed about function limits that will trigger requests to intervene? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Does the user manual describe the functions, handling and limits in an understandable way?</li> <li>• Is the driver informed if a detectable function malfunction or function limit occurs?</li> </ul>			

The concept selection phase should also account for a clear and understandable description of the ADF and its limits. These should be described in the user manual, together with a description of the expected reaction. This also comprises the selection of a transition-of-control concept in case of reaching ADF limits. Additional information regarding this topic is provided by:

- CoP ADAS (Knapp et al., 2009).

Question 4-4-4	Relevant Phase(s)	CO			
<p>Is the vehicle controllable in the case of a function malfunction or limit by overruling or switching off the function? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Is it possible for the driver to deactivate or take back control of an ADF at any time?</li> <li>• Is it ensured that driver actions, which should overrule the function or take back manual control, are intuitive?</li> <li>• Is the possibility of function activation or deactivation in situations, in which it would lead to potentially hazardous driving conditions, considered in the concept selection?</li> </ul>			

In addition to a control concept in case of ADF malfunction, the design phase should consider the safety of driver-initiated overrides and deactivations of the ADF (i.e. an interaction concept for deactivation and overriding should be defined). For example, it should be ensured that the user can take back control in an intuitive way to ensure an efficient transition. Additional information regarding this topic is provided by:

- CoP ADAS (Knapp et al., 2009).

Question 4-4-5	Relevant Phase(s)	CO			
<p>Does the behaviour of the ADF lead to non-controllable situations from the perspective of other road users? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Is the vehicle behaviour predictable for other road users if they do not know whether the vehicle was equipped or not equipped with the function?</li> <li>• Is the reaction performance of other road users sufficient to interact with a vehicle that is equipped with a rapidly (hard, intensive) reacting ADF?</li> </ul>			

The design phase should also consider the limitations and perception of other traffic participants that are not equipped with an ADF. The automated vehicle's behaviour should be designed in a way that it is controllable for these traffic participants and does not exceed motion ranges of non-equipped drivers in non-emergency situations. Additional information regarding this topic is provided by:

- CoP ADAS (Knapp et al., 2009).

Question 4-4-6	Relevant Phase(s)			DS	
Is it possible to preliminarily verify the concept based on expert controllability assessments? ( ) Yes / ( ) No					
					<ul style="list-style-type: none"> <li>• Are preliminary controllability assessments and according concept changes carried out during design iterations?</li> <li>• Is the fidelity of the prototype sufficient?</li> <li>• Are function limits, function failures, but also normal transitions being taken into account?</li> </ul>

In the design phase, a preliminary assessment of the controllability should be carried out, which is normally based on expert assessments. For these, a suitable prototype should be used that allows for an assessment of function limits / failures, but also normal driver-initiated transitions. Additional information regarding this topic is provided by:

- Controllability test methods (Bengler et al., 2018);
- Expert-based Controllability Rating (Naujoks et al., 2018-2);
- CoP ADAS (Knapp et al., 2009).

Question 4-4-7	Relevant Phase(s)				VV
Are the testing environments for controllability confirmation tests suitable? ( ) Yes / ( ) No					
					<ul style="list-style-type: none"> <li>• Are the venues for the customer clinics adequate (laboratory, test track etc.)?</li> <li>• Are adequate precautions taken for real world testing, especially with naive participants?</li> </ul>

In the verification phase, controllability assessments should be carried out in suitable test environments. When these are carried out on test tracks or on public roads, precautions regarding the safety of participants and other road users should be taken. Additional information regarding this topic is provided by:

- Controllability test methods (Bengler et al., 2018);
- CoP ADAS (Knapp et al., 2009).

Question 4-4-8	Relevant Phase(s)				VV	
<p>Is it possible to sign-off the controllability based on customer clinic results and/or expert assessments? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Can function outputs and information be perceived by the drivers quickly enough to enable them to react appropriately (e.g. take over request)?</li> <li>• Is it possible to verify that drivers respond when they are required to retake control (success of take-over)?</li> <li>• Are the function limits clearly understandable for the driver?</li> <li>• Have the drivers' behaviour adaptation over time with respect to ADF's limit been considered?</li> <li>• Are the limitations of correct operation / function limits comprehensible and predictable for the driver in different environments, weather and visibility conditions (e.g. fog, animals on the road)?</li> <li>• Can the driver control the function after a transition from full function functionality to a degraded mode?</li> <li>• Can the driver control the function after an unintended or accidental function deactivation?</li> <li>• Can the driver control the function if they want to activate the automated driving function and it is not available? This refers especially to the situation in which the driver is not informed that the function is unavailable?</li> <li>• Is a MRM initiated by the ADF controllable?</li> <li>• Are function reactions understood by other road users? If not, can they still control the situation (e.g. function based deceleration without activation of brake lights)?</li> </ul>				

The final controllability verification can be based on different evaluation methods such as expert assessments or controllability verification tests. A variety of use-cases that are listed in the table above should be considered. Additional information regarding this topic is provided by:

- Expert-based Controllability Rating (Naujoks et al., 2018-2);



- Ko-HAF Procedure to define test cases (Gold et al., 2017);
- CoP ADAS (Knapp et al., 2009).

Question 4-4-9	Relevant Phase(s)					PS
Is the ADF adequately evaluated from a human factors perspective after the start of production? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Is there any skill degradation due to the use of the ADF?</li> <li>• Is there misuse of the ADF?</li> <li>• Are there long-term effects on driver behaviour and on the usage of the ADF?</li> </ul>				

A suitable post-production evaluation strategy should be implemented that assesses the impact of the ADF on possible negative behavioural adaptations such as skill degradation and misuse. Additional information regarding this topic is provided by:

- CoP ADAS (Knapp et al., 2009).

#### 4.5.5 Driver Training & Variability of Users

This topic covers the training required for users and the variability of ADF users to be taken into account. Firstly, the training aspect is about the issue of providing users with the appropriate knowledge and skills to operate an ADF, if necessary. Secondly, there is a huge variability of the users, as different age groups, gender, cultural backgrounds and previous experiences need to be addressed. Both topics are interrelated and thus combined in one category.

Question 4-5-1	Relevant Phase(s)	DF				
Is the impact of different user groups taken into account? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Is the impact of different countries, regions and their respective cultures taken into account?</li> <li>• Are different age groups and their needs taken into account?</li> <li>• Are differences in the users' physical dimensions, anthropometry and (dis-)abilities taken into account?</li> </ul>				

Firstly, these questions target the difference between countries and regions. Infrastructural differences with regard to roads, traffic control functions and driver behaviour in general have a huge impact on the design of ADFs. These differences need to be handled appropriately. An ADF designed with only a specific country or region without taking into account the respective infrastructures and the needs and behaviours of their user groups must be avoided. Secondly, there is a general trend towards an aging population. In addition, the elderly prefer to drive their own vehicles for transportation. Due to degrading physical

abilities, this becomes more cumbersome. During the definition of ADFs, physical impairments of elderly drivers need to be taken into account. Appropriate countermeasures, if necessary, must be defined. Thirdly, there is a significant variability in users' physical dimensions and anthropometry. Size and strength differences between genders can play a role. The ADF shall be designed to be operated by variety of different users. This also includes non-age related disabilities. Additional information regarding this topic is provided by:

- Code of Practice for the Design and Evaluation of ADAS (Knapp et al., 2009).

Question 4-5-2	Relevant Phase(s)	CO	DS	
<p>Is the information that the user needs to operate the ADF available to create a training course? ( ) Yes / ( ) No</p>		<ul style="list-style-type: none"> <li>• Is there a training course needed for test drivers?</li> <li>• Is there a driver training course for ordinary users planned?</li> <li>• Is a process to train users of an ADF established?</li> <li>• Are the possible training methods for the user defined (e.g. dealer training, online material for home training, material in car, manual, use of virtual reality, digital assistants etc.)?</li> </ul>		

User training for the ADF requires a specification of the ADF's operation. This serves as a baseline to create a user training, if it is deemed necessary. Due to the complexity of ADFs, a user training course might be required or at least recommended. In case such a training course is regarded as necessary, appropriate measures need to be taken to realise it. Furthermore, the training methods shall be defined in more detail. This may range from a training course provided by the dealer to user manuals integrated within the vehicle, online material for home training, the use of digital assistants and many more. A reasonable combination of training methods shall be considered taking individual learning preferences into account.

Additional information regarding this topic is provided by:

- SIP-adus HMI 2017 report (SIP-adus 2017);
- Effects of function information on drivers' behaviour (Brusque et al., 2007);
- Code of Practice for the Design and Evaluation of ADAS (Knapp et al., 2009);
- Human Factors Design Guidance For Driver-Vehicle Interfaces (Campbell et al., 2016).

Question 4-5-3	Relevant Phase(s)	CO			
Is a representative test sample for customer studies ensured, taking into account demographic variables such as age, gender etc? <input type="checkbox"/> Yes / <input type="checkbox"/> No					

Due to the high variability of users, customer studies evaluating the ADF need to take into account various factors. Depending on the exact customer study to be conducted, this may range from age, gender, socio-cultural background to previous experience with ADFs or computers in general. Additional information regarding this topic is provided by:

- Code of Practice for the Design and Evaluation of ADAS (Knapp et al., 2009).

Question 4-5-4	Relevant Phase(s)					PS
Is a solid mix of customer education and information made available to the users post start of production? <input type="checkbox"/> Yes / <input type="checkbox"/> No		<ul style="list-style-type: none"> <li>• Is user information and training supported with appropriate information by marketing raising realistic expectations?</li> <li>• Is training material made available inside the car (e.g. integrated into infotainment functionality)?</li> </ul>				

Developers shall ensure that there is enough information available for the users of an ADF to properly operate it. There shall be sufficient training material available inside the vehicle to provide users with the required knowledge to operate the ADF quickly and safely on the road. Marketing a new ADF might tempt people to over-estimate the possibilities offered by the function. To prevent this, marketing shall support user information and training with realistic information regarding its abilities. This is aimed at e.g. at commercials and customer sales information guides. Additional information regarding this topic is provided by:

- Code of Practice for the Design and Evaluation of ADAS (Knapp et al., 2009);
- Ford Safety Report (Ford 2018);
- GM Safety Report (GM 2018).

## 5 Pilot application of draft CoP-AD

This chapter reports on the application of the draft CoP-AD in the L3Pilot project. For this purpose a questionnaire was prepared. The questionnaire was discussed with key persons of the project (e.g. subproject leaders, vehicle manufactures). In addition, there were direct contributions from other L3Pilot subprojects. More details are reported in chapter 5.1.

Both inputs were used to identify which CoP-AD questions are relevant in the context of the L3Pilot project and how they should be managed in L3Pilot. The scope of the L3Pilot project – testing of automated driving function prototypes on public roads – automatically limits the overlap of CoP-AD topics, since the CoP itself is intended to cover the entire development process. There are further aspects that need to be taken into account when the pilot application in L3Pilot is analysed. These aspects are reported in subchapter 5.2, together with an overview about the CoP-AD topics that have been addressed in L3Pilot. The final subchapter 5.3 reports how each of the topics addressed have been handled in the project, and whether the L3Pilot is in line with the approach suggested by the CoP-AD.

### 5.1 Process of information collection

The purpose of the information collection within the project was to check which topics of the draft CoP-AD have been addressed in the L3Pilot and how they have been approached in the project. For this purpose, the status of the project has been reviewed considering the CoP-AD questions. The information used for this review is based on the following pillars:

1. Information that SP2 partners have due to their involvement in the other subprojects.
2. A questionnaire that has been prepared and sent out to the partners in order to collect more detailed information about which topics have been approached. Addressees of the questionnaire have been the subproject leaders as well as the owners of test vehicles.
3. Information directly transferred to SP2 from other subprojects. For instance SP3 “Methodology” provided a rating of the applicability of test tools for different assessment in the pilot.

All the received information has been clustered and evaluated. Based on this consolidated feedback, the extent to which questions of the draft CoP-AD are in the scope of L3Pilot have been assessed and how they have been handled in the project. The results are presented in the following sub-chapters in a condensed form.

### 5.2 Identification of relevant topics for L3Pilot

The L3Pilot project aims at testing automated driving functions on public roads with different users. The prerequisite for this project is that prototype vehicles with an ADF are available for testing. The vehicles are technically equipped or updated during the project to comply with the testing requirements. However, the more resource consuming development of the ADF is

not in the scope of the L3Pilot. This limits the topics of the CoP-AD that are addressed by L3Pilot itself.

A second challenge to the pilot application of the CoP-AD is that its writing and the testing activities have started in parallel to the L3Pilot project. This means that it has not been possible to provide the CoP-AD at the beginning and to check later whether the CoP-AD has been followed throughout the course of the project. Instead, the approach taken and explained in this document has been to check to which extent the CoP-AD is in line with the independently taken L3Pilot approach. The results of this check are going to be an important input for the final CoP-AD (L3Pilot deliverable D2.3 that is due in end of February 2021) which will be based on this draft version.

The third aspect related to the reporting of the application of the CoP-AD in L3Pilot that needs to be considered is that this draft document is due only approximately two years after the start of the project. The project will continue its work for an additional two years. Therefore, the application can only be reported up to the date when the draft document is due (October 2019).

An overview about the different topics of the CoP-AD and their relevance in L3Pilot is given in the following table. In order to provide a more detailed overview about the extent to which a certain topic has been relevant in L3Pilot, we distinguish between “not in the scope”, “partly in the scope” and “fully in the scope”.

*Table 5.1: Overview on topics of the CoP-AD that are relevant in L3Pilot.*

Topic	Not in the scope	Partly in the scope	Fully in the scope
<b>Category Overall Guideline and Recommendations</b>			
Minimal Risk Manoeuvre		X	
Documentation			X
Existing Standards			X
<b>Category ODD Vehicle Level</b>			
Requirements		X	
Scenarios and Limitations			X
Performance Criteria and Customer Expectations			X
Vehicle Architecture	X		
Testing (incl. Simulation)			X
<b>Category “ODD Traffic System Level &amp; Behavioural Design”</b>			
Automated Driving Risks and Coverage Interaction with Mixed Traffic		X	
V2X Interaction	X		
Traffic Simulation			X

Topic	Not in the scope	Partly in the scope	Fully in the scope
Ethics & other Traffic related Aspects			X
<b>Category “Safeguarding Automation”</b>			
Functional Safety		X	
Cybersecurity		X	
Implementation of Updates	X		
Safety of the intended Functionality (SOTIF)		X	
Data Recording, Privacy and Protection			X
<b>Category “Human-Vehicle Integration”</b>			
Guidelines for HVI	X		
Mode Awareness, Trust & Misuse		X	
Driver Monitoring			X
Controllability & Customer Clinics		X	
Driver Training & Variability of Users		X	

Considering the goal of the L3Pilot project, it is also obvious that the CoP-AD topics which are relevant are the ones to be addressed in the “Design Phase” and “Validation & Verification Phase”. It is in these final stages of a function development that the road tests typically take place. The “Definition Phase” and “Concept Selection Phase” shall at this stage normally be finished unless the evaluation has serious feedback on the design phase. The “Post Start of Production Phase” will not be reached in L3Pilot, since these functions will not be introduced in the market.

### 5.3 Results to pilot application of draft CoP-AD in L3Pilot

In the following section it is reported per category how L3Pilot has approached the different relevant topics.

#### 5.3.1 Overall Guideline and Recommendations

This category consists of three topics: the minimal risk manoeuvre, documentation and existing standards.

By definition, a level 4 ADF includes a minimal risk manoeuvre, but most of the level 4 functions in L3Pilot are for parking. Although L3Pilot tested ADF include a MRM and some of the tested level 3 ADF will include the possibility to initiate a MRM. The first of two questions (question 0-1-1 and 0-1-2) of the CoP-AD are out of the L3Pilot scope, since these are answered in early development stages.

The third question (0-1-3) for this topic is theoretically relevant for the testing in L3Pilot. Here, it could be investigated under which condition a MRM occurs. However, it must be

considered that in most of the tested vehicles, the vehicles are prototypes and do not have the level of performance they will have in a series production, and therefore have a safety driver (see Penttinen et al., 2019) who will supervise the ADF. Since it is still under discussion at which point in time the safety driver will intervene it is not clear, whether and how many MRM will be detected in the test data.

The questions 0-1-4 and 0-1-5 are partially relevant to the project. The test scenarios for motorway and urban driving include the MRM more in an implicitly way. Thus, the MRM might be activated during the operation on public roads, but it is not explicitly when to activate it. For the parking ADF it would also be possible to include tests for the MRM explicitly. Up to the current knowledge such MRM specific tests are not foreseen in the L3Pilot test. The reason is that this question addresses the aspects that the proper operation of the MRM shall be ensured. This needs to be done before any tests on public roads are conducted. Thus, the L3Pilot partners who include a MRM in their ADF will test the MRM before the actual road tests start. These tests are not reported in L3Pilot.

The second topic of this category, documentation is fully in the scope of L3Pilot. The first question 0-2-1 is implicitly requested by the different deliverables of the project. However, it must be noted that the results differ in a research project from company internal reports. The second question of the topic (question 0-2-2) is difficult to cover in a research project, since a research project always has a defined end. Nevertheless, the results of L3Pilot that are provided in terms of reports and data implemented will be used for future research outside the project. Furthermore, the companies involved will use the data and knowledge gained for future ADF development in addition to their defined processes.

The final topic of this category, existing standards, is fully in the scope of L3Pilot. The single CoP-AD question 0-3-1 of this topic deals with the compliance with existing standards. Regarding the function development and question, which standards have been followed, not explicitly information are reported in the project. However, in most cases the standards (e.g. ISO 26262 2018) are already covered and followed in the company internal development processes and guidelines. These processes and guidelines have been applied for the ADFs and prototype vehicles used in L3Pilot. Regarding the testing approach, L3Pilot follows the FESTA Handbook (Barnard et al., 2018), which defines the process for conducting field tests in Europe. For the work of this subproject (SP2) the existing documents are considered in the CoP-AD.

### **5.3.2 Category “ODD Vehicle Level”**

The category “ODD Vehicle Level” consists of five topics: requirements: scenarios and limits, performance criteria and customer expectation, vehicle architecture as well as testing.

The first category requirements cover aspects. First, there are the direct requirements for the function (e.g. questions 1-1-2, 1-1-5 and 1-1-7). These questions are relevant for the development of the ADF, which is not in the direct scope of the L3Pilot project, which instead focuses on the testing of the ADF. Obviously the requirements have to be taken into account



by the project, when defining the test and for the evaluation. The second type of question considers the requirements related to the ODD (e.g. question 1-1-8 and 1-1-9). Also, here the requirements are important for L3Pilot in the context of defining the right test environment. However, it is less of a focus for the project to define these requirements. However, the third type of question of this topic, which assesses whether risks are considered and tackled beforehand, is clearly in the scope of the project (e.g. questions 1-1-6), since tests in appropriated environments are essential before the actual pilot on public roads start. The tests have been carried out by manufacturers of the test vehicles individually. The question 1-1-11 has been approached individually by the partners. For instance, the training of the safety driver describes which scenarios (e.g. ISO lane change at different velocities) the potential safety driver must be capable to handle. For the question 1-1-12 the pilot will provide useful information, since the testing on public roads ensures that the ADF is confronted with a manifold of situations. It is also obvious that these experiences will be used to improve future ADFs, which provides the answer to the question 1-1-14. The question 1-1-13 is not directly in scope of L3Pilot, since during the pilot the vehicles will regularly return to the manufactures' workshops. Due to this and the fact that during the pilot for most vehicles someone from the L3Pilot staff will be in the vehicle (e.g. safety driver, investigator) the monitoring of the ADF is ensured anyway.

The questions of the scenario and limits topic are complete in the scope of L3Pilot. The limits of the ADF need to be known in order to define the test environment correctly (questions 1-2-1 and 1-2-2). The limitations have been described in the deliverable D4.1 (Griffon et al., 2019). The data that are logged during the pilot will reveal, whether these descriptions are also met by the tested ADF. At this point it must be borne in mind that the tested ADFs are still prototype functions and not serial production ADFs. Therefore, deviation is likely to occur. Regarding the identification of critical situations in the pilot (question 1-2-3) the methodology subproject has provided criteria to identify such situations. The process is based on two steps: 1. Numeric criteria to pre-select potential critical situations 2. Check video data, whether a situation has been critical or not. In addition a classification for take-over-situations has been defined, in order to assess controllability of this manoeuvre. More information about this are given in the deliverable D3.3 (Metz et al., 2019).

The topic performance criteria and customer expectations is also fully in the scope L3Pilot project. The aspect of the customer expectations (questions 1-3-1 and 1-3-5) is covered in a series of international surveys investigating people's expectations related to automated driving. More details can be found in the L3Pilot deliverable D3.3 (Metz et al., 2019). The performance criteria for the L3Pilot project have been defined in the deliverable D3.1 (Hilbert et al., 2018). The performance criteria are set up to investigate the technical / traffic performance and the user acceptance of the tested ADF (questions 1-3-2, 1-3-3 and 1-3-4). The criteria have been defined based on the research questions and related hypotheses of the projects and are going to be answered based on logged data of the pilot. However, it must be taken into account that the objectives of research projects and development process of serial products require different criteria. Thus, the general criteria of the L3Pilot



investigation of automated driving have only a limited applicability for serial production development.

The four topics of this category “vehicle architecture” are very much related to the development of ADFs, which is not in the scope of the L3Pilot project. It is obvious that test vehicles require a certain architecture and additional technology to integrate the ADF and the data acquisition systems for L3Pilot in the vehicle. However, due to confidentiality the method of integration is specific to each of the manufacturers of the L3Pilot test vehicles. This makes it hard to comment for the draft CoP-AD to what extent the questions are fulfilled. The overall fact that the test vehicles fulfil the architecture questions can be derived from the fact that they operate on public roads and that the data logging is operating properly.

The last topic “Testing” is the main purpose of the L3Pilot and therefore fully in the scope of the project. The test and evaluation concept has been defined by the methodology subproject in the deliverables D3.2 (Penttinen et al., 2019) and D3.3 (Metz et al., 2019) (question 1-5-1).

It must be noted that the L3Pilot should be considered as tests for the future development and rather than tests for certification.

The details of the pilot tests (questions 1-5-2, 1-5-3 and 1-5-5) are discussed between the manufacturers of the test vehicles and their selected SP3/7 partner. This process allows individual consideration of the ADF requirements, the national requirements (question 1-5-7) as well as to ensure that the requirements of the methodology and evaluation subproject are followed. With respect to the correct selection of test tools the methodology subproject team investigated different tools and provided an overview of appropriateness of tools per research question, which can be found in annex 1. To ensure the safest possible testing (question 1-5-6) safety concepts have been developed for the test vehicles and the ADF. The question, whether the test plans have correctly been implemented (question 1-5-4), can only be assessed at the end of the project. Simulations contribute heavily to the impact assessments in L3Pilot (questions 1-5-8 and 1-5-9). However, the simulated ADF is an artificial ADF that is defined based on the function’s descriptions of the ADF that are tested in the pilots. These so-called mature ADFs are simulated, since the objective is to provide a general result of the capabilities of ADFs and not results for one single implementation. The mature ADFs allow us to compensate expected shortcomings due to the prototype status of the tested ADF and due to this will be closer to the expected serial products. The mature ADFs do not consider AI technologies.

### **5.3.3 Category “ODD Traffic System Level & Behavioural Design”**

The first topic of the category is “automated driving risks and coverage interaction with mixed traffic”. This topic is in scope, since safe testing on public roads requires a careful consideration of the topic’s questions. In particular the risks associated with the pilot activities need to be analysed before testing (questions 2-1-1 and 2-1-2). The identified risks are tackled by means of the safety concept for the test. The risk and safety concept depend on

the capabilities of the tested ADF. It is obvious that testing a parking ADF is associated with different risks to an urban ADF. Therefore, the assessment of the risk and safety concept is done individually per ADF, which makes it impossible to have a common L3Pilot approach. It's important that the risk assessment does not only cover the ego vehicle, but accounts also for the surrounding traffic. Often in L3Pilot the approach taken is to use a safety driver that is capable of intervening in case of critical situations. A critical situation can be induced by the surrounding traffic as well as a malfunction during the automated operation of vehicle. Some partners in the project also consider using a second vehicle driving behind the automated vehicle to reduce possible risks for the surrounding vehicles (questions 2-1-3, 2-1-4 and 2-1-5). However, this could limit the pilot results related to the objective to investigate the interaction with non-automated road users.

The second part of the category is the V2X interaction. According to the deliverable D4.1 (Griffon et al., 2019) the pilot tested ADFs do not consider V2X interaction. Thus, this question is not in the scope of L3Pilot project. The only exception is that a show case related to V2X is planned. However, details of the show case are not known at this point of time. Therefore, it is not possible to make further statements related to the CoP-AD questions of this topic.

Traffic simulations are applied in L3Pilot for the impact assessment, which examines: efficiency, environmental impact, as well as the safety impact assessment (question 2-3-2). The impact assessment will be conducted at the end of the project. The traffic simulations are set up according to the state-of-the-art. This applies for the methodology as well as for the simulation tools (question 2-3-1). Further information is available in the L3Pilot deliverable D3.3 (Metz et al., 2019). The traffic simulation will cover different traffic scenarios that represent the traffic in Europe (question 2-3-3) Different evaluations of ADFs are not analysed. The aim of the impact assessment is to assess the potential of the technology. Therefore, so-called mature ADFs have been defined in the project based on the pilot tested prototype ADFs. These ADFs will be integrated in the simulation as software in the loop (questions 2-3-5 and 2-3-6). The data of the pilot will be used for setting up the scenarios with the correct values as well as to update the driver behaviour models for the surrounding traffic. This step is necessary to ensure the correct interaction of the non-automated traffic with the ADF (question 2-3-7). The validation and verification of the simulation tool is a key aspect for its effective use. This aspect is covered by the partners that apply traffic simulations in L3Pilot. However, the actual work of the validation and verification of the simulation tool is outside the scope of the L3Pilot project (question 2-3-4). Up to now, no external parties have been involved in the validation and verification process of the simulation process (question 2-3-9). The extent to which traffic simulation is applied to the development of ADFs at each of the different manufactures is out of the scope of L3Pilot. However, it can be expected that traffic simulation plays a role in this field. Although not all questions of this topic are confirmed, the topic itself is relevant for the L3Pilot project.

The last topic of the category deals with the ethical and legal aspects. The compliance with these relevant laws is vital for the L3Pilot consortium. More implication on local laws (question 2-4-1) and ethical standards on the L3Pilot (question 2-4-2) are described in detail in the L3Pilot deliverables D4.2. “Legal requirements to AD piloting” (Vignard 2018) and D8.1-3 “Ethical Requirements” (Gellerman et al., 2019). The deliverable includes analysis of regulations in different countries of the pilot. The regulations have to and will be followed by the L3Pilot partners. The last question of this topic (question 2-4-3) is tackled by the project in the upcoming safety impact assessment. The safety impact assessment will be conducted at the end of project once the data from the pilot are available. The methodology is described in the L3Pilot deliverable D3.3 (Metz et al., 2019).

#### **5.3.4 Category “Safeguarding Automation”**

The application of the CoP-AD to the pilot for the category “Safeguarding Automation” is difficult to describe. The reason is that the topics of this category tackle core aspects to development that are considered throughout the entire development life cycle. Therefore, many of the questions in this category are not in the direct scope of L3Pilot and have been dealt with prior to the project.

The second challenge related to this category is that a deep knowledge about the development is required to answer its questions. The knowledge exists within the companies, but it is not shared for confidentiality reasons in a research project. Therefore, it is hard to make detailed statements to what extent the different questions are covered. However, the project partners, who are conducting the studies, have a natural interest to ensure a safe testing of ADFs on public roads. Therefore, it can be presumed that all the relevant safety measures have been taken. Additionally each company can be presumed to have followed their internal development processes and guidelines, which typically cover the principles that are dealt with in this category.

A third aspect that is relevant for this category is the fact that the tested ADF and vehicle are still prototypes. These vehicles normally run under a different certification process in order to operate on public roads as serial production vehicles. The exact process depends on the relevant country and can also involve approval by external testing organisations.

For the topic functional safety the question related to the development of ADFs, such as question 3-1-2, are not in the scope of L3Pilot. The questions related to assessing the risk during operation or testing (e.g. question 3-1-8) as well as the question to verify that the function and safety measures behave as intended are relevant in the context of L3Pilot (e.g. questions 3-1-3, 3-1-9 and 3-1-11). Here, tests with the test vehicle are performed in a closed environment before the actual L3Pilot test on public roads start. Furthermore, the L3Pilot vehicles are equipped with extra data loggers, which will measure relevant signals and indicators during the drive. Therefore, additional related questions, such as question 3-1-4 are covered by the L3Pilot.

The topic “cybersecurity” has been dealt with in work package 4.6 “Legal aspects and cybersecurity”. The related work package has prepared the deliverable 4.2 “Legal requirements to AD piloting and cyber security analysis” (Vignard et al., 2018). This deliverable has been the basis for the work in the related CoP-AD. During the actual pilot the cybersecurity aspect will play a minor role, since no dedicated analysis is planned.

Since the tested ADF is a prototype function, it is possible for ADFs to be updated during the pilot. However, it is not possible to say at this time whether this will happen or how often this might occur. Nevertheless, it is expected that the updates are developed and tested with the same care as the original development process for the ADF. These updates in L3Pilot have to be seen in a different context to the updates that the topic “implementation of updates” (chapter 4.4.3) is dealing with. The updates in L3Pilot will be done in a workshop by experts that have developed the functions / vehicles, whereas the updates that chapter 4.4.3 is dealing with are updates to be done remotely. Therefore the CoP-AD questions of the topic “implementation of updates” are not in the scope of L3Pilot.

For the topic “safety of the intended functionality” the situation is similar to the topic “functional safety”. The aspects that are covered by the SOTIF CoP-AD questions need to be dealt with in order to ensure safe development. Therefore, the company internal process should already ensure that the SOTIF principles are addressed in the development process. This also applies to prototype vehicles, which are used for the L3Pilot. In the context of L3Pilot the user related SOTIF aspects are of particular importance to reduce the risk to the users of technical failures. This includes for instance a risk assessment prior to the actual pilot study (e.g. questions 3-4-4 and 3-4-8).

The last topics of the safeguarding category are “Data Recording, Privacy and Protection”. This topic is of particular relevance, since the L3Pilot is going to collect a considerable amount of data during the pilot and the related studies. Complying with GDPR is therefore an absolute key aspect for the project. The data handling process of L3Pilot is described in the L3Pilot deliverables 8.1-3 “Ethical Requirements” (Gellerman et al., 2019). This process answers the majority of the CoP-AD question for this category. The question 3-5-3 is confirmed by means of the extra logging equipment that is used in L3Pilot. Therefore, this topic is fully in the scope of L3Pilot.

### **5.3.5 Category “Human-Vehicle Integration”**

One major objective of L3Pilot is to investigate the interaction between potential users and the ADF. The L3Pilot assessment rather aims to investigate the general attitude of users as well as the general behaviour and acceptance of users while interacting with an ADF. Thus, the aim is not to assess a single HMI solutions. Here, it must be taken into account that the demonstrator vehicles used are still prototype vehicles, which differ in the level of maturity. This aspect holds true for the HMI used and must be considered when reporting the application of the draft CoP-AD in L3Pilot. Furthermore, it must also be considered that L3Pilot – in contrast to other research project – does not include a development of HMI

solution. The applied HMIs in the demonstrator have been developed outside of the project. A third important aspect is that the study design in L3Pilot required the adaptation of the test vehicles. These adaptations, like installing additional cameras to study the users' behaviour or extra interfaces (e.g. pedals) in the front of the passenger's seat in order to comply with the safety concept to operate such vehicles on the road, would not be part of a series production car.

For the topic "Guidelines for HVI" the compliance with the draft CoP-AD depends completely on the individual HMI solution in the test vehicles. It is clear that for each test vehicle the developers tried to implement the design related CoP-AD question (question 4-1-1 to 4-1-5) in the best possible manner. To what extent this task has been fulfilled will be shown in the L3Pilot assessment. Here, it is important that different users will react differently to the HMI. Regarding the effort that the different manufactures of the test vehicles have taken prior to the project to have an adequate HMI is not available for confidentiality reasons. Regarding the last question of this topic 4-1-6 it can be concluded that this is going to be assessed as part of the applied HMI concepts in the separate L3Pilot studies.

The second topic of this category is "Mode awareness, trust & misuses". Those CoP-AD questions, which address the design phase concept phase, are outside the scope of L3Pilot (questions 4-2-1 to 4-2-11). On the other hand, the questions that cover the validation and verification phase are in the scope in the context that the L3Pilot logged data will support the analysis of the applied HMI and might deliver input to future developments (questions 4-2-12, 4-2-13 and 4-2-14). However, the study designs of the on-road tests in L3Pilot do not allow in most cases to investigate long term effect. These effects are investigated exemplarily in a separate simulator study. Thus, the questions (questions 4-2-15 and 4-2-16) regarding long-terms effects in this topic are only partly covered by L3Pilot.

The third topic of the category is driver monitoring. Due to the requirements that have been defined by SP3 the test vehicles will be equipped with additional cameras, which will allow the study of the inner compartment of the vehicle including the driver as well as the surroundings of the vehicle. Some vehicles might also be equipped with an eye-tracking system. However, at the time of the deliverable there has not been a final decision on this. This approach will allow us to investigate secondary tasks and their impact during the studies (questions 4-3-1, 4-3-2 and 4-3-4). This also covers customers' devices (question 4-3-3). To what extent the test vehicles are already equipped with in-vehicle driver monitoring systems is not known at the point in time when this deliverable is written. However, it can be expected that some test vehicles will be equipped with such systems, which are also linked to the HVI concept (Is the HVI connected with the driver monitoring function?). The question regarding the post-start of production phase (question 4-3-5) is out of scope for L3Pilot.

Prior to testing on the road, measures must be taken to ensure a safe testing process. Therefore, the controllability of the ADF during testing must be ensured. Most of the questions in this topic need to be addressed at an early stage of the development (questions 4-4-1 to 4-4-4). These questions have been covered prior to the L3Pilot project. Regarding

the question 4-4-5, the data of the L3Pilot project will deliver further results here. For the L3Pilot more relevant questions are (questions 4-4-6 and 4-4-7), since safety needs to be ensured before testing on public roads. This means that tests are required to prove the function operation as well as the safety concept for the case that something goes wrong. This typically includes tests in closed environments and assessment of the readiness of the vehicle. This procedure is done in different manners for each of the partners' L3Pilot test vehicles. Again, the questions related to post start of production phase and the actual sign-off process (questions 4-4-8 and 4-4-9) are out of the L3Pilot scope.

The last aspect of the category is the driver training. Here, it is important to distinguish between the different driver types in L3Pilot (questions 4-5-1 and 4-5-2). For some test vehicles only company internal drivers are allowed. This driver type can be divided further into professional and non-professional drivers. The professional drivers normally have been trained in a special way to control the vehicle also during critical situations. Whilst, non-professional drivers may have special internal driving licences which is linked to company specific driver training. But this can differ among the involved companies. For those test vehicles that can be driven by normal users, the driver is expected to have had no known driver training. In addition, many test vehicles use safety drivers that can intervene in a critical situation as part of the safety concept for L3Pilot. These safety drivers are trained beforehand. Regarding the question 4-5-3 it can be reported that the methodology subproject provided guidelines regarding the study design and the preferred test group. However, there are also limitations related to the operation of the vehicle, which do not allow for all test vehicles to comply with these guidelines. For instance, the limitation of using internal employees or just professional test drivers limits the option of doing the tests with different user groups. For the test vehicles that can be driven by normal users a larger variety of users is expected. The question of this topic, related to the post start of production phase (question 4-5-4) is as for the other topics not in the scope of L3Pilot.



## 6 Conclusion

This deliverable presents the draft Code of Practice for Automated Driving (AD). Furthermore, the deliverable also reports on the process of the L3Pilot project. Therefore this document must be seen as an intermediate result of the L3Pilot “Code of Practice” subproject. That is why the history of the Code of Practice to present, its development and the CoP-AD structure are described in the first part of this document.

The core of the document is the draft CoP-AD (chapter 4). Overall, the draft CoP-AD consists of 155 main questions that have been assigned to 1 of the 5 categories and 1 of the 22 topics. The document focuses on the draft CoP-AD. However, it must be considered that this document took almost two years of work and included many intense discussions. The CoP-AD questions were continuously reviewed and updated in several meetings and workshops during this time. One key task was to reduce the number of questions from the 586 in the first version to a more reasonable amount so as to make the CoP-AD more usable for readers. This aspect is of particular importance since the intended purpose is to support developers and stakeholders to design and develop meaningful ADFs.

In order to present the CoP-AD questions in a comprehensive way, a template was defined that provides all the relevant information: the main question itself, the supporting sub-question, the relevant stage in the development process, and the question’s ID. The template provides a blank space to answer each of the main questions, which have been setup as “yes/no” questions. Questions are followed by an explanation and literature references.

It must be noted that the scope of the document is not to provide technical solutions, but to support the development of ADFs by ensuring that relevant aspects have been considered and followed. This means that there is not necessarily a “right” answer to all the CoP-AD questions. The purpose of the questions is instead to make the developers and other relevant stakeholders aware of certain aspects and to ensure that the reasons for certain decisions are documented. A “no” might mean that the intended topic has been considered in another way or is not relevant for the particular ADF.

The draft CoP-AD document also describes how and to what extent the L3Pilot project has applied and followed the draft CoP-AD (chapter 5) up to the due date of the deliverable (September 2019). A series of interviews with the relevant consortium members were conducted and summarized. L3Pilot focuses on the testing of automated driving and not on the development of ADFs, therefore the application of the draft CoP-AD is limited to a few topics. Deviations from the CoP-AD were found and they are described and explained in the document.

The draft CoP-AD is to serve as a basis for future work in the subproject. The main objective of which is to finalise the CoP-AD within the course of the project. Therefore the draft CoP-AD will be discussed and reviewed in the upcoming months with the internal as well as external project stakeholders. The discussions will take place in workshops and bilateral



interviews. Feedback will be collected over the course of these interviews and workshops and will be evaluated. Afterwards it will be used to update the CoP-AD in order to develop it in the best possible way to the needs of the ADF developers and other relevant stakeholders. As a document in the public domain, it is needed to help the necessary consolidation process towards (not just) a European basis for future public acceptance of robust automated driving. The final version of the CoP-AD is expected to be available in mid-2021.



## References

- Abbink, D., Carlson, T. et al., (2018). "A Topology of Shared Control Systems – Finding Common Ground in Diversity", IEEE Transactions on Human-Machine Systems, Volume 48, Issue 5.
- Abdulkhaleq, A. (2017). "A system-theoretic safety engineering approach for software-intensive systems", Dissertation, University Stuttgart.
- ACEA (2015). "ACEA Principles of data protection in relation to connected vehicles and services", ACEA Report.
- ACEA (2017). "ACEA principles of Automobile Cybersecurity", ACEA Report.
- UTO-ISAC (2016). "Auto-ISAC Best Practices", Report.
- Barnard, Y., Chen, H., Koskinen, S., Innamaa, S., et al., (2018). "Updated Version of the FESTA Handbook", FOT-Net Deliverable D5.4.
- Bartels, A., Eberle, U., Knapp, A. (2015). "System Classification and Glossary", Adaptive Deliverable D2.1.
- Bengler, K., Drücke, J., Hoffmann, S., Manstetten, D., & Neukum, A. (2018). UR: BAN Human Factors in Traffic. In Approaches for Safe, Efficient and Stress-free Urban Traffic. Springer Wiesbaden, Germany.
- Bienzeisler, J., Cousin, C., Deschamps, V. et al., (2017). "Legal aspects on automated driving", Adaptive deliverable D2.3.
- Bosch Media Service (2017). „Bosch und Daimler zeigen fahrerloses Parken im realen Verkehr“, press report 24.07.2017. <http://www.bosch-presse.de/pressportal/de/de/bosch-und-daimler-zeigen-fahrerloses-parken-im-realen-verkehr-116096.html>
- ancelliere, R., Ghignone, L., Tango, F. et al., (2019). Real-time detection of driver distraction: random projections for pseudo-inversion-based neural training. Knowledge and Information Systems, Volume 60, Issue 3, pp 1549–1564.
- Brilon, W., Regler, M., Geistefeldt, J. (2005). "Zufallscharakter der Kapazität von Autobahnen und praktische Konsequenzen". Straßenverkehrstechnik 3(1) and 4(2).
- Brusque, C., Bruyas, M. P., Carvalhais, J., Cozzolino, M., et al., (2007) "Effects of system information on drivers' behaviour", INERTS Synthesis No. 54.
- Campbell, J., Brown, J., Graving, J., Richard, C. et al., (2016). "Human Factors Design Guidance For Driver-Vehicle Interfaces", NHTSA report DOT HS 812 360.
- Campbell, J.L., Carney, C., Kantowitz, J.L. (1997). Human Factors Design Guidelines for advanced traveler information systems (ATIS) and commercial vehicle operations CV0), Report No. FHWA-RD-98-057), Federal Highway Administration, Washington, DC.
- CATAPULT Transport Systems (2017). "Market Forecast for connected and autonomous vehicles", Report.

- Cunningham, M. L., Regan, M. A. (2018). Driver distraction and inattention in the realm of automated driving. *IET Intelligent Transport Systems*, vol. 12, no. 6, pp. 407-413, 8 2018
- Department of Transport (DOT) (2015). "The pathway to driverless cars: a code of practice for testing", Report of Department of Transport.
- Eberle, U., Jütten, V., Knapp, A. et al., (2017). "Challenges for the development of automated driving functions due to system limits and validation ", *AdaptIVe deliverable D2.2*.
- Fabio, U., Broy, M., Brüngger, R. et al., (2017). "Ethic commission: automated and connected driving" Report of ethics commission appointed by the federal minister of transport and digital infrastructure.
- Flemisch, F., Abbink, D., Itoh, M. et al., (2016). „Shared control is the sharp end of cooperation: Towards a common framework of joint action, shared control and human machine cooperation”, 13th IFAC Symposium on Analysis, Design, and Evaluation of Human-Machine Systems HMS 2016.
- Ford (2018). "A matter of trust – Ford’s approach to developing self-driving vehicles”, Ford safety report.
- Forster, Y., Hergeth, S., Naujoks, F., Krems, J. F., & Keinath, A. (2019). Empirical Validation of a Checklist for Heuristic Evaluation of Automated Vehicle HMIs. In *International Conference on Applied Human Factors and Ergonomics* (pp. 3-14). Springer, Cham.
- Fridman, L., Brown, D. E., Glazer, M., Angell, W., Spencer, D. et al., (2019). MIT Advanced Vehicle Technology Study: Large-Scale Naturalistic Driving Study of Driver Behavior and Interaction with Automation. *IEEE Access*, vol. 7, pp. 102021-102038.
- Gellerman, H., Svanberg, E., Kotiranta, R., Heinig, I., et al., (2017). "Data sharing framework", *FOT-Net Deliverable D3.1*.
- Gellerman, H., Koskinen, S., Demirtzis, E., Mäkinen, T. (2019). " Deliverable D(8.1-8.3) Ethical Requirements No.1 – No.3", *L3Pilot Deliverable*.
- General Motors (2018). "2018 self-driving safety report", GM safety report.
- Gold, C., Naujoks, F., Radlmayr, J., Bellem, H., & Jarosch, O. (2017). Testing scenarios for human factors research in level 3 automated vehicles. In *International conference on applied human factors and ergonomics* (pp. 551-559). Springer, Cham.
- Griffon, T., Sauvagt, J.-L., Geronimi, S., Bolovinou, A., Brouwe, R., (2019). "Deliverable D4.1 Description and Taxonomy of Automated Driving Functions", *L3Pilot deliverable*.
- Hallerbach, S., Xia, Y., Eberle, U., and Koester, F. (2018). "Simulation-based Identification of Critical Scenarios for Cooperative and Automated Vehicles," *SAE Technical Paper 2018-01-1066*.
- Hilbert, D., Louw, T., Aittoniemi, E., Brouwer, R. (2018). "Deliverable D3.1 From Research Questions to Logging Requirements" *L3Pilot deliverable*.

HM Government (HMG) (2017). “The Key Principles of Cyber Security for Connected and Automated Vehicles”, <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles> [7.12.19].

INCOSE (2015). Systems Engineering Handbook

Information Commissioner’s Office (ICO) (2018), “Guide to the General Data Protection Regulation (GDPR)”, Report.

International Transport Forum (ITF), Corporate Partnership Board. (2018). “Safer Roads with Automated Vehicles”, <https://www.itf-oecd.org/safer-roads-automated-vehicles-0> [21.06.2018].

ISO 21434 (20XX). “Road vehicles – Cybersecurity engineering”, ISO standard under preparation.

ISO 21448 (2019). “Road vehicles — Safety of the intended functionality”, ISO standard ISO/PAS 21448:2019.

ISO 21934 (20XX). “Road vehicles — Prospective safety performance assessment of pre-crash technology by virtual simulation — Part 1: State-of-the-art and general method overview”, ISO Technical Report under preparation.

ISO 26262 (2018). “Road vehicles — Functional safety”, ISO standard series ISO 26262.

ISO 26262 -2 (2018). “Road vehicles — Functional safety — Part 2: Management of functional safety”, ISO standard 26262-2:2018.

ISO 26262 -7 (2018). “Road vehicles — Functional safety — Part 7: Production, operation, service and decommissioning”, ISO standard 26262-7:2018.

ISO 9001 (2015). “Quality management systems — Requirements”, ISO standard ISO 9001:2015.

ISO/IEC/IEEE 15288 (2015). System and Software Engineering – System Life Cycle Processes.

ISO/IEC/IEEE 42010 (2011). Systems and software engineering – Architecture description.

Japan Automobile Manufacturers Association (JAMA) (2004). “Guidelines for In-vehicle Display Systems — Version 3.0”, Report.

Kelsch, J., Dziennus, M., Schieben, A., Schömig, N., et al., (2017). “Final functional Human Factors recommendations”, AdaptIVe Deliverable D3.3.

Knapp, A., Neumann, M., Brockmann, M., Walz, R., Winkle, T. (2009). “Code of Practice for the Design and Evaluation of ADAS“, Deliverable of PReVent - Preventive and Active Safety Applications Integrated Project, Version 5.0.

Makoto, I., (2017). Effects of system information on drivers' behaviour. SIP-adus Workshop 2017, Tokyo.

Markkula, G., Benderius, O., Wolff, K., Wahde, M. (2012). „A review of near-collision driver behavior models”, Human Factors: The Journal of the Human Factors and Ergonomics Society.

- Maurer, M., Gerdes, J.C., Lenz, Winner, H. (2016). „Autonomous Driving - Technical, Legal and Social Aspects” Springer.
- Metz, B., Rösener, C., Louw, T., Aittoniemi, E. (2019). “Deliverable D3.3 Evaluation methods”, L3Pilot deliverable.
- McGonagle, John J. and Carolyn M. Vella (2003). The Manager's Guide to Competitive Intelligence. Westport CT: Greenwood Publishing Group. p. 184.
- Ministry of Land, Infrastructure, Transport and Tourism (MLT) (2018). “Guideline regarding Safety Technology for Automated Vehicles in Japan”, Presentation, 1st Meeting of working party on automated/autonomous and connected vehicles (GRVA).
- Morgan, P., Alford, C., Parkhurst, G. (2016). “Handover issues in autonomous driving: A literature review”, Project Report. University of the West of England.
- National Motorway Traffic Safety Administration (NHTSA) (2017). “Automated Driving Systems 2.0. A vision for safety”, NHTSA Report.
- National Transport Commission (NTC) (2017). “Guidelines for trials of automated vehicles in Australia”, Report, ISBN: 978-0-6480156-2-8.
- Naujoks, F., Hergeth, S., Keinath, A., Wiedemann, K., & Schömig, N., (2019-2). Development and Application of an expert assessment method for evaluating the usability of SAE L3 ADS HMIs. ESV Conference Proceedings, Eindhoven.
- Naujoks, F., Hergeth, S., Wiedemann, K., Schömig, N., & Keinath, A. (2018-1). Use cases for assessing, testing, and validating the human machine interface of automated driving systems. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 62, No. 1, pp. 1873-1877). Sage CA: Los Angeles, CA: SAGE Publications.
- Naujoks, F., Hergeth, S., Wiedemann, K., Schömig, N., Forster, Y., & Keinath, A. (2019-3). Test procedure for evaluating the human–machine interface of vehicles with automated driving systems. Traffic injury prevention, 20(sup1), S146-S151.
- Naujoks, F., Hergeth, S., Wiedemann, K., Schömig, N., Forster, Y., & Keinath, A. (2019-4). Test procedure for evaluating the human–machine interface of vehicles with automated driving systems. Traffic injury prevention, 20(sup1), S146-S151.
- Naujoks, F., Wiedemann, K., Schömig, N., Hergeth, S. (2019-1). “Towards guidelines and verification methods for automated vehicle HMIs”, Transportation Research Part F - Traffic Psychology and Behaviour 60, p. 121 -136.
- Naujoks, F., Wiedemann, K., Schömig, N., Jarosch, O., & Gold, C. (2018-2). Expert-based controllability assessment of control transitions from automated to manual driving. MethodsX, 5, 579-592.
- P.E.A.R.S. (2019), <https://pearsinitiative.com/>, website [12.7.19].

- PEGASUS Project (2019). "PEGASUS method – an overview", Report of the PEGASUS research project funded by the federal ministry of economic affairs and energy.
- Penttinen, M., Dotzauer, M., Hibbert, D., Innamaa, S., et al (2019). "Deliverable D3.2 Experimental procedure", L3Pilot deliverable.
- Post, K., Davey, C. (2019) "Integrating SOTIF and Agile Systems Engineering", SAE Technical Paper 2019-01-0141.
- Prokop, G. (2001). "Modelling human vehicle driving by model predictive online optimization", *Vehicle System Dynamics*, 35, pp. 19–53.
- Ragan, E.D., Bowman, D.A., Kopper, R., Stinson, C., et al., (2015). "Effects of field of view and visual realism on virtual reality training effectiveness for a visual scanning task", *IEEE Transactions on visualization and computer graphics* p. 794 – 807.
- Reddy, B., Kim, Y., Yun, S., Seo, C., Jang, J. (2017). Real-time Driver Drowsiness Detection for Embedded System Using Model Compression of Deep Neural Networks. 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, HI, 2017, pp. 438-445.
- Resende, P., Nashashibi, F. (2010). "Real-time dynamic trajectory planning for highly automated driving in highways", 13th International IEEE Conference on Intelligent Transportation Systems.
- Riedmaier *et al.*, (2018). Validation of X-in-the-Loop Approaches for Virtual Homologation of Automated Driving Functions, 11<sup>th</sup> FRAZ Symposium virtual vehicle.
- SAE International (2018). "Taxonomy and Definition for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016)", J3016 Revision June 2018.
- SAE International (2016). "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (J3061)", J3061 2016.
- SAE International (2012). "Automated Driving Reference Architecture (J3131)", J3131 2012.
- SAKURA Project (2019). "Development of a Safety Assurance Process for Automated Vehicles in Japan", Article publication of the SAKURA research project funded by the Japanese Ministry of Economy, Trade and Industry (METI).
- Sato, T. (2017). Driver distraction and inattention in the realm of automated driving. SIP-adus Workshop 2017, Tokyo.
- Sena, M. (2015). "Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements", International Telecommunication Union, Collaboration intelligent Transport System Communication Standard ITS-DOC-7.
- SIP-adus (2017). "SIP-adus Workshop 2017 Summary Report", Conference report.
- State of California Department of Motor Vehicles (DCM) (2019), "Testing of Autonomous Vehicles with a Driver", website, <https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/testing> [12.7.19]

Sullivan J., Flannagan, M., Pradhan, A., Bao, S. (2016). "Literature Review of Behavioral Adaptation to Advanced Driver Assistance Systems", University of Michigan Transportation Research Institute.

Thatcham (2018). "Assisted and Automated Driving – Definition and Assessment: Summary Document" Thatcham Research Report.

Thorn, E., Kimmel, S., Chaka, M. (2018). "A Framework for Automated Driving System Testable Cases and Scenarios", DOT HS 812 623.

Transport Research Laboratory (2011). A checklist for the assessment of in-vehicle information systems (IVIS) Wokingham: TRL.

UN Task Force on Cybersecurity and Over-the-Air issues (UNTF) (2018). "Draft Recommendation on Software Updates of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA", Internal Document.

University of Michigan (Mcity) (2018). "Assessing Risk: Identifying and Analysing Cybersecurity Threats to Automated Vehicles". [https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper\\_cybersecurity.pdf](https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf) [22.02.2019].

US Department of Transport (USDOT) (2018). "Preparing for the future of transport – Automated vehicles 3.0" Report of the US Department of Transport.

Verband der Automobilindustrie e.V. (VDA, 2015). "Automatisierung: Von Fahrerassistenzsystemen zum automatisierten Fahren", September 2015.

Vignard, N., Bolovinou, A., Amditis, A., Wallraf, G. (2018). "Legal requirements to AD piloting and cyber security analysis", L3Pilot Deliverable D4.2.

Wagner, P. (2014). "Traffic control and traffic management in a transportation system with autonomous vehicles", in *Autonomous Driving*, Chapter 15, Springer.

Wann, J. P., Wilkie, R. M. (2004). "How do we control high speed steering?", in *Optic Flow and Beyond*, pp. 371– 389.

Waymo (2018). "On the Road to Fully Self-Driving - Waymo Safety Report", Waymo Reprot.

Winner, H., Wachenfeld, W. (2013). "Absicherung automatischen Fahrens" 6. FAS Tagung, Munich.

Wolter, S., Knapp, A., Jütten V., Meng, C. (2018). "Code of Practice Framework". L3Pilot deliverable D2.1.

Wood, M., Knobel, C., Garbacik, N., et al., (2019). "Safety first for automated driving", Report of different companies.

Yan, Y., Götz, M., Laqua, A., Caccia Dominioni, G., et al., (2017). "A method to improve driver's situation awareness in automated driving", HFES Europe chapter.



Zhang, F., Su, J., Geng, L., Xia, Z. (2017). Driver Fatigue Detection based on Eye State Recognition. 2017 International Conference on Machine Vision and Information Technology (CMVIT), Singapore, 2017, pp. 105-110.

## List of abbreviations and acronyms

Abbreviation	Meaning
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
ADF	Automated Driving Function
AEB	Autonomous Emergency Braking
ASIL	Automotive Safety Integrity Level
AV	Automated Vehicles
CoP	Code of Practice
DDT	Dynamic Driving Task
ECU	Electronic Control Unit
FOT	Field Operation Test
GDPR	General Data Protection Regulation
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability
HIL	Hardware-In-the-Loop
HMI	Human Machine Interface
HVI	Human Machine Integration
HW	Hardware
MIL	Modell-In-the-Loop
MRM	Minimal Risk Manoeuvre
MRC	Minimal Risk Condition
MBSE	Model Based Systems Engineering
NDS	Naturalistic Driving Study
ODD	Operation Design Domain
OEDR	Object and Event Detection Response
OTA	Over The Air
SDV	Software Defined Vehicles
SIL	Software-in-the-loop
SOTIF	Safety Of The Intended Functionality
SysML	System Modelling Language
TOR	Take Over Request
V&V	Validation and Verification
V2X	Vehicle to X
VRU	Vulnerable road users
XIL	X-In-the-Loop (X: Hardware, Modell or Software)



## Annex 1 Report of the L3Pilot SP “Methodology” on test and evaluation of ADF

### Objective data collection

Table A1.1: Overview pros and cons for different objective data collection tools by SP3.

Tool:	Description:	Pros:	Cons:
Driving simulator	<ul style="list-style-type: none"> <li>- range from low- and medium- to high fidelity simulators</li> <li>- stationary to dynamic simulators</li> <li>- standardised driving tests producing comparable results and reproducible results</li> <li>- allow for testing hazardous/dangerous situations that cannot be tested in field tests</li> </ul>	<ul style="list-style-type: none"> <li>- standardised conditions for all participants</li> <li>- naive drivers can be assessed</li> <li>- measures for assessing driver state are available and deliver comparably good data quality (e.g. eye tracking, video of all relevant perspectives)</li> <li>- layout of ADF can be systematically varied</li> <li>- suitable to systematically study various aspects of ADF and driver experience</li> </ul>	<ul style="list-style-type: none"> <li>- no real ADF testing, just a simulated system (ADF behaviour cannot be evaluated)</li> <li>- all experienced system boundaries are experimentally implemented, no test of realistic ADF behaviour</li> <li>- prototype ADF is implemented based on available ADF description, drawbacks of real ADF cannot be detected</li> <li>- not suitable to test real ADF behaviour</li> </ul>
Test track	<ul style="list-style-type: none"> <li>- cars are driven on specifically designed tracks and not on public roads</li> <li>- controlled setting compared to road tests</li> <li>- systematically test effects of ADF on driver behaviour</li> </ul>	<ul style="list-style-type: none"> <li>- suitable to systematically study various aspects of AD-functionality and ADF-behaviour</li> <li>- no permission needed to test prototype functions</li> <li>- relevant aspects of driving environment can be systematically varied (within certain limits)</li> <li>- offers experimental control through test protocol</li> </ul>	<ul style="list-style-type: none"> <li>- variation of driving environment is limited compared to public roads</li> <li>- for certain ADFs, relevant traffic environments are difficult to stage on a test track (e.g. traffic jam)</li> <li>- experience and evaluation of ADF by naïve drivers might be influenced by artificial surrounding</li> <li>- impact of ADF on certain driver aspects cannot be assessed in experimental tests (mobility behaviour, frequency of reduced driver attention / driver state, ...)</li> </ul>
Experimental road test	<ul style="list-style-type: none"> <li>- experimentation carried out with instrumented vehicles in real traffic conditions on a predefined test route</li> <li>- in order to cover different experimental conditions, participants often have to drive the same test route several times</li> <li>- generally, a researcher accompanies participants giving instructions and observing behaviours</li> </ul>	<ul style="list-style-type: none"> <li>- suitable to systematically study various aspects of AD-functionality and ADF-behaviour</li> <li>- realistic environment and traffic conditions</li> <li>- selecting public roads that are suited for testing the ADF, the amount of data being not relevant for the analysis is minimised</li> <li>- offers experimental control through test protocol</li> </ul>	<ul style="list-style-type: none"> <li>- permission of road authority for testing ADF on public roads are needed</li> <li>- impact of ADF on certain driver aspects cannot be assessed in experimental tests (mobility behaviour, frequency of reduced driver attention / driver state, ...)</li> </ul>
Wizard of Oz	<ul style="list-style-type: none"> <li>- method used to give the appearance of an app/system/function to be</li> </ul>	<ul style="list-style-type: none"> <li>- more realistic than other simulation methods in the laboratory</li> </ul>	<ul style="list-style-type: none"> <li>- duration of experiment limited due to strains on hidden driver</li> </ul>

Tool:		Description:	Pros:	Cons:
		<p>automated, when, in fact, in hasn't (e.g.) an automated vehicle is controlled by a hidden driver in the back seat</p> <ul style="list-style-type: none"> <li>- test effects of ADF on driver behaviour</li> </ul>	<ul style="list-style-type: none"> <li>- drivers (adverse) reaction to ADF can be safely tested in the field</li> <li>- naive drivers can be assessed in real traffic conditions</li> <li>- suitable to systematically study various aspects of ADF and driver experience</li> </ul>	<ul style="list-style-type: none"> <li>- demanding job for hidden driver</li> <li>- driver needs to be trained well to be able to control the vehicle from the backseat</li> <li>- 1st driver input (driver in front seat) need to correspond to the automation reaction (2nd hidden driver)</li> <li>- replication of situations limited</li> <li>- not suitable to test real ADF behaviour</li> </ul>
	Field operational test	<ul style="list-style-type: none"> <li>- field operational tests aim at investigating the effect of one or more independent variables (e.g. assistant systems, different groups, different conditions) on driving behaviour</li> <li>- experimental design allows for limited hypothesis testing and manipulation of conditions</li> <li>- data are collected continuously</li> </ul>	<ul style="list-style-type: none"> <li>- offers more experimental control than NDS (e.g. driving with system: experimental – driving without system: baseline)</li> <li>- can be designed as between-participant design</li> <li>- external validity higher than in simulator studies</li> <li>- conclusions on the effects of ADAS/ADF in the field</li> </ul>	<ul style="list-style-type: none"> <li>- lack of specific instructions and naturalistic driving internal validity not as good as in lab studies</li> <li>- permission of road authorities needed</li> </ul>
	Naturalistic driving study	<ul style="list-style-type: none"> <li>- participants usually drive an instrumental car (often their own) for a period of time on their usual routes without any limiting instructions</li> <li>- data are recorded continuously</li> <li>- NDS follow no experimental control in terms of group assignments or control conditions (variables are not actively manipulated)</li> <li>- no instructor present</li> </ul>	<ul style="list-style-type: none"> <li>- participants are not asked to alter their behaviour -&gt; observed behaviour is actual behaviour to a high degree</li> <li>- NDS data are very realistic</li> <li>- conclusions on general driving can be drawn -&gt; high external validity</li> </ul>	<ul style="list-style-type: none"> <li>- no experimental control -&gt; many factors may influence driver behaviour</li> <li>- high variance in observed behaviour requiring a large number of participants and/or kilometres driven</li> <li>- factors influencing behaviour are not controllable -&gt; NDS is internally not valid</li> <li>- replication studies only produce the same results in very few cases</li> <li>- permission of road authorities needed</li> </ul>
Analytic simulation	Driving scenario simulation	<ul style="list-style-type: none"> <li>- Simulation tools mainly foreseen for the safety impact assessment</li> <li>- Different approaches can be applied to assess the effect of technology in driving scenarios, such as re-simulation of accidents or stochastically generated driving scenarios.</li> <li>- Simulates the behaviour of individual vehicles in a driving scenario using driving behaviour models.</li> <li>- The models that are applied should be chosen according to the purpose of assessing safety and the chosen simulation approach, e.g. models of driving situation, vehicle kinematics, and</li> </ul>	<ul style="list-style-type: none"> <li>- Resource efficient way to analyse different driving scenarios</li> <li>- Any physical harm is impossible.</li> <li>- Number of simulated scenarios and variations can arbitrarily be chosen.</li> <li>- State (kinematic information, internal states etc.) of any agent (combination of driver and model) can be assessed at any point of time of simulation.</li> <li>- Specific tools are able to provide road safety measures which allow for comprehensive conclusions on impact on safety (e.g. injuries,</li> </ul>	<ul style="list-style-type: none"> <li>- Accuracy depends on values used for settings, models as well as validity of the tool.</li> <li>- Models for simulation sub-components are required - in particular function.</li> <li>- Further input might be required in addition to get to the final safety impact (e.g. for scaling up).</li> </ul>

Tool:		Description:	Pros:	Cons:
		<p>injuries/damages may be based on accident data</p> <ul style="list-style-type: none"> <li>- Quality of the simulation depends strongly on the quality of the input.</li> <li>- Commercial and open source software available.</li> </ul>	<p>damages, number of accidents).</p>	
Analytic simulation	Traffic (micro-) simulation	<ul style="list-style-type: none"> <li>- Tool for the impact assessment of various measures.</li> <li>- Simulates the behaviour of individual vehicles on a road or road network -&gt; allows for analysis to predict changes following changes to the traffic environment or to driver or vehicle behaviour, using detailed driving behaviour models.</li> <li>- Use cases for this simulation type are road stretches or intersections to simulating traffic in entire towns.</li> <li>- Models are usually very flexible, allowing for assessment of a wide range of different circumstances.</li> <li>- Quality of the simulation depends strongly on the quality of the input.</li> <li>- Commercial and open source software available.</li> </ul>	<ul style="list-style-type: none"> <li>- Resource efficient way to analyse different traffic scenarios (varying driving behaviour, penetration rates etc.)</li> <li>- Any physical harm is impossible.</li> <li>- Number of simulated scenarios can arbitrarily be chosen.</li> <li>- State (kinematic information, internal states etc.) of any agent (combination of driver and model) can be assessed at any point of time of simulation.</li> <li>- Some safety related aspects can be analysed to a extent (e.g. number of incidents, time headway, and time to collision).</li> </ul>	<ul style="list-style-type: none"> <li>- Accuracy depends on the values used for settings, models as well as validity of the tool.</li> <li>- Models for simulation sub-components are required - in particular function.</li> <li>- As far as safety related aspects are analysed, no final conclusion on impact on safety can be derived (e.g. injuries, damages).</li> </ul>

Table A1.2: Rating of the suitability of different objective data collection tools (1 of 3) for the L3Pilot research question by SP3 (●●●: well suited, ●●: moderately suited, ●: little suited).

Evaluation area	RQ area	RQ	Driving simulator	Test track	Experimental road test	
Technical & Traffic evaluation	Technical performance of the system	How reliable is system performance in a given driving and traffic scenario?		●	●●	
		How often and under which circumstances does the ADF issue a TOR?			●●	
	Impact on the ego-vehicle's driving behaviour	How do take-over requests affect driving?				●●
		What is the impact of ADF on driving dynamics?			●	●●
		What is the impact of ADF on the accuracy of driving?			●	●●
		What is the impact of ADF on the driven speed?			●	●●
		What are the impacts of ADF on energy efficiency?			●	●●

Evaluation area	RQ area	RQ	Driving simulator	Test track	Experimental road test	
		What is the impact of ADF on the frequency of near-crashes / incidents?			•	
		What is the impact of ADF on the frequency of certain events?			••	
	Impact on the interaction with other road users	What is the impact of ADF on the interaction with other road users in a defined driving scenario?			••	
		What are the impacts of ADF on traffic efficiency?			••	
		What is the impact of ADF on the number of near-crashes / incidents with other road users?			••	
	Impact on the behaviour of other traffic participants	How does the ADF influence the behaviour of subsequent vehicles?			••	
		How does the ADF influence the behaviour of preceding vehicles?			••	
		What is the impact of the ADF on the number of near-crashes / incidents of other traffic participants?			••	
	User & Acceptance Evaluation	Impact on user acceptance & awareness	Are drivers willing to use the ADF?	••	•	••
			What is the impact of the ADF on driver state?	••		
What is the impact of the ADF use on driver awareness?			••	•	••	
User experience		What is the drivers' secondary task engagement during ADF use?	••		•	
		How do drivers respond when they are required to retake control? (Reaction time, success of takeover)	••	••	••	
		How often and under which circumstances do drivers choose to activate/deactivate the ADF?	••		••	
Impact	Impact on safety	What is the impact of the ADF on the number of accidents in a certain driving scenario / for certain road users?	•			
		What is the impact of the ADF on accidents with a certain injury level / damage in a certain driving scenario?				
	Impact of the ADF on	What is the impact on the transport network efficiency				

Evaluation area	RQ area	RQ	Driving simulator	Test track	Experimental road test
	environmental aspects	(throughput) in a certain traffic scenario?			
		What is the impact of ADFs on the energy demand / pollution in a certain traffic scenario?			
	Impact of the ADF on travel behaviour (Exposure)	What is the impact of the ADF on the number of trips made?			
		What is the impact of the ADF on the frequency of road type usage?			
		What is the impact of the ADF on the trip duration/distance?			
		What is the impact of ADF on the frequency of certain driving scenarios (accidents / critical situation / normal driving)?			
		How do the ADF's limitations influence the impact on safety / efficiency?			

Table A1.3: Rating of the suitability of different objective data collection tools (2 of 3) for the L3Pilot research question by SP3 (●●●: well suited, ●●: moderately suited, ●: little suited).

Evaluation area	RQ area	RQ	Wizard of Oz	Field operational test	Naturalistic driving study
Technical & Traffic evaluation	Technical performance of the system	How reliable is system performance in a given driving and traffic scenario?		●●	●●
		How often and under which circumstances does the ADF issue a TOR?		●●	●●
	Impact on the ego-vehicle's driving behaviour	How do take-over requests affect driving?		●●	●●
		What is the impact of ADF on driving dynamics?		●●	●●
		What is the impact of ADF on the accuracy of driving?		●●	●●
		What is the impact of ADF on the driven speed?		●●	●●
		What are the impacts of ADF on energy efficiency?		●●	●●
		What is the impact of ADF on the frequency of near-crashes / incidents?		●●	●●
		What is the impact of ADF on the frequency of certain events?		●●	●●

Evaluation area	RQ area	RQ	Wizard of Oz	Field operational test	Naturalistic driving study
	Impact on the interaction with other road users	What is the impact of ADF on the interaction with other road users in a defined driving scenario?		••	••
		What are the impacts of ADF on traffic efficiency?		••	••
		What is the impact of ADF on the number of near-crashes / incidents with other road users?		••	••
	Impact on the behaviour of other traffic participants	How does the ADF influence the behaviour of subsequent vehicles?		••	••
		How does the ADF influence the behaviour of preceding vehicles?		••	••
		What is the impact of the ADF on the number of near-crashes / incidents of other traffic participants?		••	••
User & Acceptance Evaluation	Impact on user acceptance & awareness	Are drivers willing to use the ADF?	••	••	••
		What is the impact of the ADF on driver state?	••	••	••
		What is the impact of the ADF use on driver awareness?	••	••	••
	User experience	What is the drivers' secondary task engagement during ADF use?	••	••	••
		How do drivers respond when they are required to retake control? (Reaction time, success of takeover)	••	••	••
		How often and under which circumstances do drivers choose to activate/deactivate the ADF?	••	••	••
Impact	Impact on safety	What is the impact of the ADF on the number of accidents in a certain driving scenario / for certain road users?		•	☐
		What is the impact of the ADF on accidents with a certain injury level / damage in a certain driving scenario?			☐
	Impact of the ADF on environmental aspects	What is the impact on the transport network efficiency (throughput) in a certain traffic scenario?			☐
		What is the impact of ADFs on the energy demand / pollution in a certain traffic scenario?			☐
	Impact of the ADF on travel	What is the impact of the ADF on the number of trips made?			☐

Evaluation area	RQ area	RQ	Wizard of Oz	Field operational test	Naturalistic driving study
	behaviour (Exposure)	What is the impact of the ADF on the frequency of road type usage?			<input type="checkbox"/>
		What is the impact of the ADF on the trip duration/distance?			<input type="checkbox"/>
		What is the impact of ADF on the frequency of certain driving scenarios (accidents / critical situation / normal driving)?			<input type="checkbox"/>
		How do the ADF's limitations influence the impact on safety / efficiency?			<input type="checkbox"/>

Table A1.4: Rating of the suitability of different objective data collection tools (3 of 3) for the L3Pilot research question by SP3 (●●●: well suited, ●●: moderately suited, ●: little suited).

Evaluation area	RQ area	RQ	Analytic simulation Driving scenario simulation	Analytic simulation Traffic microsimulation
Technical & Traffic evaluation	Technical performance of the system	How reliable is system performance in a given driving and traffic scenario?		
		How often and under which circumstances does the ADF issue a Tor?		
	Impact on the ego-vehicle's driving behaviour	How do take-over requests affect driving?		
		What is the impact of ADF on driving dynamics?		
		What is the impact of ADF on the accuracy of driving?		
		What is the impact of ADF on the driven speed?		
		What are the impacts of ADF on energy efficiency?		
		What is the impact of ADF on the frequency of near-crashes / incidents?		
		What is the impact of ADF on the frequency of certain events?		
	Impact on the interaction with other road users	What is the impact of ADF on the interaction with other road users in a defined driving scenario?		
		What are the impacts of ADF on traffic efficiency?		

Evaluation area	RQ area	RQ	Analytic simulation Driving scenario simulation	Analytic simulation Traffic microsimulation
	Impact on the behaviour of other traffic participants	What is the impact of ADF on the number of near-crashes / incidents with other road users?		
		How does the ADF influence the behaviour of subsequent vehicles?		
		How does the ADF influence the behaviour of preceding vehicles?		
		What is the impact of the ADF on the number of near-crashes / incidents of other traffic participants?		
User & Acceptance Evaluation	Impact on user acceptance & awareness	Are drivers willing to use the ADF?		
		What is the impact of the ADF on driver state?		
		What is the impact of the ADF use on driver awareness?		
	User experience	What is the drivers' secondary task engagement during ADF use?		
		How do drivers respond when they are required to retake control? (Reaction time, success of takeover)		
		How often and under which circumstances do drivers choose to activate/deactivate the ADF?		
Impact	Impact on safety	What is the impact of the ADF on the number of accidents in a certain driving scenario / for certain road users?	•••	•
		What is the impact of the ADF on accidents with a certain injury level / damage in a certain driving scenario?	••	
	Impact of the ADF on environmental aspects	What is the impact on the transport network efficiency (throughput) in a certain traffic scenario?		•••
		What is the impact of ADFs on the energy demand / pollution in a certain traffic scenario?		•••
	Impact of the ADF on travel behaviour (Exposure)	What is the impact of the ADF on the number of trips made?		
		What is the impact of the ADF on the frequency of road type usage?		
		What is the impact of the ADF on the trip duration/distance?		•••



Evaluation area	RQ area	RQ	Analytic simulation Driving scenario simulation	Analytic simulation Traffic microsimulation
		What is the impact of ADF on the frequency of certain driving scenarios (accidents / critical situation / normal driving)?		...
		How do the ADF's limitations influence the impact on safety / efficiency?	..	...

## Subjective data collection

Table A1.5: Overview pros and cons for different subjective data collection tools by SP3.

Tool:	Description:	Pros:	Cons:
Observation	<ul style="list-style-type: none"> <li>- via human observer, camera or "medical" sensors</li> <li>- during test drive or during day-to-day mobility</li> </ul>	<ul style="list-style-type: none"> <li>- real behaviour can be observed</li> </ul>	<ul style="list-style-type: none"> <li>- the awareness of being observed can manipulate the behaviour</li> <li>- L3-ADF still cannot be observed in day-to-day mobility</li> </ul>
Focus group	<ul style="list-style-type: none"> <li>- Creating an intensive discussion between persons to understand their attitudes, expectations and requirements</li> <li>- Guiding these discussions via a moderator</li> </ul>	<ul style="list-style-type: none"> <li>- Getting answers on open questions</li> <li>- Understanding the motivations behind the answers</li> </ul>	<ul style="list-style-type: none"> <li>- Possibility of influencing peoples opinion by other participants</li> <li>- Risk of dominance by single participants</li> </ul>
Open-ended interview questions	<ul style="list-style-type: none"> <li>- Interviewing people to understand their attitudes, expectations and requirements</li> <li>- Can be face to face or via telephone</li> <li>- Getting answers on open questions</li> </ul>	<ul style="list-style-type: none"> <li>- Understanding the motivations behind the answers</li> </ul>	<ul style="list-style-type: none"> <li>- Costs a lot of time for the interview itself and the analysis of the interviews</li> <li>- Because of this only limited number of interviewees possible</li> </ul>
Close-ended interview questions	<ul style="list-style-type: none"> <li>- Interviewing people to understand their attitudes, expectations and requirements</li> <li>- Can be face to face or via telephone</li> <li>- Getting predefined answers</li> </ul>	<ul style="list-style-type: none"> <li>- Limited time effort, greater number of interviews possible</li> <li>- Fast analysis</li> </ul>	<ul style="list-style-type: none"> <li>- Costs personnel time for the interview itself</li> <li>- Insight into the motivation behind the answers rather small</li> </ul>
Close-ended survey/questions	<ul style="list-style-type: none"> <li>- Asking people to understand their attitudes, expectations and requirements</li> <li>- Can be paper and pencil or online</li> <li>- Getting predefined answers</li> </ul>	<ul style="list-style-type: none"> <li>- Once the survey is prepared, higher number of respondents is easy to realise (especially online)</li> <li>- Fast analysis</li> </ul>	<ul style="list-style-type: none"> <li>- Insight into the motivation behind the answers rather small</li> <li>- Seriousness of the answers can be a problem</li> </ul>
Travel diary	<ul style="list-style-type: none"> <li>- People write down their daily travel experiences with ADF</li> <li>- Requires a day-to-day use of the vehicles</li> </ul>	<ul style="list-style-type: none"> <li>- Easier to realise than an observation</li> </ul>	<ul style="list-style-type: none"> <li>- Risk of oblivion</li> </ul>
Standardised questionnaire	<ul style="list-style-type: none"> <li>- Two inquiries: Before and after test drive</li> <li>- Conjunction with the representative survey reasonable</li> </ul>	<ul style="list-style-type: none"> <li>- Detection of the influence of the test drive experience</li> </ul>	<ul style="list-style-type: none"> <li>- Insight into the motivation behind the answers rather small</li> </ul>

Table A1.6: Rating of the suitability of different subjective data collection tools (1 of 2) for the L3Pilot research question by SP3 (●●●: well suited, ●●: moderately suited, ●: little suited).

Evaluation area	RQ area	RQ	Observation	Focus group	Open-ended interview questions	Close-ended interview questions
User & Acceptance Evaluation	Impact on user acceptance & awareness	Are drivers willing to use an ADF?		●●●	●●	●●●
		How much are drivers willing to pay for the ADF?		●●●		●●●
		What is the user acceptance of the ADF?		●●	●●	●●●
		What is the impact of the ADF on driver state?	●●			●
		What is the impact of the ADF use on driver awareness?	●●			●
		What are drivers' expectations regarding system features?		●●●	●●	●●●
	User experience	What is the drivers' secondary task engagement during ADF use?	●●			●●
		How do drivers respond when they are required to retake control? (Success of TOR)	●●●			●●●
		How often and under which circumstances do drivers choose to activate/deactivate the ADF?	●●	●●●	●●	
		What is the impact of the ADF use on motion sickness?	●●	●●●	●●	●
		What is the impact of motion sickness on the ADF use?		●●●		●

Table A1.7: Rating of the suitability of different subjective data collection tools (2 of 2) for the L3Pilot research question by SP3 (●●●: well suited, ●●: moderately suited, ●: little suited).

Evaluation area	RQ area	RQ	Close-ended survey/questions	Travel diary	Standardised questionnaire
User & Acceptance Evaluation	Impact on user acceptance & awareness	Are drivers willing to use an ADF?	●●●	●●●	●●●
		How much are drivers willing to pay for the ADF?	●●●		●●●
		What is the user acceptance of the ADF?	●●●	●	●●●
		What is the impact of the ADF on driver state?			●
		What is the impact of the ADF use on driver awareness?			●
		What are drivers' expectations regarding system features?	●●●		●●●
	User experience	What is the drivers' secondary task engagement during ADF use?	●●	●	●●
		How do drivers respond when they are required to retake control? (Success of takeover)			●●
		How often and under which circumstances do drivers choose to activate/deactivate the ADF?	●	●●●	
		What is the impact of the ADF use on motion sickness?			●●
		What is the impact of motion sickness on the ADF use?			●●