Deliverable **D2.3** /

Code of Practice for the development of Automated Driving Functions

Final Version: 1.1

Dissemination level: PU

Lead contractor: Groupe PSA

Due date: 28.04.2021

Version date: 28.04.2021

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

Document information

Authors

Yu Cao – Groupe PSA
Thibault Griffon – Groupe PSA
Felix Fahrenkrog – BMW
Moritz Schneider – BMW
Frederik Naujoks – BMW
Fabio Tango – CRF
Stefan Wolter – Ford
Andreas Knapp – Mercedes-Benz
Yves Page – Renault Group
Jorge Lorente Mallada – Toyota
Giancarlo Caccia Dominioni – Toyota
Elias Demirtzis – Aptiv
Michele Giorelli – Aptiv
Silvia Fabello – Veoneer
Fabian Frey – Veoneer
Qi Feng – 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

Coordinator

Aria Etemad
Volkswagen Group Innovation
Hermann-Münch-Str. 1
38440 Wolfsburg
Germany

Phone: +49-5361-9-13654
Email: aria.etemad@volkswagen.de

Project funding

Horizon 2020
ART-02-2016 – Automation pilots for passenger cars
Contract number 723051
www.L3Pilot.eu

Legal Disclaimer

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

Revision and history chart

Version	Date	Comment
0.1	21.02.2020	First draft structure of Code of Practice for the development of Automated Driving Functions (CoP-ADF).
0.2	27.03.2020	First update of introduction of D2.3, news chapter “Users groups of CoP-ADF” implemented.
0.3	21.04.2020	First update of CoP-ADF by considering the comments from General Assembly of L3Pilot.
0.4	11.05.2020	Update of CoP-ADF, conclusion and glossary table.
0.5	30.06.2020	New version of CoP-ADF for the review of external L3Pilot stakeholders.
0.6	30.10.2020	Improvement of CoP-ADF by L3Pilot sub-project 2 (SP2) partners.
0.7	03.12.2020	New version of CoP-ADF by considering comments from external expert workshop.
0.8	18.12.2020	New document list and technical annex incorporated in annex part.
0.81	15.01.2021	Update of CoP-ADF Annex.
0.9	19.02.2021	New version of CoP-ADF after L3Pilot SP2 internal review.
1.0	21.04.2021	Final version of CoP-ADF after L3Pilot final review.
1.1	28.04.2021	Final version after update of SAE levels 2021

Table of contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

Abbreviation	Meaning
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
ADF	Automated Driving Functions
ALKS	Automated Lane keeping System
ASIL	Automotive Safety Integrity Level
AV	Automated Vehicle
CoP	Code of Practice
DDT	Dynamic Driving Task
ECU	Electronic Control Unit
FFOA	Functional Field of Application
FMEA	Failure Mode and Effect Analysis
FOT	Field Operation Test
FTA	Fault Tree Analysis
FuSa	Functional Safety
GDPR	General Data Protection Regulation
HW	Hardware
HARA	Hazard Analysis and Risk Assessment
HAZOP	Hazard and Operability Analysis
HIL	Hardware-In-the-Loop
HMI	Human-Machine Interface
HVI	Human-Vehicle Integration
MIL	Model-In-the-Loop
MRM	Minimal Risk Manoeuvre
MRC	Minimal Risk Condition
MBSE	Model Based Systems Engineering
NDS	Naturalistic Driving Study
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OTA	Over The Air
RTM	Requirements Traceability Matrix
SIL	Software-In-the-Loop
SOTIF	Safety Of The Intended Functionality
STPA	System Theoretic Process Analysis
SysML	System Modelling Language
TOR	Take Over Request

Abbreviation	Meaning
V&V	Validation and Verification
V2X	Vehicle-to-Everything
V2V	Vehicle-to-Vehicle
V2I	Vehicle-to-Infrastructure
V2N	Vehicle-to-Network
VRU	Vulnerable Road User
XIL	X-In-the-Loop (X: Vehicle, Hardware, Model or Software)

1 Introduction

1.1 Motivation for the L3Pilot Project

Over the years, numerous projects have paved the way for automated driving (AD). Especially, numerous vehicles are now equipped with Advanced Driver Assistance Systems (ADAS), and drivers are progressively getting used to them.

However, automation demands integrating more and better technology as well as compliance of the technology to user behaviour and acceptance of automated driving functions (ADF). In addition, there are many broad legal considerations which need to be addressed before AD can be rolled out.

The L3Pilot project is taking one of the further steps before the introduction of automated vehicles (AVs) in daily traffic. Its overall motivation is to test and study the viability of AD as a safe and efficient means of transportation, to gain knowledge base for exploring and promoting new service concepts to provide inclusive mobility.

1.2 Objectives of the L3Pilot Project

The newly-attained level of technology maturity ensures an appropriate assessment of the impact of AD, what is happening both inside and outside the vehicles, how vehicle security can be ensured, evaluating user acceptance, societal impacts and emerging business models.

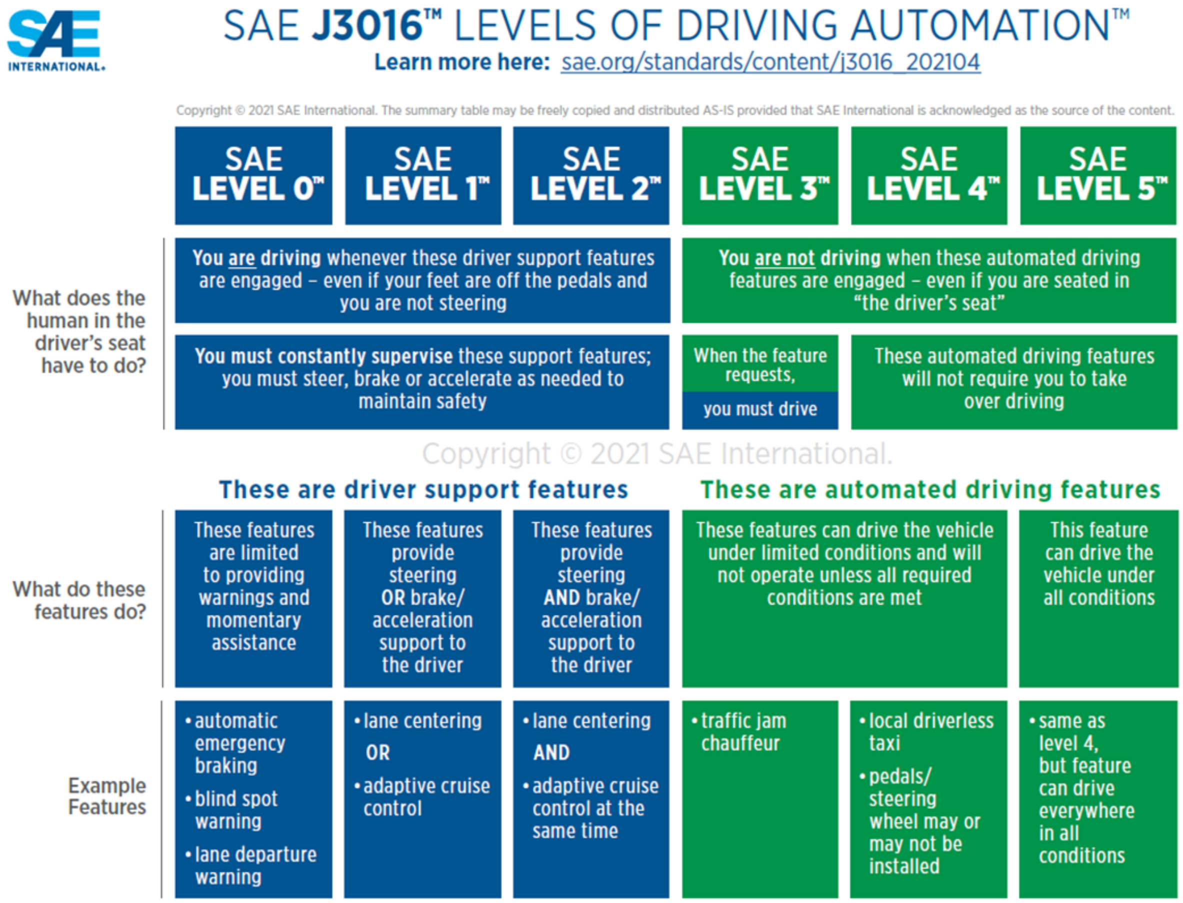
Recent work indicates how driver assistance systems and ADF can be best validated by means of extensive road tests (Pilots), with a sufficiently long operation time, to allow extensive interaction with the driver and testable functions.

The project uses 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 are also being assessed.

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 is being achieved by assessing user reactions, experiences, preferences and acceptance 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 for the development of Automated Driving Functions).

- Create a large database to enable simulation studies of the performance of ADF over time which can’t be investigated in road tests, due to the time and effort needed. The data will be one outcome of the pilots.



SAE **J3016**™ LEVELS OF DRIVING AUTOMATION™

Learn more here: sae.org/standards/content/j3016_202104

Copyright © 2021 SAE International. The summary table may be freely copied and distributed AS-IS provided that SAE International is acknowledged as the source of the content.

	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver’s seat have to do?	You **are driving** whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You **are not driving** when these automated driving features are engaged – even if you are seated in “the driver’s seat”		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			These are automated driving features		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering **OR** brake/ acceleration support to the driver	These features provide steering **AND** brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering **OR** • adaptive cruise control	• lane centering **AND** • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

Copyright © 2021 SAE International.

*Figure 1.1: SAE Levels of Driving Automation J3016_202104(Copyright 2021 SAE International).*The consortium addresses four major technical and scientific objectives listed below:

- Create a standardised Europe-wide piloting environment for AD.
- Coordinate activities across the piloting community to acquire the required data.
- Pilot, test and evaluate ADF and connected automation.
- Innovate and promote AD for wider awareness and market introduction.

1.3 Approach and Scope

The L3Pilot project focuses on large-scale piloting of ADFs, primarily L3 functions, with additional assessment of some L4 functions. The key in testing is to ensure that the functionality of the systems used is exposed to variable conditions, and performance is consistent, reliable, and predictable. This enhances 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.

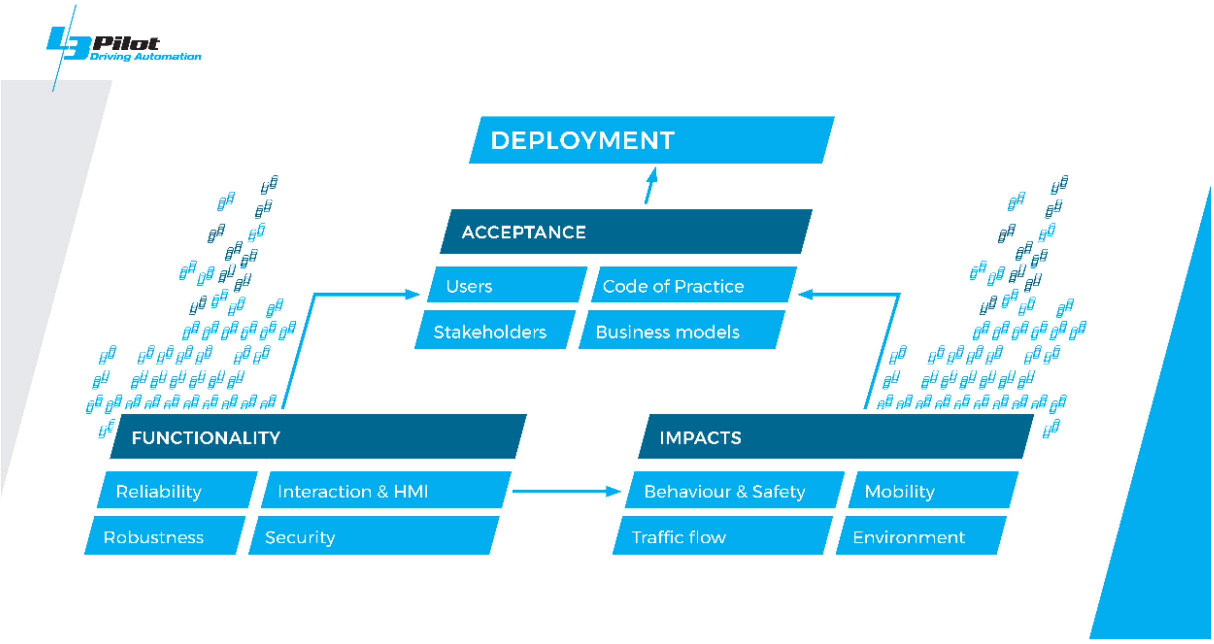
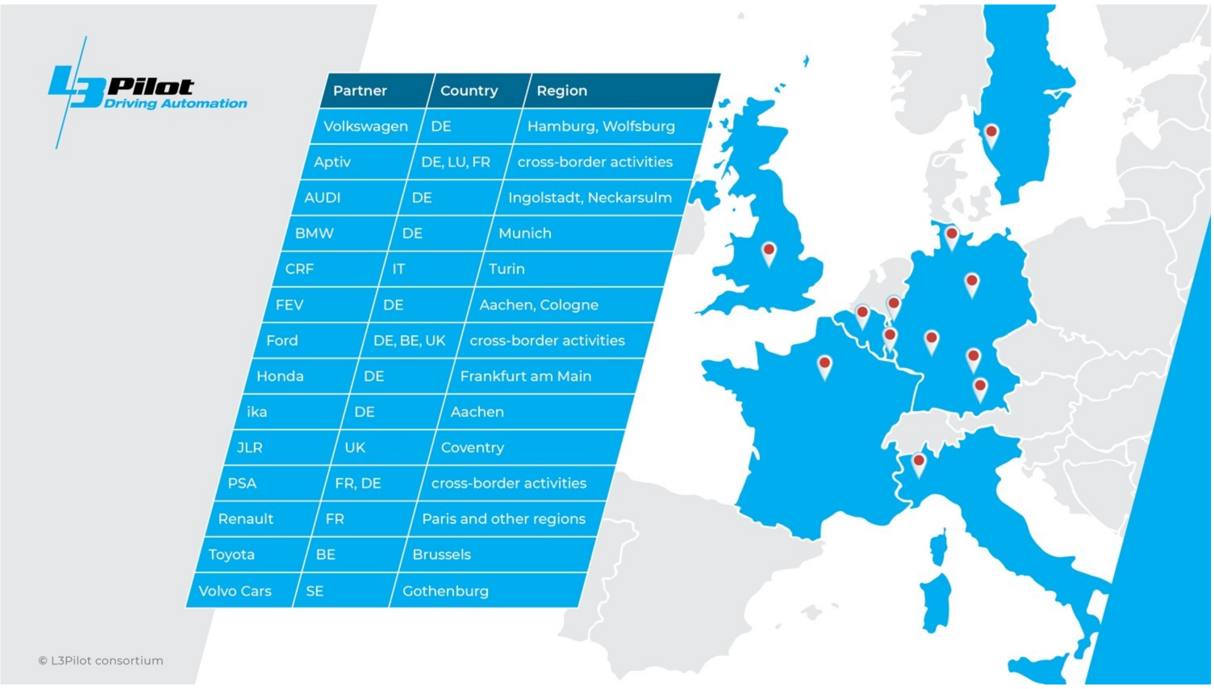


Figure 1.2: L3Pilot approach and the mechanism for deployment

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 750 users tested 70 vehicles across Europe with bases in 7 Countries, including: Belgium, France, Germany, Italy, Luxembourg, Sweden, and the United Kingdom, as shown in Figure 1.3.



Partner	Country	Region
Volkswagen	DE	Hamburg, Wolfsburg
Aptiv	DE, LU, FR	cross-border activities
AUDI	DE	Ingolstadt, Neckarsulm
BMW	DE	Munich
CRF	IT	Turin
FEV	DE	Aachen, Cologne
Ford	DE, BE, UK	cross-border activities
Honda	DE	Frankfurt am Main
ika	DE	Aachen
JLR	UK	Coventry
PSA	FR, DE	cross-border activities
Renault	FR	Paris and other regions
Toyota	BE	Brussels
Volvo Cars	SE	Gothenburg

© L3Pilot consortium

Figure 1.3: L3Pilot testing areas and cross-borders

2 Introduction to the Code of Practice

2.1 General Aspects

The European research project L3Pilot combines different activities, one of the most important is to report on the Code of Practice for the development of Automated Driving Functions (CoP-ADF), which is the main objective of this document. The CoP-ADF shall provide a comprehensive guideline for supporting the automotive industry and relevant stakeholders in the development of the AD technology. The CoP-ADF is derived from gained knowledge in the industry as well as collected best practices in different topics. Thus, the CoP-ADF includes the following aspects:

- Collection of best practices on the topics that have been identified in L3Pilot as relevant;
- A typical process for the development and release of ADF;
- Safety aspects and methods to confirm a safe operation of ADF;
- Checklist targeting on engineers or to support the community.

This document is structured in the following way: after the general introduction to the L3Pilot project, the history of the CoP and its scope for AD are outlined, the user groups and application of CoP-ADF are described as well. The third chapter describes the approach for the development and validation of CoP-ADF and clarifies the adaptations regarding the development phases, topics as well as categories that have been updated during the compilation of the CoP-ADF, compared to the initial plan of CoP-ADF framework in deliverable D2.1 (Wolter et al. 2018). The CoP-ADF is described in chapter four, which is based on the draft of CoP-ADF in deliverable D2.2 (Fahrenkrog et al. 2020). The summary of CoP-ADF activities and lessons learnt are comprised in chapter five.

It is important to note that this document (deliverable D2.3) presents the final results of the CoP-ADF in L3Pilot project, therefore several updates and improvements of the draft of CoP-ADF (deliverable D2.2) have been discussed and implemented by considering the feedback and comments from internal / external L3Pilot stakeholders (for more details, see chapter 3).

2.2 History of the Code of Practice

The CoP activities started with the rise of ADAS at the end of last century. Back then, it became clear that these functions have a high potential to improve traffic safety, however technical limits as well as liability issues delayed the market introduction of ADAS. Based on these circumstances, the RESPONSE 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 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 this path in context of the PReVENT project. The outcome of RESPONSE 3 was the final "Code of Practice for the Design and Evaluation of ADAS" (CoP-ADAS) (Knapp et al. 2009). The CoP provided the vehicle industry with tools and a common understanding to overcome and manage the issue regarding safety and liability for ADAS.

Since the PReVENT project, research and development has progressed and led to technologies that support the driver or even take over the driving task entirely in a wider range of situations. Similar to ADAS, an ADF faces different challenges that need to be addressed to avoid hindrance to their market introduction.

Therefore, the CoP activities continued in the European research project AdaptIVe (2014 – 2017) that dealt with the development of ADF. The RESPONSE 4 – sub-project of AdaptIVe – focused on the classification (Bartels et al. 2015) and legal aspects of AD (Bienzeisler et al. 2017). Furthermore, by identifying the challenges within the development of AD (Eberle et al. 2017), it provided the basis for the development of this CoP-ADF in L3Pilot.

This CoP-ADF in L3Pilot must be seen in the tradition of the RESPONSE 3 CoP, since it shall support the developers of these technologies in order to overcome main challenges in the development. For L3Pilot, the focus is on L3 and L4 ADF in passenger cars, and therefore it is complementary to the previous CoP documents.

2.3 Scope of the Code of Practice for the development of ADF

The CoP-ADF should be used as a guideline to develop and validate ADF. The target user groups are mainly engineers and stakeholders in the field of AD (for more elaboration, see chapter 2.5). The CoP-ADF focused on L3 and L4 ADF in passenger cars, for 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 L3 functions; at the end of the Operational Design Domain (ODD) for L4 functions;
- To cover driving scenarios outside the scope of the function (e.g. function limits, outside of the ODD, ADF switched off); and
- To retake control from the ADF 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 (ERTRAC CAD 2019). Traffic Jam Chauffeur for lane following in traffic jams or motorway chauffeur for lane following and lane changes are L3Pilot examples on how to perform the dynamic driving task (DDT) (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-ADF is set to cover L3 and L4 functions. L0, L1 and L2 functions are not in the focus of this document, they are covered by the CoP-ADAS (Knapp et al. 2009). Regarding the covered region and ODD, it must be recognized that the deliverable is written from a European standpoint and focuses mainly on motorway and parking ADF. However, the mentioned aspects will apply to large extend as well for ADF beyond this scope, namely:

- ADF operating in other regions outside the EU-market, such as China, Japan or the USA;
- ADF with higher levels of automation (L4 or L5 functions) or driverless operation (e.g. robot taxi operating in a geo-fenced ODD);
- ADF with other ODD, like urban or rural roads.

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

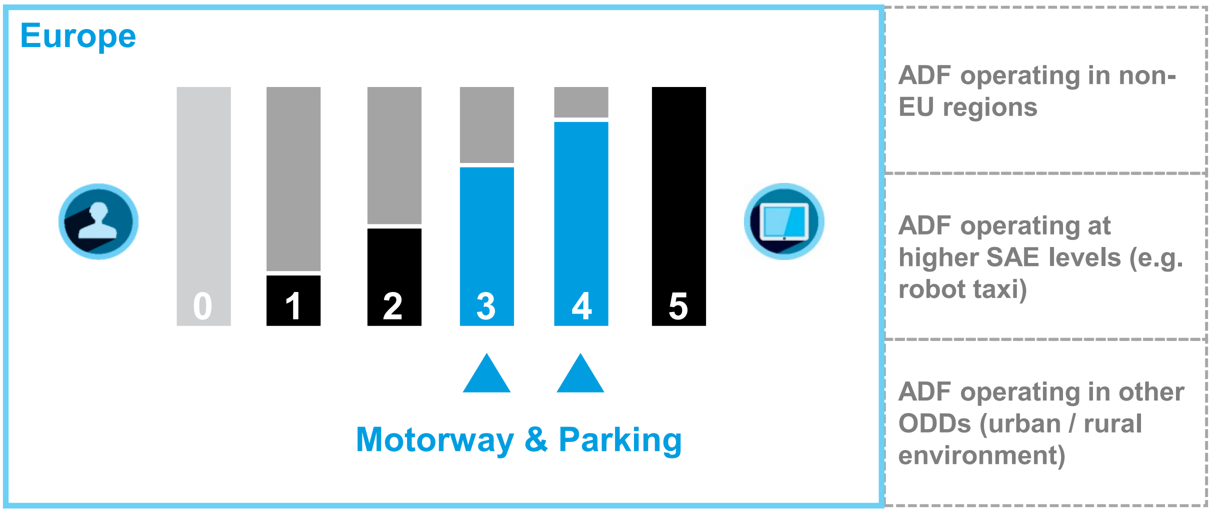

Europe
0
1
2
3
4
5
Motorway & Parking
ADF operating in non-EU regions
ADF operating at higher SAE levels (e.g. robot taxi)
ADF operating in other ODDs (urban / rural environment)

Figure 2.1: Scope of the CoP-ADF

2.4 Application of the Code of Practice for the development of ADF

The CoP-ADF is intended to support developers of ADF by providing several questions that have been defined based on the so far gained experience in the development process[1]. These questions should guide the user through different topics that are relevant for the development of an ADF. There might be some redundancy and similarities of questions in different topics, which depend on the angle we see things. It is important to note that it is not necessarily required to answer all CoP-ADF questions with “Yes” to develop an ADF. Depending on the question, a “No” might also be an appropriate answer. Some questions

[1] See chapter 4.

might also not be relevant for certain ADF. Thus, the purpose of the question is not necessarily to lead to a specific answer, but to initiate the developers' reflection about a question and to report whether and how a certain topic has been addressed in the development.

Furthermore, the questions allow to document the decision and approaches taken in the development process. In case a question has not been addressed in the development of an ADF, it is strongly recommended to document the reason for this decision. By this the CoP-ADF should lead to a more comprehensive view on the development of ADF.

L3Pilot does not prescribe on how the CoP-ADF shall later be used within companies that develop ADF. One option would be to address the questions directly in a dedicated process, the other option is to include the questions in already existing development processes. Thus, the taken approach needs to be decided by each company individually.

2.5 Users groups of the Code of Practice for the development of ADF

The CoP-ADF is an engineering-oriented guideline, which can be widely applied in industry to guide the development process as well as to provide best practices when developing and validating ADF. It is intended to be used by the user groups as listed in Table 2.1. The scope of a typical application of the CoP-ADF by these user groups is also included in this table.

Table 2.1: Overview of potential user groups and application of the CoP-ADF

User priority	User groups	Application of the CoP-ADF
1	OEMs, 1st or 2nd tier suppliers, start-ups / new comers.	CoP-ADF serves as a guideline for the development and validation of ADF. Project leaders and developers in engineering departments could benefit from collected best practices regarding relevant ADF topics through the whole development process from definition phase to post industrialization phase to establish and enrich the internal development process of ADF.
2	Public authorities	CoP-ADF could be employed as a reference to set up development strategies and regulations to pave the way for implementing AD with L3 / L4 functions into market.
2	Regulation / Type approval bodies	CoP-ADF provides the best practices from automobile industry, which could be helpful to support the process of creating regulation,

User priority	User groups	Application of the CoP-ADF
		certification or type-approval and the development / validation of ADF.
3	Academics (Universities, research institutes, Institution, etc.).	CoP-ADF could provide the best practices from automobile industry to academic institutions as a reference to the research scope regarding relevant topics.
3	Insurance bodies.	The safety aspects as well as the scenarios / limitations of ADF with L3 / L4 functions in CoP-ADF could provide a reference for insurance bodies for developing relevant products for industry and market.
3	General Public	CoP-ADF is a public document and by this help potential customers to get familiar with development / validation of relevant topics in order to give confidence and improve acceptance of ADF products.

The CoP-ADF provides applicable best practices to all stakeholders occupied with ADF to facilitate their actual development work on L3 and L4 functions. The following chapters will introduce the development process utilized to structure CoP-ADF.

3 Development Process of Code of Practice for the development of ADF

3.1 Description of Development Process of CoP-ADF

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

- The topic / process poses a common challenge in the development process that requires cooperation;
- A wrongly applied approach to 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 to a topic / process is highly likely;
- The topic / process has already been identified as relevant by others, for instance German Ethics commission on AV (di 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-ADF 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-ADF started. The first step was to collect relevant literatures based on the status at the end of 2020, which include project reports, industry documents, scientific publications, standards, regulations, and to analyse them. Based on the literature research, a set of relevant questions for the draft of CoP-ADF (Fahrenkrog et al. 2020) were defined and then improved and consolidated using an iterative update process. The outcome is the final version of the CoP-ADF that is presented in chapter 4 of this document.

A major objective of the CoP-ADF is to initiate the discussion with further stakeholders inside and outside L3Pilot project. The stakeholders’ feedback is required in order to ensure broad acceptance of the final CoP-ADF. As first step, the draft of CoP-ADF was presented to L3Pilot partners in a dedicated workshop in General Assembly of L3Pilot project in November 2019. The collected feedback was used to prepare an updated version of the CoP-ADF, which was then presented to a list external stakeholders not involved in L3Pilot, and at the same time 12 experts from different disciplines, e.g. Functional Safety (FuSa), Cybersecurity, Human-Machine Interface (HMI), Vehicle-to-Everything (V2X), Regulation, and Verification and Validation (V&V). A dedicated workshop took place in October 2020 and was arranged as a virtual event to collect the external experts' feedback and to discuss their applicability to a new version of CoP-ADF. The validation process ended up with the final review of 4 experts in L3Pilot project, the collected feedback was used to derive the final CoP-ADF in this document that is going to be published in 2021.

Furthermore, feedback from all L3Pilot sub-project have also been collected and considered. Therefore, the leaders of the other L3Pilot's sub-projects have been asked which topics of the CoP-ADF have been involved in their sub-project. Relevant topics have been discussed in more detail. An example are the findings of the sub-project "Methodology (SP3)", which prepared an internal report summarising important aspects for evaluation tools related to AD (see Annex 1). However, it must be taken into account that the L3Pilot project focuses mainly on the testing of AD on public roads with prototype vehicles. For this reason, not all topics outlined in the CoP-ADF are covered by L3Pilot project.

3.2 Development Phases in CoP-ADF

In the development of a technology, different aspects become relevant at different stages. In order to consider this aspect, the CoP-ADF is split along the development process into different phases. For the definition of the development phase, the Response 3 CoP-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-ADF, 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 the field as requested by ISO 26262 (ISO 26262-2:2018 and ISO 26262-7:2018).

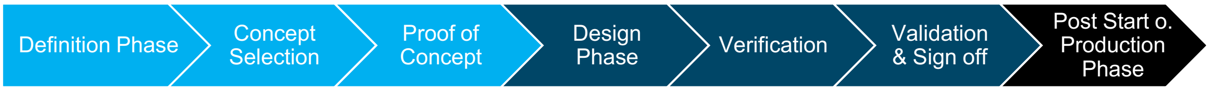


Figure 3.1: Development phases that have been proposed in deliverable D2.1 (Wolter et al. 2018)

During the course of the work, there was consensus that merging of two pairs of phases to two single phases would improve structure and comprehensibility of the CoP document without leading to a loss of content. 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 both phases.

The new structure of the phases is presented in Figure 3.2.

After defining the development phases, the categories and related topics of the CoP-ADF were established. Each question is assigned to a certain topic and development phase. One CoP question can be assigned to multiple development phases.

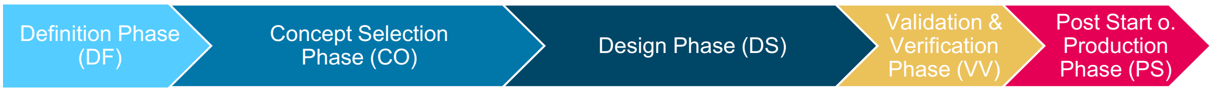

Definition Phase (DF)
Concept Selection Phase (CO)
Design Phase (DS)
Validation & Verification Phase (VV)
Post Start o. Production Phase (PS)

Figure 3.2: Development phase applied in the CoP-ADF

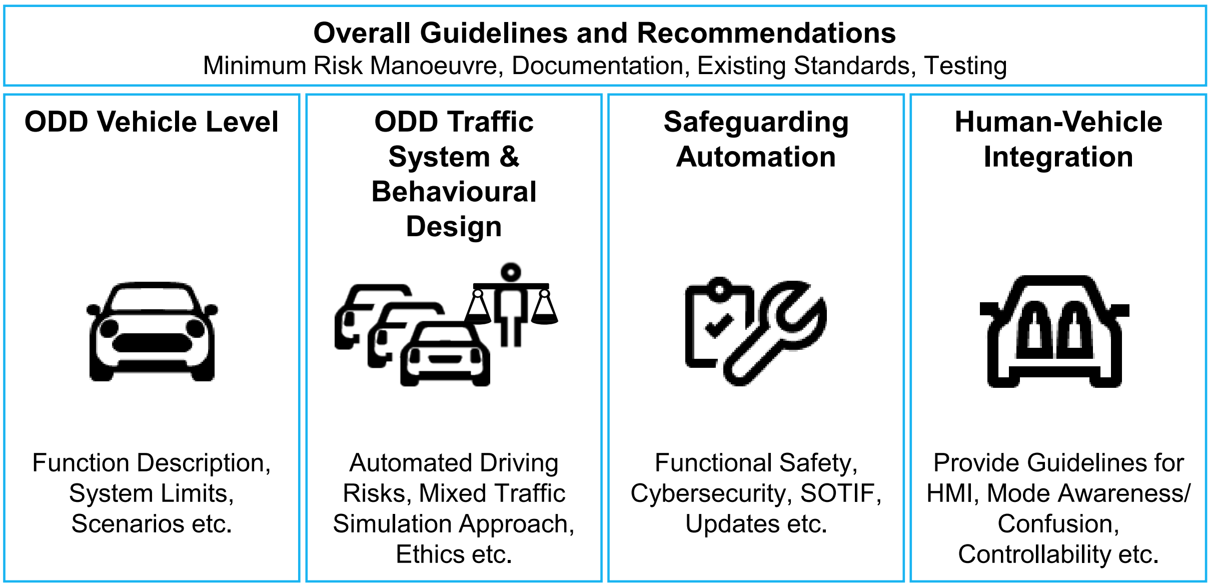
3.3 Categories and Topics in the CoP-ADF

The categories were derived from the survey among L3Pilot partners. Next to the development phases, they represent the second dimension of the CoP-ADF. Within a category, different topics are grouped. In the CoP-ADF framework (Wolter et al. 2018), five different categories have been described. These five categories are:

- Operational Design Domain (ODD) - Vehicle Level: description of the function and scenarios at vehicle level.
- Operational Design Domain (ODD) - Traffic System Level: description of the function at the level of the overall environment.
- Safeguarding Automation: how to ensure a safe operation of the function.
- Human-Machine Interaction: interaction between the driver[2] and the vehicle’s displays and control elements.
- Behavioural Design: how to take into account the behaviour of other road users.

During the work it has become clear that category 2 and 5 have many overlaps. Therefore, both categories have been merged into one category. Furthermore, certain topics have been identified as relevant to more than one category and therefore have been moved to an overall category. The updated structure of the categories is provided in Figure 3.3.

[2] Please note that the term “driver” covers in this deliverable also users outside the vehicle that operate the vehicle.



Overall Guidelines and Recommendations
Minimum Risk Manoeuvre, Documentation, Existing Standards, Testing

ODD Vehicle Level
Function Description, System Limits, Scenarios etc.

ODD Traffic System & Behavioural Design
Automated Driving Risks, Mixed Traffic Simulation Approach, Ethics etc.

Safeguarding Automation
Functional Safety, Cybersecurity, SOTIF, Updates etc.

Human-Vehicle Integration
Provide Guidelines for HMI, Mode Awareness/ Confusion, Controllability etc.

Figure 3.3: Categories used for CoP-ADF

Therefore, the CoP-ADF covers 22 different topics in one of five categories. The following table provides an overview of the different topics and the related categories covered by the CoP-ADF.

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

Category	Topics
Overall Guidelines and Recommendations	• Minimal Risk Manoeuvre (4.1.1) • Documentation (4.1.2) • Existing Standards (4.1.3) • Testing (incl. Simulation) (4.1.4)
ODD Vehicle Level	• Requirements (4.2.1) • Scenarios and Limitations (4.2.2) • Performance Criteria and Customer Expectations (4.2.3) • Architecture (4.2.4)
ODD Traffic System & Behavioural Design	• Automated Driving Risks and Coverage of Interaction with Mixed Traffic (4.3.1) • V2X Interaction (4.3.2) • Traffic Simulation (4.3.3) • Ethics & other Traffic related Aspects (4.3.4)
Safeguarding Automation	• Functional Safety (4.4.1) • Cybersecurity (4.4.2) • Implementation of Updates (4.4.3)

Category	Topics
	● Safety of the intended Functionality (4.4.4) ● Data Recording, Privacy and Protection (4.4.5)
Human-Vehicle Integration	● Guidelines for HVI (4.5.1) ● Mode Awareness, Trust & Misuse (4.5.2) ● Driver Monitoring (4.5.3) ● Controllability & Customer Clinics (4.5.4) ● Driver Training & Variability of Users (4.5.5)

4 Code of Practice for the development of ADF

Following the development process of CoP-ADF in chapter 3, this chapter presents each CoP-ADF question in the design of a card. The sub-chapters are structured by the CoP-ADF categories and topics. All cards follow a template that presents the main question, sub-questions, the ID and the relevant development phases. Each card is followed by a short explanation of the questions, which can also include hints regarding relevant literature and links to other topics.

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

Question X-Y-Z	Relevant Phase(s)	DF	CO	DS	VV	PS
Main question ( ) Yes / ( ) No		• Sub-Question 1 • Sub-Question 2 • Sub-Question 3				

In the upper left corner each 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 question within 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.

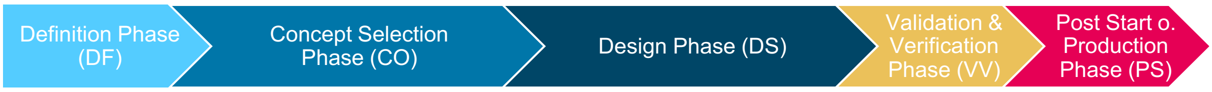

Definition Phase (DF)
Concept Selection Phase (CO)
Design Phase (DS)
Validation & Verification Phase (VV)
Post Start o. Production Phase (PS)

Figure 4.1: Development phase applied in the CoP-ADF.

The cell on the left side includes the main question, which should be answered by checking yes or no. 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 topics of the main question, 2) they should support readers in answering the main questions.

Additional explanations on the question and referenced literatures are also available for each question. It is important to note that the blow mentioned literatures have been described based on the status at the end of 2020, their corresponding topics are listed in Annex 3 Documentation List and relevant Topics in CoP-ADF. In total the CoP-ADF consists of 155 main questions that have been assigned to one of 5 categories and one of the 22 topics.

4.1 Overall Guideline and Recommendations

Before questions of the dedicated categories are presented, 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 / and the driver does not respond to take over requests (TOR). The general objective of the vehicle's manoeuvre is to reach the safest possible state in the given situation and minimising risks in traffic. It is not possible to define one single MRM for all types of ADF. The specification of the MRM depends on the kind of ADF and the L3 function definition (see **Error! Reference source not found.**) is followed. Theoretically, there is no need of an MRM because the driver should always be able to take over. Nevertheless, if the driver is not able to take over there is a strategy needed. One example could be as specified in "UN ECE ALKS Regulations" (UN ECE ALKS 2020).

Question 0-1-1	Relevant Phase(s)	DF				
Is there an appropriate mechanism for a fall-back solution for the ADF planned? ( ) Yes / ( ) No		• Is there a process to automatically and safely stop the vehicle (MRM strategy) if the TOR leads to no appropriate reaction from the driver?				

Different characteristics for initiation and non-initiation of an MRM depending on the TOR status (not issued, issued and noted, issued and not noted), automation level (L3 or L4) and the driver reaction (no reaction, reaction) are possible. For a L3 function which is defined with a driver who is able to take over at any time, the MRM strategy could be very simple. But with respect to product liability, it is recommended to define an ADF reaction in case the driver does not take over. L4 ADF needs such a strategy by definition. The TOR is a key consideration for a L3 or L4 ADF with dependencies to MRM. Information about the design of Human-Vehicle Integration (HVI) can be found in category 4.5. The TOR must be carefully considered and designed, which could help to reduce the likelihood that the MRM will need to be activated. This aspect is also of relevance, when considering safety of the intended functionality (SOTIF) (see topic 4.4.4).

For more information with examples for MRM and minimal risk condition (MRC) please check:

- "Safety first for automated driving", (Wood et al. 2019) and the related ISO technical report ISO/PRF TR 4804 (2020);
- "UN ECE ALKS Regulations", (UN ECE ALKS 2020).

Question 0-1-2	Relevant Phase(s)	DF	CO			
Is an adequate and validated concept for MRM planned? ( ) Yes / ( ) No		• Is a concept for the MRM in the ADF foreseen (e.g. degradation, take-over)? • Is the concept defined for the different driving situations and conditions? • Is the targeted / final MRC defined? • Is the condition(s) clearly defined under which the MRM shall / must be activated? • Is a concept for a safe operation during MRM available? • Is the concept (e.g. timing, handling) of the MRM validated in terms of effectiveness and safety? • Is a concept available how MRM ends (e.g. Driver take-over during MRM)?				

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 not. Furthermore, it must be ensured in the concept that the MRM can be operated safely (FuSa and SOTIF, see topics 4.4.1 and 4.4.4). The analysis should not only be limited to the ego vehicle but also consider the surrounding traffic and other road users.

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		• Is the ADF capable of performing an MRM in all the various conditions that the vehicle encounters in its ODD (including fault conditions)? • Is the ADF able to decide on appropriate characteristics of MRM (e.g. stop in lane)? • Is a function redundancy required for the chosen architecture of the MRM?				

The MRM only becomes relevant when the ADF reaches its limits (see category 4.2 "ODD Vehicle Level"). 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. The MRM strategy shall reduce situations in which a gap between available and required information (e.g., redundancy could be an adequate measure) occurs to an absolute minimum.

For more information, please check:

- “A Framework for Automated Driving System Testable Cases and Scenarios Final Report”, NHTSA (Thorn et al. 2018);
- “Safety first for automated driving”, (Wood et al. 2019) and the related ISO technical report ISO/PRF TR 4804 (2020);
- “UN ECE ALKS Regulations”, (UN ECE ALKS 2020).

Question 0-1-4	Relevant Phase(s)			DS	VV	
Are appropriate MRM implemented to cover all the various scenarios and conditions required? ( ) Yes / ( ) No		• Are different characteristics of MRM considered for different driving scenarios? • Is an adequate and appropriate interaction with the driver (and with other road users, e.g. direction indicator) ensured by the MRM (relevant criteria: safety, driving experience, trust, situation awareness)? • Is the MRM implemented according to the concept and its specification? • Is the MRM implementation tested sufficiently in different conditions (criteria: safety, performance, reliability / robustness)? • Do the MRM test scenarios consider possible reactions of the surrounding road users?				

Once a concept has been decided on, it must be ensured that the MRM is correctly implemented. For this purpose, different validation and verification (V&V) steps (e.g., analysis, reviews, test and simulation) are required in order to prove completeness and correctness of the MRM.

For more information, please check:

- “Thatcham Research Report”, (Thatcham 2018);
- “Safety first for automated driving”, (Wood et al. 2019) and the related ISO technical report ISO/PRF TR 4804 (2020);
- “UN ECE ALKS Regulations”, (UN ECE ALKS 2020).

Question 0-1-5	Relevant Phase(s)				VV	PS
Do the test cases consider all the different MRM activation conditions? ( ) Yes / ( ) No		- Does the ADF reach the safe state after MRM? (Also during post start of production). - Is the MRM validated with respect to the safe state that the MRM achieves the end?				

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.

More information about V&V can be found in topic 4.1.4.

4.1.2 Documentation

During the development of ADF a huge amount of information is generated. It is obvious that certain information needs to be documented in order to use them for specific purposes. These purposes are for instance the homologation process, internal approval process or evidence in case of court disputes. In some cases, there are explicit requirements for documentation, e.g. as given in the “UN ECE ALKS Regulation” (UN ECE ALKS 2020). However, this is not always the case.

This topic mainly deals with the documentation of test 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. It must be noted that the tests to be conducted depend on the ADF’s status and its scope. Hence, the documentation shall also consider the requirements of the ADF in order to make the chosen tests understandable.

Question 0-2-1	Relevant Phase(s)	DF	CO	DS		
Are the requirements checked during the tests documented? ( ) Yes / ( ) No		- Is a format and process defined to document the ADF requirements that shall be tested? - Is a process established to document updates for the requirements?				

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 the company.

<table>
<tr><th>Question 0-2-2</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th>DS</th><th>VV</th><th></th></tr>
<tr><td colspan="2">Is a documentation and reporting process in place with regard to assessing, testing and validating the ADF capabilities as well as design decisions?
(   ) Yes / (   ) No</td><td colspan="5">• Is a process established to document the performed tests and compliance (fail/pass)?
• Is a process established to document updates of the test plan?
• Does the documentation format comply with requirements of external stakeholders?
• Is a safety argumentation (analogous safety case in ISO 26262) set up and described?</td></tr>
</table>

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 V&V 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.

<table>
<tr><th>Question 0-2-3</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th>DS</th><th>VV</th><th>PS</th></tr>
<tr><td colspan="2">Is a reporting process established to feedback the knowledge / lessons learnt during testing and development?
(   ) Yes / (   ) No</td><td colspan="5">• Is a reporting process established in which faulty behaviour can be recorded during testing?
• Is a reporting process established to review the results obtained and to address reporting of identified deficiency?
• Is a reporting process established to update test cases based on the experiences of past projects?</td></tr>
</table>

Question 0-2-3	Relevant Phase(s)		CO	DS	VV	PS
		- Does the reporting system cover the required steps to handle the identified deficiency? - Does the reporting process consider data from all test methods (test track, simulation and test on public roads, etc.)?				

These questions address how lessons learnt can be collected during testing and development of future ADF. 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.

In case deficiencies are detected, such information shall be reported to allow to reconstruct the deficiency at a later point in time. Therefore, the more information (amount and detail) is available, in general the better it is for the reconstruction of the deficiency. However, often a trade-off between the information amount and the available on-board and off-board storage needs to be found. A minimum set of information should at least include the following set of information:

- Time;
- Location;
- Weather conditions;
- Description of the conducted test;
- Description of the deficiency;
- Vehicle state;
- Road and infrastructure state;
- Traffic state;
- Software Version of ADF.

The knowledge that is gained in the test activities or about deficiency 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.

<table>
<tr><th>Question 0-3-1</th><th>Relevant Phase(s)</th><th>DF</th><th>CO</th><th>DS</th><th>VV</th><th>PS</th></tr>
<tr><td colspan="2">Are (industry) standards and best practices according to their current availability followed?
(   ) Yes / (   ) No</td><td colspan="5">• Are relevant standards and best practices (according to their current availability) been identified and evaluated?</td></tr>
</table>

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

- Potential hazards caused by the intended function (e.g. due to sensor performance boundaries), ISO/PAS 21448 “SOTIF“(ISO/PAS 21448 2019);
- Foreseeable misuse, ISO/PAS 21448 “SOTIF“(ISO/PAS 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/PAS 21448 2019);
- Influences from the humans behaviour, ISO/PAS 21448 “SOTIF“(ISO/PAS 21448 2019).

In addition, the UN document / regulation should be adhered to:

- UN documents / regulations, “Framework document on automated / autonomous vehicles“ (UN 2019);
- UN ECE R-155 (2020), “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system” (UN ECE Cyber Security);
- UN ECE R-156 (2020), “Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System” (UN ECE Software Update and Software Updates Management System);
- “UN ECE (2020) ALKS Regulations”, (UN ECE ALKS).

The state-of-the-art is changing over time. Therefore, the compliance with this question requires a constant review and update process. One comprehensive document to start with for example is the “Safety First for Automated Driving” document (Wood et al. 2019). The Safety first of automated driving activity is continued under the umbrella of ISO (technical report ISO/PRF TR 4804 has been finished; the technical specification ISO/TS 5083 is currently under development). However, there are other activities by other international organizations such as SAE and FISITA. ADFs that focus on traffic jams must comply with the UN ECE ALKS regulations.

Also, the L3Pilot project contributes with its research activities to the evolving state-of-the-art for AD.

There are other related topics that are not covered in detail by the CoP-ADF. 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, where the AdaptIVe deliverable D2.3 (Bienzeisler et al. 2017) provides further insights.

4.1.4 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 (see topic 4.2.1) and to be validated regarding its design (see topic 4.2.4). All these steps require testing by means of one or more test tools (see Annex 1). Typical testing tools are:

- X-in-Loop Tests (Hardware-in-the-Loop, Model-in-the-Loop, Software-in-the-Loop, computer simulation, etc.),
- Driving simulators tests,
- Test in controlled environments like test tracks (test with demonstrator vehicles, Vehicle-in-the-Loop tests),
- Field test.

The objective of the document is not to state which testing tool or approach shall be selected for a certain test. The objective of this topic is rather to ensure that the planning and execution of the testing is done in proper and safe manner.

The following questions 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 0-4-1a	Relevant Phase(s)	DF				
Is a test concept for the development, certification / homologation, (internal and external) V&V of the ADF and its subcomponents available? (Test purpose) ( ) Yes / ( ) No		• Is a test concept defined which verifies / validates the technical maturity of the ADF? • Is a test concept defined that verifies that the requirements for the ADF are met? • Is any (specific) security testing planned covering not only the function and architecture but also the AD scope (e.g. operation as fleet vehicles)?				

Question 0-4-1a	Relevant Phase(s)	DF				
		• Is a test concept defined which investigates the safe operation of the ADF in the corresponding ODD in conjunction with the driver? • Is a test concept defined which investigates additional risks associated with ADF in conjunction with the driver compared to manual driving? • Is a test concept defined which validates that the ADF fulfils its intended purpose? • Is a test concept defined that validates a positive balance of risks?				

Question 0-4-1b	Relevant Phase(s)	DF				
Is a test concept for the development, certification / homologation, (internal and external) V&V of the ADF and its subcomponents available? (Test execution) ( ) Yes / ( ) No		• Does the concept define appropriate test tools / environments for the tests? • Considering the purpose of test (e.g. homologation /certification of the ADF), is the required data identified? • Does the test concept include an execution plan / time plan for the tests? • Are all requested tests included in the concept? • Is testing with different penetration rates considered at every traffic layer (from vehicle infrastructure up to network components)?				

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 on the interaction with the user(s) in different driving scenarios, like e.g. a lane change.

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 expectations as well as societal expectations. 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 (di 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 topic 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) and the related ISO technical report ISO/PRF TR 4804 (ISO/PRF TR 4804 2020);
- “Road vehicles — Terms and definitions of test scenarios for automated driving systems” (ISO 34501-4 20XX).
- “UN ECE ALKS Regulations”, (UN ECE ALKS 2020).

Question 0-4-2a	Relevant Phase(s)		CO			
Is each single test of the (test) concept specified properly? (Test planning) ( ) Yes / ( ) No		• Are the test parameters (including among others length, number of tests) defined for each test (e.g. the number of test repetitions, test duration, test subjects)? • Are the test parameters in line with the situations that the ADF will encounter in its ODD? • Is defined, how many test repetitions / test persons / mileage driven / time driven is/are required? • Are guidelines for the conduction of tests available? • Are success criteria for each test defined? If not, is it defined when the test needs to be repeated? • Is the criticality of the test (potential safety risk resulting from the test) evaluated beforehand?				

Question 0-4-2b	Relevant Phase(s)		CO			
Is each single test of the (test) concept specified properly? (Test execution) ( ) Yes / ( ) No		• Is it defined which information from the tests needs to be documented? • Is it defined, how the information from the tests should be stored? • Is the reference data (ground truth data) for the test defined? • Are data privacy aspects considered? • Are safety measures for the participants considered? • Is the approach for the training of safety drivers or remote operators been defined / implemented?				

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. Verifying the completeness of the tests remains a challenge, since there will be unknown situations and parameters. A first step is to analyse the known area of the test space in transparent manner. This means to describe the data and information on which the test criteria are defined. In a second step a process should be defined which ensures a continuous reduction of the unknown areas in test space.
- 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 an authoritative analysis. The test amount also covers 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 topic 4.1.2).
- If reference data are required 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 train safety drivers. Robust procedures to ensure the competency of safety drivers and operators must be developed.

<table>
<tr><th>Question 0-4-3</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Is the test space defined according to the function design and the intended ODD? (Test planning)
(   ) Yes / (   ) No</td><td colspan="5">• Are the relevant driving scenarios defined covering the entire ODD?
• Are relevant rare driving scenarios taken into account?
• Are relevant critical scenario taken into account?
• Is a process established that ensures that the right relevant scenarios are selected?
• Are scenarios taken into account that cover the entire operation of the ADF (not available, ready, activation, active and operating, deactivation)?
• Are all (relevant) requirements of the ADF tested?</td></tr>
</table>

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). This concept relies also on deriving test cases from a database, in which contains several real world driving scenarios and which is manufacture independent. Such a database would be of course very helpful to ensure the correct definition of the test space and the test cases. However, it must also be noted that such database must be available and could miss some rare event that are of importance for a certain ADF. In the latter case the “injection” of expert defined test cases could be an approach to fulfil these gaps in the database.

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.

It must also be ensured that all (relevant) requirements of ADF are covered by tests and checked whether the function fulfils them. Here, it is important to note that function's requirements can change in the course of development. These changes must be considered in the test plan continuously during the development process. Therefore a process shall be established that ensures that updated in the requirements leads also to an updated of the test plan.

Question 0-4-4	Relevant Phase(s)				VV	
Is the test plan implemented and followed correctly? (Test execution) ( ) Yes / ( ) No		• Are any deviations from the test concept / plan documented? • Are any reasons for the deviation from test concept / plan documented? • Are all required data for the sign-off, homologation or certification process available?				

Once the tests have been executed, the question, whether the test plan is correctly implemented and followed, becomes relevant. While testing, different limitations or constrains 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. The answer to the question, what the required data quality is depends strongly on the purpose of testing. To a certain extend the requirements need to be defined by the (external) stakeholders. In case there are no clear requirements set by the external stakeholders, it is important to ensure that the data provide clear and not contradicting results, for instance a high deviation between single tests with identical input parameters could be an indicator for a deficient data quality.

<table>
<tr><th colspan="2">Question 0-4-5</th><th colspan="2">Relevant Phase(s)</th><th>DF</th><th>CO</th><th>DS</th><th>VV</th><th>PS</th></tr>
<tr><td colspan="4">Is the execution of the planned tests with the ADF feasible? (Test planning)
(   ) Yes / (   ) No</td><td colspan="5">• Are the interfaces for the test tools properly defined and implemented?
• Are all required licenses (incl. testing and driving licenses) for the test available?
• Is the ADF mature enough to conduct the planned test?
• Are safety and security aspects investigated before the test?
• Are the required test tools available for testing?
• In particular in case of tests on public roads, have relevant stakeholders (e.g. road operators, police) been informed about the testing activities beforehand.
• Are the applied test tools verified and validated before they are used?
• Are the required inputs available?</td></tr>
</table>

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 needs to be checked and ensured. This addresses already such simple aspects, like the ADF is activated on the test track for the testing? 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 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 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 must 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) and the related ISO technical report ISO/PRF TR 4804 (ISO/PRF TR 4804 2020).

Question 0-4-6	Relevant Phase(s)	DF	CO	DS	VV	PS
Is the testing activity safe? (Test planning) ( ) Yes / ( ) No		• Is a risk assessment conducted before the test? • Does the risk assessment consider individuals who are not directly involved (e.g. surrounding traffic)? • If V&V is carried out on public roads, are potential effects to other traffic participants considered and safety measures defined? • Are safety measures for the testing process taken? • Is it been defined how test engineers should respond in case of a failure during the testing process? • Is the staff (e.g. test and safety driver, V2X-operator) involved in the test been properly trained? • Is it been ensured that vehicle operators are allowed to operate a vehicle (following company internal and legal requirements) and have received appropriate training?				

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, individuals involved in testing should take all necessary precautions to ensure the testing process is completed as safe as possible. In this context, the use of tools, e.g. Hazard Analysis and Risk Assessment (HARA), Failure Mode and Effect Analysis (FMEA) and checklists can support the identification and addressing of potential risks.

These precautions which need to be taken should be 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 obeyed.

Question 0-4-7	Relevant Phase(s)		CO	DS	VV	PS
Are the national testing guidelines / regulations being followed? (Test planning) ( ) Yes / ( ) 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 AD, 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 this topic to which the last few questions relate.

<table>
<tr><th>Question 0-4-8</th><th>Relevant Phase(s)</th><th>DF</th><th>CO</th><th>DS</th><th>VV</th><th></th></tr>
<tr><td colspan="2">Are X-in-the-loop systems (XIL) tests like simulation part of the test concept and testing? (Test planning / execution)
(   ) Yes / (   ) No</td><td colspan="5">• Are SIL, MIL and / or HIL considered in the test plan?
• Is it analysed, which tests can be performed as open- and as close-loop simulation tests?
• Are the XIL test tools been validated for their intended purpose?
• Is it ensured that training data, validation data and testing data are independent?
• Are all relevant scenarios (as well) covered in XiL tests?</td></tr>
</table>

The application of simulation tools comes with some associated challenges. The challenge of V&V is already addressed by the questions 0-4-5. 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 option 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.
- When applying XIL testing tools the test cases and interfaces need to be described properly. In recent times, different activities are ongoing to standardize the description of test cases. Examples are OpenDrive (ASAM OpenDrive 2020) and OpenScenario (ASAM OpenScenario 2020) ASAM activities or the German funded project Set Level 4 to 5 (Set Level 4 to 5 2020). Standardized test case descriptions and interfaces make in particular sense in case exchangeability of test or models with other organizations is of importance.
- 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) and the related ISO technical report ISO/PRF TR 4804 (ISO/PRF TR 4804 2020);
- ASAM XIL Standard (ASAM XIL 2020).

4.2 Category “ODD Vehicle Level”

The ODD describes the specific scenarios and conditions in which the AVs are designed to function. The scope of the ODD is dependent on the feature of the ADF embedded in the AVs. This category 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.

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 function’s behaviour. This topic is strongly related to chapter 4.5 Category “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.

4.2.1 Requirements

Right from the definition phase, it is imperative that all requirements are identified and clearly defined. This is essential in order to provide the basis for good design, development and testing. Lack of requirements impedes traceability and ability to do design reviews. The requirements for the ADF describe the system’s desired behaviour under a dynamic environment based on available information. Moreover, the requirements have to take into account all regulations.

The questions described below provide a starting point for specifying the minimum level of ADF requirements that define ODD conditions. Indeed, further questions can be added in the future while the maturity level of the technology will increase.

Question 1-1-1	Relevant Phase(s)	DF				
Are the different attributes of the requirements considered? (E.g. specific, measurable, attainable, relevant, testable, etc.) ( ) Yes / ( ) No		• Are target-values defined for all the requirements? • Is the controllability considered? • Are the feasibility and the usage condition of the requirements considered (i.e. when and in which cases can the requirement be realised)? • Are the expected completion times for these requirements defined? • Are appropriate metrics and thresholds available? • Do system requirements meet known quality standards?				

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 characteristics are required instead of abstract goals in order to be able to properly trace component functionalities. The following characteristics are generally accepted for 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, vague statements like 'acceptable' should be avoided, but instead measurement units shall be used;
- Attainable – The requirement should be implemented within the ODD constraints and the resulting deployment of the release;
- Relevant – The requirements should meet the actual ODD need;
- Testable –The requirements were met by the ADF and can be inspected and verified.

Question 1-1-2	Relevant Phase(s)	DF				
Is the traceability ensured between requirements and other streams as in design, development and testing? ( ) Yes / ( ) No		• Is the requirement workflow defined? • Are requirement tools used (e.g. DOORS, Polarion, Visure, etc)? • Is changing requirement process managed?				

In principle requirements traceability is defined as the ability to describe and follow the life of a requirement through the whole system life cycle. In order to achieve this the adoption of a tool such as DOORS (Doors, 2020) can spark such discipline.

Many times, a requirements traceability matrix (RTM) does not exist although there is a need to ensure requirements completion and to understand change impact. Requirements evolve over time due to technical limitations, legal aspects or different market needs. New requirements are added while others change. However, as the system requirements evolve, the quality of tracing has to be always maintained to avoid inaccurate and untrusted links over the streams.

Question 1-1-3	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. 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 1-1-4	Relevant Phase(s)	DF				
Does the ADF comply with the key requirements (such as system boundaries, functional stability, composability, redundancy, etc.)? ( ) Yes / ( ) No						

The core technical requirements for ADF must be addressed. Those requirements should be the basis for operational approval. Creating consistent requirements and meeting key attributes will enable a stable development process, which facilitates operational approval and guarantees the ADF’s compliance with the specifications and rules and its synchronisation with the overall system. 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 maximising performance, reliability and overall system stability.

Question 1-1-5	Relevant Phase(s)	DF				
Is a means (e.g. graphical representations and state diagrams) provided for comprehensive analysis of the requirements? ( ) Yes / ( ) No						

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) (Szymanski, 2018) 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 an approach to deal with the limitations of document-based approaches while being capable of identifying problems and reducing the risk of having ambiguous requirements. MBSE utilises System Modelling Language (SysML) which can use requirements diagrams to efficiently capture functional, performance and interface requirements.

Question 1-1-6	Relevant Phase(s)	DF				
Are the ADF states defined (e.g. Non-operational, Operational without notifications, Operational with some notifications, Operational with all notifications available)? ( ) Yes / ( ) No						

Fundamental to ADF is the need to be safe even if 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 fall-back. However, the redundancy of a system is not designed by default, but it has to be defined by a safety analysis. 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. The following generally accepted operational scenarios may be considered:

- 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 1-1-7	Relevant Phase(s)	DF			
Do the function limitations cover the identified / considered risks? ( ) Yes / ( ) No		• Are the risks analysed to understand which are acceptable and which are unacceptable? • Is it ensured that the ADF can reach a MRC?			

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 SOTIF (see topic 4.4.4).

Question 1-1-8	Relevant Phase(s)	DF			
Is / Are 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 significantly 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 a 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 in higher computing requirements to execute more complex software. From fully manual to fully automated capabilities, the SAE's approach to automated driving (SAE J3016) remains the industry's most widely accepted classification system. Please consider in this context also the SOTIF (see topic 4.4.4).

Question 1-1-9	Relevant Phase(s)	DF			
Is a checklist considering ODD requirements for the ADF defined? ( ) Yes / ( ) No		• Are the ODD requirements for the specific ADF defined with respect to a standardized ODD taxonomy (e.g. appendix A of Thorn et al. 2018, ISO/WD 34503 and BSI/PAS 1883)?			

Such a list is unlikely to be comprehensive, but an attempt to compile a list can be a starting point for stating 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 1-1-10	Relevant Phase(s)	DF				
Is a formal verification strategy for the chosen ODD defined? ( ) Yes / ( ) No		• Is the right interaction between the vehicle and its environment ensured? • Is the coverage of the requirements by the V&V tools (e.g. MIL, SIL, HIL, proving ground and real-world driving) checked? • Is a requirements concept for a test case deployed?				

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 quality 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 (see topic 4.1.4). 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 1-1-11	Relevant Phase(s)	DF				
Are the requirements analysed taking into account the safety impact? ( ) Yes / ( ) No		• Is safety verified beyond the single component? • Is the safety impact considered for changes of human and automation roles? • Are there any trade-offs between safety and performance? • Is safety aspects of compromised security taken into account as well?				

Requirements analysed from the safety perspective must address the highly adaptive and non-deterministic behaviour of these systems.

Therefore, the answer to this question will address several aspects of safety that apply to ADF. An important goal for ADF is to reduce the potential of risks occurring during operation. Especially for assessing the safety at all levels from individual components and subsystems to the vehicle as a whole, a 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 1-1-12	Relevant Phase(s)				VV	
Is the actual technical performance verified to be in line with the defined ODD? ( ) Yes / ( ) No		• Is the actual performance rated against the ODD requirements (e.g. not-compliant vs. compliant)?				

In general requirements are not completed without an understanding of how they will be tested. For the same reason they must also be verified and validated (V&V) in order for the ADF to exert trust. 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 ADF 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 1-1-13	Relevant Phase(s)				VV	PS
Is a general strategy available to monitor released vehicles in the field? ( ) Yes / ( ) No						

In order to assess an ADF, it is needed to drive it in real traffic and observe its performance. Moreover, an ADF system is expected to detect whether it has left the ODD, then it must be able to monitor the ODD at runtime and it must be able to detect the nearby-events, warning the vehicle, that it will be soon out of ODD. In the VV and PS phases, it is important to monitor the ADF to understand issues and improve the system. Developers of AVs rely on data to evaluate and improve their systems.

Question 1-1-14	Relevant Phase(s)				VV	PS
Is a strategy available to feedback learnings into the development cycle and to release updates for already delivered vehicles? ( ) Yes / ( ) No						

An ADF 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 ADF. A strategy must exist to explore and highlight challenges associated with the deployment of the system in real world. In addition to that, using feedback-based retrieval techniques, we can make this stage of the process more efficient because we will be able to analyse data from real field.

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 are defined intentionally and are known, but it can be expected that there will be cases where the specified 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? ( ) Yes / ( ) No		• Are function limitations reproducible (e.g. in the same situations / under the same conditions)? • Are the ADF tasks (DDT) that the function must cope with analysed? • Are limitations considered in the selection of the perception platform? • Are function limitations measurable?				

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 object classes, which the driving ADF 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 ADF 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 within the ODD limitations? ( ) Yes / ( ) No		• Can each inherent ODD limitation be detected by the function once it is reached?				

An ADF that operates outside 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 and,
- 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, operation in degraded mode, etc.).

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 0-4-3).

Question 1-2-3	Relevant Phase(s)		CO			
Is a scenario-based approach utilized that sufficiently covers the ADF's ODD? ( ) Yes / ( ) No		• Is a structured approach used to identify critical scenarios? • Is a test catalogue utilised in order to guide the V&V activities? • Are functional, logical and concrete scenarios considered for verification?				

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 (see topic 4.3.3).

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 a test – ranging from functional via logical up to concrete test scenarios. Additional information regarding this topic and a corresponding scenario database is for instance provided by the PEGASUS project (PEGASUS 2019). Regarding V&V methods, new methods for the evaluation of ADF (L4, L5 functions) are being investigated for example by the project “VV methods” (VV Methoden).

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 would need to be supported in order to have an understanding about the ADF’s performance and his / her role and responsibilities during automated driving (ITF 2018).

Question 1-3-1	Relevant Phase(s)	DF		DS		
Is a concept defined to identify user requirements? ( ) Yes / ( ) No		• Are customer abilities and limitations considered? • Are customer preferences and expectations of the ADF that is being designed considered? • Is customer feedback in previous projects considered?				

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, considering not 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 identified customers / users groups. 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		DS		
Are realistic and objective performance criteria considered? ( ) Yes / ( ) No		• Are means established to ensure that criteria are realistic (e.g. usage of customer clinics)?				

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		
Are cooperative systems between ADF and driver considered? (The driver may be inside or outside the vehicle). ( ) Yes / ( ) No		• Is the specific performance of the ADF (including performance boundaries) clearly defined for the user? • Is a concept developed to validate each of the performance criteria which have been set?				

Transport systems can be improved in terms of efficiency and safety by cooperative behaviour among different traffic participants (Bartels et al. 2015). Since L3 functions which are in the scope of the CoP-ADF focus on ADF in which the driver needs to be ready to take over control of the vehicle and so it is essential that it is defined how the cooperation between the involved agents (vehicle ADF, user, infrastructure and other road users) is established, considering that the driver must understand when s/he is in control of the vehicle and when a transfer of control occurs. 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	
Is a method implemented to validate the target performance and the customer requirements? ( ) Yes / ( ) No		• Are performance boundaries validated?				

A V&V concept is required to ensure that the targets that were defined in the design phase can be met. Then, the V&V concept must be implemented. This V&V 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 topic 4.1.4).

Additional information regarding this topic is provided by:

- “A Framework for Automated Driving System Testable Cases and Scenarios”, NHTSA (Thorn et al. 2018).

Question 1-3-5	Relevant Phase(s)				VV	
Is a process established to understand how customer expectations can be satisfied? ( ) Yes / ( ) No		• Does the process consider how customer expectations and capabilities change based on their driving experience in automated driving mode? • Does the process consider how customer expectations evolve based on their driving experience in manual driving?				

As part of the validation phase, it is necessary to review whether the customers’ 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 are 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 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 HVI (see category 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.

<table>
<tr><th>Question 1-4-1</th><th>Relevant Phase(s)</th><th>DF</th><th>CO</th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Is a rationale for the chosen physical architecture put in place?
(   ) Yes / (   ) No</td><td colspan="5">• Is a rationale for the chosen sensor set put in place?
• Is a rationale for the chosen actuator(s) put in place?
• Is a rationale for the chosen Electronic Control Unit (ECU) put in place?</td></tr>
</table>

According to ISO 15288:2015 (ISO 15288 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			
Is a verification / analysis undertaken to ensure that the selected architecture can detect, recognise and classify any (relevant) object within the ODD? ( ) Yes / ( ) No						

Once the ODD is defined, the Object and Event Detection and Response (OEDR) capabilities must be specified. OEDR refers to "the subtasks of the DDT that include monitoring the driving environment (detecting, recognising, 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 fall-back)". (SAE 2018)

The OEDR capabilities are derived from two inputs. First the objects defined in the ODD must be analysed 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 analysed, 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 x #E x #R) is reduced to the number of feasible combinations.

Question 1-4-3	Relevant Phase(s)	DF	CO			
Is a verification / analysis completed to ensure that the selected architecture responds to any (relevant) object when the ADF is operating under the ODD limit[3]? ( ) 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) suggest 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

[3] ODD limit here includes also the continued operation during a take-over request until the driver has taken over the control or a minimal risk manoeuvre starts. Operation during the minimal risk manoeuvre shall also be covered in an appropriated way.

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).

More information regarding OEDR strategy can be found in topic 4.4.1.

Question 1-4-4	Relevant Phase(s)		CO			
Does the chosen functional architecture cover the specified functionalities? ( ) Yes / ( ) No						

The SAE J3016 standard describes the classification for road-bound vehicles with ADF. Each of the six defined levels is classified by the (minimum) requirements on how much the driver has to be involved in the 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 L3, the DDT fall-back strategy relies either upon the attentive driver to respond by resuming manual driving or by achieving a MRC. For L4, the function shall perform the fall-back by automatically achieving a MRC (see topic 4.1.1).

Question 1-4-5	Relevant Phase(s)		CO			
Are the architectural aspects between function and other elements outside vehicles considered? ( ) Yes / ( ) No		• Is the interface to backend, clouds services and other vehicles considered? • Is security and integrity of the architectural interfaces considered?				

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

Question 1-4-6	Relevant Phase(s)	DF	CO			
Are requirements for safety, security and maintainability considered for the selection of an appropriate architecture? ( ) Yes / ( ) No		• 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? • Does ADF's architecture fulfil standards like the SAE architecture (SAE 2012) or other state-of-the-art published architecture (e.g. Wood et al. 2019)?				

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, maintainability, reliability, availability and scalability. Since such aspects have a huge impact on the architecture and ADF design, the category 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 – see section 4.4.1);
- The function is secure with respect to state-of-the-art security methods and standards, see section 4.4.2;
- 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 the references within) which specifies architecture viewpoints, architecture frameworks and architecture description languages for use in architecture descriptions.

Question 1-4-7	Relevant Phase(s)		CO			
Is a rational for the allocation of logical and functional architectures to the physical architecture available? ( ) Yes / ( ) No		• Are sensing, perception, world modelling and navigation and planning supported by the software and hardware components?				

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 development 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 comply with the processes of ISO 26262 (ISO 26262 2018) and SOTIF (ISO/PAS 21448 2019). To evaluate the confidence of a software tool in the development the following criteria shall be considered:

- The possibility that a malfunctioning software tool could produce erroneous outputs, which could take it in turns;
- 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, Automotive Safety Integrity Level (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 models provides the required level of realism of real world (see question 0-4-5 and 0-4-6).

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

4.3 Category “ODD Traffic System Level & Behavioural Design”

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

- Safety impacts in the context of mixed traffic system,
- V2X Interaction (Interaction between automated driving cars and environment),
- 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 surrounding traffic (automated and / or manual). Only if the risks are well understood, mitigation strategies can 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	PS
Are the risks of the ADF within its ODD considered? ( ) Yes / ( ) No		• Are the risks at entry to and exit from the ODD considered? • Are the risks from infrastructure or other road users considered? • Are unspecified or unexpected events identified from studies in real traffic? • Are unspecified or unexpected events considered in the HARA? • Are the function limitations within the ODD considered? • Is a recording of ADF accident data or disengagements considered to help identify risks? • Is the mechanism for publication or sharing of the disengagements with a third party considered?				

This question addresses directly, whether all ADF related risks have been considered and identified within the ODD related to the surrounding traffic. The sub-questions should assist the analysis of this main question by providing hints towards the types of risks that might be present within the ODD. They target specific risk types, which could occur within the ODD and prompt further thoughts on whether the risks have been fully understood. The obvious risk of the driver not regaining full situational awareness when a transfer of control has been completed is one which will require significant research & validation to ensure it is minimised. The ability for the ADF to respond appropriately in all kinds of mixed traffic scenarios is also a high risk which could affect the safety of the ADF itself as well as the user's acceptance and trust in the ADF.

The HARA is an important step to ensure that the risks of the ADF within its ODD are fully understood. Through hazard analysis all the possible hazards which could potentially occur during the development, integration and use of the ADF need to be considered. Through the risk assessment of these hazards, any hazard which causes an unacceptable amount of risk requires a solution which mitigates it. It is recommended that this exercise is conducted at an early stage so that the system design can take the mitigating solutions into account. The HARA should be maintained throughout the life of the ADF as new hazards are identified.

Additional information regarding this topic is provided by:

- International Transport Forum, "Safer Roads with Automated Driving" (ITF 2018).

Question 2-1-2	Relevant Phase(s)	DF	CO	DS	VV	
Are the ADF capabilities identified and verified in terms of OEDR? ( ) Yes / ( ) No		• Is the response of the ADF considered for road obstructions, lane allocation & re-routing, road etiquette for emergency vehicles and interpreting gestures of other road users? • Is the negotiation of difficult objects such as aggressive drivers, jaywalkers, bicyclists, delivery trucks, construction, unprotected left turns, 4-way stop signs and other factors that arise when driving in the city considered? • Is external information from other vehicles, infrastructure and/or back-end supporting the pre-emption of OEDR?				

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.

It is also worth considering the input from other vehicles and infrastructure through the connected vehicle and infrastructure capabilities. There may be some benefit to OEDR which can be gained from connectivity with other road users and the road infrastructure, rather than relying completely on the data from the ego vehicle's sensors.

Additional information regarding this topic is provided by:

- "A Framework for Automated Driving System Testable Cases and Scenarios", NHTSA (Thorn et al. 2018).

<table>
<tr><th>Question 2-1-3</th><th>Relevant Phase(s)</th><th>DF</th><th></th><th></th><th>VV</th><th></th></tr>
<tr><td colspan="2">Is the ADF designed, verified and validated with surrounding road users and infrastructure?
(   ) Yes / (   ) No</td><td colspan="5">• Does the ADF operate with a natural and predictable driving style?
• Are the active safety capabilities of the vehicle been validated in normal driving scenarios as well as in corner cases[4]?
• Is it identified whether the ADF can exchange info about ADF intentions with other equipped vehicles or road users?</td></tr>
</table>

Mixed traffic is the term used to describe traffic on the road which is made up of a miscellany of different objects such as vehicles, lorries, motorbikes, bicycles and pedestrians. The interaction with mixed traffic can be extremely complex as the responses of different road users vary significantly in different scenarios. Dangerous situations 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 similar 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

[4] Corner cases are very important to be considered 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 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.

It is also important to understand the exchange of information between road users. The ADF can make use of connected capabilities to improve the performance of its interaction with other road users and infrastructure.

Additional information regarding this topic is provided by:

- "A Framework for Automated Driving System Testable Cases and Scenarios", NHTSA (Thorn et al. 2018).

<table>
<tr><th>Question 2-1-4</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th>DS</th><th></th><th></th></tr>
<tr><td colspan="2">Are the risks to the surrounding traffic during transition of control identified and assessed?
(   ) Yes / (   ) No</td><td colspan="5">• Can the ADF recognise function or driver limits that do not allow a safe driver take-over, and react to minimise the risk?
• Is it considered how to initiate take-over to the driver in a robust, safe and intuitive manner?
• Does the ADF take the driver's reduced situational awareness into account to mitigate risks once the driver has regained control of the vehicle?</td></tr>
</table>

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 entirety for all scenarios. Additional information regarding this topic is provided by:

- "Safety first for automated driving", (Wood et al. 2019) and the related ISO technical report ISO/PRF TR 4804 (ISO/PRF TR 4804 2020).

Question 2-1-5	Relevant Phase(s)			DS		
Are the potential ADF failure modes due to interaction with mixed traffic identified within the ODD and have relevant failure mitigation strategies been implemented? ( ) Yes / ( ) No		• Are potential failure mitigation strategies considered including both fail-operational and fail-safe techniques? • Is the limited capability of the ADF considered, based on the mitigation strategies selected? • Is setting a hierarchy of mitigation strategies considered depending on its impact and effectiveness? • Is there a safety concept for cooperation between the ego vehicle and other road users?				

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:

- “A Framework for Automated Driving System Testable Cases and Scenarios”, NHTSA (Thorn et al. 2018).

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 performance of automation at all levels (USDOT 2018). V2X refer to the technology that allows vehicles to communicate with other objects around them; V2X encompasses Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) (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 Wi-Fi DSRC based systems or cellular network-based systems. It is also not in the scope of this section to refer to Vehicle-to-Network (V2N) communications. The key aspects related to V2N are addressed under topics 4.4.2 Cybersecurity, 4.4.3 Implementation of Updates and 4.4.5 Data Recording, Privacy and Protection.

Question 2-2-1	Relevant Phase(s)	DF	CO	DS	VV	PS
Are the V2X interactions that the AD vehicle may encounter identified? ( ) Yes / ( ) No		• Are the high-level interfaces in the high level architecture planned considering the identified V2X interactions within its ODD? • Is it defined which is the required functionality from other users (e.g. infrastructure, other road users) to cover the V2X interactions identified?				

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 (e.g. route planning, interaction with infrastructure), tactical level (e.g. manoeuvre control) and operational level (e.g. braking, accelerating…).

Once the interactions have been identified, a high-level system architecture needs to be defined in order to understand how the ADF 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).

Additional information regarding this topic is provided by:

- "A Framework for Automated Driving System Testable Cases and Scenarios", NHTSA (Thorn et al. 2018).

Question 2-2-2	Relevant Phase(s)	DF	CO	DS	VV	PS
Is a plan defined to integrate and validate the V2X interactions within the sensor architecture? ( ) Yes / ( ) No		• Does the plan also consider a back-up solution when a required infrastructure is no longer available?				

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. Such strategy shall also include which is the required level of Quality of Service (QoS) from the V2X interfaces, such as availability, reliability, accuracy. 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. In this context, refer also to Question 1-4-5 of topic 4.2.4 (Architecture) and topic 4.4.2 (Cybersecurity).

Some of these alternative strategies include the consideration of back-up solutions which shall be part of the overall safety strategy of the ADF.

Additional information regarding this topic is provided by:

- “A Framework for Automated Driving System Testable Cases and Scenarios”, NHTSA (Thorn et al. 2018).

Question 2-2-3	Relevant Phase(s)		CO			
Is a safety concept of V2X interactions defined? ( ) Yes / ( ) No		• Is a validation strategy defined for the safe operation of a combined V2X sensor architecture (e.g. comprising sensor and communication errors or in case of missing infrastructure)? • Are potential failure modes of V2X interactions identified? • Are appropriate countermeasures for each potential failure drafted and planned?				

A safety concept of V2X interactions shall be defined, considering in this context the addressed topics under category 4.4 “Safeguarding Automation”. This shall also include a common trust concept that defines how to rely on information from other vehicles and infrastructure. It shall also be considered compliance of such a concept with its applicable regulations at both international and national level.

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:

- “A Framework for Automated Driving System Testable Cases and Scenarios”, NHTSA (Thorn et al. 2018).

Question 2-2-4	Relevant Phase(s)				VV	
Is the validation strategy for V2X interactions followed and implemented? ( ) Yes / ( ) No		• Are test reports generated for the V2X interactions that were identified? • Are test reports prepared for the failures identified in the concept?				

At the V&V stage, it must be ensured that the validation strategy of the concept phase is implemented and followed (see topic 4.1.4). 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 when design or validate ADF. 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 AVs and traffic environment. This topic consists of several main and sub-questions which may occur when develop and validate traffic simulation, from definition phase to validation / verification phase.

Question 2-3-1	Relevant Phase(s)	DF	CO			
Is the technological state-of-the-art of the traffic simulation addressed and researched? ( ) Yes / ( ) No		• Are the sensor suite and vehicle architecture documented? • Are the appropriate toolchains or models selected for satisfying the needs of traffic simulation and ADF within the chosen ODD? • Does the simulation approach comply with one of the three approaches in ISO 21934-1? • Is a state-of-the-art regarding traffic simulation performed, which combined with ADF simulation and covering existing solutions including their strength and weaknesses? • Are the hardware and software of the simulation well defined and documented?				

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

- 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).
- Studies of ISO 21934-1, which provide a prospective safety performance assessment of pre-crash technology by virtual simulation (ISO 21934 20XX).
- 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				
Is the analysis and assessment of the impact regarding the applied ADF on traffic flow simulation conducted? ( ) Yes / ( ) No		• Does the impact analysis of applied ADF consider the safety, the efficiency and the interaction with infrastructure or other road users?				

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):

- The microscopic approach describes the relevant characteristics of a single vehicle, like its speed, temporal headway or spatial separation, and
- 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 implementing different scenarios and traffic models? ( ) Yes / ( ) No		• Are different scenarios, different environments or regions and different traffic flows considered and implemented in the simulation? • Are emergent, cooperative and interoperability aspects addressed in the simulation? • Are there appropriate metrics to identify the critical scenarios in the traffic flow simulation? • Are there appropriate countermeasures to cover the critical scenarios in the traffic flow simulation?				

Several scenarios and traffic flows could be implemented in the simulation approach in order to evaluate the ADF evolution (see topic 4.2.2). 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 AVs 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).

A guidance on traffic disturbance critical scenarios for ADF up to 60 kph is provided by ALKS regulation. Traffic critical scenarios is defined as the conditions under which ALKS may not be able to avoid a collision, several traffic parameters are classified for describing the pattern of the traffic critical scenarios. The cut-in, cut-out as well as deceleration of other vehicle in front of ego vehicle are in the scope of traffic critical scenarios (UN ECE ALKS 2020). Besides, appropriate countermeasures should be applied for vehicle in the boundary of the ODD or in the definition of the ADF, to cover the identified critical scenarios by simulation and mitigate the potential risks.

<table>
<tr><th>Question 2-3-4</th><th>Relevant Phase(s)</th><th>DF</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Is a strategy defined to validate / verify the traffic flow simulation?
(   ) Yes / (   ) No</td><td colspan="5">• Are the different test scenarios defined?
• Are the main research questions been clarified for traffic flow simulation?
• Are the critical scenarios which are unpreventable for a skilled and attentive human driver, preventable for ADF?
• Is there a strategy towards higher levels of realism concerning the simulation approach?</td></tr>
</table>

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).

Critical scenarios for an ADF could be divided into preventable or unpreventable. The question what is preventable and unpreventable leaves rooms for discussion. For instance the ALKS is asking for a performance of the ADF equal to competent and careful human driver. (UN ECE ALKS 2020). To validate an ADF, it is expected that the critical scenarios which are unpreventable for a human driver would be preventable for ADF.

Compared with real-world tests, another challenge of the simulation approach is to model the systems as realistically as possible, since the model quality and accuracy decide how close the simulation is to the real world behaviour (Ragan et al. 2015). Thus, a strategy towards higher levels of realism of the simulation is very important to ensure a high quality and accuracy of simulation, which is helpful to argue safety of an ADF without real-world driving activities.

<table>
<tr><th>Question 2-3-5</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th>DS</th><th></th><th></th></tr>
<tr><td colspan="2">Does the simulation toolchain consider co-simulation approaches?
(   ) Yes / (   ) No</td><td colspan="5">• Does the simulation consider separate details of co-simulation such as: traffic simulation, vehicle dynamic simulation and cooperation simulation (traffic management)?
• Can the applied simulations be synchronized?
• Can the applied simulations exchange data between them?</td></tr>
</table>

A simulation concept should take into account co-simulation approach, which may incorporate mixed elements such as traffic environment, traffic flow, vehicle architecture, sensor data, and communication aspects. It could consist of a traffic simulation, a vehicle dynamics simulation, and a cooperation simulation. The traffic simulation provides the surrounding traffic environment for the AV, 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 traffic management 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, co-simulation 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 SIL defined? ( ) Yes / ( ) No		• Is there a right fidelity for specific simulation components (including sensors components)? • Is there more hardware-based XIL, which is beyond SIL applied?				

In a virtual environment, High fidelity is not always necessary or advantageous when conducting SIL test in software or software interactions. 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.

Different types of simulation exist and could lead to different testing goals. The hardware-based XIL approaches use virtualisation of the physical components and the embedded function architectures to allow engineers to test ADF at different levels, such as component level, subsystem level or vehicle level. Thus, by using these approaches faster development and validation cycles could be achieved (Riedmaier et al. 2018).

Question 2-3-7	Relevant Phase(s)		CO			
Is there real driving data guiding the simulation approaches? ( ) Yes / ( ) No		• Is the behaviour of the traffic agents in line with the real world behaviour? • Are the sensor models based on real driving data? • Are variations of the parameters applied in this context, and covered reality? • Are the applied simulations based on Naturalistic Driving Study (NDS) database, accident database or records of real-world drives?				

Simulation of the ADF leads to an enormous amount of simulated miles. In order to ensure that these miles are worthwhile and useful, having realistic and various virtual scenarios is extremely important. These virtual 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.). In the meantime, virtual sensor models shall be based on real sensor data, which is considered a central component of the virtual environmental perception, to closely match reality. 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 for the generation of novel scenarios, 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 model used in the simulation? ( ) Yes / ( ) No		• Does the driver behaviour model appropriately cover driving tasks? • Is the driver behaviour model in line with driver behaviour of a skilled and attentive human drivers, even from different regions? • Does the driver behaviour model cover the interaction of non-automated drivers to AVs?				

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 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 AV also needs to be covered.

A driver behaviour model is typically applied in the simulation in order to simulate the surrounding traffic, to predict driver maneuver / driver intention, or 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 behaviour model, which could be variable according to the driving skill in different regions. 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 the simulation approach? ( ) Yes / ( ) No		• Are internal processes of the company followed / complied with and are they compatible with a community/industry-wide approach? • Is the public informed about the role of the simulation in the validation of ADF, the impact of ADF, as well as the validation process?				

The designed vehicles must comply with federal, state and local laws within their geographic area of operations. The validation process shall 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, therefore, the sub-questions should be addressed carefully.

Question 2-4-1	Relevant Phase(s)	DF	CO	DS	VV	
Are all laws and regulations associated with the development, testing and sale of the ADF been considered? ( ) Yes / ( ) No		• Are the applicable traffic laws considered and followed by the ADF? • Are country specific laws and regulations considered and followed by the ADF? • Are laws and regulations for testing considered and followed? • Are data protection laws and regulations followed through the entire process?				

By means of this question, it should be ensured that the development as well as the function behaviour follows all laws and regulations. An important aspect is that laws and regulations 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/certification but also for any development activity. The design of the function should take national road traffic laws into account. 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 topic 4.1.4);
- “UN ECE Regulation” (e.g. ALKS Regulations);
- National antitrust laws.

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

<table>
<tr><th>Question 2-4-2</th><th>Relevant Phase(s)</th><th>DF</th><th>CO</th><th>DS</th><th>VV</th><th>PS</th></tr>
<tr><td colspan="2">Are research and development activities planned according to the applicable (national) ethical standards?
(   ) Yes / (   ) No</td><td colspan="5">• Are mechanisms established to minimise the risk of harm to people in the development, testing and operation phases?
• Are ethical standards considered during the test planning process and the collection and analysis of data?
• Does the ADF consider the protection of human lives as a paramount?</td></tr>
</table>

In addition to legislation, it is also essential to comply with ethical standards. 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, protection of human lives must be paramount. For example, the German ethic commission stated “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” (di Fabio et al. 2017).

Another example is “Safety first white paper” (Wood et al. 2019), which for instance transferred these ethical standards into twelve principles for AD. Additional information regarding this topic is provided by:

- “Report of German ethic commission”, (di Fabio et al. 2017);
- Report of the European Commission on “Ethics of Connected and Automated Vehicles” (Bonnefon et al. 2020);

Question 2-4-3	Relevant Phase(s)	DF	CO	DS	VV	PS
Does he ADF achieve a positive risk balance compared to human driving (e.g. reported in accident statistics)? ( ) Yes / ( ) No		• Is a positive risk balance considered all the way through the life cycle of the ADF? • Is the baseline and treatment (with ADF) condition properly defined for assessment? • Is the risk (accidents, accidents of certain severity) of the baseline identified? • Are the risked induced by the ADF minimised? • Does the ADF reach a consistent improvement of the overall safety in comparison to human drivers / comparable functions while minimising new risks induced by the automated function? • Is a (validated) method / tool available to investigate the risk balance? (See topics 4.1.4 and 4.3.3). • Does the ADF avoid unreasonable risks for the vehicle occupants or any other road users? • Does the ADF not cause any collisions that are reasonably foreseeable and preventable				

By means of this question it should be investigated whether the ADF is beneficial in terms of traffic safety. For example, 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” (di 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 challenge of investigating a positive 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. These methods might be applicable at later stage, once a sufficient market penetration rate of the ADF is reached. Other methods (e.g. simulation based prospective impact assessment, ISO 21934 20XX or L3Pilot deliverables D3.4) 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 conditions for the assessment (baseline and treatment) are defined and which driving scenario and accident types / severities are analysed. For the baseline, data sources such as accident data and / or Naturalistic Driving Study (NDS) / Field Operation Test (FOT), might be required. The relevant information for the assessment can be stored in a centralized database.

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 positive risk balance 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.

One example, how the concept of a positive risk balance can be transferred into threshold for the development, is given in Annex 2.

Additional information about the entire topic is provided by:

- Report of the European Commission on “Ethics of Connected and Automated Vehicles” (Bonnefon et al. 2020);
- ISO 26262;
- ISO/PAS 21448 Road vehicles — Safety of the intended functionality (ISO/PAS 21448 2019);
- ISO/WD 34501 Road vehicles — Terms and definitions of test scenarios for automated driving systems (ISO 34501 20XX);
- ISO/WD 34502 Road vehicles — Engineering framework and process of scenario-based safety evaluation (ISO 34502 20XX);
- ISO/WD 34503 Road vehicles — Taxonomy for operational design domain for automated driving systems (ISO 34503 20XX);
- ISO/WD 34504 Road vehicles — Scenario attributes and categorization (ISO 34504 20XX);
- ISO/PWI 34505 Road vehicles — Evaluation of test scenarios for automated driving systems (ISO 34505 20XX);
- L3Pilot Deliverable D3.4 (Innamaa et al. 2020);
- PEGASUS (PEGASUS 2019);
- “Safety first for automated driving”, (Wood et al. 2019);
- SAKURA project in Japan (SAKURA Project 2019);

- SVA project in France (SVA project 2018);
- “UN ECE ALKS Regulations”, (UN ECE ALKS 2020).

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 user / 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, safety related aspects are also covered in the other categories (e.g. when defining the 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 FuSa is closely linked to the ISO 26262 standard (ISO 26262: 2018). ISO 26262 serves as a basis for this topic. This topic 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 FuSa activity based on the function description (item definition) is to identify the hazards that may arise by the functionality to be developed and to assign the required ASIL. 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				
Is possible malfunctioning behaviour and the related hazardous events analysed? ( ) Yes / ( ) No		• Are the relevant hazards identified for the considered function based on its description (item definition)? • Is inadequate control by a driver or a function identified? • Is a systematic approach (e.g. FMEA, FTA, STPA, and HAZOP) used for the analysis? • Is malfunctioning behaviour identified for cases where the vehicle is in manual driving mode and in automated driving mode? • Is malfunctioning behaviour being clearly documented? • Is the potential absence of a take-over ready driver considered that may have an impact on the controllability of the vehicle? • Is the role of the infrastructure considered? • Is the vehicle reaction in case of a failure defined to avoid malfunctioning behaviour when no take over ready driver is present"?				

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				
Is there a process in place to derive safety requirements (including safety goals) to avoid unsafe functional behaviour? ( ) Yes / ( ) 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 to 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 topic 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**			
Does a strategy exist to validate the safety concept? ( ) Yes / ( ) No		• Are there measures to confirm the effectiveness of the safety concept? • Do criteria exist that allow to define whether a vehicle behaviour can be accepted as safe?				

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 inacceptable new risks are introduced. One example is the following case: in case a L3 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)? ( ) Yes / ( ) 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 topic 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 data collection mechanisms are DSSAD (Data Storage System for Automated Driving) as mandated by UN ECE ALKS Regulation and EDR (Event data recorders) data for post-crash evaluation or data for disengagement reports as required for AVs by the State of California (DCM 2019). The use of such methods will allow analysing what was the reason for any incident and prepare necessary documentation.

Question 3-1-5	Relevant Phase(s)			DS		
Are the included safety mechanisms based on accompanying safety analysis? ( ) Yes / ( ) No		• 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? • Are child-requirements covering the higher level requirements (correctness and completeness)?				

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		
Are function reactions specified that transition the function to a safe state in the presence of a fault (depending on the kind of fault)? ( ) Yes / ( ) No		• Is degraded operation or transition to a safe state sufficiently safe for the specific failure scenarios? • Are 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)?				

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	
Is a verification and validation process defined, which is covering the various integration steps of software, hardware, function, and vehicle? ( ) Yes / ( ) No		• Is the successful mitigation of all findings from the hazard analysis confirmed during verification activities?				

A verification and validation process shall be defined to clarify the responsibilities of each stakeholder involved in the development process 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 details, see topic 4.1.4). For FuSa 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 V&V activities assessed? ( ) Yes / ( ) No		• If V&V is carried out on public roads, are potential effects to other traffic participants considered and safety measures defined? • Is it ensured that safety drivers are allowed to operate a vehicle (following company internal and legal requirements) and have received appropriate training?				

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 that 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. It shall also be considered to include appropriate testing for the test engineers so they can take necessary actions in case of an issue during testing.

Question 3-1-9	**Relevant Phase(s)**				**VV**	
Do the test cases for the safety requirements cover the entire ODD? ( ) Yes / ( ) No		• Do test cases cover both ODD and edge cases' scenarios?				

Test cases have to cover the entire ODD (for details, see topic 4.1.4). 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. Additionally, a test catalogue shall be taken into account (refer to Question 1-2-3) which shall consider both ODD and edge cases' scenarios. One approach for testing 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? ( ) Yes / ( ) 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 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 are appropriate and keep 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

In the context of road vehicles, Cybersecurity refers to the protection of each function and electrical or electronic components from cyber-attacks. Based on the increased connectivity to which AVs will be exposed, the potential for cyber-attacks also grows, providing an additional challenge for ensuring safety to both customer and fleet vehicles, on top of the need of fulfilling the applicable regulations.

Therefore, as first step it is important that cybersecurity principles and practices are well established and followed. To do so, it is important to acknowledge the technologies to which the AVs are exposed, which may vary depending on the level of automation.

Since this topic has been developing in the recent years, there are several upcoming standards and regulations which are applicable, such as:

- ISO/SAE 21434 “Road Vehicles – Cybersecurity Engineering“ (ISO 21434 20XX);
- ISO/PRF TR 4804 “Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation” (ISO/PRF TR 4804 2020);
- UN ECE R-155 “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system” (UN ECE Cyber Security 2020).

The terms used in this topic may differ from the ones used in the above mentioned references since the main scope of this topic is to highlight the most relevant cyber-security aspects that shall be addressed in the development of an ADF.

Question 3-2-1	Relevant Phase(s)	DF	CO	DS	VV	PS
Is there an established and followed cybersecurity process within the organisation to ensure the security architecture of the overall function? ( ) Yes / ( ) No		• Is there a list of measures to be followed established within the organisation (e.g. awareness programs, adequate trainings)? • Is there a similar culture existing at sub-contractors, suppliers and potential 3rd parties directly or indirectly working with the organisation? • Is a self-audit process established to gather information about the policies and procedures followed? • Does the self-audit process include a procedure to log the (hazardous) events (e.g. potential security breach) with impact on security and also procedures to report eventual vulnerabilities? • Does the self-audit process include a procedure to document the tests performed including the test reports?				

In order to ensure that all stakeholders dealing directly or indirectly with this topic can follow the required steps and behave responsibly, it is necessary to establish a cybersecurity culture within the organisations through well-established cyber-security processes. To do so, a Cyber Security Management System (CSMS) shall be established, which will gather the required set of systems and processes to be put in place and which will cover the entire development phases, including Post-production phase to ensure secure development lifecycle (SDL). When implementing a cybersecurity culture, several measures shall be considered such as programs to raise cybersecurity awareness among the organisation and establishing adequate trainings to employees (ENISA, 2019). Having a clear and structured process within the whole organisation will help reducing the potential for successful attacks. Relationship with external stakeholders such as suppliers shall be considered, including definition of appropriate guidelines to make sure that they follow similar practices (ENISA, 2019). Information sharing with trusted industry partners on threats, vulnerabilities and risks shall also be considered (Auto-ISAC, 2016)

A self-audit process is part of the cybersecurity culture as it will help to institute and maintain a continuous improvement approach. The audit shall be able to collect all the information related to the policies and procedures established by the company, not only internally but also involving Tier’1s and subcontractors. Some examples may include the procedures followed for logging of hazardous events, for reporting eventual vulnerabilities and also to include documentation with test reports.

Additional information regarding this topic is provided by:

- “ENISA Good practices for Security of Smart Cars”, (ENISA 2019);
- “Auto-ISAC Best practices (2016)”, (AUTO-ISAC 2016).

<table>
<tr><th>Question 3-2-2</th><th>Relevant Phase(s)</th><th>DF</th><th>CO</th><th>DS</th><th>VV</th><th>PS</th></tr>
<tr><td colspan="2">Is security by design considered in order to minimise the risks / threats and responding appropriately to them once identified?
(   ) Yes / (   ) No</td><td colspan="5">• Are security by design measures considered at all levels, from component level up to vehicle level?</td></tr>
</table>

Security by design is a principle that has to be followed along all the development phases, to make sure vulnerabilities are timely identified and ensuring a good integration of all security systems and components. In the first place it shall identify which are the security objectives and requirements of the ADF. At a later phase, during the design it shall take into account cybersecurity key principles such as defence in depth, principle of least privilege, disabling of test/debug features and ports, etc. (ENISA, 2019)

Security by design shall be considered at all levels, from component level which can refer to vehicle sensors and actuators (e.g. sensors which collect data from outside of the vehicle) and vehicle ECU’s (including both hardware and software components used to process the data from the sensors) up to vehicle level which includes in-vehicle communication networks (e.g. CAN, Ethernet) and communication protocols (e.g. Bluetooth, Wi-Fi…) and extended vehicle level which deals with server communications also referred to as V2N (e.g. systems which communicate with back-end systems or map data servers), infrastructure communications (e.g. traffic sign) and mobile devices such as smartphones. As mentioned before, the level of automation shall be considered, since there may be a difference of the exposed components or systems.

Additional information regarding this topic is provided by:

- “ENISA Good practices for Security of Smart Cars”, (ENISA 2019).

Question 3-2-3	Relevant Phase(s)	DF	CO	DS	VV	PS
Are asset management and threat analysis and risk assessment performed? ( ) Yes / ( ) No		• Does the threat analysis consider potential types of attack vectors and their characteristics (e.g. description of attack, likelihood, impact, risk...)? • Are external connectivity and connections considered in the asset management and threat analysis? (Some examples of external connectivity and connections are software updates, remote diagnostics, and fleet management).				

At first, Asset management is required to identify all the assets that are specific to the organisation and the ADF and it requires a consistent up-to-date asset inventory (ENISA, 2019). This step allows the organisation to identify possible vulnerabilities.

As a second step, threat analysis and risk assessment (TARA) shall be performed, taking into account that it is an iterative task along the development process. This step allows identifying possible threats to the function and how they relate to critical assets. After identifying them, security risks on the function can be clarified which can lead to the definition of the required mitigation strategies. This task should be revised upon any major change or in case of detection of critical security vulnerabilities or critical security incidents (ENISA, 2019). 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. Additionally, a TARA+ methodology which has been developed in L3Pilot SP4 and captured in the deliverable D4.2 “Legal requirements for AD piloting and Cybersecurity analysis” shall be considered. TARA+ incorporates the notions of controllability and observability of an attack for L3 and above systems, taking into account both the system and the driver role (TARA+, 2019).

External connectivity offers the possibility to perform several tasks remotely without the need to be performed physically at a dealer or garage, using V2N communications. This also increases the potential attack vectors that AVs can be exposed to. That is why both asset management and threat analysis and risk assessment should carefully analyse all the possible external connections of the ADF. Remote diagnostics and fleet management are good examples of operations which have been enabled thanks to external connectivity and which would have not been applicable years ago and which could have serious implications if any potential attack would occur. For details about software updates, please refer to topic 4.4.3

Additional information regarding this topic is provided by:

- “ACEA principles of Automobile Cybersecurity”, (ACEA 2017);
- “ENISA Good practices for Security of Smart Cars”, (ENISA 2019);
- “L3Pilot D4.2 Legal requirements for AD piloting and Cybersecurity analysis”, (2020)
- “TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems”, (TARA+ 2019)

Question 3-2-4	Relevant Phase(s)	DF	CO	DS		
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		• Are clear methods defined to address confidentiality, authenticity, integrity and availability of the communications and the transferred data?				

Cybersecurity requirements may be derived directly from applicable standards and regulations such as the upcoming ISO/SAE 21434, the ISO/PRF TR 4804 and UN ECE Cybersecurity R-155. Besides that, high-level cybersecurity requirements also known as cyber-security goals have to be defined for the whole ADF. From those, specific requirements applicable to different components of the whole architecture shall be described, taking into account not only component level but also vehicle level and extended vehicle level.

The cyber-security requirements shall take into account aspects such as confidentiality, availability, integrity and authenticity, for example ensuring software authenticity and integrity before its installation and during its execution, or defining availability of data from back-end services. Other examples can be related to the use of standardised and publicly available cryptographic methods and authentication protocols that can ensure data privacy, or the use of standardised and publicly available secure communication protocols that can ensure data integrity and authenticity. For further details on data privacy, refer to topic 4.4.5.

Other requirements that shall be considered are related to detection mechanisms, protection of networks and protocols, software security, cloud security, cryptography and access control among others (ENISA, 2019)

Additional information regarding this topic is provided by:

- “ENISA Good practices for Security of Smart Cars”, (ENISA 2019);
- “ACEA principles of Automobile Cybersecurity”, (ACEA 2017).

Question 3-2-5	Relevant Phase(s)		CO	DS	VV	
Is a review of the architectural design considered based on refined requirements? ( ) Yes / ( ) No		- Is a process established to verify the implementation of cybersecurity requirements?				

As development process evolves, the integration of components takes place, which may lead to potential new vulnerabilities which have to be prevented. For that it shall be considered a refinement of the previously defined cybersecurity requirements. This task may be an iterative process during the design and validation phase since all the systems and components are gradually built in.

When implementing the requirements, it is important to follow technical best practices such as secure programming, software development guidelines or hardware redundancy mechanisms among other techniques. It shall also be considered if the requirements have been correctly allocated and implemented to each system or component by means of verification (e.g. detailed inspection and analysis as well as appropriate testing).

Question 3-2-6	Relevant Phase(s)	DF	CO	DS	VV	PS
Is a cybersecurity Incident Response process established? ( ) Yes / ( ) No		- Is a procedure established to properly inform the user when cybersecurity incidents may have an impact on them (e.g. security breach to back-end server, or system support malfunction)? - Is a clear strategy for OTA updates defined based on cybersecurity requirements?				

The first step of setting a cybersecurity Incident response process is to be able to monitor and detect cybersecurity events, so that relevant incidents can be identified and classified. This will help to prioritise them and to also respond to them efficiently, a task that may require having dedicated teams, which can assign responsibilities and the necessary actions to be taken.

A procedure to inform about incidents to the user shall also be considered, including elaboration of appropriate communication plans with the involvement of relevant parties. This shall be done to ensure that the right information is communicated to users. Some examples are when security breaches happen in V2N communications, such as to an OEM server, which could impact vehicle functions and software updates, or system support malfunction, which could happen if the system does not behave as intended due to external perturbation (e.g. traffic signal spoofing which make sensors to misclassify traffic signs).

Regarding software updates, it is a practice that will become more and more common with the deployment of ADF. Since this usually happens via connection to OEM back-end servers via V2N communications, a strategy shall be put in place to not only ensure the update but also to inform the user timely and effectively about its implementation. For further details on software updates, refer to topic 4.4.3.

Additional information regarding this topic is provided by:

- “ENISA Good practices for Security of Smart Cars”, (ENISA 2019).

<table>
<tr><th>Question 3-2-7</th><th>Relevant Phase(s)</th><th></th><th></th><th></th><th>VV</th><th>PS</th></tr>
<tr><td colspan="2">Is a cybersecurity validation process clearly defined and followed?
(   ) Yes / (   ) No</td><td colspan="5">• Are roles and responsibilities as well as the required expertise for conducting specific validation activities clearly defined?</td></tr>
</table>

Validation of the implemented measures is key to understand if cybersecurity goals have been achieved and if requirements have been correctly implemented. This step shall also be considered whenever new threats are identified or major updates are implemented. The validation process shall include how relevant activities related to cybersecurity validation are planned, conducted and documented, from component level up to vehicle level.

The validation process should also define clear roles and responsibilities among all involved members (within the organisation and also from outside such as Tier 1’s), what will help avoiding possible duplications and will ensure its efficiency and robustness. Additionally, the validation process should consider specific validation activities such as conducting security evaluations by appropriate means (e.g. penetration testing, vulnerability scanning or fuzz testing) and covering all the levels in the ADF, so the required expertise to conduct them shall also be clearly defined in this process or this topic, it is recommended to follow the guidelines under ISO/SAE 21434 as reference.

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). OTA is defined as an update process that utilises wireless internet connectivity to make requests to an OEM cloud service via V2N in order to download the latest firmware or software. This will optimise the customer vehicle without having to take it to a dealership. As there is a paradigm shift away from dealership visits to OTA, there is a growing set of principles to govern best practice of the update process. Some of these are mentioned in the following text, however some are still in development, such as ISO 24089 (ISO 24089 20XX).

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		
Are international regulations and standards being followed where appropriate during the development of software update processes? ( ) Yes / ( ) No		• Are the relevant type approval organisations being contacted and provided with all the information to certify the update process and any modifications made by an update on the vehicle? • For any new update is compliance with the existing type approval still maintained?				

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 topic 4.1.3 for more information on existing standards.

The following documents provide current information as of the day of publication:

- UN ECE WP29 GRVA, “Draft Recommendation on Software Updates” (UNTF 2018);
- “Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements”, (Sena 2015).

Question 3-3-2	Relevant Phase(s)	DF		DS	VV	
Is a clearly defined OTA and software update strategy developed to manage the end-to-end process? ( ) Yes / ( ) No		• Is there a defined vehicle state when updates can and cannot be completed? • Vehicle state - is a robust strategy put in place to manage updates when the vehicle is required in a certain state and part way through the update the state changes? • Location - are certain updates only available at predefined locations, such as the registered address of the vehicle? • Status of network connectivity - do updates require local wireless networks, or can some be installed using a cellular network connection? • Is there a clear strategy to notify users about the updates? • Is due consideration given to ensure the software update is conducted in a safe and secure manner? • Is there an appropriate V&V strategy to check software updates before they are sent out?				

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. The strategy should also set out the vehicle condition (the 'safe state') that updates can occur in, and this should be robust enough to handle a change in the vehicle state. The 'safe state' may take into consideration factors, such as the vehicle charge, whether the vehicle is in motion, and many other vehicle properties.

Additional information can be found here:

- "ENISA Good practices for Security of Smart Cars", (ENISA 2019);
- "A System-Theoretic Safety Engineering Approach for Software-Intensive Systems", (Abdulkhaleq 2017);
- "Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System", (UN ECE Software Update and Software Updates Management System).

Question 3-3-3	Relevant Phase(s)	DF	CO		VV	
Is hardware / software compatibility for the lifetime of a vehicle and for future updates considered? ( ) Yes / ( ) No		• Does the update enable new / additional functionality? • Are there any unintended impacts on vehicle systems not planned as part of the update? • Is the possibility of performing an OTA update on the ADF considered? • During vehicle design, has the chosen HW been future proofed? (I.e. the HW capability is extended to meet future potential requirements or the system is designed as such that the HW can be upgraded easily as part of a dealership visit).				

As part of 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.

Furthermore, it is essential due to increasing software complexity and vehicle feature interrelation that sufficient V&V testing is done before releasing updates to the customer. This ensures there are no unintended faults to safety critical features of the vehicle. More on testing can be found in section 4.1.4. Where possible, safety critical software should be shielded from non-safety critical software to minimise the risks of safety critical faults occurring from future updates.

These documents provide initial guidance to consider:

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

Question 3-3-4	Relevant Phase(s)	DF				
Are software safety requirements identified at a function level? ( ) Yes / ( ) No		• Where applicable, are relevant standards (ISO 26262, ISO/SAE 21434 etc.) followed during the definition of OTA processes and software updates?				

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 FuSa must be modified to comply with future regulations.

For more current information, see these documents:

- "Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements", (Sena 2015);
- ISO 26262 (ISO 26262 2018);
- ISO/PAS 21448: Road vehicles - Safety of the intended functionality (ISO/PAS 21448 2019);
- ISO/SAE 21434 (ISO/SAE 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 to update the current OTA update process when relevant.

See section 4.4.2 for further information on Cybersecurity. Related software security information can be found here:

- "ENISA Good practices for Security of Smart Cars", (ENISA 2019).

Question 3-3-6	Relevant Phase(s)		CO			PS
Is the function being updated safety critical? ( ) Yes / ( ) No		• Is a robust V&V procedure developed to ensure OTA updates on safety critical functions are sufficiently tested prior to release?				

A vehicle contains both safety and non-safety critical functions. Depending on the safety criticality of the affected function, the requirements for the update might differ. A failure in the vehicle infotainment introduced by a fault 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:

- “Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements”, (Sena 2015).

<table>
<tr><th>Question 3-3-7</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th></th><th>VV</th><th></th></tr>
<tr><td colspan="2">Is a method implemented to notify the user and OEM of each successful update installation?
( ) Yes / ( ) No</td><td colspan="5">• As part of the notification process is the user advised on the expected duration of the installation?</td></tr>
</table>

It is important that users are informed on the duration of an update, when it is successfully installed and when the vehicle is ready to use. In failure cases it is important that the user is notified to enable him / her to take further action (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 here:

- “Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System”, (UN ECE Software Update and Software Updates Management System);
- “Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements”, (Sena 2015).

<table>
<tr><th>Question 3-3-8</th><th>Relevant Phase(s)</th><th></th><th></th><th>DS</th><th></th><th>PS</th></tr>
<tr><td colspan="2">Is a process for managing failed updates implemented?
( ) Yes / ( ) No</td><td colspan="5">• As part of the update process is there a method for identifying the reason for a failed update?
• As part of the process is there a clearly defined method for pushing updates to the customer’s vehicle?
• Is a method for reverting to the previous software version when an update fails or until a software patch has been developed implemented into the update process?</td></tr>
</table>

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, for example reverting 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 all instances the manufacturer must be aware of any fleet-wide issues and must work swiftly to resolve the issue and ensure the safety of the customer.

For more information, see:

- “Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System”, (UN ECE Software Update and Software Updates Management System);
- “Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements”, (Sena 2015).

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

With the introduction of OTA updates manufacturers will move – at least partly – away from the traditional approach of customers visiting a dealership for servicing to a remote service approach used by technology companies. This approach has risks, which are potentially safety critical. This means that the customer must have confidence that updates are from a trusted source and not a malicious attack. To ensure only legitimate software is installed, the vehicle must be able to confirm the authenticity and integrity of the update. Typically, technology companies use certifications to indicate the authenticity of a software update. For additional details, refer to topic 4.4.2, question 3-2-4.

For further information, see:

- “ENISA Good practices for Security of Smart Cars”, (ENISA 2019);
- “Safe and Secure Automotive Over-the-Air 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		• Does this method consider the fact that the owner is not necessarily the driver of the vehicle? • For software patches that fix a security vulnerability, is there a method to make the update mandatory and ensure timely installation. • For mandatory updates is the user still adequately informed of the update and its purpose?				

Just as it is important for the manufacturer to provide proof of the authenticity of an update, it is also important that only authorised people can accept or decline updates and that they are adequately informed on performing the update safely. This is to stop interference from individuals who may seek to install malicious software or may try to stop new updates from being installed. It is also important that the OEM can mandate certain updates to maintain the integrity of the vehicle system and the user safety. In these cases, it is important that the update can be installed as soon as possible. In some critical instances the OEM may restrict certain vehicle functionality or full vehicle usage until the updates are installed.

Further information can be found here:

- "Proposal for a New UN Regulation on Uniform Provisions Concerning the Approval of Vehicles with Regards to Software Update and Software Updates Management System", (UN ECE Software Update and Software Updates Management System).

4.4.4 Safety of the Intended Functionality

The ISO 26262 series define the vehicle safety as the absence of unreasonable risks that arise from malfunctions of the E/E systems, it specifies HARA to determine vehicle level hazards as well (see topic 4.4.1). With the increase in the implementation of ADF in vehicles, more and more systems rely on sensing the external or internal environment, there can be potential hazardous behaviour caused by the intended functionality or performance limitation of a system when identifying hazardous events, which is free from the faults in the scope of ISO 26262 series. The absence of unreasonable risk due to these potentially hazardous behaviours related to such limitations is considered as the SOTIF (ISO/PAS 21448 2019).

The cause of SOTIF relevant hazardous events could be derived from system aspect, as well as from external factor aspect. Such cause of hazardous events mainly include (ISO/PAS 21448 2019):

- Performance limitations, insufficient situational awareness with or without reasonably foreseeable user misuse;
- Reasonably foreseeable misuse, incorrect HVI (user confusion, user overload, etc.);
- Impact from car surroundings (other users, "passive" infrastructure, environmental conditions, weather, electromagnetic interference, etc.).

In this topic, main points for achieving the SOTIF are discussed when develop an ADF, during definition, conception, design phase as well as verification/validation and post start of production phase. This topic does not necessarily apply the same terms as used in the ISO standard, but rather tries to point out the sense of important aspects in this context in the language used throughout the document.

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 ISO/PAS 21448 provides a guidance on an iterative function development process to achieve the target of the avoidance of unreasonable risk in both known or unknown and unsafe scenarios. This process includes design, V&V activities, and aims to avoid a malfunctioning behaviour in the system in the absence of technical faults, which might result from technological and definitional shortcomings.

The SOTIF relevant issues, regarding the systematically developing of ADF to support safety by design, have also been addressed and discussed in other latest international standards, such as ISO/PRF TR 4804. It focuses on the steps for developing and validating ADF, as well as the consideration of safety- and cybersecurity-by-design in the scope of the ADF with L3 and L4.

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. Several European organizations work to modify and update the Geneva Convention and provide advice on the regulation regarding the development and deployment of AVs to European Union.

Question 3-4-2	Relevant Phase	DF				
Is a functional and system specification about ADF defined (including the ODD description)? ( ) Yes / ( ) No		• Is the functionality, its dependencies on, and interaction with the environment defined and described?				

The functional and system specification provides an adequate understanding of the system and its functionalities so that the SOTIF related activities in subsequent phases can be performed. This functional and system specification serves as the beginning for the SOTIF related activities. 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:

- The use cases in which it is activated;
- The sensing and arbitration concept and technologies;
- The level of authority over the vehicle dynamics;

- 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, etc., 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	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		• Is there a hazard analysis in order to conduct the identification of necessary SOTIF activities / measures? • Is there an assessment of severity and controllability to determine whether a credible harm can result of the SOTIF risk? • Does the assessment of safety impact look at not only the direct intended effects of ADF but also the indirect and unintended effects?				

A hazard analysis is employed to identify the different hazards that may arise from a function or its environment and may lead to hazardous events which can bring potential harms to AV. 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. 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 include a consistency check of FuSa concept in topic 4.4.1.

Based on the identification of hazardous events caused by the hazards from 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 (ISO/PAS 21448).

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

A TOR of ADF is a key issue for the L3 or L4 functions, 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 user 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 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" (topic 4.5.2).

Additionally, an MRM will be performed by the system in case the user does not respond to TOR. The MRM leads to an MRC (e.g. limited / end of ADF operation) to minimize the risk and ensuring the safety of the user. For the aspects related to MRM, please see also topic "Minimal Risk Manoeuvre" (topic 4.1.1).

Question 3-4-5	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 detects distraction or drowsiness of a driver during automated mode, as well as the availability of a driver to respond to a transition demand (UN ECE ALKS 2020). This monitoring 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: identify 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 or inattention is detected; ensure the appropriate takeover (otherwise to conduct an MRM), etc.

An appropriate driver monitoring function can help ADF 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 more information related to driver monitoring, please see also topic "Driver Monitoring" (topic 4.5.3).

Question 3-4-6	Relevant Phase	DF			VV	
Is there a V&V strategy to prove the compliance of SOTIF aspects? ( ) Yes / ( ) No		• Does V&V strategy make sure that the test goals and V&V targets (such as acceptance criteria) are sufficiently covered? • Is there an appropriate testing environment that matches the validation strategy?				

A V&V strategy can support the process of ensuring 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:

- The ability of sensors and the sensor processing algorithms to model the encountered driving environment;
- 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;
- The robustness of the system or function;
- The ability of the HVI to prevent reasonably foreseeable misuse;
- The manageability of the handover scenario by the driver.

In order to achieve this strategy, several issues, which are based on the driving test cases should be addressed, especially the test goals and V&V targets (see topic 4.1.4). 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 environments should also be specified to match the validation strategy (ISO/PAS 21448 2019).

Question 3-4-7	Relevant Phase	DF				
Are users of the ADF informed about the functional limitations (including the ODD limits)? ( ) Yes / ( ) No		• Are users of the ADF informed about their responsibilities? • Are users of the ADF informed about their correct / appropriate interaction with the ADF? (avoid misuse).				

Before the usage of the AVs 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 AVs safely and appropriately (see topic 4.5.1). Additionally, the notification about the consequences of system misuses can significantly reduce the misuses of functionalities by users (MILT 2018).

<table>
<tr><th>Question 3-4-8</th><th>Relevant Phase</th><th></th><th>CO</th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Are there improvements regarding functional and system specification to avoid or mitigate SOTIF related risks?
(   ) Yes / (   ) No</td><td colspan="5">• Are there triggering events related to sensors, algorithms and actuators identified?
• Is there an assessment whether the system appropriately responds to triggering events?</td></tr>
</table>

Triggering events 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 and correctly 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 HVI regarding the controllability of vehicle and avoidance of misuse, etc. (ISO/PAS 21448 2019).

<table>
<tr><th>Question 3-4-9</th><th>Relevant Phase</th><th></th><th></th><th>DS</th><th>VV</th><th></th></tr>
<tr><td colspan="2">Is the ADF performance verified in hazardous events and foreseeable misuse case by conducting appropriate testing (XIL, real world and test track test)?
(   ) Yes / (   ) No</td><td colspan="5">• Is the ADF validated regarding the aspect that it does not cause any unreasonable level of risk in real-life use cases?</td></tr>
</table>

Several methods of the V&V of system performance, such as MIL, SIL, 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 (see topic 4.1.4 and Annex 1). 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 2019):

- 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.
- 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 approaches can significantly help to achieve SOTIF safety goals.

Question 3-4-10	**Relevant Phase**				**VV**	**PS**
Are methodology and criteria for SOTIF release performed at the end of SOTIF activities? ( ) Yes / ( ) No						

SOTIF release shall be conducted in order to review whole SOTIF activities preformed in this topic as well as evaluate the acceptability of the residual risks. Several issues need to be evaluated in this context:

- Whether all the specified use cases be taken into account by the validation strategy within the scope of the intended functions;
- Whether the intended functionality achieve a minimum fall-back risk condition;
- Whether the V&V acceptance criteria sufficiently to ensure that the risk is unreasonable;
- Whether sufficient evidence provided to argue the absence of unreasonable risk in case of an unintended behaviour.

SOTIF release can be accepted when bullet points 1, 2 and 3 are satisfied. SOTIF release could be conditionally accepted when bullet points 1, 2 and 4 are assured, the condition is satisfied when the risk is not unreasonable by the specified use cases. It is recommended to reject SOTIF release and make functional improvements when all above issues cannot be assured. (ISO/PAS 21448 2019)

4.4.5 Data Recording, Privacy and Protection

The realization of ADF will enable the collection of massive amounts of data (e.g. movement patterns, customer preferences). In order to protect the customers' data recorded, this process needs to be done in accordance with international, national and regional laws.

Data needs to be stored in the car and off-board 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 customers and also other road users. Following established procedures, misuse will be minimised and the benefits of 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.

<table>
<tr><th>Question 3-5-1</th><th>Relevant Phase(s)</th><th>DF</th><th></th><th>DS</th><th></th><th>PS</th></tr>
<tr><td colspan="2">Is the purpose of the data collected made clear, and especially to the customer?
( ) Yes / ( ) No</td><td colspan="5">• Is the customer informed about the data which is considered as personal, and in which categories it is divided?
• 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?
• Is this information made available clearly and easily accessible (contract, website, manual etc.)?
• Are contact points (such as customer service websites, emails, and addresses) for the customer maintained?
• Is the customer given the choice to share or not share data where possible?
• Is it necessary to provide data to relevant authorities upon request?</td></tr>
</table>

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. In case requested by authorities, the data shall be made available in an appropriate manner and in accordance with the law, if necessary.

Additional information regarding this topic is provided by:

- “Guide to the general data protection regulation”, GDPR (ICO 2018);
- “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);
- “UN ECE ALKS Regulations”, (UN ECE ALKS 2020).

Question 3-5-2	Relevant Phase(s)	DF		DS		
Is it defined who owns the data? ( ) Yes / ( ) No		• Is it clear where the data will be stored? • Is it clear who is responsible for maintaining the data, allowing data access? • Is there a process to ask for the deletion of data? • Is personal data accurate and kept up-to-date? • Are the responsibilities clear, which come along with ownership of data? • Is it authorized if third parties (such as marketing companies) may access the data?				

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 storing 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 established 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. This will make it clear where the responsibilities for data ownership lie.

Additional information regarding this topic is provided by:

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

<table>
<tr><th>Question 3-5-3</th><th>Relevant Phase(s)</th><th>DF</th><th></th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Is necessary data collected which is related to the occurrence of malfunctions or failures to reconstruct the cause of any incident or crash?
(   ) Yes / (   ) No</td><td colspan="5">• 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?
• What parameters / resolutions / frequency of logging is used?
• Is relevant information shared with the government authorities for crash reconstruction?</td></tr>
</table>

In order to help with the analysis of incidents and 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);
- “UN ECE ALKS Regulations”, (UN ECE ALKS 2020).

<table>
<tr><th>Question 3-5-4</th><th>Relevant Phase(s)</th><th></th><th></th><th>DS</th><th></th><th></th></tr>
<tr><td colspan="2">Is data protection impact assessment carried out?
(   ) Yes / (   ) No</td><td colspan="5">• Is the societal impact as of customer rejection assessed?
• Is the impact assessed as data is used as evidence of ADF operation in accident cases?
• Is the impact assessed as data is used by jurisdictions and insurance companies?</td></tr>
</table>

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		
Are appropriate measures (technical, security, organizational) to protect customer data implemented? ( ) Yes / ( ) No		• Are contractual safeguards to protect personal data in case of outsourcing imposed? • Is data privacy addressed by using publicly available and well tested cryptographic methods? • Is anonymization, pseudonymization and de-identification applied where appropriate? • Is the data processed based on a contract, with consent of customers, to comply with legal obligation? • Is the data processed lawfully, fairly and in a transparent manner in relation to individuals? • Are data collected for specified, explicit and legitimate purposes only? • Is personal data adequate, relevant and limited to what is necessary in relation to purposes for which they are processed? • 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? • Is the user enabled to erase sensible data on functions and connected functions? • Is personally identifiable data managed appropriately (what is stored/transmitted, usage, control of data owner)? • Is personal data retained only as long as necessary? • Is the data securely stored? • How does the customer can exercise his/her rights?				

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 and pseudonymize them. The data must furthermore only be processed with consent 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. The goal is a high level of confidentiality, authenticity and integrity, including privacy friendly technologies.

Additional information regarding this topic is provided by:

- "ACEA principles of data protection in relation to connected vehicles and services", (ACEA 2015);
- "Guide to the general data protection regulation", GDPR (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		• Is evidence of the steps taken to comply with the GDPR available?				

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. It needs to be documented as part of a company's standard protocols. Additional information regarding this topic is provided by:

- "Guide to the general data protection regulation", GDPR (ICO 2018).

Question 3-5-7	Relevant Phase(s)			DS		
Are (security) risk assessment and management procedures in place? ( ) Yes / ( ) No		• Are security risks identified and managed by secure coding practices including supply chain, contractors etc.? • Is authenticity and origin of all supplies ascertained? • Are the guidelines considered, which are intended by Question 3-2-1?				

As vehicles get smarter, cybersecurity is becoming an increasing concern in the automotive industry (further information is provided in topic 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? ( ) Yes / ( ) No		• Is a process established that treats data from incoming sources as unsecure until validated?				

A key enabling technology for road vehicle automation is V2N communication requiring back-end functions. However, back-end functions might provide access to personal data and 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 topic 4.4.1)? ( ) Yes / ( ) No		• Is the function designed resilient and fail-safe if safety critical functions are compromised (link to topic 4.4.1)?				

Nevertheless, principles of functional safety have to be considered for cybersecurity 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 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 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. The user is informed about the vehicle’s current status via the HMI and vice versa, so the HMI allows the user to interact with the vehicle. 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 is the impact of non-driving related activities (in the following referred to as secondary tasks) operated while driving with a highly automated function.
- A fourth topic is controllability and customer clinics. On the one hand it refers 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 HVI.

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.

Question 4-1-1	Relevant Phase(s)	DF	CO		VV	
Are design guidelines followed when defining, assessing & validating the HVI concept? ( ) Yes / ( ) No		• Are user requirements collected based on market research or based on other sources of data?				

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 AVs were presented by Naujoks et al. (2019-1) and validated in empirical studies (Forster et al., 2019; Naujoks et al., 2019-2). Additionally, 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? ( ) Yes / ( ) No		• Are the ADF controls designed in such a manner to reduce accidental activation / deactivation? • Is the ADF able to determine accidental activations / deactivations vs intentional ones? • Is a fall-back considered for the case where an accidental deactivation occurs and the driver is not in the loop?				

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 in case where 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, understand and interpret? ( ) Yes / ( ) No		• Do the text size, aspect ratio and contrast designed follow the standards? • Are commonly accepted or standardised symbols used? • Are the texts and symbols designed to be easily readable and understandable from the user's seating position? • Is the visual interface designed to have a sufficient contrast in luminance and/or colour between foreground and background? • Are the messages designed to convey the correct information in the language of the users? • Does the workload required to interpret the visual information compromise the driver’s focus on the driving task? • Are HVI elements grouped together based upon their function?				

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 they should appear. It can be confusing if these elements are spread across different locations as the driver may then have to check in multiple locations for the feedback, leading to a longer period of time where the driver is distracted from the road. It is important that new icons, messages and HVI elements are added to these standards and guidelines so that HVI can be standardised for AVs. During the development of the ADF, these standards need to be consulted, especially when making design decisions on the HVI. If possible, the standards and guidelines should be included in requirements against which the developed HVI can be validated.

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);
- “European Statement of Principles on human- machine interface”, (ESOP 2006);
- AdaptIVe D3.3 (Kelsch et al. 2017).

Question 4-1-4	Relevant Phase(s)		CO			
Is the HVI designed to portray the urgency of the message? ( ) Yes / ( ) No		• Are the semantics and tone of a message designed to be in accordance with its urgency? • Are high priority messages presented in a multimodal way? • 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? • Are messages containing high priority information positioned close enough to the user's line of sight? • Are HVI elements designed to clearly initiate a response from the driver? • Are messages with higher safety relevance given higher priority? • Are urgent messages portrayed in an accurate and timely manner? • Can urgent audible warnings be heard over the sounds generated by other systems?				

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);
- "European Statement of Principles on human- machine interface”, (ESOP 2006);
- AdaptIVe D3.3 (Kelsch et al. 2017).

Question 4-1-5	Relevant Phase(s)				DS	
Is the HVI installed in the optimum position? ( ) Yes / ( ) No		• Is the HVI located and fitted in line with regulations & standards? • Is the HVI installed in a position where it does not block the driver’s view of the road? • Is the HVI installed in a position where it does not obstruct vehicle controls and displays required for driving? • Are the visual displays prioritised so they are positioned as close as practicable to the driver’s line of sight? • Are the visual displays designed to reduce glare and reflection?				

The installation of the HVI is a topic which can often be overlooked until it is too late in the development. It is important that the position of the user interface is considered early on as this will affect many design decisions further down the line. For highly L3 ADF, the driver is still the focus of much of the HVI. Interfaces should be positioned to optimise the driver’s interaction with them, whether simply through glances or through physical interactions. If this is done correctly the workload to operate the ADF through the HVI is minimised and therefore so are the risks to the driver while using the ADF. Interfaces positioned within easy reach or close to the driver’s line of sight reduce the eyes off the road time allowing the driver to concentrate more on the road around them. It is also imperative that the HVI does not conflict with the driver’s view of the road or the primary vehicle controls. The interiors of passenger cars are becoming adorned with bigger and better screens to help the driver interact with the many systems the vehicle can offer, but it is important that these screens don’t have too much glare or reflection so that the driver can use them in all light levels. If the driver struggles to read urgent messages or does not react to certain instructions in time, then a hazardous situation may occur.

Additional information regarding this topic is provided by:

- “European Statement of Principles on human- machine interface“, (ESOP 2006);
- “Guidelines for In-vehicle Display Systems — Version 3.0”, (JAMA 2004).

Question 4-1-6	Relevant Phase(s)				VV	
Is the user acceptance of ADF assessed? ( ) Yes / ( ) No		• Is the user acceptance assessed as part of a customer clinic? • Is the user acceptance assessed based upon the guidelines in the CoP-ADF questions? • Is it determined that users are willing to use the ADF? • Is the user workload when interpreting the HVI messages assessed? • Is the user distraction due to HVI messages during use of the ADF assessed? • Is the driver able to keep one hand on the steering wheel while interacting with the ADF?				

To improve the user acceptance of the ADF’s HVI, a combination of customer clinics, heuristic expert assessments and various other user trials can be carried out to gain both subjective and objective data. The HVI can then be modified based on this data. 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 / users are able to trust the ADF and are willing to use it. It is worth noting that user acceptance is influenced by many factors and therefore even when the HVI meets the correct standards, it might be possible that the ADF is still not fully accepted by the user.

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) ;
- ”European Statement of Principles on human- machine interface”, (ESOP 2006).

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. On the one hand side, the awareness of the current automated driving mode is key for a safe operation of the vehicle. On the other hand side, trust at the right level of the automation level needs to be built and misuse prevented.

Question 4-2-1	Relevant Phase(s)	DF		DS		
Are all possible automated driving modes explicitly defined in terms of how the users 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 user's roles. The user's role may vary depending on the automated driving mode. For example, the user should understand three main modes: (1) fully manual mode, (2) partial automated mode (e.g. longitudinal control only), (3) automated mode (longitudinal and lateral control).

Relevant automated driving conditions could for example be the vehicle speed (ex. above 70 km/h), the type of road (ex. Motorway), and the weather conditions (ex. not in heavy rain).

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						

This question focuses on how the currently active automated driving modes (which automated driving mode is currently active) are communicated to both the user 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		• Are all of the possible user mistakes related to the HVI considered? • Are all of the possible user failures related to the HVI considered? • Are all of the possible intentional misuse cases considered?				

The purpose of this question is to ensure that possible user 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 user indicators (e.g. eyes-on-road time) described? ( ) Yes / ( ) No		• Are possible HVI countermeasures to mitigate driver distraction considered?				

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 user 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).

<table>
<tr><th>Question 4-2-5</th><th>Relevant Phase(s)</th><th>DF</th><th>CO</th><th>DS</th><th>VV</th><th></th></tr>
<tr><td colspan="2">Is an appropriate and clear way to communicate the automated driving modes to the user investigated and confirmed?
(   ) Yes / (   ) No</td><td colspan="5">• Are the appropriate numbers of different automated driving modes communicated to the driver investigated and confirmed?
• Is the necessity, to permanently display to the driver the active automated driving mode, investigated and confirmed?
• Is the necessity, to communicate to the driver the automated driving mode changes, investigated and confirmed?
• Is the appropriate recognition by the driver of automated driving mode changes investigated and confirmed?
• Is the appropriate recognition by other road users of the active automated driving mode investigated and confirmed?
• Is the current function mode designed to display continuously to the user?
• Is communication of mode changes easily and quickly recognised by the users?
• Are colours used to communicate function states in accordance with common conventions and stereotypes?</td></tr>
</table>

For ADF, a clear communication of the mode is crucial. The user must understand when s/he is in control of the vehicle and when a transfer of control occurs. If the mode is not clearly understood by the user, the results could lead to an incident. There are many ways to communicate the mode to the user 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 user 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 to inform the user 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 the HVI to improve driver alertness and time to get back in-the-loop investigated? ( ) Yes / ( ) No		• Are different HVI modality combinations investigated? • Is speech being considered for a TOR?				

The purpose of this question is to draw the attention on the crucial topic related to whether the user 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 user is supposed to be kept "in-the-loop" as much as possible during stretches of AD, not only during and after a TOR. In case of an unplanned take over event, this would be needed (until L3) in order to shorten the time that users 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.

Multi-modal HVIs can be considered in order to reach this goal, such as the combination of visual and/or auditory and / or haptic feedback and information. 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 user considered? ( ) Yes / ( ) No		• Is the information provided to the user about the vehicle currently being in the ODD investigated? • Is the information provided to the user about the start of the next ODD investigated? • Is the information provided to the user about the end of the current ODD investigated?				

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

- The vehicle is currently in the ODD: the function should inform the user so that the user can decide whether to activate the function;
- The vehicle is not yet in the ODD but will soon get into the next one: the function should inform the user so that the user can get ready for it and possibly decide to activate the function;
- The vehicle is currently in the ODD, and the end of the current ODD is known: the function should inform the user so that the user 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 user about an ADF-initiated MRM being considered? ( ) Yes / ( ) No						

An MRM typically happens if the user 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 user in case the function has initiated the MRM in order to provide the user with the necessary information, such as what is going on, why, and what the user could do after that (see topic 4.1.1).

Question 4-2-9	Relevant Phase(s)		CO	DS	VV	
Is the communication to the user, of the user's responsibilities in each defined automated driving mode(s) investigated and confirmed? ( ) Yes / ( ) No		• Is a method implemented to clearly inform the user of his responsibilities and of vehicle capabilities and possibly of the result of not acting within these capabilities? • Is the communication to the user, of the ADF's capabilities in each defined automated driving mode(s) investigated and confirmed? • Is there clear information in the user's manual, about the ADF's boundaries, and has this been confirmed? • Is additional training material to communicate the ADF's boundaries and the user's responsibilities considered? • Is a process defined on how the user will be informed about any new potential functionality of the ADF based on software updates?				

One of the crucial aspects of HVI is to make sure that the user fully understands her / his responsibilities during each of the defined AD modes, and therefore to understand the function's capabilities under these modes (i.e. what the user must control, in what situations the system can work, and when and how user would get TOR). Users may be informed by several means, including advertisement and owner's manual written explanations. Users may get explicit information by the in-vehicle HVI, during the AD activation itself, just before and just after it. Users may of course also learn by experience. Additionally, a simple and intuitive HVI can help the users 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 user's understanding of the automated driving modes communication being investigated?		• Is there different feedback information to the user depending on the driving scenarios investigated?				

Question 4-2-10	Relevant Phase(s)		CO			
( ) Yes / ( ) No						

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 user. 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 user awareness of automated driving modes being investigated? ( ) Yes / ( ) No		• Is user awareness of automated driving modes transition also being investigated?				

User awareness is a very important topic. Ensuring “user awareness of automated driving modes” means making sure that the user is fully aware of the available and possible automated driving modes, of the currently active driving mode, and of the occurring driving mode transitions.

Other than “situational awareness” treated by questions 4-2-4 and 4-2-6 , it is important to ensure user “mode awareness”, as previously addressed by questions 4-2-1, 4-2-2, 4-2-5, 4-2-9, 4-2-10. Question 4-2-11 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 user expectations regarding the ADF’s features considered? ( ) Yes / ( ) No		• Does the function provide the information the user is expecting? • Can the user easily find the necessary information? • Is the information presented in such a way as to not annoy or distract the user?				

During the V&V 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 HVI, for example the balance between the amount of information and its conciseness or simplicity can be considered.

Question 4-2-13	Relevant Phase(s)				VV	PS
Is the users' trust in the ADF being investigated? ( ) Yes / ( ) No		• Is the ADF trusted by the user? • Is the ADF not over-trusted?				

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. Trust could be measured by comparing the user's behaviour before using the system and after, for example.

Additional information regarding this topic is provided by:

- "Ford Safety Report", (Ford 2018).

Question 4-2-14	Relevant Phase(s)				VV	PS
Is the appropriate usage of the ADF by users confirmed? ( ) Yes / ( ) No		• Is the appropriate usage of the system sufficiently described in the user manual? • Are other methods of conveying the appropriate usage to the user considered? • Is there a way to give immediate feedback to the user when using the ADF in the appropriate way as well as in an inappropriate way (e.g. text message)? • Is there a feedback loop to the OEM in case the ADF is used in the appropriate way as well as in an inappropriate manner?				

This question is a general summary confirming that users 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 users do not read the manual, it must be ensured that other methods are available to ensure that users use the ADF appropriately. For example, trying to use the ADF in "bad conditions" if it is possible to turn on but would cancel soon later. Or users may have an inappropriate behaviour during ADF is on, such as watching a movie during L2.

There must be direct and immediate feedback, for instance via the vehicle display, in case the ADF is misused. Statistics shall be gathered anonymously 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)				VV	PS
Are long-term effects of the ADF on the users investigated? ( ) Yes / ( ) No		• 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?				

Long-term effects of the ADF 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 users 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 user workload over long journeys being investigated? ( ) Yes / ( ) No						

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, as we can assume professionals would get accustomed to the system earlier.

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.

Real time monitoring of a driver's inattention / attention is a crucial topic, especially when discussing AD. In fact, not only the driver distraction is one of the main causes of accidents on the roads, but also the knowledge of driver status (namely, if s/he is attentive or distracted) 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 most of relevant secondary tasks considered? ( ) Yes / ( ) No		• Are plausible secondary tasks possible today and in the near future taken into account? • Which secondary tasks are legal or in what timeframe will they become legal? • Which metrics shall be measured via a driver monitoring function? • Are the metrics appropriate for the ADF defined? • Which apps / secondary tasks can be integrated into the vehicle HVI?				

This question (and related sub-questions) addresses which secondary tasks are allowed during AD (at least from L3 functions). 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		• Does it give feedback to the driver? • Are inappropriate / dangerous driver states (e.g. drowsiness) communicated to the driver?				

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 by means of one or more defined HVI channel(s). For example, in case of drowsy driver, since this is extremely dangerous - especially in L3 functions - the communication shall be given in a reinforced way, until stopping the vehicle if the driver continues not responding. Of course, the specific driver's state shall be communicated also the ADF system, in order to select the most appropriate MRM, in case the driver does not respond to the TOR (within a given time).

Under this perspective, the feedback about the driver states should be communicated, if possible, in a standardized manner. However, it should be discussed inside some HVI standardization and certification group how this can happen, at least as possible guidelines to follow.

<table>
<tr><th>Question 4-3-3</th><th>Relevant Phase(s)</th><th></th><th>CO</th><th></th><th></th><th></th></tr>
<tr><td colspan="2">Is it possible to mirror the customers' devices on the vehicle HVI?
(   ) Yes / (   ) No</td><td colspan="5">• Is it possible to restrict certain apps or certain activities altogether (e.g. laptop) in general due to their potential distraction level?
• In cases where mirroring is possible, is the content restricted according to the driving mode?
• Is it possible to show warning messages despite the mirroring?</td></tr>
</table>

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?

If the messages are related to relevant driver's state (impairment, drowsiness, etc.), the mirroring on e.g. Apple / Android systems (using, for example, "AppleCar" or "AndroidAuto") is a possibility, as a way to communicate with the driver. This becomes especially important if the system "knows" that the driver is engaged in some activities on the smartphone.

Question 4-3-4	Relevant Phase(s)				VV	
Is the impact of typical secondary tasks on take-over time(s) and quality identified? ( ) Yes / ( ) No		• Is a customer clinic or expert assessment data available on this? • Can this be simulated?				

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 and accessed after the start of production, to assess if a selected secondary task (to be defined) has been performed and which is its impact on driving behaviour, traffic safety, etc.? ( ) Yes / ( ) No		• Which types of data should be measured after the start of production? This includes privacy and technical aspects: the possibility to access the data (due to delicate information) and to actually measure them (e.g. because of specific sensors availability), respectively.				

The last question of the driver monitoring section is related to measuring the long-term effects of AD on secondary task, 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

L3 AD requires 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 shall also be considered from this perspective. This topic outlines measures to support the controllability of L3 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		• Is controllability of function limits / failures from L3 to lower levels of automation considered in the design phase? • Are human factors design guidelines followed when defining user needs regarding these transitions? • Are potential users of the ADF and samples for customer clinics selected based on adequate data (e.g. market research)?				

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 AD to lower levels of automation 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			
Are limitations of the human driver taken into account based on available guidelines? ( ) Yes / ( ) No		• Is colour blindness considered by avoiding non-suitable colour combinations? • Is visual impairment considered by choosing sufficiently large enough text and icons for visually impaired drivers? • Is it ensured that the flash rate of icons does not cause epilepsy or similar conditions? • Is it ensured that the audio tones can be perceived by individuals without a full hearing range? • 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)?				

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			
Is the driver informed about function limits that will trigger requests to intervene? ( ) Yes / ( ) No		• Does the user manual describe the functions, handling and limits in an understandable way? • Is the driver informed if a detectable function malfunction or function limit occurs?				

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			
Is the vehicle controllable in the case of a function malfunction or limit by overruling or switching off the function? ( ) Yes / ( ) No		• Is it possible for the driver to deactivate or take back control of an ADF at any time? • Is it ensured that driver actions, which should overrule the function or take back manual control, are intuitive? • 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?				

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			
Does the behaviour of the ADF lead to non-controllable situations from the perspective of other road users? ( ) Yes / ( ) No		• 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? • Is the reaction performance of other road users sufficient to interact with a vehicle that is equipped with a rapidly (hard, intensive) reacting ADF?				

The design phase should also consider the limitations and perception of other traffic participants that are not equipped with an ADF. The AV’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		• Are preliminary controllability assessments and according concept changes carried out during design iterations? • Is the prototype representative of the final system design? • Are function limits, function failures, but also normal transitions being taken into account?				

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		• Are the venues for the customer clinics adequate (laboratory, test track etc.)? • Are adequate precautions taken for real world testing, especially with naive participants?				

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	
Is it possible to sign-off the controllability based on customer clinic results and/or expert assessments? ( ) Yes / ( ) No		• Can function outputs and information be perceived by the drivers quickly enough to enable them to react appropriately (e.g. TOR)? • Is it possible to verify that drivers respond when they are required to retake control (success of take-over)? • Are the function limits clearly understandable for the driver? • Have the drivers' behaviour adaptation over time with respect to ADF's limit been considered? • 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)? • Can the driver control the function after a transition from full function functionality to a degraded mode? • Can the driver control the function after an unintended or accidental function deactivation? • Can the driver control the function if they want to activate the ADF and it is not available? This refers especially to the situation in which the driver is not informed that the function is unavailable. • Is the MRM initiated by the ADF controllable? • 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)?				

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? ( ) Yes / ( ) No		• Is there any skill degradation due to the use of the ADF? • Is there misuse of the ADF? • Are there long-term effects on driver behaviour and on the usage of the ADF?				

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 information and training required for users and the variability of ADF users. 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 this category.

Question 4-5-1	Relevant Phase(s)	DF				
Is the diversity of different user groups taken into account? ( ) Yes / ( ) No		• Is the impact of different countries, regions and their respective cultures taken into account? • Are different age groups and their needs taken into account? • Are differences in the users' physical dimensions, anthropometry and (dis-) abilities taken into account? • Are infrastructural differences between countries and regions taken into account?				

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 significant 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, elderly drivers 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 a variety of different users. This also includes non-age-related disabilities.

Additional information regarding this topic is provided by:

- ”CoP-ADAS”, (Knapp et al. 2009).

Question 4-5-2	**Relevant Phase(s)**		**CO**	**DS**		
Is there a training course needed for drivers? ( ) Yes / ( ) No		• Is the information that the user needs to operate the ADF available to create a training course? • Is a driver training course for users planned? • Is a process to train users of an ADF established? • 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.)?				

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);
- ”CoP-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 variables such as age, gender etc.? ( ) Yes / ( ) 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:

- ”CoP-ADAS”, (Knapp et al. 2009).

Question 4-5-4	Relevant Phase(s)					PS
Is an effective approach of customer information and education available to the users post start of production? ( ) Yes / ( ) No		• Is user information and training supported with appropriate information by marketing and other sources raising realistic expectations? • Is training material made available inside the car (e.g. integrated into infotainment functionality)?				

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 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, by providing accurate commercials and customer sales information guides.

Additional information regarding this topic is provided by:

- ”CoP-ADAS”, (Knapp et al. 2009);
- ”Ford Safety Report”, (Ford 2018);
- ”GM Safety Report”, (GM 2018).

5 Conclusion

5.1 Summary

This deliverable presents the final version of Code of Practice for the development of Automated Driving Functions of the L3Pilot project. The CoP-ADF provides a comprehensive guideline for supporting the automotive industry and relevant stakeholders in the design, development, verification and validation of the AD technologies. The main target user of CoP-ADF are project leaders and developers of ADF, stakeholders occupied with AD can also be concerned by CoP-ADF, which include public authorities, regulation and type approval groups, academic organizations, insurance bodies and the general public.

The CoP-ADF consists of 155 main questions (plus sub-questions) assigned to one of 5 categories and one of the 22 topics, the questions shall be checked and evaluated by user during the development process of ADF. These 22 topics have been identified by L3Pilot partners as the common challenges or that could lead to a frequent misapplication during the ADF development process. The scope of the CoP-ADF is on L3 and L4 ADF in passenger cars for motorway and parking. However, extensions to other ODDs or automation levels are feasible as well.

The path to a final version of the CoP-ADF took 3 years, which incorporates several discussions or interviews with the internal stakeholders of L3Pilot as well as a widely external industrial scope. During the CoP-ADF development process, each question has been continuously reviewed and updated by L3Pilot sub-project 2 partners. The key challenges were to structure these questions, to reduce the number of questions from the 586 initial questions to a more reasonable number and to condense each question in order to allow the user to easily comprehend and work with the CoP-ADF. A regularly update process of each question has been followed to make sure that each question is in line with the latest industrial reports, standards or regulations, which are based on the status at the end of 2020.

A validation phase was considered to check the comprehensiveness, understandability, consistency and best use of the CoP-ADF. The validation process started with an internal consultation of all Sub-Project Leaders in L3Pilot. They were asked to give feedback on a draft version based on their works on L3Pilot. In a second step, a workshop was organised during the L3Pilot General Assembly in November 2019. All L3Pilot partners were consulted and were able to give comments and feedback on the draft of CoP-ADF (Deliverable D2.2). A new version of the CoP-ADF was prepared by taking into consideration of the given comments and feedback. The new version was then sent to 12 external experts from different disciplines (FuSa, cybersecurity, HMI, V2X, regulation, V&V, etc.). A workshop has been held in October 2020 to collect the external experts' feedback and to discuss CoP-ADF applicability. Feedback ranged from general topics to specific questions, was carefully considered and integrated one by one in the final version of the CoP-ADF. The validation process ended up with a final review of a selection of 4 experts inside the L3Pilot project.

It must be noted that the scope of the CoP-ADF is not to provide technical solutions, but to support the development of ADF by ensuring that relevant aspects have been considered. Therefore, there is not necessarily a right answer to all CoP-ADF questions. The purpose of the questions is rather to make the developers and other relevant stakeholders aware of certain aspects and to ensure that reasons for decisions are taken and documented. As a document in the public domain, CoP-ADF contributes to the consolidation of development process towards (not only) a European basis for the wide public acceptance of the robust and safe ADF.

5.2 Lessons Learnt

The CoP-ADF has been developed between 2019 and 2021, the final results are presented in this document. The entire process involved intensive discussions among the L3Pilot partners about broad spectrum of topics related to the complex technology of automated driving. As in each project and development, the process is accompanied with learnings. This sub-chapter reports on these lessons learned as well as on how L3Pilot's findings have been considered for in the CoP-ADF's work. It will not go into detail for the lessons learned of other L3Pilot sub-projects. Their lessons learned will be report in the upcoming final project report.

- There is no single solution for the implementation of automated driving

Considering different L3Pilot prototypes and approaches taken by the different manufacturers (see L3Pilot project deliverables D6.3 Pre-test results and D6.5 Piloting reporting outcomes), it became clear from the beginning that there would be no single approach for the implementation of a safe ADF – at least not at the current stage, which represents the transition from research to deployment. Therefore, a key aspect for the CoP-ADF was to try to be neutral in terms of technology and to let room open for different technical solutions. This aspect is also recommended for other activities – such standardization activities, regulatory activities etc. – as long as the knowledge and on-road experience with the technology is limited, i.e. most of the experience bases on prototype tests. Once the technology has gone into mass production and the experience with this technology in the field has grown, more concrete recommendation can be given.

Nevertheless, in the near future experience and knowledge related to AD will further increase heavily. In this sense, L3Pilot marks with it pan European pilot tests a significant step forward. Information gained in the project has been considered in the CoP-ADF up to release of the document via experience of the SP2 (CoP) partners, who in the majority provided prototypes as well, and the L3Pilot workshops. More information is provided in deliverable D2.2 (Fahrenkrog et al. 2020).

- Trade-off between detailed information and broad understanding

A particular challenge for the CoP-ADF was to find the right level of detail. This challenge is related to the question, how is the main stakeholder for this document. On the one hand, there are developers, which ask for detailed technical guidance. On the other hand, there are political- and management-oriented stakeholder, which ask for rather an overview about the entire topic. Satisfying both requests is not an easy task. If the document is set up in a very detailed way, there is the high risk of losing track for not topic related experts. A too broad overview will not help the developers, since only obvious aspect are discussed.

The taken approach in the CoP-ADF is to use questions in order to ensure that relevant aspects are not forgotten. In order to tackle both level of detail, each question consists of a main question (high level) and / or detailed sub-questions. In addition, links to further literature have included to refer to the simple repetition of information that has been published in other documents. To which extend this solution will satisfy the different stakeholders will be proven in the future. The feedback from the consortium that has been collected during the workshops (L3Pilot internal and external expert workshop) has been positive. Consider the range of partners in L3Pilot and experts this is a good indication that the chosen setting works.

One aspect that has been started, but can be more elaborated in following up activities, is the use of technical annex (comparable to an ISO technical report) in order to report in more detail on technical implementation. It is expected that both stakeholder groups will benefit from these reports that provide more insights. Here, the lessons learned from L3Pilot can provide a good basis for future technical annexes. However, it must always be taken into account that the described solution might not be the only solution. Thus, there is as well the risk that the technical annexes might be misleading.

- Communication of results

Communication of the final result, namely the CoP-ADF, is a key aspect of the work of this sub-project. It must be taken into account that the CoP-ADF is not intended to be simple L3Pilot project related document, but its intention is to support the development of automated driving in the future. The big challenge here is that the final version CoP-ADF become available at the end of the project, which makes the marketing difficult. Presentations at conference have been made – as far as possible (e.g. ITS Virtual Congress, EUCAR Reception). However, these could only be teaser for the final document.

This deliverable provides the complete overview about the process, the CoP-ADF questions and related information. Therefore, this document is and will remain the CoP-ADF. However, the authors of CoP-ADF expect that this deliverable presents the final results of CoP-ADF as well as the whole process to develop and to validate the CoP-ADF questions, it will not be the easiest handy approach for users to work with the CoP-ADF. Therefore, the decision has been taken to use further publications and other media to generate a more work friendly version of the CoP-ADF. The final format has not been decided, but the work on this will start with finalization of this deliverable. Main criteria for the handier version are: it should be appealing, allow for quick navigation, offers opportunities to provide feedback as well as easy integration for updates. Furthermore, it should allow for a smooth continuation in the following up activity in the project Hi-Drive.

- Automated driving is fast evolving technology

The biggest challenges for the CoP-ADF was that rapidly development in the topic of automated driving. Several activities have been started and ended during last three years. Several documents have been published by governments, regulation authority, manufactures, suppliers, insurance companies, research organization, universities, think tanks etc. This leads to flood of information that need to be process, evaluated with respect to its importance and structured in a readable format. This results in two challenges: 1) there is high risk of losing track of the state-of-the-art and not be able to identify relevant information and 2) a report can always only provide snapshot from its release date.

For the first challenge, it is important to involve difference experienced experts in the work. Here, L3Pilot consortium is in a unique situation. The combination of industry partners, insurance companies, research organisations, universities and user organisation allow already to cover a broad spectrum of experiences and knowledge. The experience of the consortium has been used directly (involved L3Pilot SP2 partners) as well as indirectly (workshop, meetings) for generation of the CoP-ADF. In particular, the fact that nearly all SP2 partners were directly involved in the pilot activities (via prototypes, common database etc.) ensured a direct transfer of the lessons learned for the pilot into the CoP-ADF. The information transfer might not in all cases be directly visible, because the L3Pilot's information needed to be generalized for the CoP-ADF. This is necessary since L3Pilot focus mainly on testing on public roads. Testing is only on part of the ADF's development. But L3Pilot's findings are also relevant for other phases of the development.

For the second challenge the solution within L3Pilot is not so easy, since it requires rather regular updates of the CoP-ADF. The current CoP-ADF and its structure provides here already a format that can easily be updated by e.g. adding sub-questions or adding literature references. Furthermore, it is highly appreciated that the CoP activity will be continued in the following Hi-Drive project. However, the updates in the technical format of CoP-ADF need to be considered to faster current update process. One option could be an online version. The authors hope to make a first step with aforementioned additional version of the CoP-ADF in the last period of L3Pilot. Independent of this, providing fast regular updates need to be considered by any future activity.

Annex 1 Report of the L3Pilot SP “Methodology” on Test and Evaluation of ADF

Examples of inputs from L3Pilot into the CoP-ADF can be found in the draft of CoP-ADF, deliverable D2.2 (Fahrenkrog et al. 2019). Test and evaluation tools are reported here to collect objective and subjective data for impact assessment.

A1.1 Objective Data Collection

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

Tool:	Description:	Pros:	Cons:
Driving simulator	- Driving Simulators range from low- and medium- to high fidelity simulators as well as from stationary to dynamic. - It allows for a standardised tests procedure. - It allows for testing hazardous/dangerous situations without the risk of harming anyone.	- It provides standardised conditions for all participants. - Naive drivers can be assessed. - Measures for assessing driver state are available and deliver comparably good data quality. - ADF behaviour can be easily changed. - It is suitable to systematically study various user-related ADF aspects.	- It does not test a real ADF, but just a simulated system (-> no technical assessment). - All experienced system boundaries are staged. - It is not suitable to test real ADF behaviour. - Impact of ADF on certain driver aspects cannot be assessed in experimental tests (e.g. mobility behaviour).
Test track	- Cars are driven on specifically designed tracks and not on public roads. - The test track provides a controlled setting compared to road tests.	- It is suitable to systematically study various aspects of ADF functionality and –behaviour. - It provides easier access to test prototype functions. - Relevant aspects of driving environment can be systematically varied.	- Variation of driving environment is limited compared to public roads. - For certain traffic environments are difficult to stage (e.g. traffic jam). - Tests with naïve drivers might be influenced by artificial surrounding. - Impact of ADF on certain driver aspects cannot be assessed in experimental tests (e.g. mobility behaviour).
Experimental road test	- Experimentation carried out with instrumented vehicles in real traffic conditions on a predefined test route. - Generally, a researcher accompanies participants giving instructions and observing behaviours.	- It is suitable to systematically study various aspects of ADF functionality and -behaviour. - Realistic environment and traffic conditions is used. - It offers experimental control through test protocol and the test route.	- Permission of road authority for testing ADF on public roads are needed. - In order to cover different experimental conditions, participants often have to drive the same test route several times. - Impact of ADF on certain driver aspects cannot be assessed in experimental tests (e.g. mobility behaviour).
Wizard of Oz	- Method used to give the appearance of an automated function although it is not an automated vehicle. Instead it is controlled by a hidden driver (wizard).	- The WoO is more realistic than other simulation methods in the laboratory. - Drivers (adverse) reaction to ADF can be tested more safely in the field. - Naive drivers can be assessed in real traffic conditions. - Suitable to systematically	- Duration of experiment limited due to strains on hidden driver. - The test is associated with a demanding job for the “wizard”, who needs to be trained well to be able to control the vehicle. - Special permission is required to operate the WoO

Tool:	Description:	Pros:	Cons:
		study various aspects of ADF and driver experience.	vehicle. - Replication of situations is limited. - It is not suitable to test the technical ADF behaviour.
Field operational test	- Field operational tests (FOT) aim at investigating the effect of one or more independent variables (e.g. assistant systems, different groups, different conditions) on driving behaviour. - During the FOT data are collected continuously.	- FOT offers more experimental control than NDS (e.g. driving with system: experimental – driving without system: baseline). - It can be designed as between-participant design. - It external validity higher than in simulator studies. - Function is assessed in a real world environment. - Conclusions on the effects of ADAS/ADF in the field can be drawn.	- FOT lacks of specific instructions and naturalistic driving internal validity not as good as in lab studies. - Permission to test function on public roads needed. - It is resource consuming.
Naturalistic driving study	- Participants usually drive an instrumental car (often their own) for a period of time on their usual routes without any limiting instructions. - During the study data are recorded continuously. - NDS follows no experimental control in terms of group assignments or control conditions (variables are not actively manipulated).	- NDS data are highly realistic. Therefore, conclusions on general driving behaviour can be drawn. - Participants are not asked to alter their behaviour. Valid observed behaviour is actual behaviour to a high degree. - No instructor present.	- There is no experimental control. - High variance in observed behaviour requires a large number of participants and/or kilometres driven. - Depending on scope permission of authorities needed. - The methods is quite resource consuming.
Analytic simulation - Driving scenario simulation	- Simulation tools mainly foreseen for the safety impact assessment. - Different approaches can be applied to assess the effect of technology, such as re-simulation of accidents or stochastically generated driving scenarios. - Quality of the simulation depends strongly on the quality of the input and models. - Commercial and open source software available.	- Resource efficient way to analyse different driving scenarios. - Any physical harm is impossible. - Number of simulated scenarios and variations can arbitrarily be chosen. - Tools can cover the entire driving process up to the collision and by this allow for the assessment of traffic safety.	- Accuracy depends on values used for settings, models as well as validity of the tool. - Models for simulation sub-components are required - in particular function. - Further input might be required in addition to get to the final safety impact (e.g. for scaling up).
Analytic simulation - Traffic (micro-) simulation	- Tool for the impact assessment (safety & environmental). - Simulates the behaviour of individual vehicles on a road or road network. - Quality of the simulation depends strongly on the quality of the input. - Commercial and open source software available.	- Resource efficient way to analyse different traffic scenarios (varying driving behaviour, penetration rates etc.). - Any physical harm is impossible. - Number of simulated scenarios can arbitrarily be chosen. - Some safety related aspects can be analysed (e.g. number of incidents, time headway, and time to collision).	- Accuracy depends on the values used for settings, models as well as validity of the tool. - Models for simulation sub-components are required - in particular function. - As far as safety related aspects are analysed, no final conclusion on impact on safety can be derived (e.g. injuries, damages).

A1.2 Subjective Data Collection

Table A1.2: Overview pros and cons for different subjective data collection tools by SP3

Tool:	Description:	Pros:	Cons:
Observation	- Via human observer, camera or "medical" sensors. - During test drive or during day-to-day mobility.	- Real behaviour can be observed.	- The awareness of being observed can manipulate the behaviour. - L3-ADF still cannot be observed in day-to-day mobility.
Focus group	- Creating an intensive discussion between persons to understand their attitudes, expectations and requirements. - Guiding these discussions via a moderator.	- Getting answers on open questions. - Understanding the motivations behind the answers.	- Possibility of influencing peoples opinion by other participants. - Risk of dominance by single participants.
Open-ended interview questions	- Interviewing people to understand their attitudes, expectations and requirements. - Can be face to face or via telephone. - Getting answers on open questions.	- Understanding the motivations behind the answers.	- Costs a lot of time for the interview itself and the analysis of the interviews. - Because of this only limited number of interviewees possible.
Close-ended interview questions	- Interviewing people to understand their attitudes, expectations and requirements. - Can be face to face or via telephone. - Getting predefined answers.	- Limited time effort, greater number of interviews possible. - Fast analysis.	- Costs personnel time for the interview itself. - Insight into the motivation behind the answers rather small.
Close-ended survey/questions	- Asking people to understand their attitudes, expectations and requirements. - Can be paper and pencil or online. - Getting predefined answers.	- Once the survey is prepared, higher number of respondents is easy to realise (especially online). - Fast analysis.	- Insight into the motivation behind the answers rather small. - Seriousness of the answers can be a problem.
Travel diary	- People write down their daily travel experiences with ADF. - Requires a day-to-day use of the vehicles.	- Easier to realise than an observation.	- Risk of oblivion.
Standardised questionnaire	- Two inquiries: Before and after test drive. - Conjunction with the representative survey reasonable.	- Detection of the influence of the test drive experience.	- Insight into the motivation behind the answers rather small.

Annex 2 Positive Risk Balance: Safety Thresholds for the Development of ADF

As described in topic 4.3.4, a positive risk balance in terms of traffic safety is essential for the ethical legitimisation of introducing AD. A positive risk balance means that the ADF should drive at least as safe as today’s human traffic safety performance that stems from human driver, infrastructure, current active safety systems, etc. This requirement has been set in different forms by several bodies:

- Report of the German Ethic commission on automated driving (di Fabio et al. 2017):

> Article 2 “…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.”
>
> Article 3: “… The guiding principle is the avoidance of accidents, although technologically unavoidable residual risks do not militate against the introduction of AD if the balance of risks is fundamentally positive.”

- Report of the European Commission on “Ethics of Connected and Automated Vehicles” (Bonnefon et al. 2020):

> Recommendation 1: “Ensure that CAVs reduce physical harm to person - To prove that CAVs achieve the anticipated road safety improvements, it will be vital to establish an objective baseline and coherent metrics of road safety that enable a fair assessment of CAVs’ performance relative to non CAVs and thereby publicly demonstrate CAVs’ societal benefit. ...”

- UN ECE ALKS Regulations (UN ECE 2020):

> Paragraph 5.2.5 “… For conditions not specified in paragraphs 5.2.4., 5.2.5. or its subparagraphs, this shall be ensured at least to the level at which a competent and careful human driver could minimize the risks “.

The positive risk balance is defined by these documents, but it is rather a high-level goal and it remains rather unclear what this means in detail and how this can be transferred into safety performance targets that can be applied in the course of the development of ADF.

Therefore, an approach is outlined that aims to transfer the target of the positive risk balance in threshold values for the development of ADF.

The given approach does not claim to be an exclusive approach, but it is a possible way for deriving the related targets. Other approaches to prove a positive risk balance or derive a threshold can also be applied. Thus, the annex does not claim to provide the only possible approach, but proposes one approach.

Within in the approach two exemplary ADF are considered. The first ADF is a motorway ADF that covers the entire motorway which is limited up to 130 km/h and can perform lane changes. The second ADF is a traffic jam function that can only operate up to 60 km/h. It does not perform any lane changes and the activation of the function is only possible while being in a traffic jam. Both functions operate at L3 functions. Furthermore, to demonstrate the approach, we use accident data from Germany. However, the basic principles of the approach can be applied for any other country.

A2.1 Identification of the adequate Accident Types for the Risk Balance

In general, for a sound comparison of two results, it is obvious that both results (safety performance of the ADF vs safety performance of today's traffic) shall be derived under comparable circumstances. The core metric of traffic safety is the number of accidents, which can further be detailed by the number of accidents of a certain severity. Typically, this information can be obtained through accident statistic or a database.

Thus, the first step is to identify the accident types that shall be considered for the assessment. This step seems to be easy on the first glance, since the ODD of an ADF needs to be described anyway. The intuitive approach would be to analyse, which accidents happen within the ODD and take this as a basis for deriving the accident encountered in the ODD. However, the ODD describes only the conditions under which the function can operate. It does not describe explicitly the conditions under which the ADF does not operate. And here it needs to be considered, that the exclusion of certain driving manoeuvres or driving conditions, can also affect the risk of an accident (in a positive or negative manner).

Let's have a look at the second function – the traffic jam ADF. This function is not capable of performing a lane change automatically. However, there are accidents occurring during lane changes in a traffic jam. With the ADF in place, these types of accidents are not going to happen – it is presumed that the function is operating properly and no technical issue occurs – since the pre-required manoeuvre cannot happen for the ADF and is outside the ODD.

As this example demonstrates, it is not enough to analyse only the accident in the ODD, but it needs rather to be checked for all accidents that are directly or indirectly affected by the ADF in question. In order to highlight this extended view on the accidents that are relevant for the risk assessment the term "functional field of application" (FFoA) is used in the following.

The relation between the FFoA and the ODD is visualized in Figure A1. The ODD is always a subset of the FFoA. As a maximum, the ODD can cover the same scenarios as the FFoA. The FFoA is – except in case of L5 functions – always subset of the entire traffic space.

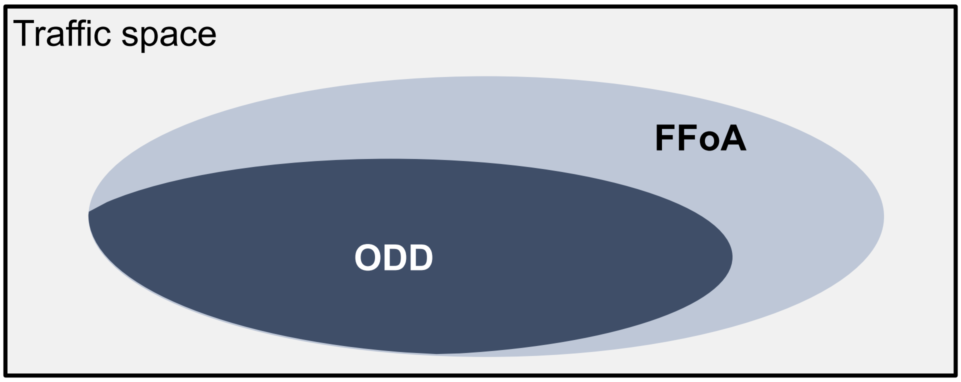


Figure A1: Visualization of the relation of ODD & FFoA

Next to the accident scenarios, it needs to be further defined which accidents of the scenarios should be considered for the risk balance. Each accident has different parameters, like type of traffic participants, location, time, weather, participant at fault, kinematic conditions etc. Different accident statistics and databases report different levels of information.

Considering the variety of human driving, it is rather obvious that primarily the focus for the risk balance assessment should be national or international accident statistics / databases, since they collect typically a representative number of accidents. The question, which country needs to be analysed, can be answered considering the planned application for the ADF.

However, the national accident statistics / databases report typically the traffic safety situation rather on an abstract level with only a few accident parameters. These parameters should be used to describe the safety performance baseline as accurate as possible. This means for example that accidents should be further filtered for the involved vehicle type. In case the ADF is only intended for passenger cars, only the accidents should be considered where at least one passenger car was involved. Truck-versus-Truck accidents would be excluded.

A more difficult question for the assessment is, whether only accidents shall be considered in which the passenger car was at fault. In theory, this filtering for accidents should be applied. However, the decision, who is at fault is often not clear. The number of traffic accidents-related court cases in Germany shows how difficult this topic is. The German court handled 135,900 cases related to traffic accidents in 2019 (DESTATIS Justice 2020). Due to this uncertainty, it is recommended to not include this filter criterion for identifying the baseline for the positive risk balance.

In conclusion, the baseline for the assessment of the positive risk balance is the number of accidents in the FFoA which involves at least one passenger car neglecting the aspect who is at fault. The baseline sets the threshold that needs to be achieved by the ADF in question.

A2.2 Analysis of Accident Data to derive Thresholds according to the positive Risk Balance

Once the FFoA is identified, the task of deriving the actual threshold for the positive risk balance can start. In order to get to the thresholds, three aspects need to be considered:

- What is a suitable metric for the threshold in terms of severity and unit?
- How to identify accident values in case they cannot be directly derived from the national statistics?
- How to deal with annually changing accident statistics?

First, the metric shall be chosen in which the threshold should be provided per accident severity category. The unit and injury severity depend on the requirements of the analysed ADF, i.e. in case of a traffic jam function, a time-wise metric is properly more useful than a distance-related one.

There are three different main metrics to provide a threshold to the positive risk balance. The first one is the risk of an accident respectively incident per operational year (ipoa). Here, one has to quantify the time, for how long ADF will operate through the year (e.g. 15 hours). The second one is the risk of an incident per driven kilometre. And the third one is the risk of an incident per driving hour. All these metrics can be derived once accident exposure data (i.e. average distance between to accidents) is known. This indicator can be calculated based on the number of accidents, which has to be derived from accident statistics, as well as the annual driven distance of the fleet that has been taken into account for the accident statistics.

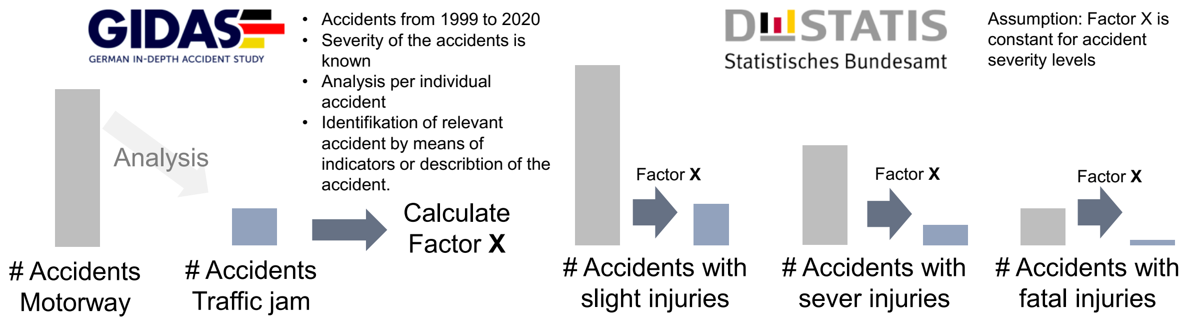
Regarding the accident severity there are different options. These options are for instance: number of accidents, number of accidents without personal damage, number of accidents with slightly or more severe injured persons, number of accidents with fatally injured persons. In order to cover the entire accident scene, it is recommended to analyse at least the number of property damages as well as the number of accidents with slightly, severely and fatally injured persons.

The key indicator for the threshold calculation is the average distance between two accidents. For the analysis the FFoA as well as the above-mentioned filter criteria shall be applied. In case the accident statistic directly provides the values according to the FFoA and filter criteria this process step is rather simple. This is for instance the case for first exemplary ADF (FFoA: motorway, additional filter: all accident with a passenger car involvement). The values are given in the table below.

Table A2.1: Number of accidents with passenger car involvement on German motorways according to (DESTATIS 2015 – 2019)

Accidents with passenger Cars		2015	2016	2017	2018	2019	Mean	STD
Severity	**Fatal**	287	250	236	248	230	**250.2**	**22.2**
	Severe	3495	3753	3627	35473	3457	**3581.0**	**116.8**
	Slight	14342	15258	14973	14518	14308	**14679.8**	**418.0**
	Property damage	129966	140626	152572	133684	136851	**138739.8**	**8674.6**

However, in most cases deriving the thresholds will not be so simple. Hence, a closer look is taken for the second ADF (FFoA: Accidents in traffic jam, all accident with a passenger car involvement). The German national accident statistics do not provide any details on accidents in jammed-traffic conditions. Therefore, a second more detailed accident database is utilized, here the GIDAS database (VUFO (2018), GIDAS (2020)). GIDAS provides more information than the national statistic, which allows to filter for the FFoA and the additional filter criteria. Of course, the second database needs to include a sufficient number of cases to represent the national accident scene. Once such an in-depth database is identified, the accident data are filtered for the FFoA and the additional criteria. The number of identified accidents is then put into perspective to the overall number of accidents in order to derive a proportional factor "x" between the number of the national statistics and the in-depth database. This factor is afterwards applied to the national accident statistic in order to estimate the number of accidents in the FFoA on national level, see Figure A2. Individual factors per injury severity would be desirable. However, due to the low number of relevant accidents even in the detail accident database, a more precise approach is not feasible for the given example.



- Accidents from 1999 to 2020
- Severity of the accidents is known
- Analysis per individual accident
- Identifikation of relevant accident by means of indicators or describtion of the accident.

Assumption: Factor X is constant for accident severity levels

Figure A2: Application of the reduction x that is calculated based on a second accident database for the example a traffic jam ADF in Germany

In analogy to the first function the resulting numbers for the second function are given below:

Table A2.2: Estimation of the number of accidents with passenger car involvement on German motorways in traffic jam according to GIDAS analysis and (DESTATIS 2015 – 2019)

Accidents with passenger Cars		2015	2016	2017	2018	2019	Mean	STD
Severity	Fatal	1.4	1.3	1.5	1.6	1.5	**1.5**	**0.1**
	Severe	20.2	22.1	21.6	22.3	21.1	**21.4**	**0.8**
	Slight	110.2	116.9	114.6	114.1	110.2	**113.2**	**2.9**
	Property damage	2183.3	1113.0	1091.8	1086.9	1049.4	**1304.9**	**491.6**

The last missing information is the overall driven mileage in the FFoA. This number can be more difficult to derive due to missing data. For instance, in Germany only the overall mileage of passenger cars per year is reported only every 5 years then extrapolated for the other years. For the annual driven mileage in traffic jams the same approach is followed, although the applied factor needs to be calculated differently. An overview about the average driven mileage for the two exemplary ADF is given in the table below:

Table A2.3: Estimation of annually driven mileage of passenger cars in Germany for two exemplary ADF based on (BMVI 2019)

Driven mileage passenger cars [km]	ODD	2015	2016	2017	2018	2019
ADF Example 1	Motorway	1.69E+11	1.74E+11	1.76E+11	1.78E+11	1.80E+11
ADF Example 2	Traffic jam	6.43E+09 (estimation for all years)				

Accident numbers are affected by many different contributing factors. Not all of these factors can be controlled for the analysis. For instance, different weather condition in different years, could lead to a significant change in certain years. In order to avoid a too strong influence of single results, it is suggested to take the average of the accident number over five years.

Another aspect that needs to be considered is the decreasing trend in the accident statistic. Since the 1970's the number of accidents is decreasing. These improvements for traffic safety shall be taken into account. Therefore, regular updates of the threshold with the most recent statistics shall be considered.

In order to demonstrate the process, the thresholds for the above mentioned exemplary ADF are calculated based on the accident situation in Germany. For this purpose, the national accident data for the years from 2015 to 2019 (DESTATIS 2015 – 2019), the GIDAS database (VUFO (2018), GIDAS (2020)) and the mileage statics from 2015 to 2019 (BMVI 2019) are utilized.

Table A2.4: Calculated threshold to achieve a positive risk balance for the two exemplary ADF based on the accident situation in Germany

ADF Example Motorway	Acc. w. property damage	Acc. w. slight injuries	Acc. w. sever injuries	Acc. w. fatal injuries
Average distance between two accident [km]	1.27E+06	1.20E+07	4.90E+07	7.06E+08
Threshold incidents per operational year (ipoa) [1/a]	2.41E-03	2.55E-04	6.22E-05	4.32E-06
Threshold incidents per hour [1/h]	7.10E-05	7.53E-06	1.84E-06	1.27E-07
Threshold incidents per km [1/km]	7.89E-07	8.37E-08	2.04E-08	1.42E-09
ADF Example Traffic Jam				
Average distance between to accident [km]	1.10E+07	4.72E+07	2.81E+08	4.41E+09
Threshold incidents per operational year (ipoa) [1/a]	1.32E-05	3.07E-06	5.17E-07	3.29E-08
Threshold incidents per hour [1/h]	2.73E-06	6.35E-07	1.07E-07	6.80E-09
Threshold incidents per km [1/km]	9.10E-08	2.12E-08	3.56E-09	27E-10

A2.3 Safety Margins for development targets

The above-mentioned threshold defines the today's traffic safety performance. In this case for the example Germany. The values represent average values – time wise as well as driver type wise. For the development of ADF, the company internal targets can consider certain safety margin towards these thresholds in order to make the reaching of the threshold more certain or to cover a sophisticated driver performance (e.g. attentive drivers). However, it is up to the developing company to decide to which extend to go beyond. It is important to underline independent of the risk balance that regulatory requirements need to be always followed. They represent the minimum requirements for the ADF and its development. In the following the reason for adding safety margins is briefly described. How the margins are implemented needs to be defined by the developers.

There are two main areas of uncertainties when defining development targets. The first area is related to statistic, which defines the thresholds for the target values. The second area is related to the uncertainties in the development process around the applied models and used data. It must be kept in mind that these uncertainties in a negative way could lead to a negative risk balance, which would violate the ethical standards above. This would put the operation of the ADF in traffic in jeopardy.

Statistics have underlying uncertainties that need to be considered. These uncertainties apply for the target values. They are related to the assumption that have to be made during the calculation as well as to the deviation of the values for different year (see Table A2.2). Safety margins can here be calculated by means of statistical approaches.

The uncertainties related to the applied development tools and the required safety margins to overcome these uncertainties are more difficult to determine, because:

- often a combination of tools and data sources is used (each can be associated with an uncertainty);
- the function to be developed might not be defined in all details;
- possible influencing parameters (e.g. drivers' usage behavior) might be unknown or not fully known during the development;
- the accuracy of certain tools (e.g. expert opinion) and data source can hardly be quantified.

These aspects shall be considered when defining a sufficient safety margin for these uncertainty area.

A2.4 Estimation of ADF's required Safety Performance during the Development

Once the targets are defined, these values can be used to estimate which safety performance needs to be achieved by the ADF. The approach is independent of the chosen metric. It is only important that one metric is chosen and used consistently throughout the calculations.

Furthermore, it is important to note that the targets for the positive risk balance apply for the overall function. However, since the function will encounter different scenarios, in which the ADF will properly perform differently, the overall targets need to be transferred in targets for the individual scenarios. The approach for this needs to be chosen depending on the number of scenario and the scenarios itself, which depend on the FFoA. The simplest approach is to equally distribute a risk to each considered scenario.

In the next step the anticipated risk with respect to traffic safety in different scenarios needs to be derived. The risk calculation is basically a multiplication of different risk factors. These factors can be split into three categories:

- Factors ($RF_{Scenario}$) that describe the risk that a certain scenario (event) occurs. These can be either dependent on or independent of the ADF design. A scenario that is typically independent of the ADF design, for instance, is the scenario “obstacle in the ego vehicle’s lane”: the likelihood of an obstacle risk it does not change with the ADF design. On the contrary, the likelihood to encounter a fast-approaching vehicle during a lane change is dependent on ADF design. This scenario only becomes relevant in case the ADF is capable of automatically executing lane changes.
- Factors (RF_{ODD}) that are related to the operation of the ADF. The factors of this category should consider how often an ADF is in operation while encountering the scenario. One factor is for instance the presumed usage rate.
- Factors (RF_{IRF}) to describe the consequences of a potential accident on a certain severity in a scenario. In the FuSa domain often the so called “S”-values are used. These values are used to describe the accident risk of certain severity with a probability of 10% (e.g. S3 is an AIS 5 or 6 injury with a 10% probability). Thus, in case the S-values are used, a certain safety margin is considered. Therefore, it is recommended to use more precise estimations, like it is provided by, for example, injury-risk-functions. The IRF need to be chosen according to the crash configuration. A further advantage of the IRF-approach is that the risk for different injuries could be calculated at the same time. Therefore, in the presented approach the IRF-approach is chosen.

The only remaining factor is that something goes wrong, i.e. that an accident occurs. In the traditional approach is that this factor is determined (e.g. by test, simulations) or estimated in the assessment and multiplied with previous factors. However, in this case the development thresholds shall be calculated. Therefore, this parameter related to required system performance, i.e. how often can something go wrong to ensure that the overall objective of a positive risk balance is still met, is the requested value? These values can be calculated per injury category by dividing the threshold value with the multiplication of the previously mentioned factors (see red and green arrows in the figure below). The basic principle is the risk factors is given in the Figure A3.

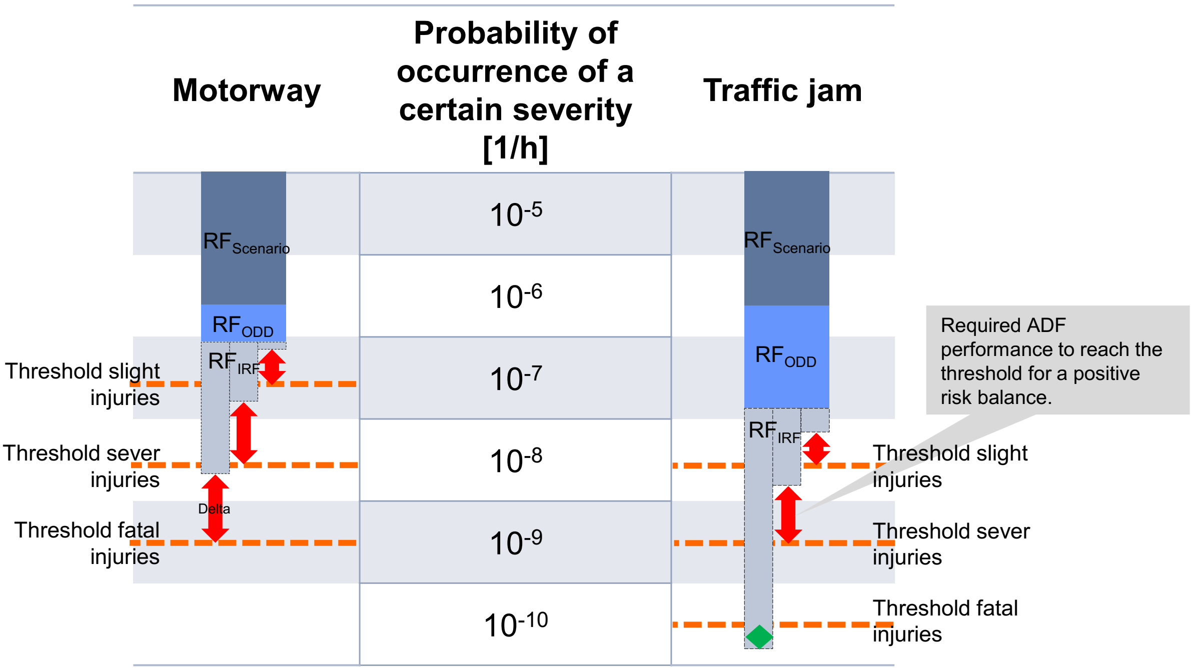


Figure A3: Calculation of required safety performance for the two exemplary ADFs in the example of an obstacle on the road

A2.5 Challenge to investigate rare Events

The derived thresholds imply that an accident is a very seldom event. And this will stay the same for ADF. Therefore, it needs to be discussed, how to deal with these seldom events.

In order to underline this aspect, an example is given. A manufacturer sells 10.000 vehicles with an ADF each year. Each of the vehicles drives 10.000 km on the motorway each year and the ADF is active 50% of the time. Since the cars are sold constantly over the year, a factor of 0.5 is considered for the vehicles that are sold in that year. Furthermore, it is considered that every car that encountered a crash is removed from the fleet. The table below lists the cumulative number of ADF accidents under the assumption that accident frequency is as high as for human drivers (see average distance between an accident in Table A2.5).

The example indicates that in particular for the most relevant category – the fatal accidents - the duration until a statistical relevant number of accidents is detected will be quite long. In the example a statistical relevant number of cases is not reached in even 10 years. Therefore, it is suggested for statistical analysis to focus rather on the accident dealing with no, slight or severe injuries. It is important to underline that this statement refers to the statistical analysis. It does explicitly not mean that certain accidents should not be investigated. Each accident with an AV should be detected and analysed by means of the available tools. Furthermore, the accidents, which could potentially lead to fatal accidents, should be treated with special care. Although statistical analysis might be difficult due to the lower number of cases compared to other accidents, they must be considered, e.g. in a detailed analyses of corner cases.

Table A2.5: Prediction of cumulative number of accidents of motorway ADF for years after market introduction for the given scenario based on the calculated human drivers' accident risk

Year [-]	Considered amount of vehicles [-]	Cumulative number of accidents with property damage [-]	Cumulative number of accidents with slight injuries [-]	Cumulative number of accidents with severe injuries [-]	Cumulative number of accidents with fatal injuries [-]
1	5000	19.7	2.1	0.5	0.0
2	14978	78.7	8.3	2.0	0.1
3	24911	176.7	18.7	4.6	0.3
4	34800	313.7	33.2	8.1	0.6
5	44644	489.5	51.8	12.7	0.9
6	54445	703.8	74.5	18.2	1.3
7	64202	956.6	101.2	24.8	1.7
8	73916	1247.6	132.0	32.3	2.2
9	83586	1576.7	166.9	40.9	2.8
10	93213	1943.7	205.7	50.4	3.5

Annex 3 Documentation List and relevant Topics in CoP-ADF

This Annex consists of a list that can help reader to quickly search the referenced articles and their corresponding topics in CoP-ADF. The titles of articles as well as the authors / sources and relevant topics are presented in Table A3.1. For more details of the referenced articles in CoP-ADF, please see References.

Table A3.1: Documentation list and relevant topics in CoP-ADF.

Name of document	Authors	Relevant topics in CoP-ADF
“A method to improve driver's situation awareness in automated driving “.	Yan, Y et al.	4.5.2 Mode Awareness, Trust & Misuse 4.5.3 Driver Monitoring
“A System-Theoretic Safety Engineering Approach for Software-Intensive Systems”.	Abdulkhaleq, A.	4.4.3 Implementation of Updates
“A Topology of Shared Control Systems – Finding Common Ground in Diversity“.	Abbink, D et al.	4.2.3 Performance Criteria and Customer Expectations
”ACEA principles of Automobile Cybersecurity“, ACEA.	ACEA Report.	4.4.2 Cybersecurity
“ACEA principles of data protection in relation to connected vehicles and services “, ACEA.	ACEA Report.	4.4.5 Data Recording, Privacy and Protection
“An Update on Japanese Initiatives for Automated Driving”.	SIP-adus HMI 2017 report	4.5.3 Driver Monitoring 4.5.5 Driver Training & Variability of Users
“Autonomous Driving - Technical, Legal and Social Aspects”.	Maurer, M et al.	4.3.3 Traffic Simulation
“Auto-ISAC Best practices”, UTO-ISAC.	UTO-ISAC Report.	4.4.2 Cybersecurity
“Automated driving systems 2.0: a vision for safety “, NHTSA.	NHTSA Report.	4.5.3 Data Recording, Privacy and Protection
“Operational design domain (ODD) taxonomy for an automated driving system (ADS). Specification”, BSI.	BSI Standard	4.2.1 Requirements
“Code of Practice for the Design and Evaluation of ADAS”, RESPONSE 3.	Andreas, K et al.	4.1.3 Existing Standards 4.5.2 Mode Awareness, Trust & Misuse 4.5.4 Controllability & Customer Clinics 4.5.5 Driver Training & Variability of Users
“Development of a Safety Assurance Process for Automated Vehicles in Japan”, METI.	SAKURA Project	4.3.4 Ethics & other Traffic related Aspects
“Draft Recommendation on Software Updates”, UN ECE.	UNTF Document.	4.4.3 Implementation of Updates

Name of document	Authors	Relevant topics in CoP-ADF
“Driver distraction and inattention in the realm of automated driving “.	Cunningham, M. L. et al.	4.5.3 Driver Monitoring
“Driver Fatigue Detection based on Eye State Recognition “.	Zhang, F et al.	4.5.3 Driver Monitoring
“ENISA Good practices for Security of Smart Cars”, ENISA.	ENISA Report.	4.4.2 Cybersecurity 4.4.3 Implementation of Updates
“European Statement of Principles on human-machine interface”, EC.	EC Report.	4.5.1 Guidelines for HVI
“Evaluation of driver's condition and keeping driver's state by HMI “.	Sato, T.	4.5.3 Driver Monitoring
Evaluation plan, L3Pilot deliverable D3.4.	Innamaa, S et al,	4.3.4 Ethics & other Traffic related Aspects
“Expert-based controllability assessment of control transitions from automated to manual driving”.	Naujoks, F et al.	4.5.4 Controllability & Customer Clinics
“FESTA Handbook “.	Barnard, Y et al.	4.4.5 Data Recording, Privacy and Protection
“Final functional Human Factors recommendations”, Adaptive D3.3.	Kelsch, J et al.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse
“FOT-Net Data - Data Sharing Framework”.	Gellerman, H et al.	4.4.5 Data Recording, Privacy and Protection
“Ford Safety report 2018”, Ford.	Ford Report.	4.5.2 Mode Awareness, Trust & Misuse 4.5.5 Driver Training & Variability of Users
“Framework document on automated / autonomous vehicles”, UN ECE.	UN Regulation.	4.1.3 Existing Standards
“Framework for Automated Driving System Testable Cases and Scenarios“, NHTSA.	NHTSA Report.	4.1.1 Minimal Risk Manoeuvre 4.2.1 Requirements 4.2.3 Performance Criteria and Customer Expectations 4.3.1 Automated Driving Risks and Coverage of Interaction with Mixed Traffic 4.3.2 V2X Interaction
“Guide to the general data protection regulation”, GDPR.	GDPR Regulation.	4.4.5 Data Recording, Privacy and Protection
“GM Safety report 2018”, GM.	GM Report.	4.5.2 Mode Awareness, Trust & Misuse 4.5.5 Driver Training & Variability of Users
“Guidelines for In-vehicle Display Systems”, JAMA.	JAMA Report.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse
“Guidelines for trials of automated vehicles in Australia“, NTC.	NTC Report.	4.1.4Testing

Name of document	Authors	Relevant topics in CoP-ADF
“Human Factors Design Guidance For Driver-Vehicle Interfaces“.	Campbell, J et al.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse 4.5.3 Driver Monitoring 4.5.5 Driver Training & Variability of Users
ISO 15288:2015 “Systems and software engineering — System life cycle processes”.	ISO Standard.	4.2.4 Architecture
ISO 26262 “Road vehicles — Functional safety”.	ISO Standard.	4.1.3 Existing Standards 4.2.1 Requirements 4.2.4 Architecture 4.3.4 Ethics & other Traffic related Aspects 4.4.1 Functional Safety 4.4.3 Implementation of Updates 4.4.4 Safety of the intended Functionality
ISO 9001 “Quality management systems — Requirements”.	ISO Standard.	4.1.2 Documentation
ISO/CD 24089 “Road vehicles — Software update engineering”.	ISO Standard.	4.4.3 Implementation of Updates
ISO/DTR 21934-1 “Road vehicles — Prospective safety performance assessment of pre-crash technology by virtual simulation”.	ISO Standard.	4.3.3 Traffic Simulation 4.3.4 Ethics & other Traffic related Aspects
ISO/IEC/IEEE 42010 “Systems and software engineering — Architecture description”.	ISO Standard.	4.2.4 Architecture
ISO/PAS 21448 2019 “Road vehicles — Safety of the intended functionality”.	ISO Standard.	4.1.1 Minimal Risk Manoeuvre 4.1.3 Existing Standards 4.2.1 Requirements 4.2.4 Architecture 4.3.4 Ethics & other Traffic related Aspects 4.4.3 Implementation of Updates 4.4.4 Safety of the intended Functionality
ISO/PRF TR 4804 “Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation”.	ISO Standard.	4.1.1 Minimal Risk Manoeuvre 4.1.3 Existing Standards 4.1.4 Testing 4.3.1 Automated Driving Risks and Coverage of Interaction with Mixed Traffic 4.4.2 Cybersecurity 4.4.4 Safety of the intended Functionality

Name of document	Authors	Relevant topics in CoP-ADF
ISO/SAE 21434 “Road Vehicles – Cybersecurity Engineering”.	ISO Standard.	4.1.3 Existing Standards 4.4.2 Cybersecurity 4.4.3 Implementation of Updates
ISO/WD 34501 “Road vehicles — Terms and definitions of test scenarios for automated driving systems “.	ISO Standard.	4.1.4 Testing 4.3.4 Ethics & other Traffic related Aspects
ISO/WD 34502 “Road vehicles — Engineering framework and process of scenario-based safety evaluation“.	ISO Standard.	4.3.4 Ethics & other Traffic related Aspects
ISO/WD 34503 “Road vehicles — Taxonomy for operational design domain for automated driving systems”.	ISO Standard.	4.2.1 Requirements 4.3.4 Ethics & other Traffic related Aspects
ISO/WD 34504 “Road vehicles — Scenario attributes and categorization”.	ISO Standard.	4.3.4 Ethics & other Traffic related Aspects
ISO/PWI 34505 “Road vehicles — Evaluation of test scenarios for automated driving systems”.	ISO Standard.	4.3.4 Ethics & other Traffic related Aspects
“Legal aspects on automated driving”, Adaptive D2.3.	Bienzeisler, J et al.	4.1.3 Existing Standards 4.3.4 Ethics & other Traffic related Aspects
“Market Forecast for connected and autonomous vehicles”.	CATAPULT Report.	4.3.2 V2X Interaction
“Modelling human vehicle driving by model predictive online optimization”.	Prokop, G.	4.3.3 Traffic Simulation
“MIT Advanced Vehicle Technology Study: Large-Scale Naturalistic Driving Study of Driver Behavior and Interaction with Automation“, MIT.	Fridman, L et al.	4.5.3 Driver Monitoring
“On the Road to Fully Self-Driving - Waymo Safety Report”, Waymo.	Waymo Report.	4.3.3 Traffic Simulation
PEGASUS method – an overview 2019	PEGASUS Project.	4.1.4 Testing 4.2.2 Scenarios and Limitations 4.3.4 Ethics & other Traffic related Aspects
“Preparing for the future of transport – Automated vehicles 3.0”, USDOT.	USDOT Report	4.3.2 V2X Interaction
“Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”, UN ECE.	UN Regulation.	4.1.3 Existing Standards 4.4.2 Cybersecurity

Name of document	Authors	Relevant topics in CoP-ADF
"Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system", UN ECE.	UN Regulation.	4.1.3 Existing Standards 4.4.3 Implementation of Updates
"Real-time detection of driver distraction: random projections for pseudo-inversion-based neural training".	Botta, M. et al.	4.5.3 Driver Monitoring
"Real-time Driver Drowsiness Detection for Embedded System Using Model Compression of Deep Neural Networks".	Reddy, B et al.	4.5.3 Driver Monitoring
Report of the European Commission on "Ethics of Connected and Automated Vehicles", EC.	EC Report.	4.3.4 Ethics & other Traffic related Aspects
"Report of German ethic commission", BMVI.	BMVI Report.	4.1.4 Testing 4.3.4 Ethics & other Traffic related Aspects
"Safety first for automated driving", SaFAD 2019.	Wood, M, et al.	4.1.1 Minimal Risk Manoeuvre 4.1.3 Existing Standards 4.1.4 Testing 4.3.1 Automated Driving Risks and Coverage of Interaction with Mixed Traffic 4.3.4 Ethics & other Traffic related Aspects
"Safer Roads with Automated Vehicles", ITF 2018.	ITF Report.	4.2.3 Performance Criteria and Customer Expectations 4.3.1 Automated Driving Risks and Coverage of Interaction with Mixed Traffic
"Safe and Secure Automotive Over-the-Air Updates - Operational and Functional Requirements".	Sena, M.	4.4.3 Implementation of Updates
"Shared control is the sharp end of cooperation: Towards a common framework of joint action, shared control and human machine cooperation".	Flemisch, F et al.	4.2.3 Performance Criteria and Customer Expectations
"Simulation-based Identification of Critical Scenarios for Cooperative and Automated Vehicles".	Hallerbach, S et al.	4.3.3 Traffic Simulation
Simulation of Autonomous Vehicle Safety (SVA project)	SVA Project.	4.3.4 Ethics & other Traffic related Aspects

Name of document	Authors	Relevant topics in CoP-ADF
“System Classification and Glossary”, AdaptIVe D2.1.	Bartels, A et al.	4.2.3 Performance Criteria and Customer Expectations
“Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities”.	INCOSE Report.	4.2.4 Architecture
“Taxonomy and Definition for Terms Related to Driving Automation Systems for On-Road Motor Vehicles” (J3016).	SAE Report.	4.2.2 Scenarios and Limitations 4.2.4 Architecture
"TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems".	Bolovinou, A. et al.	4.4.2 Cybersecurity
“Testing scenarios for human factors research in level 3 automated vehicles”.	Gold, C et al.	4.5.4 Controllability & Customer Clinics
“Test procedure for evaluating the human–machine interface of vehicles with automated driving systems”.	Naujoks, F et al.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse
“Thatcham Research Report”.	Thatcham Research Report.	4.1.1 Minimal Risk Manoeuvre
“The pathway to driverless cars: a code of practice for testing“.	DoT Report.	4.1.4 Testing 4.4.5 Data Recording, Privacy and Protection
“The key principles of vehicle cybersecurity for connected and automated vehicles”.	HMG Report	4.4.5 Data Recording, Privacy and Protection
“Towards guidelines and verification methods for automated vehicle HMIs”.	Naujoks, F et al.	4.3.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse 4.5.4 Controllability & Customer Clinics
“UN regulation on Automated Lane Keeping Systems”, UN ECE	UN Regulation.	4.1.1 Minimal Risk Manoeuvre 4.1.2 Documentation 4.1.3 Existing Standards 4.1.4 Testing 4.3.3Traffic Simulation 4.3.4 Ethics & other Traffic related Aspects 4.4.1 Functional Safety 4.4.4 Safety of the Intended Functionality 4.4.5 Data Recording, Privacy and Protection
“UR: BAN Human Factors in Traffic. In Approaches for Safe, Efficient and Stress-free Urban Traffic”.	Bengler, K et al.	4.5.4 Controllability & Customer Clinics

Name of document	Authors	Relevant topics in CoP-ADF
“Use cases for assessing, testing, and validating the human machine interface of automated driving systems”.	Naujoks, F et al.	4.5.4 Controllability & Customer Clinics
“Validation of X-in-the-Loop Approaches for Virtual Homologation of Automated Driving Functions”.	Stefan, R et al.	4.3.3 Traffic Simulation

Annex 4 Glossary

Table A4.1: Glossary table.

Term	Definition
Accident	An accident (motor vehicle collision, motor vehicle accident, car accident, or car crash) is when a road vehicle collides with another vehicle, pedestrian, animal, road debris, or other geographical or architectural obstacle. Traffic collisions can result in injury, property damage, or fatality death.
Attacks	A path or route used by the adversary to gain access to the target (asset).
Automated Driving Functions	Activity or purpose of a vehicle to enable automated driving.
Automated Driving System	A combination of hardware and software to realise an automated driving function.
Driver	A user who performs in real-time part or all of the DDT and/or DDT fall-back for a particular vehicle.
Dynamic Driving Task	All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints.
Driving Mode	A type of driving scenario with characteristic dynamic driving task requirements (e.g., expressway merging, high speed cruising, low speed traffic jam, closed-campus operations, etc.).
Driving Scenarios	The abstraction and the general description of a driving situation without any specification of the parameters of the driving situation. Thus, it summarises a cluster of homogenous driving situations. Driving scenarios are typically short in time (t < 30 s) and only a few vehicles are involved. An example is lane change to the left lane.
Driving Situation	A driving situation is a specific driving manoeuvre (e.g. a lane change with defined parameters). Thus, the driving situation describes in detail a situation that can be simulated and analysed. An example of a driving situation is a lane change at 60.8 km/h with a second vehicle driving at a distance of 10 m behind the host vehicle in the adjacent lane and with a velocity of 65 km/h.
Events	Events are either single time-points or segments of time in time-series data for which one or several criteria are fulfilled. An event can be short (e.g. crash) or long, such as 1) start of evasive manoeuvre, 2) car following, 3) overtaking, 4) speeding. Events do not include randomly selected segments of time, even if there would be some top level matching. E.g. matched baseline epochs are not events.
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.
Functional Improvement	Modification to a function, system or element specification to reduce risk.
Incident	Something unforeseen in the course of an action. In driving a vehicle in traffic, something which changes the foreseeable action (speed, direction) of the vehicle.

Term	Definition
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.
Minimal Risk Condition	A condition to which a user or an automated driving system bring a vehicle after performing the minimal risk manoeuvre in order to reduce the risk of a crash when a given trip cannot be completed.
Minimal Risk Manoeuvre	A procedure aimed at minimizing risks in traffic, which is automatically performed by the system, e.g. when the driver does not respond to a transition demand.
Misuse	Usage of the system by a human in a way not intended by the manufacturer of the system.
Object and Event Detect and Response	The subtasks of the dynamic driving task (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 fall-back).
Operational Design Domain	Specific conditions under which a given driving automation system or feature thereof is designed to function, including, but not limited to, driving modes.
Over The Air	Data transfer via a wireless method, such as a mobile network, as opposed to using a physical connection.
Passenger	A user in a vehicle who has no role in the operation of that vehicle.
Personal Data	Any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
Real-World Data	Data collected in a non-experimental, non-virtual situation.
Safety	The absence of unreasonable risk.
Scenario	Description of the temporal development between several scenes in a sequence of scenes.
Scene	Snapshot of the environment including the scenery, dynamic elements, and all actor and observer self-representations, as well as the relationships between those entities.
Security	The protection of system against intentional subversion or forced failure.
Sensor	A device that responds to a physical stimulus (as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse which can be interpreted as a measure by an instrument/observer.
Take Over Request	Notification by an ADS to a driver indicating that s/he should promptly perform the DDT fall-back.
Technical Maturity	Determining a technology’s readiness for operations across a spectrum of environments with a final objective of transitioning it to the user. One scale to describe to rate the maturity is the technology readiness level.

Term	Definition
Test Scenarios	The test setup in which scenarios are triggered in order to collect data specific to this scenario.
Threat	A potential cause of an unwanted incident, which may result in harm to a system, organization or individual.
Triggered Events	Specific conditions of a driving scenario that serve as an initiator for a subsequent system reaction possibly leading to a hazardous event.
Use Cases	A list of actions or event steps in which a system or its specific function is expected to interact with a user or another system to achieve a goal.
User	A general term referencing the human role in driving automation.
User acceptance	The assessment that a system meets the user's expectations. The focus being on the HMI and delivery of the feature, not the technical aspects behind the implementation. The customer should be satisfied with the system both during and after operation for it to pass this acceptance stage.
Vehicle-to-Everything	Technology that allows a vehicle to exchange additional information with infrastructure, other vehicles and other road users.
Verification & Validation	Verification is an evaluation of whether the "system" complies with certain requirements. This includes that it is determined if the "system" has the required functionalities and if these functionalities are working as intended, without errors, considering certain constraints. Validation is an evaluation of how appropriate the "system" is for the intended use. This includes requirements like user acceptance, appropriate workload, increased safety, etc.
Vulnerabilities	A weakness of an asset or mitigation that can be exploited by one or more threats.
Vulnerable Road Users	Non-motorised road users, such as pedestrians and cyclists as well as motor-cyclists and persons with disabilities or reduced mobility and orientation.

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", Disseration, 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.

Andreone, L. et al. (2020). "Pre-Tests Results", L3Pilot deliverable D6.3.

Andreone, L. et al. (2021). "Pilot Reporting Outcomes", L3Pilot deliverable D6.5.

ASAM OpenDrive (2020). (https://www.asam.net/standards/detail/opendrive/).

ASAM OpenScenario (2020). (https://www.asam.net/standards/detail/openscenario/).

ASAM XIL Standard (2020). (https://www.asam.net/standards/detail/xil/).

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., Drüke, 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.

BMVI (2019). "Verkehr in Zahlen 2019/2020", Bundesministerium für Verkehr und digitale Infrastruktur, 48th annual report.

Bonnefon, J.-F, Cerny, D., Danaher, J. et al. (2020). "Ethics of connected and automated vehicles report", Horizon 2020 Commission Expert Group to advise on specific ethical issues raised by driverless mobility (E03659), Publication Office of the European Union, Luxembourg.

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).

Botta, M., Cancelliere, 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.

BSI/PAS 1883 (2020) "Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification", British Standards Institution.

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.

Commission of the European Communities, "European Statement of Principles on the design of human-machine interface" (ESOP 2006).

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.

DESTATIS Justice (2020). "Justice - Civil law cases completed in local courts", Statistisches Bundesamt (Destatis). (https://www.destatis.de/EN/Themes/Government/Justice/_Graphic/_Interactive/civil-law-cases.html, Accessed: 24.10.2020).

DESTATIS (2015). "Verkehr – Verkehrsunfälle 2015", Statistisches Bundesamt (Destatis), Fachserie 8 Reihe 7, 2016.

DESTATIS (2016). "Verkehr – Verkehrsunfälle 2016", Statistisches Bundesamt (Destatis), Fachserie 8 Reihe 7, 2017.

DESTATIS (2017). "Verkehr – Verkehrsunfälle 2017", Statistisches Bundesamt (Destatis), Fachserie 8 Reihe 7, 2018.

DESTATIS (2018). "Verkehr – Verkehrsunfälle 2018", Statistisches Bundesamt (Destatis), Fachserie 8 Reihe 7, 2019.

DESTATIS (2019). "Verkehr – Verkehrsunfälle 2019", Statistisches Bundesamt (Destatis), Fachserie 8 Reihe 7, 2020.

Di 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.

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.

ENISA, “ENISA Good practices for Security of Smart Cars”, European Union Agency for Cybersecurity (ENISA 2019).

ERTRAC, “Connected Automated Driving Roadmap”, European Road Transport Research Advisory Council (ERTRAC CAD 2019).

Fahrenkrog, F. et al. (2019). “Draft and results from pilot application of draft CoP”, L3Pilot deliverable D2.2.

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.

GIDAS (2020) (www.gidas.org/en/).

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., Sauvaget, 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].

Innamaa, S., Silla, A., Aittoniemi, E. et al, Evaluation plan, L3Pilot deliverable D3.4.

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 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/CD 24089 (20XX). “Road vehicles — Software update engineering”, ISO standard ISO/CD 24089.

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

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

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

ISO/PRF TR 4804 (2020). “Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation”, ISO standard ISO/PRF TR 4804.

ISO/PWI 34505 (20XX) “Road vehicles — Evaluation of test scenarios for automated driving systems”, ISO Proposed Work Item.

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

ISO/WD 34501 (20XX) “Road vehicles — Terms and definitions of test scenarios for automated driving systems”, ISO Working Document.

ISO/WD 34502 (20XX) “Road vehicles — Engineering framework and process of scenario-based safety evaluation”, ISO Working Document.

ISO/WD 34503 (20XX). “Road vehicles — Taxonomy for operational design domain for automated driving systems”, ISO Working Document.

ISO/WD 34504 (20XX) “Road vehicles — Scenario attributes and categorization”, ISO Working Document.

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 (MILT) (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.

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.

Riedmaier et al. (2018). Validation of X-in-the-Loop Approaches for Virtual Homologation of Automated Driving Functions, 11th 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”. (https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/testing) [12.07.19].

SVA Simulation of Autonomous Vehicle Safety (2020). (https://www.irt-systemx.fr/en/projets/sva/).

Szymanski D., Scharrer M., Macher G., Armengaud E., Schmidt H. (2018) “Model-Based Functional Safety Engineering”. Comprehensive Energy Management - Safe Adaptation, Predictive Control and Thermal Management. Springer Briefs in Applied Sciences and Technology.

Bolovinou, A., Atmaca, U., Sheik, A. T., Ur-Rehman, O., Wallraf, G. and Amditis, A. (2019). "TARA+: Controllability-aware Threat Analysis and Risk Assessment for L3 Automated Driving Systems," IEEE Intelligent Vehicles Symposium (IV), Paris, France.

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.

TÜV Rheinland. “SET Level 4 to 5 - Simulation-based development and testing of Level 4 and 5 systems (2019)”. (http://www.tuvpt.de/index.php?id=setlevel4to5).

UN ECE (2020). “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System”, ECE/TRANS/WP.29/2020/32.

UN ECE (2020). “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system”, ECE/TRANS/WP.29/2020/79.

UN ECE (2020). “Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to software update and software updates management system”, ECE/TRANS/WP.29/2020/80.

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 UN ECE WP.29 GRVA”, Internal Document.

UN (2019). Framework document on automated/autonomous vehicles. United Nations World Forum for Harmonization of Vehicle Regulations (WP.29).

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

UTO-ISAC (2016). “Auto-ISAC Best Practices”, Report.

VUFO (2018). Die German In-Depth Accident Study (GIDAS) – Der Goldstandard? (https://www.gidas.org/en/gidas-publikationen/?action=getfile&t4m_id=503).

VV Methoden Project (VVM-Projekt). (https://www.vvm-projekt.de/en/).

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.