

CODE OF PRACTICE

for the
Development
of Automated
Driving
Functions

Relevant Phase(s):

Question x-y-z

Question

No

- Sub-Question 1
- Sub-Question 2
- Sub-Question 3

DF

CO

DS

VV

PS

Legal Disclaimer

The information in this publication 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.

This publication is based on the L3Pilot public deliverable D2.3 “Code of Practice for the Development of Automated Driving Functions”. The full deliverable is available online at www.L3Pilot.eu.



Authors

Yu Cao – Stellantis

Thibault Griffon – Stellantis

Felix Fahrenkrog – BMW Group

Moritz Schneider – BMW Group

Frederik Naujoks – BMW Group

Fabio Tango – Stellantis | Centro Ricerche Fiat

Stefan Wolter – Ford

Andreas Knapp – Mercedes-Benz

Yves Page – Renault Group

Jorge Lorente Mallada – Toyota Motor Europe

Giancarlo Caccia Dominiononi – Toyota Motor Europe

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 Automobile

Ulrich Eberle – Opel Automobile

Roland Schindhelm – BAST

Elisabeth Shi – BAST



Contents

About	6
An Achievement with History	7
Facts and Partners	9
Introduction	12
Overall Guidelines and Recommendations	22
Minimal Risk Manoeuvre	
Documentation	
Existing Standards	
Testing	
ODD Vehicle Level	42
Requirements	
Scenarios and Limits	
Performance Criteria and Customer Expectations	
Architecture	
ODD Traffic System Level and Behavioural Design	62
Automated Driving Risks and Coverage Interaction with Mixed Traffic	
V2X Interaction	
Traffic Simulation	
Ethical & Other Traffic-Related Aspects	
Safeguarding Automation	82
Functional Safety	
Cybersecurity	
Implementation of Updates	
Safety of the Intended Functionality	
Data Recording, Privacy and Protection	
Human-Vehicle Integration	126
Guidelines for HVI	
Mode Awareness, Trust & Misuse	
Driver Monitoring	
Controllability & Customer Clinics	
Driver Training & Variability of Users	
Perspectives	154
Annex	159
Literature and Relevant Topics in CoP-ADF	
Glossary	
List of Abbreviations and Acronyms	

1.0 About

The Code of Practice for the Development of Automated Driving Functions (CoP-ADF) is one of the major achievements of the EU-funded automotive research project L3Pilot running from 2017 to 2021. It provides comprehensive guidelines for supporting the design, development, verification and validation of automated driving technologies. This publication is an adapted version of the full public project deliverable, which is publicly accessible online.

A number of stakeholders in the automotive environment will make use of the CoP-ADF: project leaders and developers of Automated Driving Functions, stakeholders occupied with automated driving such as public authorities, regulation and type approval groups, academic organisations, insurance bodies and the general public.

The scope of the CoP-ADF is on SAE Level 3 and 4 functions in passenger cars for motorway and parking. However, extensions to other Operational Design Domains (ODDs) or automation levels are feasible as well. It consists of 155 main questions plus sub-questions assigned to one of five categories and one of 22 topics.

As a document in the public domain, CoP-ADF contributes to the consolidation of the development process towards a basis for the wide public acceptance of robust and safe ADF for Europe and beyond.



2.0 An Achievement with History

Automated driving technology has matured over the past ten years to a state in which road tests are required to answer key questions before the systems are introduced to the market. In the European research project L3Pilot, we test the viability of automated driving as a safe and efficient means of transportation. More than 750 users have tested 70 vehicles across Europe in seven countries. But how do we achieve coherent and harmonised guidelines for the development of these functions?

One of the major outcomes of the L3Pilot project is this Code of Practice for the Development of Automated Driving Functions. The activities started long before L3Pilot with the rise of Advanced Driver Assistance Systems (ADAS) at the end of the last century. It then became clear that these functions had a high potential to improve traffic safety; however, technical limits as well as liability issues delayed their market introduction. Three RESPONSE projects running from 1998 to 2008 ultimately produced the final Code of Practice for the Design and Evaluation of ADAS (CoP-ADAS), providing the vehicle industry with tools and a common understanding to overcome and manage the issues regarding safety and liability for ADAS.

Since then, research and development has progressed and led to automated driving technologies. The CoP activities continued in the European research project Adaptive running from 2014 to 2017 which, amongst other results, proposed the foundations for the development of this CoP-ADF in L3Pilot. This Code of Practice is a major and joint effort from a large pan-European partner network building upon long years of manifold experiences and excellent expertise in the field of automated driving.

We hope that the guidelines we provide will support your efforts to develop safe and reliable Automated Driving Functions.

Yours sincerely,



Aria Etemad

Volkswagen AG, L3Pilot Coordinator



3.0 Facts and Partners

Research budget of €68 million, €36 million of which has been co-funded by the European Commission under Horizon 2020

Coordinated by Aria Etemad, Volkswagen AG

Contact aria.etemad@volkswagen.de

Duration of more than 4 years; September 1, 2017 – October 31, 2021

Consortium includes 34 partners from 12 countries: Austria, Belgium, France, Finland, Germany, Greece, Italy, The Netherlands, Norway, Sweden, Switzerland, UK; including 13 OEMs, 3 suppliers, 12 research institutes and universities, 2 insurers, 1 authority, 1 user group and 2 SMEs.



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



Supported by the European Council
for Automotive R&D



4.0

Introduction

4.0 Introduction

The CoP-ADF consists of 155 main questions plus sub-questions assigned to one of five categories and one of 22 topics:

- Overall Guidelines and Recommendations: Minimal Risk Manoeuvre / Documentation / Existing Standards / Testing including Simulation
- ODD Vehicle Level; description of the function and scenarios at vehicle level: Requirements / Scenarios and Limitations / Performance Criteria and Customer Expectations / Architecture
- ODD Traffic System and Behavioural Design; description of the function at the level of the overall environment: Automated Driving Risks and Coverage of Interaction with Mixed Traffic / V2X Interaction / Traffic Simulation / Ethics and Other Traffic-Related Aspects
- Safeguarding Automation; how to ensure the safe operation of the function: Functional Safety / Cybersecurity / Implementation of Updates / Safety of the Intended Functionality / Data Recording, Privacy and Protection
- Human-Vehicle Integration; how to take into account the behaviour of other road users: Guidelines for HVI / Mode Awareness, Trust & Misuse / Driver Monitoring / Controllability & Customer Clinics / Driver Training & Variability of Users

These 22 topics are common challenges that could lead to frequent complications during the ADF development process. The questions shall be checked and evaluated by the user during the development process of ADF.

The CoP-ADF does not provide technical solutions, but supports 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 CoP-ADF user aware of certain aspects and to ensure that reasons for decisions are taken and documented.

The CoP-ADF focuses on L3 and L4 ADF in passenger cars, for which steering

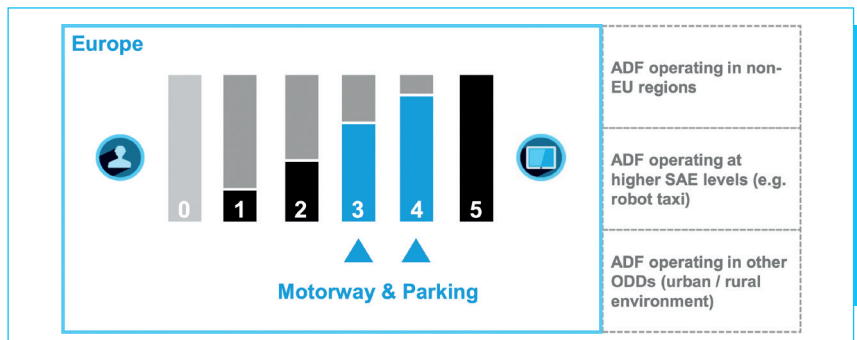
wheels and pedals are normally available in the vehicle all the time. In addition, the driver shall be available:

- 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.

L0, L1 and L2 functions are not the focus of this document; they are covered by the CoP-ADAS (Knapp et al. 2009). Regarding the covered region and ODD of the function, it must be recognised that the CoP-ADF is written from a European standpoint and focuses mainly on motorway and parking ADF. However, the mentioned aspects will apply to a large extent 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 of L4 or L5 functions or driverless operation, e.g. robot taxi operating in a geo-fenced ODD;
- ADF with other ODD, such as urban or rural roads.

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



Application of the Code of Practice for the Development of Automated Driving Functions

The CoP-ADF is intended to support developers of ADF by providing several questions that have been defined based on the experience gained thus far in the development process. 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 among questions in different topics, which approach issues from different angles. 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 might also not be relevant for certain ADFs. Thus, the purpose of the question is not necessarily to lead to a specific answer, but to initiate the developers' reflection about an issue and to report whether and how a certain topic has been addressed during development.

Furthermore, the questions make it possible to document the decisions and approaches taken in the development process. In the event that a question has not been addressed in the development of an ADF, it is strongly recommended that the reason for this decision be documented. In this way the CoP-ADF should lead to a more comprehensive view of the development of ADF. L3Pilot does not prescribe 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 approach taken needs to be decided by each company individually.

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 utilised to structure CoP-ADF.

Development Phases in CoP-ADF

In the development of a technology, different aspects become relevant at different stages. With this in mind, 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. For the CoP-ADF, an additional phase has been added that also considers the time after the start of production phase. Although not traditionally 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 required by ISO 26262 (ISO 26262-2:2018 and ISO 26262-7:2018).



*Development phases applied
in the CoP-ADF*



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.

To achieve functional safety, the ISO 26262 series of standards:

- a) provides a reference for the automotive safety lifecycle and supports the tailoring of the activities to be performed during the lifecycle phases, i.e. development, production, operation, service and decommissioning;
- b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASILs)];
- c) uses ASILs to specify which of the requirements of ISO 26262 are applicable to avoid unreasonable residual risk;
- d) provides requirements for functional safety management, design, implementation, verification, validation and confirmation measures; and
- e) provides requirements for relations between customers and suppliers.

The ISO 26262 series of standards is concerned with the functional safety of E/E systems, which is achieved through measures including safety mechanisms. It also provides a framework within which safety-related systems based on other technologies (e.g. mechanical, hydraulic and pneumatic) can be considered.

The achievement of functional safety is influenced by the development process (including such activities as requirements specification, design, implementation, integration, verification, validation and configuration), the production and service processes and the management processes. Safety is intertwined with common function-oriented and quality-oriented activities and work products. The ISO 26262 series of standards addresses the safety-related aspects of these activities and work products.

From: International Standard 26262-1 Road vehicles – Functional safety – Part 1, Vocabulary


Categories and Topics in the CoP-ADF

The categories were derived from a survey among L3Pilot partners. Next to the development phases, these 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. The following table provides an overview of the different topics and the related categories covered by the CoP-ADF.

CATEGORY	TOPICS
Overall Guidelines and Recommendations	<ul style="list-style-type: none"> Minimal Risk Manoeuvre (4.1.1) Documentation (4.1.2) Existing Standards (4.1.3) Testing (incl. Simulation) (4.1.4)
ODD Vehicle Level (description of the function and scenarios at vehicle level)	<ul style="list-style-type: none"> 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 (description of the function at the level of the overall environment)	<ul style="list-style-type: none"> 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 (how to ensure the safe operation of the function)	<ul style="list-style-type: none"> Functional Safety (4.4.1) Cybersecurity (4.4.2) Implementation of Updates (4.4.3) Safety of the Intended Functionality (4.4.4) Data Recording, Privacy and Protection (4.4.5)
Human-Vehicle Integration (the factors related to the interaction between the vehicle and the user)	<ul style="list-style-type: none"> 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)

Overview of the CoP-ADF categories and the corresponding topics

Each **TOPIC** includes **several questions** that should be considered during the development of automated driving functions.



The questions are presented in the form of question cards.

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 tips regarding relevant literature and links to other topics.

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

Relevant Phase(s):	DF	CO	DS	VV	PS
Question x-y-z					
Main question Yes / No	<ul style="list-style-type: none">• 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 number, "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. 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.

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, and 2) they should support readers in answering the main question. Additional explanations and referenced sources are also available for each question. 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 Guidelines and Recommendations

4.1 Overall Guidelines and Recommendations

The topics of the overall category are the Minimal Risk Manoeuvre, documentation and compliance with existing standards.

4.1.1 Minimal Risk Manoeuvre

The Minimal Risk Manoeuvre (MRM) is the manoeuvre which is applied in the event 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 minimise risks in traffic. The specification of the MRM depends on the kind of ADF and the L3 function definition.

Relevant Phase(s):	DF
Question 0-1-1	
Is there an appropriate mechanism for a fall-back solution for the ADF planned? Yes / No	<ul style="list-style-type: none">• 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 are possible, 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).

For an L3 function that 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 for the event that the driver does not take over. L4 ADF needs such a strategy by definition. The TOR must be carefully considered and designed, which could help to reduce the likelihood that the MRM would need to be activated. This aspect is also of relevance when considering the safety of the intended functionality (SOTIF) (see topic 4.4.4).

Relevant Phase(s):	DF	CO
Question 0-1-2		
Is an adequate and validated concept for MRM planned? Yes / No	<ul style="list-style-type: none"> Is a concept for the MRM in the ADF foreseen (e.g. degradation, take-over)? Is the concept defined for different driving situations and conditions? Is the targeted / final MRC defined? Is / Are the condition(s) clearly defined under which the MRM shall / must be activated and ended? <p>More questions are provided in the deliverable.</p>	

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 conditions. The concept should define under which conditions 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.

Relevant Phase(s):	DF	CO	DS
Question 0-1-3			
Is / Are the sensor(s) and the function setup appropriate to perform the MRM in different conditions? Yes / No	<ul style="list-style-type: none"> 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 to execute the MRM. The MRM strategy shall reduce to an absolute minimum any situations in which a gap between available and required information occurs (e.g. redundancy could be an adequate measure).

Relevant Phase(s):	DS	VV
Question 0-1-4		
<p>Are appropriate MRMs implemented to cover all the various scenarios and conditions required?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are different characteristics of MRM considered for different driving scenarios? • Is an adequate and appropriate interaction with the driver (and with other road users) ensured by the MRM? • 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. When defining the test cases, it must be ensured that they cover the entire operation of the MRM, including different traffic and environmental conditions.

Question 0-1-5

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 at the end?

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 for use in, for instance, the homologation process, internal approval process or evidence in the event of court disputes. In some cases, there are explicit requirements for documentation, e.g. as given in the “UNECE ALKS Regulation” (UNECE ALKS 2020). However, this is not always the case. The main purpose of the documentation is to enable a later analysis of the ADF’s capabilities and performance, as well as decisions made during development.

The intention of the regulation is to establish uniform provisions concerning the approval of vehicles with regard to Automated Lane Keeping Systems (ALKS). ALKS controls the lateral and longitudinal movement of the vehicle for extended periods without further driver command. ALKS is a system whereby the activated system is in primary control of the vehicle. This Regulation is the first regulatory step for an automated driving system (as defined in ECE/TRANS/WP.29/1140) in traffic and it therefore provides innovative provisions aimed at addressing the complexity related to the evaluation of the system safety. It contains administrative provisions suitable for type approval, technical requirements, audit and reporting provisions and testing provisions. ALKS can be activated under certain conditions on roads where pedestrians and cyclists are prohibited and which, by design, are equipped with a physical separation that divides the traffic moving in opposite directions and prevents traffic from cutting across the path of the vehicle.

In a first step, the original text of this Regulation limits the operational speed to 60 km/h maximum and applies to passenger cars (M1 vehicles). This Regulation includes general requirements regarding system safety and failsafe response. When the ALKS is activated, it shall perform the driving task instead of the driver, i.e. managing all situations including failures, and shall not endanger the safety of the vehicle occupants or any other road users. There is, however, always the possibility for the driver to override the system at any time.

The Regulation also lays down requirements for how the driving task shall be safely handed over from the ALKS to the driver, including the capability for the system to come to a stop in the event that the driver does not reply appropriately.

Finally, the Regulation includes requirements for the Human-Machine Interface (HMI) to prevent misunderstanding or misuse by the driver. The Regulation requires, for instance, that on-board displays used by the driver for activities other than driving when the ALKS is activated, shall be automatically suspended as soon as the system issues a transition demand.

UNECE ALKS Regulation. Regulation Addendum 156 to UN Regulation No. 157 (March 2021)

Relevant Phase(s):

DF

CO

DS

Question 0-2-1

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

Other aspects might be defined by company internal rules, which follow for instance the ISO 9001 (ISO 9001 2015). If uncertain as to whether information for another purpose needs to be documented, please consult the responsible individuals in the company.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 0-2-2					
<p>Is a documentation and reporting process in place with regard to assessing, testing and validating the ADF capabilities as well as design decisions?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Is a process established to document the performed tests and pass / fail compliance? • 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? 				

In addition to the test activities, the documentation shall cover updates to the test plan, and for comprehensibility, it is also recommended to document the reasons for these changes. If documentation of test activities needs to be shared with external stakeholders, it shall be checked whether the documentation format complies with their requirements.

Relevant Phase(s):	CO	DS	VV	PS
Question 0-2-3				
<p>Is a reporting process established to feedback the knowledge / lessons learnt during testing and development?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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? • 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 tests 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.

4.1.3 Existing Standards

A general requirement of technology development is – in particular for safety-related aspects – that the state-of-the-art is followed. Hence, existing standards and best practices must be adhered to in the development.

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

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

4.1.4 Testing

At different stages of the development process the ADF needs to be assessed with regard to technical capabilities, verified with respect to compliance with the function requirements (see topic 4.2.1) and validated regarding its design (see topic Architecture, 4.2.4).

All these steps require testing by means of one or more test tools. Typical testing tools are: X-in-Loop Tests (Hardware-in-the-Loop, Model-in-the-Loop, Software-in-the-Loop, computer simulation, etc.), driving simulator tests, in controlled environments such as test tracks (tests with demonstrator vehicles, Vehicle-in-the-Loop tests) and field tests. The objective of this topic is to ensure that the planning and execution of the testing is done in a proper and safe manner.

Relevant Phase(s):

DF

Question 0-4-1a

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 that 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)?
 - Is a test concept defined that validates that the ADF fulfils its intended purpose?
 - Is a test concept defined that validates a positive balance of risks?
- More questions are provided in the deliverable.

Relevant Phase(s):

DF

Question 0-4-1b

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 the 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 required 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 that 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 development and before market introduction to ensure a sufficiently safe 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 to reduce the potential risk for all involved persons to the technical minimum. The test concept needs to include and detail safety measures for the tests.

The test concept shall define the tests that are required to verify that the function meets its internal and external requirements (e.g. homologation and certification). 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 as in e.g. a lane change. In the validation phase, it must be assessed whether the ADF fulfils its purpose and meets external expectations. The external expectations cover the customer's expectations as well as societal expectations.

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

Relevant Phase(s):

CO

Question 0-4-2a

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)?
 - Is defined, how many test repetitions / test persons / mileage driven / time driven is / are required?
 - Are guidelines for the conducting of tests available?
 - Is the criticality of the test (potential safety risk resulting from the test) evaluated beforehand?
- More questions are provided in the deliverable.

Relevant Phase(s):

CO

Question 0-4-2b

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 of whether a certain test has been specified in a proper manner. For this purpose, the specification shall include information about the following items: test parameter, test amount (e.g. number of repetitions, number of test persons, driven mileage, driven time), success criteria, guidelines for the test execution, data and information to be documented (see also topic 4.1.2), reference data, privacy aspects to be considered, interaction with other participants and training protocols.

Relevant Phase(s):	CO
Question 0-4-3	
<p>Is the test space defined according to the function design and the intended ODD? (Test planning)</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are the relevant driving scenarios defined to cover the entire ODD? • Are relevant critical scenarios taken into account? • Is a process established that ensures that the appropriate relevant scenarios are selected? • Are all (relevant) requirements of the ADF tested? <p>More questions are provided in the deliverable.</p>

The tests must be in line with the driving scenarios that the ADF will encounter while operating in real traffic. 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 that contains several real-world driving scenarios, and that is manufacturer independent. It must also be noted that such a database must be available and could miss some rare event that is of importance for a certain ADF. In the latter case the “injection” of expert defined test cases could be an approach to fill these gaps in the database.

The PEGASUS project has addressed the following problem: before prototypes for highly automated driving can be turned into series vehicles, it must be demonstrated that these vehicles are sufficiently safe. For this purpose, the vehicles with their automated driving functions must be tested in a variety of traffic situations. In real traffic, these tests would require an immense amount of time and money, which would correspond to a number of well over 100 million test kilometres. In addition, every change to an automated driving function would require a new verification of its safety. The project defined a uniform procedure for testing and trialling automated vehicle systems in simulation, on test benches and under real conditions. A continuous and flexible tool chain was developed to secure automated driving and the tests were integrated into the development processes at an early stage. In addition, a cross-manufacturer method for safeguarding highly automated driving functions was created. In the PEGASUS project a database was developed that can be used to make relevant traffic scenarios usable for safety assurance purposes. For this purpose, data from various sources (field tests, accident databases, simulation, UAV, etc.) were first harmonised and then further processed using a uniform process chain. In this way, test specifications for the release of highly automated driving functions can be derived based on scenarios contained in the data sources. The overall aim of the database is to collect relevant scenarios that would otherwise be created when testing a function with a high number of test kilometres, in order to be able to prove functional safety much more efficiently. With the help of the database, these scenarios do not have to be generated anew each time during the validation process, but can be analysed directly in suitable test environments with regard to the effect of the highly automated driving function.

www.pegasusprojekt.de

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.

Relevant Phase(s):	VV
Question 0-4-4	
Is the test plan implemented and followed correctly? (Test execution) Yes / No	<ul style="list-style-type: none"> • 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 of whether the test plan is correctly implemented and followed becomes relevant. While testing, different limitations or constraints can occur that lead to intended or unintended deviations from the test plan. Intended deviation might be necessary to overcome detected issues. 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.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 0-4-5					
Is the execution of the planned tests with the ADF feasible? (Test planning) Yes / No	<ul style="list-style-type: none"> • Are the interfaces for the test tools properly defined and implemented? • Are all required licences (incl. testing and driving licences) 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 applied test tools verified and validated before they are used? <p>More questions are provided in the deliverable.</p>				

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 safety & security aspects.

Regarding each 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 be validated and verified before the test. The use of test tools often comes with additional requirements that 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 may need to be defined or certain licences (incl. testing and driving licences) for the testing may be required. It must be assessed whether the function is mature enough to be tested in the target environment. Safety and security must be ensured while performing the tests. Security aspects need to be thought through in a wider sense, since new cyber security risks have arisen, especially now that communications such as V2X and remote vehicle control are being developed.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 0-4-6					
<p>Is the testing activity safe? (Test planning) Yes / No</p>	<ul style="list-style-type: none"> • 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 on other traffic participants considered and safety measures defined? • Is it been defined how test engineers should respond in the event of a failure during the testing process? <p>More questions are provided in the deliverable.</p>				

A key aspect for the testing of ADF is to try to prevent any risk of material damage or personal harm. Individuals involved in testing should take all necessary precautions to ensure that the testing process is completed as safely as possible. In this context, the use of tools such as Hazard Analysis and Risk Assessment (HARA), Failure Mode and Effect Analysis (FMEA) and checklists can support the identification and addressing of potential risks. This risk assessment must also include individuals that are not directly involved in the testing (e.g. other users of the test track). Before the testing it must be ensured that the planned safety measures are available and operating successfully. The test engineers should receive the necessary training that informs them of the appropriate action to take in the event of an issue during testing. Company internal rules as well as governmental rules need to be obeyed.

Relevant Phase(s):	CO	DS	VV	PS
Question 0-4-7				
<p>Are the national testing guidelines / regulations being followed? (Test planning) Yes / No</p>				

During the testing national testing guidelines and regulations must be followed. Examples of testing guidelines include 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 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.

Relevant Phase(s):	DF	CO	DS	VV
--------------------	----	----	----	----

Question 0-4-8

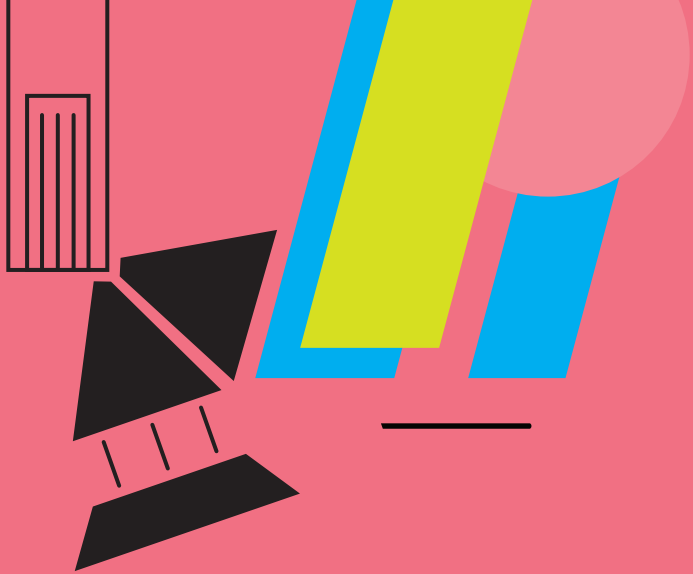
<p>Are X-in-the-loop systems (XIL) tests such as simulation part of the test concept and testing? (Test planning / execution) Yes / No</p>	<ul style="list-style-type: none"> Are SIL, MIL and / or HIL considered in the test plan? Is it analysed, which tests can be performed as open- and as close-loop simulation tests? Are the XIL test tools been validated for their intended purpose? <p>More questions are provided in the deliverable.</p>
---	---

The application of simulation tools comes with some associated challenges. The challenge of V&V has already been addressed by question 0-4-5. However, there are further aspects that need to be considered for virtual testing:

- It must be decided how the ADF is represented in the simulation tool. The three basics options are software-in-the-loop (SIL), model-in-the-loop (MIL) or hardware-in-the-loop (HIL).
- 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 closed-loop testing.
- When applying XIL testing tools, the test cases and interfaces need to be described properly. In recent times, different projects have sought to standardise 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). Standardised test case descriptions and interfaces make particular sense if exchangeability of tests or models with other organisations is of importance.







4.2

ODD Vehicle Level

4.2 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 the vehicle level, that is, all the functional aspects of a vehicle are taken into consideration. In particular, the following topics illustrate requirements, scenarios and limits, performance criteria and customer expectations as well as architecture.

4.2.1 Requirements

Right from the definition phase, it is imperative that all requirements are identified and clearly defined. This is essential to provide the basis for good design, development and testing. A lack of requirements impedes traceability and the 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 as the maturity level of the technology increases.

Relevant Phase(s):	DF
Question 1-1-1	
Are the different attributes of the requirements considered? (e.g. specific, measurable, attainable, relevant, testable) Yes / No	<ul style="list-style-type: none">• Are target values defined for all the requirements?• Is the controllability considered?• Are the feasibility and the usage conditions 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 among 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, Measurable, Attainable, Relevant, Testable.

Relevant Phase(s):	DF
Question 1-1-2	
<p>Is traceability ensured between requirements and other streams, such as design, development and testing? Yes / No</p>	<ul style="list-style-type: none"> • Is the requirement workflow defined? • Are requirement tools used (e.g. DOORS, Polarion, Visure)? • Is there a process to manage changing requirements?

In principle, requirement traceability is defined as the ability to describe and follow the life of a requirement through the whole system life cycle. To achieve this the adoption of a tool such as DOORS (Doors, 2020) can spark such discipline. Many times, a requirement traceability matrix (RTM) does not exist although there is a need to ensure requirements completion and to understand change impact. During development new requirements are added while others change. As the system requirements evolve, the quality of tracing has to be constantly maintained to avoid inaccurate and untrusted links across the streams.

Relevant Phase(s):	DF
Question 1-1-3	
<p>Are the requirements classified as functional and non-functional? Yes / No</p>	

Functional requirements include descriptions of the ADF and 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. 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 and detail constraints, targets or control mechanisms related with the qualities of the ADF and its success. These can be conceptualised mainly with performance requirements, design constraints and quality attributes. 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.

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

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.

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

To ensure that the complete system is built according to the established 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.

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

Fundamental to ADF is the need for safety even if the 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 has to be defined by a safety analysis. 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

Relevant Phase(s):	DF
---------------------------	-----------

Question 1-1-7	
<p>Do the function limitations cover the identified / considered risks?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are the risks analysed to understand which are acceptable and which are unacceptable? • Is it ensured that the ADF can reach an MRC?

ADFs are limited in the way their algorithms react to 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 the system encounters an exception or other situation for which it was not designed. Please consider in this context also the SOTIF (see topic 4.4.4).

Relevant Phase(s):	DF
---------------------------	-----------

Question 1-1-8	
<p>Is / Are the intended level(s) of driving automation defined?</p> <p>Yes / No</p>	

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. Higher levels of automation do not rely on the human driver as a fall-back solution, but they are also limited by ODD. 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.



SAE J3016™ LEVELS OF DRIVING AUTOMATION™

Learn more here: [sae.org/standards/content/j3016_202104](https://www.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	

Copyright © 2021 SAE International.

	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	<ul style="list-style-type: none"> • automatic emergency braking • blind spot warning • lane departure warning 	<ul style="list-style-type: none"> • lane centering OR • adaptive cruise control 	<ul style="list-style-type: none"> • lane centering AND • adaptive cruise control at the same time 	<ul style="list-style-type: none"> • traffic jam chauffeur 	<ul style="list-style-type: none"> • local driverless taxi • pedals/steering wheel may or may not be installed 	<ul style="list-style-type: none"> • same as level 4, but feature can drive everywhere in all conditions

SAE J3016. Copyright 2021 SAE International

SAE J3016

Relevant Phase(s):	DF
Question 1-1-9	
<p>Is a checklist considering ODD requirements for the ADF defined?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are the ODD requirements for the specific ADF defined with respect to a standardised 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.

Relevant Phase(s):

DF

Question 1-1-10

Is a formal verification strategy for the chosen ODD defined?

Yes / No

- Is the appropriate 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 there a requirements concept for test cases?

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 and 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.

Relevant Phase(s):

DF

Question 1-1-11

Do the requirements analysed take 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?
- Are 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. 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 guidelines before system deployment.

Relevant Phase(s):	VV
Question 1-1-12	
<p>Is the actual technical performance verified to be in line with the defined ODD?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> Is the actual performance rated against the ODD requirements (e.g. non-compliant vs. compliant)?

Requirements are not complete without an understanding of how they will be tested. For the same reason they must also be verified and validated (V&V) for the ADF to gain trust. The minimum performance criteria define how the ADF is expected to perform and indicate 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 exceptions beyond the defined ODD.

Relevant Phase(s):	VV	PS
Question 1-1-13		
<p>Is a general strategy available to monitor released vehicles in the field?</p> <p>Yes / No</p>		

To assess an ADF, it is necessary to drive it in real traffic and observe its performance. Moreover, if an ADF system is expected to detect whether it has left the ODD, then it must be able to monitor the ODD at runtime and it must be able to detect events nearby, 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.

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

An ADF is not enabled by one single technology or component, but rather by a combination of technologies. Numerous lessons can 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 the 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 the 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, that were not considered during development.

Relevant Phase(s):	CO	DS
Question 1-2-1		
Are the function limitations known? Yes / No	<ul style="list-style-type: none"> • 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 road-way characteristics (SAE 2018). In addition, all object classes that 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 daytime. The ODD might, however, change during development. Therefore, a constant review of the function limits in relation to the ODD is necessary.

Relevant Phase(s):	DF	CO
Question 1-2-2		
Is the function operating within the ODD limitations? Yes / No	<ul style="list-style-type: none"> • 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 as well as recognising the ODD boundaries before leaving them. To ensure 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).

Relevant Phase(s):	CO
Question 1-2-3	
<p>Is a scenario-based approach utilised that sufficiently covers the ADF's ODD?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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?

4.2.3 Performance Criteria and Customer Expectations

This topic covers the performance criteria for the ADF as well as the customer expectations of the ADF. The link between the two aspects is necessary, since the customer would need to be supported in order to have an understanding about the ADF's performance and her / his role and responsibilities during automated driving (ITF 2018).

Relevant Phase(s):	DF	DS
Question 1-3-1		
<p>Is a concept defined to identify user requirements?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are customer abilities and limitations considered? • Are customer preferences and expectations of the ADF that is being designed considered? • Is customer feedback from 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 abilities and limitations shall be identified, considering different learning curves. Finally, the consideration of customer feedback refers to the information that can be obtained after deployment and that can be fed into the next development or ADF update.

Relevant Phase(s):	DF	DS
Question 1-3-2		
<p>Are realistic and objective performance criteria considered?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are means established to ensure that criteria are realistic (e.g. usage of customer clinics)? 	

On top of customer expectations, it is important to address aspects such as safety, comfort and drivability. This is something that 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.

Relevant Phase(s):	DS
Question 1-3-3	
<p>Are cooperative systems between ADF and the driver considered? (The driver may be inside or outside the vehicle.)</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 that have been set?

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 the control strategy or in the cooperation balance (Ab-
bink 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.

Relevant Phase(s):	VV
Question 1-3-4	
Is a method implemented to validate the target performance and the customer requirements? Yes / No	<ul style="list-style-type: none"> • 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. This V&V shall include not only the performance criteria and customer requirements but also the identified boundaries that affect cooperative control. The applied method shall include different test tools (see topic 4.1.4).

Relevant Phase(s):	VV
Question 1-3-5	
Is a process established to understand how customer expectations can be satisfied? Yes / No	<ul style="list-style-type: none"> • 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 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).

4.2.4 Architecture

An architecture framework for an ADF is made up of several standardised viewpoints, among which are typically a functional, 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 the 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. 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 (see category 4.5).

Relevant Phase(s):	DF	CO
Question 1-4-1		
Is a rationale for the chosen physical architecture put in place? Yes / No	<ul style="list-style-type: none"> 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? 	

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.

Relevant Phase(s):	DF	CO
--------------------	----	----

Question 1-4-2

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 with regard to 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 can use, to respond to the event triggered by the object. 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.

Relevant Phase(s):	DF	CO
---------------------------	-----------	-----------

Question 1-4-3

<p>Is a verification / analysis completed to ensure that the selected architecture responds to any (relevant) object when the ADF is operating within the ODD limit¹? Yes / No</p>	
--	--

ODD and OEDR allow the derivation of logical scenarios. Logical scenarios, in combination with requirements, form the input for testing the architecture response. 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.

Relevant Phase(s):	CO
---------------------------	-----------

Question 1-4-4

<p>Does the chosen functional architecture cover the specified functionalities? Yes / No</p>	
---	--

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 needs 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. Therefore, it is important 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 the event that the ODD is exceeded (see topic 4.1.1).

¹ 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 begins. Operation during the Minimal Risk Manoeuvre shall also be covered in an appropriate way.

Relevant Phase(s):	CO
Question 1-4-5	
Are the architectural aspects between function and other elements outside vehicles considered? Yes / No	<ul style="list-style-type: none"> • Is the interface to back-end, cloud services and other vehicles considered? • Is security and integrity of the architectural interfaces considered?

It is necessary to ensure that the required interfaces of the function(s) to back-end solutions, cloud services and other vehicles are considered. This ensures function integrity in a specific context. An interface Control Document should be available. Additionally, relevant documentation for FuSa, cybersecurity and SOTIF can support safety and cybersecurity analyses.

Relevant Phase(s):	DF	CO
Question 1-4-6		
Are requirements for safety, security and maintainability considered for the selection of an appropriate architecture? Yes / No	<ul style="list-style-type: none"> • 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 such as 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 the 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. Good practice is therefore to check whether current architecture standards are available to provide guidelines for designing the ADF architecture. This document refers, for example, to the ISO/IEC/IEEE 42010:2011 standard and the references within.

Relevant Phase(s):	CO
Question 1-4-7	
<p>Is there an appropriate rationale for the allocation of logical and functional architectures to the physical architecture?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are sensing, perception, world modelling, 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 whether the selected ADF elements have been found capable of satisfying the defined functions.

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

If 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).

The evaluation considers two main aspects: tool usage and 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 tool usage. 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).





4.3

ODD Traffic System Level and Behavioural Design

4.3 ODD Traffic System Level and Behavioural Design

Aspects of ODD with a focus on the AV have been described in category 4.2. Nevertheless, the operation of the AV depends also on its surroundings. 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 systems, V2X interaction (interaction between automated driving cars and their environment), traffic simulations and ethical and other traffic-related aspects.

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 can mitigation strategies be developed.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 2-1-1					
<p>Are the risks of the ADF within its ODD considered? Yes / No</p>	<ul style="list-style-type: none"> 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? Does the HARA consider unspecified or unexpected events? Are the function limitations within the ODD considered? Is the recording of ADF accident data or disengagements utilised to help identify risks? Is there a mechanism for the publication or sharing of disengagements with a third party? 				

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 target specific risk types that could occur within the ODD. The obvious risk of the driver not regaining full situational awareness when a transfer of control has been completed is one that will require significant research & validation to ensure it is minimised. The ability of the ADF to respond appropriately in all kinds of mixed traffic scenarios is also a high risk that 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. The HARA should be maintained throughout the life of the ADF as new hazards are identified.

Relevant Phase(s):	DF	CO	DS	VV
Question 2-1-2				
<p>Are the ADF capabilities identified and verified in terms of OEDR? Yes / No</p>	<ul style="list-style-type: none"> Does the response of the ADF take into account road obstructions, lane allocation & re-routing, road etiquette for emergency vehicles and interpreting gestures of other road users? Is the negotiate 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? Does external information from other vehicles, infrastructure and / or back-end support the pre-emption of OEDR? 			

The number of different types of objects that 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. An incorrect classification may lead to an incorrect response by the ADF. It is also worth considering the input from other sources through connected vehicles and / or infrastructure. These may provide benefits to OEDR.

Relevant Phase(s):	DF	VV
Question 2-1-3		
<p>Is the ADF designed, verified and validated with regard to surrounding road users and infrastructure?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Does the ADF operate with a natural and predictable driving style? • Are the active safety capabilities of the vehicle being validated in normal driving scenarios as well as in corner cases²? • Is it identified whether the ADF can exchange info about ADF intentions with other equipped vehicles or road users? 	

Mixed traffic is the term used to describe traffic on the road that is made up of a miscellany of different objects such as vehicles, lorries, motorbikes, bicycles and pedestrians. 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 to other road users, there is the risk that misunderstandings occur or that other road users might take advantage of the ADF's behaviour.

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 following traffic. If the active safety is not sensitive enough, accidents might not be prevented. The active safety of the ADF must be finely balanced to reduce the risks in mixed traffic.

² Corner cases are scenarios that 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.

Relevant Phase(s):	CO	DS
Question 2-1-4		
<p>Are the risks to the surrounding traffic during transition of control identified and assessed?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 by 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? 	

The transfer of control is likely to be associated with risks for the ego vehicle and 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 to ensure that the driver has regained situational awareness. The HVI is a key component, in order to communicate whether the driver or the ADF is responsible for controlling the vehicle.

Relevant Phase(s):	DS
Question 2-1-5	
<p>Are the potential ADF failure modes due to interaction with mixed traffic identified within the ODD and have relevant failure mitigation strategies been implemented?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 be identified and mitigation strategies put in place. Whenever possible, fail operational strategies should be implemented in such a way that the ADF can remain in control of the driving task for at least a certain time without initiating an emergency handover. There may be several mitigation strategies to handle individual failure modes. These should be considered and prioritised depending on their effectiveness.

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 refers 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 addresses the V2X interactions that an AD vehicle may have to deal with. It is not in the scope of this section to provide 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.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 2-2-1					
<p>Are the V2X interactions that the AD vehicle may encounter identified?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> Are the high-level interfaces in the high-level architecture been planned considering the identified V2X interactions within its ODD? Is the necessary functionality from other users (e.g. infrastructure, other road users) defined that will 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 from the strategic level (e.g. route planning, interaction with infrastructure) via the tactical level (e.g. manoeuvre control) to the operational level (e.g. braking, accelerating).

Once the interactions have been identified, a high-level system architecture needs to be defined to determine how the ADF will be able to cope with them.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 2-2-2					
Is a plan defined to integrate and validate the V2X interactions within the sensor architecture? Yes / No	<ul style="list-style-type: none"> Does the plan also consider a back-up solution when a required infrastructure is no longer available? 				

This question addresses how the identified interactions will be integrated into the sensor architecture. It is expected that the plan considers how each sensor should deal with the different interactions, including a validation strategy by means of appropriate testing. Such a strategy shall also include 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 cybersecurity threats and consider alternative strategies in the event that the required infrastructure is not available.

In this context, refer also to Question 1-4-5 of topic 4.2.4 Architecture as well as 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.

Question 2-2-3**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 the event 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 topics addressed 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. Compliance of such a concept with the applicable regulations at both the international and national level should also be considered.

After identifying the V2X interactions and developing a plan for their 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 consider 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.

Relevant Phase(s):	VV
Question 2-2-4	
Is the validation strategy for V2X interactions being followed and implemented? Yes / No	<ul style="list-style-type: none"> • Are test reports being generated for the V2X interactions that were identified? • Are test reports being prepared for the failures identified in the concept?

4.3.3 Traffic Simulation

The traffic simulation is an important method of evaluating ADF in a virtual traffic environment when designing or validating ADF. It is necessary 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 of the traffic flow and the interaction effect between AVs and the traffic environment.

Relevant Phase(s):	DF	CO
Question 2-3-1		
Is the technological state-of-the-art of the traffic simulation addressed and researched? Yes / No	<ul style="list-style-type: none"> • Are the sensor suite and vehicle architecture documented? • Are the appropriate toolchains or models selected for satisfying the needs of the 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 traffic simulation being used, combined with ADF simulation and covering existing solutions including their strengths and weaknesses? • Are the hardware and software of the simulation well defined and documented? 	

The technological state-of-the-art for traffic simulations should be investigated during the definition phase. The preliminary research is deployed across 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 which could be applied in the traffic flow simulation and in 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 2021).
- studies of benchmark activities, which include gathering, analysing and applying information, measures or practices about the latest simulation technology 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.

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

The impact of the applied ADF on traffic flow simulation can be related to the safety aspect, the efficiency aspect and the interaction aspect. The impact on the safety aspect focuses 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 considers the interaction between the ego vehicle and infrastructure or other road users.

Relevant Phase(s):	DF
---------------------------	-----------

Question 2-3-3

<p>Are traffic flow simulations being used to evaluate ADF evolution by implementing different scenarios and traffic models?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 counter-measures 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 safe circulation of the ego vehicle, as well as other road users. All scenarios identified as potentially critical, such as hard deceleration or an accident, should be addressed and studied. Feedback from the simulations will allow the evolution of the ADF and could help ensure that it handles real world driving safely.

The critical scenarios mainly arise from malfunctions of AVs but also from unpredictable manoeuvres from other road users and the traffic flow. 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). Guidance on traffic disturbance critical scenarios for ADF up to 60 km/h is provided by the ALKS regulation.

Relevant Phase(s):

DF

Question 2-3-4

Is a strategy defined to validate / verify the traffic flow simulation?

Yes / No

- Are the different test scenarios defined?
- Have the main research questions been clarified for traffic flow simulation?
- Are the critical scenarios that 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?

During the design phase of the simulation approach, it is recommended to consider a strategy to validate / verify the traffic flow simulation to facilitate the 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 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 of what is preventable or unpreventable leaves room for discussion. For instance, the ALKS demands a performance from the ADF equal to that of a competent and careful human driver (UNECE ALKS 2020).

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 determine how close the simulation is to real-world behaviour (Ragan et al. 2015).

Relevant Phase(s):	CO	DS
Question 2-3-5		
<p>Does the simulation toolchain consider co-simulation approaches? Yes / No</p>	<ul style="list-style-type: none"> • 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 synchronised? • Can the applied simulations exchange data between them? 	

A simulation concept should consider the co-simulation approach, which may incorporate mixed elements such as traffic environment, traffic flow, vehicle architecture, sensor data and communication aspects. In order to guarantee the high quality of the global simulation concept, co-simulation should be synchronised within the same simulation environment. At the same time, data generated by different simulations also needs to be shared between simulations.

Relevant Phase(s):	CO
Question 2-3-6	
<p>Are the requirements for the level of fidelity of the SIL defined? Yes / No</p>	<ul style="list-style-type: none"> • Is there an appropriate fidelity for specific simulation components (including sensors components)? • Is there more hardware-based XIL, beyond SIL applied?

In a virtual environment, high fidelity is not always necessary or advantageous when conducting SIL tests in software or software interactions. The relevant fidelity for specific simulation components must be considered in order to maintain the effectiveness of the simulation as well as a relatively 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.

Question 2-3-7**Is there real driving data guiding the simulation approaches?**

Yes / No

- Is the behaviour of the traffic agents in line with real-world behaviour?
- Are the sensor models developed based on real driving data?
- Are variations of the parameters applied in this context, and covered reality?
- Are the applied simulations based on the Naturalistic Driving Study (NDS) database, accident database or records of real-world drives?

Simulation of the ADF leads to an enormous quantity of simulated kilometres. To ensure that these kilometres are worthwhile and useful, having realistic and varied 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). Simulations 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 considered, by adding simulated traffic agents (pedestrians, joggers, motorcycles, vehicles, animals, objects, etc.) with realistic behaviours.

However, when utilising real-world data, the aspects of traceability of the data source and the influence on the result of the simulation also need to be considered (Waymo 2018).

Relevant Phase(s):

CO

Question 2-3-8

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 the driver behaviour of skilled and attentive human drivers, even from different regions?
- Does the driver behaviour model cover the interaction of non-automated drivers with 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. This should be in line with real human drivers' behaviours. A driver behaviour model is typically applied in the simulation in order to simulate the surrounding traffic. Each traffic participant possesses its own adjustable driver behaviour model, which could vary according to the driving habits 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 appropriate driver behaviour model should be used.

Relevant Phase(s):

VV

Question 2-3-9

Are internal and external stakeholders involved in approving the simulation approach?

Yes / No

- Are internal processes of the company being 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 validation process of the simulation shall follow regulations and involve internal and external stakeholders. It is assumed that communication of the validation strategy through immersive simulation will improve public acceptance of the AV. Therefore, it is important that these communications are done carefully to produce a positive impression on 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.

Relevant Phase(s):	DF	CO	DS	VV
Question 2-4-1				
<p>Are all laws and regulations associated with the development, testing and sale of the ADF been considered?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> 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 being followed through the entire process? 			

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 a function is developed, in which countries test drives are conducted and in which countries drivers can use the ADF.

In addition to the laws related to ADF behaviour or testing activities, there are laws that are relevant to the development process itself. Here, for instance national data protection and antitrust laws must be considered and followed. For all the aspects related to data protection please also refer to the topic “Data Recording, Privacy and Protection” (topic 4.4.5).

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 2-4-2					
<p>Are research and development activities planned according to the applicable (national) ethical standards?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 paramount? 				

In addition to legislation, it is also essential to comply with ethical standards. One fundamental principle is to prevent causing physical or mental harm to people. This should be ensured, within the realms of technical possibility, throughout 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 to minimise any harm to individuals both inside and outside of the vehicle.

For the operation of the ADF, protection of human lives must be paramount. For example, the German Ethics 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 the “Safety First White Paper” (Wood et al. 2019), which for instance transferred these ethical standards into twelve principles for AD.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 2-4-3					
<p>Does the ADF achieve a positive risk balance compared to human driving (e.g. reported in accident statistics)?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 risks induced by the ADF minimised? <p>More questions are provided in the deliverable.</p>				

The Safety First for Automated Driving (SaFAD) white paper was published by 11 industrial companies – Aptiv, Audi, Baidu, BMW, Continental, Daimler, FCA US LLC, HERE, Infineon, Intel and Volkswagen – in 2019. The document aims at providing an industrial perspective on the safety of automated driving. It summarises widely known safety by design and verification and validation (V&V) methods of SAE L3 and L4 automated driving. The SaFAD outlines requirements for maximising the evidence of a positive risk balance of automated driving solutions compared to the average human driving performance. For this purpose, the SaFAD systematically breaks down safety principles into safety by design capabilities, elements and architectures and then summarises the V&V methods to demonstrate the positive risk balance. Through its comprehensive perspective the SaFAD provides guidance on methods and considerations in development and V&V. For this reason, the SaFAD was a major contributor in the development of the CoP-ADF.

The SaFAD does not aim to provide final statements. Instead, the intent of the SaFAD has been rather to contribute to the current activities working towards the industry-wide standardisation of automated driving.

The concepts drafted in the SaFAD White Paper were further elaborated in the ISO technical report TR 4804 “Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation”. Currently, a related ISO technical specification (ISO TS 5083) is under preparation.

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 Ethics Commission the 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 rely solely 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 has been reached.

Other methods (e.g. simulation-based prospective impact assessment, ISO 21934 2021 or L3Pilot deliverable D3.4) shall be applied instead. When applying a method, it must be ensured that it can provide valid results, although it is clear that any assessment before market introduction is a forecast with various uncertainties.





4.4



Safeguarding Automation

4.4 Safeguarding Automation

The category of Safeguarding Automation addresses cross-functional topics that need to be considered to develop an ADF so 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: functional safety, cybersecurity, implementation of updates, safety of the intended functionality as well as data recording, privacy and protection.

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 from 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 a few 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.

Relevant Phase(s):	DF
---------------------------	-----------

Question 3-1-1

<p>Is possible malfunctioning behaviour and the related hazardous events analysed?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> 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 clearly documented? <p>More questions are provided in the deliverable.</p>
---	---

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, such as an ADF that does not require a take-over-ready driver, need to be reflected in the analysis. On this basis, the risks are assessed.

Relevant Phase(s):	DF
---------------------------	-----------

Question 3-1-2

<p>Is there a process in place to derive safety requirements (including safety goals) to avoid unsafe functional behaviour?</p> <p>Yes / No</p>	
--	--

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. The definition of a safety concept according to ISO 26262 (ISO 26262 2018) includes: the required reaction to bring the vehicle to a safe state, the required time within which the transition needs to be achieved and the required involvement of persons (the driver or other traffic participants), information about the warning strategy and / or applied degradation concepts (see for instance 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.

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

Once a safety concept has been defined, a confirmation of the effectiveness of the measures is needed. In this sense effectiveness means that the risk of the original hazardous event is reduced, and no unacceptable new risks are introduced.

Relevant Phase(s):	DS
Question 3-1-4	
<p>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</p>	

Requirements for data collection may come 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 must 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 the Data Storage System for Automated Driving (DSSAD) as mandated by the UNECE ALKS Regulation, Event Data Recorder (EDR) data for post-crash evaluation and data for disengagement reports as required for AVs by the State of California (DCM 2019).

Each vehicle equipped with ALKS shall be fitted with a Data Storage System for Automated Driving (DSSAD) that meets the requirements specified below. This Regulation is without prejudice to national and regional laws governing access to data, privacy and data protection.

8.2. Recorded occurrences

8.2.1. Each vehicle equipped with a DSSAD shall at least record an entry for each of the following occurrences upon activation of the system:

- (a) Activation of the system
- (b) Deactivation of the system, due to:
 - (i) Use of dedicated means for the driver to deactivate the system;
 - (ii) Override on steering control;
 - (iii) Override by accelerator control while holding steering control;
 - (iv) Override by braking control while holding steering control.
- (c) Transition Demand by the system, due to:
 - (i) Planned event;
 - (ii) Unplanned event;
 - (iii) Driver unavailability (as per para. 6.1.3);
 - (iv) Driver not present or unbuckled (as per para. 6.1.2.);
 - (v) System failure;
 - (vi) System override by braking input;
 - (vii) System override by accelerator input.

- (d) Reduction or suppression of driver input;
- (e) Start of Emergency Manoeuvre;
- (f) End of Emergency Manoeuvre;
- (g) Event Data Recorder (EDR) trigger input;
- (h) Involved in a detected collision;
- (i) Minimum Risk Manoeuvre engagement by the system;
- (j) Severe ALKS failure;
- (k) Severe vehicle failure.

8.3. Data elements

8.3.1. For each event listed in paragraph 8.2., the DSSAD shall at least record the following data elements in a clearly identifiable way:

- (a) The occurrence flag, as listed in paragraph 8.2.;
- (b) Reason for the occurrence, as appropriate, and listed in paragraph 8.2.;
- (c) Date (Resolution: yyyy/mm/dd);
- (d) Timestamp:
 - (i) Resolution: hh/mm/ss timezone e.g. 12:59:59 UTC;
 - (ii) Accuracy: +/- 1.0 s.

8.3.2. For each event listed in paragraph 8.2., the R15XSWIN for ALKS, or the software versions relevant to ALKS, indicating the software that was present at the time when the event occurred, shall be clearly identifiable.

8.3.3. A single timestamp may be allowed for multiple elements recorded simultaneously within the timing resolution of the specific data elements. If more than one element is recorded with the same timestamp, the information from the individual elements shall indicate the chronological order.

8.4. Data availability

8.4.1. DSSAD data shall be available subject to requirements of national and regional law.

8.4.2. Once the storage limits of the DSSAD are achieved, existing data shall only be overwritten following a first in first out procedure with the principle of respecting the relevant requirements for data availability. Documented evidence regarding the storage capacity shall be provided by the vehicle manufacturer.

- 8.4.3. The data shall be retrievable even after an impact of a severity level set by UN Regulations Nos. 94, 95 or 137. If the main on-board vehicle power supply is not available, it shall still be possible to retrieve all data recorded on the DSSAD, as required by national and regional law.
- 8.4.4. Data stored in the DSSAD shall be easily readable in a standardised way via the use of an electronic communication interface, at least through the standard interface (OBD port).
- 8.4.5. Instructions from the manufacturer shall be provided on how to access the data.

8.5. Protection against manipulation.

- 8.5.1. It shall be ensured that there is adequate protection against manipulation (e.g. data erasure) of stored data such as anti-tampering design.
- 8.6. Availability of DSSAD operation
- 8.6.1. DSSAD shall be able to communicate with the system to inform that the DSSAD is operational.

On Data Storage System for Automated Driving (DSSAD), from: UNECE ALKS Regulation.

Article 6**Advanced vehicle systems for all motor vehicle categories**

1. Motor vehicles shall be equipped with the following advanced vehicle systems:

- (a) intelligent speed assistance;
- (b) alcohol interlock installation facilitation;
- (c) driver drowsiness and attention warning;
- (d) advanced driver distraction warning;
- (e) emergency stop signal;
- (f) reversing detection; and
- (g) event data recorder.

...

4. Event data recorders shall meet the following requirements in particular:

- (a) the data that they are capable of recording and storing with respect of the period shortly before, during and immediately after a collision shall include the vehicle's speed, braking, position and tilt of the vehicle on the road, the state and rate of activation of all its safety systems, 112-based eCall in-vehicle system, brake activation and relevant input parameters of the on-board active safety and accident avoidance systems, with high level of accuracy and ensured survivability of data;
- (b) they cannot be deactivated;
- (c) the way in which they are capable of recording and storing data shall be such that:
 - (i) they operate on a closed-loop system;
 - (ii) the data that they collect is anonymised and protected against manipulation and misuse; and
 - (iii) the data that they collect enables precise vehicle type, variant and version, and in particular the active safety and accident avoidance systems fitted to the vehicle, to be identified; and

(d) the data that they are capable of recording can be made available to national authorities, on the basis of Union or national law, only for the purpose of accident research and analysis, including for the purposes of type approval of systems and components and in compliance with Regulation (EU) 2016/679, over a standardised interface.

5. An event data recorder shall not be capable of recording and storing the last four digits of the vehicle indicator section of the vehicle identification number or any other information which could allow the individual vehicle itself, its owner or holder, to be identified.

From: Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019

Relevant Phase(s):	DS
Question 3-1-5	
<p>Are the included safety mechanisms based on accompanying safety analysis? Yes / No</p>	<ul style="list-style-type: none"> • 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? • Do child-requirements cover the higher-level requirements (correctness and completeness)?

A clear structure of the requirements for an ADF and a systematic approach to eliciting requirements are key to establishing 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 defining requirements.

Relevant Phase(s):

DS

Question 3-1-6

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 of the current operating mode or the driving scenario of the vehicle. At each possible operating mode an appropriate safety mechanism must keep the vehicle in a safe state in the event of a failure. To achieve this there are several options:

- Switch off the function and inform the driver
- Provide a backup with full functionality for a limited amount of time
- Switch to a degraded mode

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

Relevant Phase(s):

VV

Question 3-1-7

Is a verification and validation process defined, that covers 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, needs 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.

Relevant Phase(s):	VV
Question 3-1-8	
<p>Are risks to equipment and involved persons and equipment resulting from safety V&V activities assessed?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • If V&V is carried out on public roads, are potential effects on 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 simulations or similar), it needs to be considered that the tests can be either passed or failed. Note that ISO 26262 is applied to achieve safe products and does not have a focus on safe development. Moreover, 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 if the test were to fail (see section 4.1.4).

Relevant Phase(s):	VV
Question 3-1-9	
<p>Do the test cases for the safety requirements cover the entire ODD?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Do test cases cover both ODD and edge case scenarios?

Test cases must 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 as to 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 that considers both ODD and edge case scenarios. One approach for testing safety requirements is for faults to be injected, in order to stimulate the safety mechanisms. As described above, if these mechanisms depend on the operating state, then all these states need to be tested.

Relevant Phase(s):	VV
Question 3-1-10	
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 must be included in the testing to sufficiently cover the safety requirements.

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

When all safety requirements have been verified and successfully implemented there is one final step: it needs to be checked whether the implemented safety concept with all its safety mechanisms is appropriate and keeps the vehicle safe in the event of a fault. Independent of the automation level it must also be checked whether the safety concept protects people from harm in the event of a failure.

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 to follow the applicable regulations. Therefore, as a first step it is important that cybersecurity principles and practices are well established and followed. For this, it is important to acknowledge the technologies to which the AVs are exposed, which may vary depending on the level of automation. The terms used in this topic may differ from those used in the above related 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.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 3-2-1					
<p>Is there an established and followed cybersecurity process within the organisation to ensure the security architecture of the overall function?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> Is there an established list of measures to be followed within the organisation (e.g. awareness programs, adequate trainings)? Is there a similar culture existing at sub-contractors, suppliers and potential 3rd parties working directly or indirectly 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) and their 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? 				

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. To do so, a Cyber Security Management System (CSMS) shall be established, which will gather the necessary set of systems and processes to be put in place and which will cover all development phases, including the post start of production phase, to ensure a secure development lifecycle (SDL). When implementing a cybersecurity culture, several measures shall be considered, such as programmes to raise cybersecurity awareness among the organisations and adequate training for employees (ENISA 2019). This will help to reduce the potential for successful attacks. Relationships with external stakeholders such as suppliers shall be considered, including the 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.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 3-2-2					
<p>Is security by design considered in order to minimise the risks / threats and respond appropriately to them once identified?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are security by design measures considered at all levels, from component level up to vehicle level? 				

Security by design is a principle that has to be followed throughout all the development phases, to make sure vulnerabilities are identified in time and to ensure a good integration of all security systems and components. In the first place it shall identify the security objectives and requirements of the ADF. At a later phase, during the design, it shall take into account key cybersecurity 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 and vehicle ECUs, 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 signs) and mobile devices such as smartphones.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 3-2-3					
<p>Are asset management and threat analysis and risk assessment performed? Yes / No</p>	<ul style="list-style-type: none"> • 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 requires the identification of all the assets that are specific to the organisation and the ADF, and this 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 the identification of possible threats to the function and how they relate to critical assets. Once they are identified security risks to 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 the event 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 potential attacks (so-called attack vectors), the likelihood of the attack, the impact, the risk and further details such as the expertise required to perform such attacks and the possible attack methods. Additionally, a TARA+ methodology shall be considered (TARA+ 2019). External connectivity offers the possibility to perform several tasks remotely without the need to be physically present at a dealer or garage, using V2N communications. This also increases the potential attack vectors that AVs can be exposed to. That is why asset management, threat analysis and risk assessment should carefully analyse all the possible external connections of the ADF (e.g. remote diagnostics). For details about software updates, please refer to topic 4.4.3.

Relevant Phase(s):	DF	CO	DS
Question 3-2-4			
<p>Are (cyber-) security requirements identified for the entire function, including not only those related to hardware/software development but also those related to network design and communication?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 ISO/SAE 21434, the ISO/PRF TR 4804 and UNECE Cybersecurity R-155. In addition, high-level cybersecurity requirements, also known as cyber-security goals, have to be defined for the entire ADF. 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 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).

Relevant Phase(s):

CO

DS

VV

Question 3-2-5

Is a review of the architectural design considered based on frequently updated requirements?

Yes / No

- Is a process established to verify the implementation of cybersecurity requirements?

ISO/SAE DIS 21434 Road Vehicles – Cybersecurity Engineering:

The joint working group of the standardisation organisations ISO and SAE has been working on the development of a cybersecurity standard for road vehicles since 2016. They have recently established and published a draft international specification of the “ISO/SAE DIS 21434 Road Vehicles – Cybersecurity Engineering” standard. This standard represents the results of the industry consensus on key cybersecurity practices to be applied across the automotive market. **The key principles of the standard refer to cybersecurity activities in all phases of the vehicle’s lifecycle**, ranging from design and development, production, operation and maintenance to decommissioning.

A framework is defined that includes requirements for a cybersecurity process and a common language for communicating and managing cybersecurity risk among stakeholders. This standard does not prescribe specific technology or solutions related to cybersecurity. However, a risk-oriented approach for prioritisation of actions and methodical elicitation of cybersecurity measures is mentioned.

ISO/SAE 21434

ISO/TR 4804 Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation:

The ISO organisation has been further developing the SaFAD (Safety First for Automated Driving) White Paper that was published in 2019. The technology report ISO/TR 4804 Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation was published in 2020 and was the first step for ISO standardisation.

This standard considers safety and cybersecurity by design, as well as verification and validation methods for automated driving with SAE L3 and L4. It provides an overview of and guidance about the general steps for developing, verifying and validating automated driving system safety, and highlights cybersecurity evaluation in conjunction with functional safety and SOTIF.

The further development of the ISO standard technical specification ISO/AWI TS 5083 Road vehicles — Safety for automated driving systems — Design, verification and validation has begun as the next step for ISO/TR 4804 in 2021.

UNECE R-155 Cyber security and cybersecurity management system:

The UN regulation was prepared by the Informal Working Group on Cyber Security and Over-the-Air issues, and endorsed by the Working Party on Automated/Autonomous and Connected Vehicles (GRVA). According to this regulation, new requirements for cybersecurity can be classified into two main categories as follows:

- 1.) Establishment of a **Cybersecurity Management System (CSMS)** covering organisations' policies and processes for handling cyber risks related to the entire lifecycle of vehicles, equipment and services; and
- 2.) Activities and documentation related to the secure development of automotive items, as well as post-development activities such as production, operation, maintenance and decommissioning.

In the European Union, the new regulation on cybersecurity (UNECE WP.29/R155) will be mandatory for all new vehicle types from July 2022 and will become mandatory for all new vehicles produced from July 2024.

As the development process evolves, the integration of components takes place, which may lead to potential new vulnerabilities which have to be prevented. For that it will be necessary to refine the previously defined cybersecurity requirements. This task may be an iterative process, since all the systems and components are gradually incorporated.

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. The correct allocation and implementation of the requirements for each system or component should also be verified.

Relevant Phase(s):	DF	CO	DS	VV	PS
Question 3-2-6					
<p>Is a cybersecurity Incident Response process established? Yes / No</p>	<ul style="list-style-type: none"> • 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 there a clear strategy for OTA updates based on cybersecurity requirements? 				

The first step of setting up 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 also to respond to them efficiently, a task that may require having dedicated teams, that can assign responsibilities and undertake the necessary actions. A procedure to inform the user about incidents shall also be considered, including elaboration of appropriate communication plans with the involvement of relevant parties. This shall be done to ensure that the appropriate information is communicated to users. Regarding software, a strategy shall be put into place to not only ensure updates but also to inform the user promptly and effectively about their implementation. For further details on software updates, refer to topic 4.4.3.

Relevant Phase(s):	VV	PS
Question 3-2-7		
Is a cybersecurity validation process clearly defined and followed? Yes / No	<ul style="list-style-type: none"> • Are roles and responsibilities as well as the required expertise for conducting specific validation activities clearly defined? 	

Validation of the implemented measures is key to understanding whether cybersecurity goals have been achieved and 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 1s), which will help to avoid possible duplication 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. The required expertise to conduct them shall also be clearly defined in this process or this topic and it is recommended to follow the guidelines under ISO/SAE 21434 as a reference.

4.4.3 Implementation of Updates

Over The Air (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 optimises the vehicle without necessitating a trip to a dealership. There is a growing set of principles to govern best practice of the update process. Some of these are mentioned in the following text, but some are still in development, such as ISO 24089 (ISO 24089 20XX).

Relevant Phase(s):	DF	DS
Question 3-3-1		
<p>Are international regulations and standards being followed where appropriate during the development of software update processes?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 to 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 rapidly developing field in the automotive sector, it is important to continuously check for new legislative standards required in the relevant markets (see topic 4.1.3).

Relevant Phase(s):	DF	DS	VV
Question 3-3-2			
<p>Is there a clearly defined OTA and software update strategy to manage the end-to-end process?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 partway through the update the state changes? • Location: are certain updates only available at predefined locations, such as the registered address of the vehicle? 		

Question 3-3-2

- Status of network connectivity: do updates require local wireless networks, or can some be installed using a cellular network connection?
- Is there an appropriate V&V strategy to check software updates before they are sent out? More questions are provided in the deliverable.

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”) in which updates can occur, and this should be robust enough to handle a change in the vehicle state.

Relevant Phase(s):

DF

CO

VV

Question 3-3-3

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 be done before releasing updates to the customer (see 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.

Relevant Phase(s):	DF
Question 3-3-4	
Are software safety requirements identified at a function level? Yes / No	<ul style="list-style-type: none"> 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 be identified and incorporated into the design. As safety standards develop, the system's FuSa must be modified to comply with future regulations.

Relevant Phase(s):	DF	DS	PS
Question 3-3-5			
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.

Relevant Phase(s):	CO	PS
Question 3-3-6		
<p>Is the function being updated safety critical? Yes / No</p>	<ul style="list-style-type: none"> Is there a robust V&V procedure to ensure that 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.

Relevant Phase(s):	CO	VV
Question 3-3-7		
<p>Is a method implemented to notify the user and OEM of each successful update installation? Yes / No</p>	<ul style="list-style-type: none"> As part of the notification process is the user advised on the expected duration of the installation? 	

It is important that users be informed about 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 be notified, to enable her / him to take further action (e.g. contact the manufacturer / dealership). The manufacturer should also be aware of successful or failed updates to enable a rapid reaction.

Relevant Phase(s):		DS	PS
Question 3-3-8			
<p>Is a process for managing failed updates implemented? Yes / No</p>	<ul style="list-style-type: none"> • 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 encouraging updates to the customer's vehicle? • Does the update process include a method for reverting to the previous software version when an update fails or until a software patch has been developed? 		

Any updates sent out to customers should have been sufficiently tested beforehand to ensure that 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 them.

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

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 the remote service approach used by technology companies. This means that the customer must have confidence that updates are from a trusted source and not a malicious attack. To ensure that 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 (see topic 4.4.2).

Relevant Phase(s):	DF
Question 3-3-10	
<p>Is there a (robust) method for the authorised owner of the vehicle to accept or reject updates?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 how to perform 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.

4.4.4 Safety of the Intended Functionality

The ISO 26262 series defines 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 and there can be potential hazardous behaviour caused by the intended functionality or performance limitation of a system when identifying hazardous events, even when free from faults in the scope of the ISO 26262 series.

The absence of unreasonable risk from these potentially hazardous behaviours related to such limitations is considered as the SOTIF (ISO/PAS 21448 2019).

The safety of road vehicles during their operation phase is of paramount concern for the road vehicles industry. Recent years have seen a huge increase in the number of advanced functionalities included in vehicles. These rely on sensing, processing of complex algorithms and actuation implemented by electrical and/or electronic (E/E) systems.

An acceptable level of safety for road vehicles requires the avoidance of unreasonable risk caused by every hazard associated with the intended functionality and its implementation, especially those not due to failures, e.g. due to performance limitations or insufficiencies of specification. For the achievement of functional safety, ISO 26262-1 defines functional safety as the absence of unreasonable risks that arise from malfunctions of the E/E system. ISO 26262-3 specifies a Hazard Analysis and Risk Assessment (HARA) to determine vehicle level hazards. This evaluates the potential risks due to malfunctioning behaviour of the item and enables the definition of top-level safety requirements, i.e. the safety goals necessary to mitigate the risks. The other parts of the ISO 26262 series provide requirements and recommendations to avoid and control random hardware failures and systematic failures that could violate safety goals.

For some E/E systems, which rely on sensing the external or internal environment to build situational awareness, there can be potentially hazardous behaviour caused by the intended functionality of a system that is free from the faults addressed in the ISO 26262 series. Examples of the causes of such potentially hazardous behaviour include:

- The inability of the function to correctly comprehend the situation and operate safely; this also includes functions that use machine learning algorithms;
- Insufficient robustness of the function, system or algorithm with respect to sensor input variations, heuristics used for fusion or diverse environmental conditions.

The absence of unreasonable risk due to these potentially hazardous behaviours related to such limitations is defined as the safety of the intended functionality (SOTIF). Functional safety (addressed by the ISO 26262 series) and SOTIF are distinct and complementary aspects of safety. To address the SOTIF, measures are implemented during the following phases:

- Measures in the design phase (e.g. requirements for sensor performance).
- Measures in the verification phase (e.g. technical reviews, test cases with a high coverage of relevant scenarios, injection of potential triggering conditions, in the loop testing (e.g. SIL : Software in the loop / HIL : Hardware in the loop / MIL : Model in the loop) of selected SOTIF-relevant scenarios.
- Measures in the validation phase (e.g. long-term vehicle test, simulation-based testing).
- Measures in the operation phase (e.g. field monitoring of SOTIF incidents)

Furthermore, a proper understanding by the user of the function, its behaviour and its limitations (including the human / machine interface) is critical to ensuring safety.

In many instances, triggering conditions are necessary to cause a potentially hazardous behaviour; hence the importance of analysing hazards in the context of particular use cases. In this document, potentially hazardous system behaviour is considered both for use cases when the vehicle is correctly used and for use cases when it is incorrectly used in a

reasonably foreseeable way (this excludes intentional alterations made to the system's operation).

EXAMPLE Lack of driver attention while using a level 2 driving automation

In addition, reasonably foreseeable misuse, which could lead directly to potentially hazardous system behaviour, is also considered as a possible triggering condition.

EXAMPLE Mode confusion (e.g. the driver thinks the function is activated when it is deactivated) can directly lead to hazard.

A successful attack exploiting vehicle security vulnerabilities can also have very serious consequences (i.e. data or identity theft, privacy violation). Although security risks can also lead to potentially hazardous behaviour that needs to be addressed, security is not addressed by this document. In addition, ensuring compliance with local driving laws, policies or road norms is beyond the scope of this document, except in cases where not following laws and rules of the road could lead to safety hazards. The activities mentioned in this document are complementary to those given in the ISO 26262 series.

While functional insufficiencies with the potential to lead to hazardous behaviour, as addressed in this document, could be interpreted as systematic faults, the measures to address these insufficiencies are specific and complementary to the ones described in ISO 26262. On the other hand, ISO 26262 assumes that the intended functionality is safe, and addresses faults that can cause hazardous behaviour due to a deviation from the intended functionality. The requirement derivation process for the system and its elements can include aspects of both standards. It is assumed for this document that the E/E random hardware faults and systematic faults of the E/E system are addressed using the ISO 26262 series.

From: ISO/CD 21448 2019

The cause of SOTIF-relevant hazardous events could derive from some aspect of the system, as well as from external factors. Such causes of hazardous events mainly include (ISO/PAS 21448 2019): performance limitations, reasonably foreseeable misuse and impact from car surroundings.

This topic discusses the main points for achieving the SOTIF when developing an ADF. 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.

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

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 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.

The SOTIF-relevant issues, regarding the systematic development of ADF to support safety by design, have also been addressed and discussed in other recent international standards, such as ISO/PRF TR 4804.

Additionally, the latest guidelines or regulations on the development of SOTIF should also be taken into account, such as the latest guidelines of NHTSA and SAE for the US. Several European organisations are working to modify and update the Geneva Convention and provide advice on regulations regarding the development and deployment of AVs in the European Union.

Relevant Phase(s):	DF
---------------------------	-----------

Question 3-4-2

<p>Is a functional and system specifications about ADF defined (including the ODD description)? Yes / No</p>	<ul style="list-style-type: none"> • Is the functionality and its dependencies on and interaction with the environment defined and described?
---	--

The functional and system specifications provide an adequate understanding of the system and its functionalities so that the SOTIF-related activities in subsequent phases can be performed. These functional and system specifications serve as the starting point 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 should be developed to serve as an input for the development of SOTIF.

Relevant Phase(s):	DF
---------------------------	-----------

Question 3-4-3

<p>Is there a systematic identification and evaluation of SOTIF risks including possible hazardous events arising from the system or external environment? Yes / No</p>	<ul style="list-style-type: none"> • 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 credible harm can result from a 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 that could bring potential harm 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 includes a consistency check of the FuSa concept in topic 4.4.1.

Based on the identification of hazardous events caused by hazards from the system or external environment, the systematic identification and evaluation of SOTIF risks can be executed 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 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. 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).

Relevant Phase(s):	DF
Question 3-4-4	
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. 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 the event that the user does not respond to TOR. The MRM leads to an MRC (e.g. limited / end of ADF operation) to minimise the risk and ensure the safety of the user. For aspects related to the MRM, please see also topic "Minimal Risk Manoeuvre" (topic 4.1.1).

Relevant Phase(s):	DF
Question 3-4-5	
Does the ADF monitor the driver in order to ensure her / his 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 (UNECE ALKS 2020). This monitoring system could also invoke action to remind and maintain the driver's attention in both manual and automated driving. An appropriate driver monitoring function can help ADF to make better decisions to improve comfort and safety. In particular, it can ensure the controllability of the intended function of the vehicle by the driver. For more information related to driver monitoring, please see also topic "Driver Monitoring" (topic 4.5.3).

Relevant Phase(s):	DF	VV
Question 3-4-6		
Is there a V&V strategy to prove the compliance of SO-TIF aspects? Yes / No	<ul style="list-style-type: none"> • Does the 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 performance 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 regarding the risk of safety violations without system faults include integration-testing activities. In order to achieve this strategy, several issues, which are based on 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).

Relevant Phase(s):	DF
Question 3-4-7	
Are users of the ADF informed about the functional limitations (including the ODD limits)? Yes / No	<ul style="list-style-type: none"> • 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 AVs in real-life conditions, the users need to be informed about the functionalities to improve their knowledge of the ADF. The approaches taken to inform the users on how to use the ADF safely within the scope of ODD (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 limits of the ADF during a driving task so that they can use the AVs safely and appropriately (see topic 4.5.1). Notification about the consequences of system misuse can significantly reduce misuse by users (MILT 2018).

Relevant Phase(s):	CO
Question 3-4-8	
Are there improvements regarding functional and system specifications to avoid or mitigate SOTIF related risks? Yes / No	<ul style="list-style-type: none"> • Are there triggering events related to sensors, algorithms and actuators identified? • Is there an assessment as to whether the system appropriately responds to triggering events?

Triggering events represent specific conditions of a driving scenario that serve to initiate 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 related scenarios that could result in an identified hazard. Identified events shall be addressed by functional improvements of the ADF to respond appropriately and correctly. Functional improvements could incorporate several aspects, for instance sufficient performance of sensors, sufficient performance of detection and decision algorithms, as well as appropriate HVI regarding the controllability of the vehicle and avoidance of misuse, etc. (ISO/PAS 21448 2019).

Relevant Phase(s):	DS	VV
Question 3-4-9		
<p>Is the ADF performance verified in the event of hazardous events and foreseeable misuse by conducting appropriate testing (XIL, real world and test track tests)?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> Is the ADF validated regarding the aspect that it does not cause any unreasonable level of risk in real-life use cases? 	

Several methods of the V&V of system performance, such as MIL, SIL, HIL, test track experiments and long-term endurance tests (real world tests) with the injection of potential triggering events, could be implemented in order to ensure the safety of intended functionalities (see topic 4.1.4 and Annex 1). According to the ISO/PAS 21448, the ADF should be validated to ensure that it causes minimum risk, especially any unreasonable level of risk, in real-life use cases. Therefore, two different approaches could be applied as below (ISO/PAS 21448 2019):

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

These two approaches can significantly help SOTIF safety goals be achieved.

Question 3-4-10

Are methodology and criteria for SOTIF release performed at the end of SOTIF activities?

Yes / No

SOTIF release shall be conducted by reviewing all SOTIF activities as well as evaluating the acceptability of the residual risks. Several issues need to be evaluated in this context:

1. whether all the specified use cases are taken into account by the validation strategy within the scope of the intended functions;
2. whether the intended functionality achieves a minimum fall-back risk condition;
3. whether the V&V acceptance criteria sufficiently ensure that the risk is reasonable;
4. whether sufficient evidence is provided to argue the absence of unreasonable risk in the event of an unintended behaviour.

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

4.4.5 Data Recording, Privacy and Protection

The realisation of ADF will enable the collection of massive amounts of data (e.g. movement patterns, customer preferences). To protect the customers' data recorded, this process needs to take place 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 legal and reasonable justification have access to the personal data gathered from customers and other road users. By following established procedures, misuse will be minimised and the benefits of data collection highlighted. Furthermore, customers need to be aware of how their data is handled and processed.

Relevant Phase(s):	DF	DS	PS
Question 3-5-1			
<p>Is the purpose of the data collected made clear, especially to the customer? Yes / No</p>	<ul style="list-style-type: none"> • Is the customer informed about the data that is considered as personal, and the categories into which it is divided? • Is the customer informed about the purpose for which data is shared with, third parties (categories of third parties) and the identity of the company (group of companies) that governs data processing? • Is this information made clearly available and easily accessible (contract, website, manual, etc.)? • Are contact points (such as customer service websites, emails, and addresses) for the customer maintained? <p>More questions are provided in the deliverable.</p>		

The customer requires an understanding of why personal data is collected. There shall be informational material available explaining the reasons. There must be a clear communication of which data is considered as personal information and which is not. If applicable, the customer should also be informed about different data categories.

This also includes information about other organisations that access the data and the reasons for this. 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 is given the choice to decide to share data or not, depending on the purpose.

Relevant Phase(s):	DF	DS
Question 3-5-2		
<p>Is data ownership clearly defined? Yes / No</p>	<ul style="list-style-type: none"> • 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 that accompany data ownership clear? • Is it authorised for third parties (such as marketing companies) to access the data? 	

There needs to be a clear definition of 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 what reason. The site of data storage shall be well defined. In the event that a data retention deadline is reached, there must be a known and easy process established to request the deletion of the data. If it is necessary to keep personal data, it must be accurate and up-to-date.

Relevant Phase(s):	DF
Question 3-5-3	
<p>Is necessary data collected that is related to the occurrence of malfunctions or failures, in order to reconstruct the cause of any incident or crash? Yes / No</p>	<ul style="list-style-type: none"> • Does the 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? • What parameters / resolutions / frequency of logging are used? • Is relevant information shared with the government authorities for crash reconstruction?

To help with the analysis of incidents and accidents and the improvement of ADFs, pertinent 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 upon request.

Relevant Phase(s):	DS
Question 3-5-4	
<p>Is a data protection impact assessment carried out? Yes / No</p>	<ul style="list-style-type: none"> • Is the societal impact, as in the case of customer rejection, assessed? • Is the impact assessed of how data is used as evidence of ADF operation in the event of an accident? • Is the impact assessed of how data is used by legal authorities and insurance companies?

There must be an assessment conducted to analyse the impact of the data protection measures employed. This includes the impact on the societal level, such as customer acceptance or rejection.

Relevant Phase(s):	DS
Question 3-5-5	
<p>Are appropriate measures (technical, security, organisational) in place to protect customer data? Yes / No</p>	<ul style="list-style-type: none"> • Are there contractual safeguards to protect personal data in the event of outsourcing? • Is data privacy addressed by using publicly available and well-tested cryptographic methods? • Is anonymisation, pseudonymisation and de-identification applied where appropriate?

Question 3-5-5

- Is the data processed based on a contract, with the consent of the customer, to comply with legal obligations?
 - Is personal data kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which it is stored?
- More questions are provided in the deliverable.

The measures implemented to protect customer data must be appropriate for the technical, security and organisational levels. This is especially problematic in the case of outsourcing personal data. Only relevant and adequate personal data shall be processed, using means to anonymise and pseudonymise them. Personal data shall be analysed according to the applicable laws in a transparent way. If personal data are stored, this must be limited to what is necessary, for the purposes for which it is processed. Personal data shall be kept in a form that allows an individual to be identified only when necessary and for no longer than necessary.

Relevant Phase(s):

DS

Question 3-5-6

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 must be ensured that the developed ADFs are compliant with the data protection regulations that apply in the respective countries. For the European Union, the General Data Protection Regulation (GDPR) has to be considered. Most importantly, evidence of the steps taken to comply with the GDPR is necessary. This needs to be documented as part of a company's standard protocols.

Relevant Phase(s):	DS
Question 3-5-7	
Are (security) risk assessment and management procedures in place? Yes / No	<ul style="list-style-type: none"> • Are security risks identified and managed using secure coding practices including by the supply chain, contractors, etc.? • Are the authenticity and origin of all supplies ascertained? • Have the guidelines intended by Question 3-2-1 been considered?

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.

Relevant Phase(s):	DS
Question 3-5-8	
Are back-end functions protected appropriately? Yes / No	<ul style="list-style-type: none"> • 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.

Relevant Phase(s):

DS

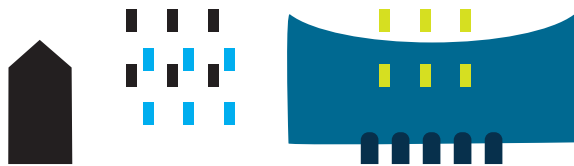
Question 3-5-9

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 to be resilient and fail-safe if safety critical functions are compromised (link to topic 4.4.1)?

Nevertheless, principles of functional safety must 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.







4.5

Human-Vehicle Integration

4.5 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 such 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 topics of this category are guidelines for HVI, mode awareness, driver monitoring, controllability & customer clinics, and driver training & variability of users.

4.5.1 Guidelines for HVI

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.

Relevant Phase(s):	DF	CO	VV
Question 4-1-1			
Are design guidelines followed when defining, assessing & validating the HVI concept? Yes / No	<ul style="list-style-type: none">• 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 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, Forster et al. 2019 and 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 for familiarisation with the HVI, thus improving the experience of first-time users.

Relevant Phase(s):	CO
Question 4-1-2	
<p>Are unintentional activations and deactivations of the ADF prevented?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are the ADF controls designed so as 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 that 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. 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 on 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 when designing this part of the HVI.

Question 4-1-3

Is the visual interface designed to be easy to read, understand and interpret?

Yes / No

- Do the design of the text size, aspect ratio and contrast 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 user?
- 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?

Guidelines and standards of strategy for the visual HVI 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 is important that new icons, messages and HVI elements are added to these standards and guidelines so that HVI can be standardised for AVs.

Question 4-1-4

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?
- More questions are provided in the deliverable.

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 convey 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.

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.

Question 4-1-5**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 that 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. Interfaces should be positioned to optimise the driver's interaction with them, whether simply through glances or through physical interactions. 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 increasingly equipped 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.

Question 4-1-6**Is 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 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. Having a clear and high-quality HVI that meets all the guidelines outlined in this CoP and the additional material is a good first step to ensuring user acceptance. 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.

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

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

The goal of this question is to ensure that the possible AD mode 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.

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 Phase(s):	DF
Question 4-2-2	
<p>Are the modalities to communicate the relevant active (automated) driving modes described?</p> <p>Yes / No</p>	

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

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

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

This question is related to the negative and positive impacts that an 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.

Relevant Phase(s):	DF	CO	DS	VV
--------------------	----	----	----	----

Question 4-2-5

<p>Is an appropriate and clear way to communicate the automated driving modes to the user investigated and confirmed?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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? <p>More questions are provided in the deliverable.</p>
--	---

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

Relevant Phase(s):	CO
--------------------	----

Question 4-2-6

<p>Are measures investigated to improve driver alertness and the time to get the driver back in-the-loop?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Are different HVI modality combinations investigated? • Is speech being considered for a TOR?
--	--

The purpose of this question is to draw attention to 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 the event of an unplanned take-over event, this would be necessary (until L3) to shorten the time that users would need to return to alertness / awareness. On the other hand, it shall not be forgotten that the HVI is assumed to be no more intrusive than necessary. It should not be a burden, but rather an aid to 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.

Relevant Phase(s):	CO
Question 4-2-7	
<p>Is the provision of ODD information to the user considered? Yes / No</p>	<ul style="list-style-type: none"> • 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?

Three major kinds of ODD information are especially relevant to the user and shall be displayed:

- 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 to take over the controls.

Relevant Phase(s):

CO

Question 4-2-8

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 the event that 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 should do next (see topic 4.1.1).

Relevant Phase(s):

CO

DS

VV

Question 4-2-9

Is the communication to the user of the user's responsibilities in each defined automated driving mode(s) investigated and confirmed?

Yes / No

- Is there a method to clearly inform the user of her / his responsibilities and of vehicle capabilities and possibly of the consequences 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?
More questions are provided in the deliverable.

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 understands the function's capabilities in these modes. Users may be informed by several means, including advertisement and written explanations in the owner's manual. Users may get explicit information from 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 users understand the situation and take the appropriate actions. This concept complements the above-mentioned concept of situational awareness and being "in-the-loop" (4-2-6).

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

The purpose of this question is that the driving scenarios may impact the way and the extent to which 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 this, the displayed feedback information needs to be appropriate according to the situation.

Relevant Phase(s):	CO
Question 4-2-11	
<p>Is user awareness of automated driving modes being investigated?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> Is user awareness of automated driving mode transitions 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 transitions among driving modes.

Relevant Phase(s):	VV
Question 4-2-12	
<p>Are user expectations regarding the ADF’s features considered?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 provided to make sure that the process will be considered.

Relevant Phase(s):	VV	PS
Question 4-2-13		
<p>Is the users’ trust in the ADF being investigated?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 to ensure the correct amount of trust.

Relevant Phase(s):	VV	PS
Question 4-2-14		
<p>Is the appropriate usage of the ADF by users confirmed? Yes / No</p>	<ul style="list-style-type: none"> • 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 an appropriate way as well as in an inappropriate way (e.g. text message)? • Is there a feedback loop to the OEM when the ADF is used in an appropriate as well as inappropriate manner? 	

This question is a general summary confirming that users should appropriately use the ADF. Also, they shall not misuse the system. In order to make sure the user is aware of appropriate usage, the user manual shall contain a description of how to appropriately use the ADF. In the event that the users do not read the manual, it must be ensured that other methods are available to ensure that users use the ADF appropriately. There must be direct and immediate feedback, for instance via the vehicle display, if the ADF is misused. Statistics shall be gathered anonymously via the vehicle to inform the OEM about occurrences of misuse to prevent further misuse.

Relevant Phase(s):	VV	PS
Question 4-2-15		
<p>Are the long-term effects of the ADF on users being investigated? Yes / No</p>	<ul style="list-style-type: none"> • Are all the appropriate metrics to evaluate the long-term effects of the ADF being 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 shall 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 to do so. Typically, the main risks of long-term effects are skill degradation and building over-trust in the function.

Relevant Phase(s):	PS
Question 4-2-16	
Is the HVI impact on user workload over long journeys being investigated? Yes / No	

The last question of the topic addresses the impact of the HVI over long journeys. It could be investigated by taking advantage of dedicated fleets with typically long travel times.

4.5.3 Driver Monitoring

Real time monitoring of a driver’s inattention / attention is a crucial topic, especially when discussing AD. In fact, not only is driver distraction one of the main causes of accidents on the roads, but also 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.

Relevant Phase(s):	DF
Question 4-3-1	
Are most of the relevant secondary tasks considered? Yes / No	<ul style="list-style-type: none"> • 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 the secondary tasks 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. 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.

Relevant Phase(s):	CO	VV
Question 4-3-2		
Is the HVI connected with the driver monitoring function? Yes / No	<ul style="list-style-type: none"> • 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 the 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). From this perspective, feedback about the driver states should be communicated, and further discussion regarding standardisation is required.

Relevant Phase(s):	CO
Question 4-3-3	
<p>Is it possible to mirror the customers' devices on the vehicle HVI?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> 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?

This question focuses on the problem of mirroring contents / apps from the user's own mobile device directly onto 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 that requires particular attention (e.g. when the ADF leaves its ODD). If the mirroring is on e.g. Apple / Android systems (using, for example, "AppleCar" or "AndroidAuto"), then messages relevant to the driver's state (impairment, drowsiness, etc.) could be possible, as a way to communicate with the driver. This becomes especially important if the system "knows" that the driver is engaged in certain activities on the smartphone.

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

Strongly related to the previous question, the impact of secondary tasks on the TOR provided by the function in the validation phase needs to be understood. From this, an answer to the previous point can be given: if the impact is high (i.e. affecting vehicle safety) certain secondary tasks (e.g. mirroring) shall be forbidden.

Relevant Phase(s):	PS
Question 4-3-5	
<p>Can data be measured and accessed after the start of production, to assess whether a selected secondary task (to be defined) has been performed and to ascertain its impact on driving behaviour, traffic safety, etc.?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 sensitive information) and to actually measure them (e.g. because of specific sensor availability), respectively.

The last question of the driver monitoring section is related to measuring the long-term effects of AD on secondary tasks, considering data (if available). 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.

4.5.4 Controllability & Customer Clinics

L3 AD requires the driver to take over the driving task in the event 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 for 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.

Relevant Phase(s):

DF

Question 4-4-1

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 factor 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. 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.

Relevant Phase(s):

CO

Question 4-4-2

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 such as colour-blindness, general vision, sensory-motor and hearing impairments.

Relevant Phase(s):	CO
Question 4-4-3	
<p>Is the driver informed about function limits that will trigger requests to intervene?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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 the event that ADF limits are reached.

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

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.

Relevant Phase(s):	CO
Question 4-4-5	
Does the behaviour of the ADF lead to non-controllable situations from the perspective of other road users? Yes / No	<ul style="list-style-type: none">• Is the vehicle behaviour predictable for other road users if they do not know whether the vehicle is 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.

Relevant Phase(s):	DS
Question 4-4-6	
Is it possible to preliminarily verify the concept based on expert controllability assessments? Yes / No	<ul style="list-style-type: none">• Are preliminary controllability assessments and resulting 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.

Relevant Phase(s):	VV
Question 4-4-7	
<p>Are the testing environments suitable for controllability confirmation tests?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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.

Relevant Phase(s):	VV
Question 4-4-8	
<p>Is it possible to sign-off the controllability based on customer clinic results and / or expert assessments?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • Can function outputs and information be perceived by the drivers quickly enough to enable them to react appropriately? • 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 the ADF's limits been considered?

Question 4-4-8

- Are the limitations of correct operation / function limits comprehensible and predictable for the driver in different environments and 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?
More questions are provided in the deliverable.

The final controllability verification can be based on different evaluation methods such as expert assessments or controllability verification tests.

Relevant Phase(s):

PS

Question 4-4-9

Is the ADF adequately evaluated from a human factor 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.

4.5.5 Driver Training & Variability of Users

The training aspect is about the issue of providing users with the appropriate knowledge and skills to operate an ADF. Secondly, there is a huge variability among users, as different age groups, gender, cultural backgrounds and previous experiences need to be addressed. The two topics are interrelated and thus combined in this category.

Relevant Phase(s):	DF
Question 4-5-1	
<p>Is the diversity of different user groups taken into account?</p> <p>Yes / No</p>	<ul style="list-style-type: none"> • 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?

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 should not be designed for only a specific country or region without considering these aspects.

Secondly, there is a general trend towards an aging population. Due to degrading physical abilities, activities become more cumbersome. During the definition of ADFs, physical impairments of elderly drivers need to be considered.

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 those with non-age-related disabilities.

Relevant Phase(s):

CO

DS

Question 4-5-2

Is a training course necessary 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 the specification of the ADF's operation. This serves as a baseline to create a user training course, if deemed necessary. If such a training course is regarded as necessary, appropriate measures need to be taken to realise it. 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 combination of training methods shall be considered as well.

Relevant Phase(s):

CO

Question 4-5-3

Has a representative test sample for customer studies ensured, taking into account variables such as age, gender, etc.?

Yes / No

Due to the high variability among users, customer studies evaluating the ADF need to consider various factors. Depending on the exact customer study to be conducted, this may range from age, gender and socio-cultural background to previous experience with ADFs or computers in general.

Relevant Phase(s):	PS
Question 4-5-4	
<p>Is an effective approach of customer information and education available to the users post start of production? Yes / No</p>	<ul style="list-style-type: none"> • Is user information and training supported with appropriate information from 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. The marketing of 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 ADF's abilities, by providing accurate advertising and customer sales information guides.

5.0

Perspectives



No single approach for the implementation of ADF

It is clear that there is 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 leave room open for different technical solutions. This aspect is also recommended for other activities – such as standardisation activities, regulatory activities, etc. – as long as the knowledge and on-road experience with the technology is limited, i.e. with most of the experiments based on prototype tests. Once the technology has gone into mass production and the experience with this technology in the field has grown, more concrete recommendations can be given.

Nevertheless, in the near future, experience and knowledge related to AD will continue to increase dramatically. In this sense, the pan-European pilot tests of L3Pilot mark a significant step forward.

Trade-off between detailed information and broad understanding

A particular challenge for the CoP-ADF is to find the right level of detail. This challenge is related to the question of who the main users of this document are. On the one hand, there are developers asking for detailed technical guidance. On the other hand, there are political- and management-oriented stakeholders asking rather for an overview of the entire topic. Satisfying both requests is challenging. If the document is set up in a very detailed way, there is the high risk for non-experts of losing track. An overly broad overview will not help the developers, since only obvious aspects would be discussed. The approach taken in the CoP-ADF is to use questions to ensure that relevant aspects are not forgotten. To tackle both levels of detail, each question consists of a main high-level question and detailed sub-questions. In addition, links to further literature have been included.

Automated driving is a rapidly evolving technology

The biggest challenge for the CoP-ADF is the rapid development in the topic of AD. Many activities have begun and ended during the last three years. Many documents have been published by governments, regulation authorities, manufacturers, suppliers, insurance companies, research organisations, universities, think tanks and others. This leads to a flood of information that needs to be processed and evaluated with respect to its importance and structured in a readable format. This results in two challenges:

First, there is a high risk of losing track of the state-of-the-art and not being able to identify relevant information.

Second, the report risks only providing snapshots from its release date.

For the first challenge, it is important to involve different experienced experts in the work. Here, the L3Pilot consortium was a unique opportunity: the combination of industry partners, insurance companies, research organisations, universities and a user organisation makes it possible to cover a broad spectrum of experiences and knowledge. The experience of the consortium has been used directly to generate the CoP-ADF.

The second challenge requires regular updates. The CoP activity will be continuing in further EU-funded projects, namely the Hi-Drive project.

6.0

Annex

Literature and Relevant Topics in CoP-ADF

Reference	Relevant topics in CoP-ADF
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.	4.4.3 Implementation of Updates
Abdulkhaleq, A. (2017). "A system-theoretic safety engineering approach for software-intensive systems", Dissertation, University Stuttgart.	4.2.3 Performance Criteria and Customer Expectations
ACEA (2015). "ACEA Principles of data protection in relation to connected vehicles and services", ACEA Report.	4.4.2 Cybersecurity
ACEA (2017). "ACEA principles of Automobile Cybersecurity", ACEA Report.	4.4.5 Data Recording, Privacy and Protection
ASAM OpenDrive (2020). (https://www.asam.net/standards/detail/opendrive/).	4.1.4 Testing
ASAM OpenScenario (2020). (https://www.asam.net/standards/detail/openscenario/).	4.1.4 Testing
ASAM XIL Standard (2020). (https://www.asam.net/standards/detail/xil/).	4.1.4 Testing
Barnard, Y., Chen, H., Koskinen, S., Innamaa, S., et al. (2018). "Updated Version of the FESTA Handbook", FOT-Net Deliverable D5.4.	4.4.5 Data Recording, Privacy and Protection
Bartels, A., Eberle, U., Knapp, A. (2015). "System Classification and Glossary", AdaptIVe Deliverable D2.1.	4.2.3 Performance Criteria and Customer Expectations
Bengler, K., Drücke, J., Hoffmann, S., Manstetten, D., & Neukum, A. (2018). UR: BAN Human Factors in Traffic. In Approaches for Safe, Efficient and Stress-free Urban Traffic. Springer Wiesbaden, Germany.	4.5.4 Controllability & Customer Clinics
Bienzeisler, J., Cousin, C., Deschamps, V. et al. (2017). "Legal aspects on automated driving", AdaptIVe deliverable D2.3.	4.1.3 Existing Standards 4.3.4 Ethics & Other Traffic-Related Aspects

Reference	Relevant topics in CoP-ADF
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.	4.3.4 Ethics & Other Traffic-Related Aspects
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.	4.5.3 Driver Monitoring
Brusque, C., Bruyas, M. P., Carvalhais, J., Cozzolino, M., et al. (2007) "Effects of system information on drivers' behaviour", INERTS Synthesis No. 54.	4.5.5 Driver Training & Variability of Users
BSI/PAS 1883 (2020) "Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) – Specification", British Standards Institution.	4.2.1 Requirements
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.	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
CATAPULT Transport Systems (2017). "Market Forecast for connected and autonomous vehicles", Report.	4.3.2 V2X Interaction
Commission of the European Communities, "European Statement of Principles on the design of human-machine interface" (ESOP 2006).	4.5.1 Guidelines for HVI
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.	4.5.3 Driver Monitoring
Department of Transport (DOT) (2015). "The pathway to driverless cars: a code of practice for testing", Report of Department of Transport.	4.1.4 Testing 4.4.5 Data Recording, Privacy and Protection

Reference	Relevant topics in CoP-ADF
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.	4.3.4 Ethics & Other Traffic-Related Aspects
ENISA, "ENISA Good practices for Security of Smart Cars", European Union Agency for Cybersecurity (ENISA 2019).	4.4.2 Cybersecurity 4.4.3 Implementation of Updates
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.	4.2.3 Performance Criteria and Customer Expectations
Ford (2018). "A matter of trust – Ford's approach to developing self-driving vehicles", Ford safety report.	4.5.2 Mode Awareness, Trust & Misuse 4.5.5 Driver Training & Variability of Users
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.	4.5.1 Guidelines for HVI
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.	4.5.3 Driver Monitoring
Gellerman, H., Svanberg, E., Kotiranta, R., Heinig, I., et al. (2017). "Data sharing framework", FOT-Net Deliverable D3.1.	4.4.5 Data Recording, Privacy and Protection
General Motors (2018). "2018 self-driving safety report", GM safety report.	4.5.2 Mode Awareness, Trust & Misuse 4.5.5 Driver Training & Variability of Users

Reference	Relevant topics in CoP-ADF
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.	4.5.4 Controllability & Customer Clinics
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.	4.3.3 Traffic Simulation
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].	4.4.5 Data Recording, Privacy and Protection
Innamaa, S., Silla, A., Aittoniemi, E. et al. Evaluation plan, L3Pilot deliverable D3.4.	4.3.4 Ethics & Other Traffic-Related Aspects
INCOSE (2015). Systems Engineering Handbook.	4.2.4 Architecture
Information Commissioner's Office (ICO) (2018), "Guide to the General Data Protection Regulation (GDPR)", Report.	4.4.5 Data Recording, Privacy and Protection
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].	4.2.3 Performance Criteria and Customer Expectations 4.3.1 Automated Driving Risks and Coverage of Interaction with Mixed Traffic
ISO 21934-1 (20). "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.	4.3.3 Traffic Simulation 4.3.4 Ethics & Other Traffic-Related Aspects

Reference	Relevant topics in CoP-ADF
ISO 26262 (2018). "Road vehicles — Functional safety", ISO standard series ISO 26262.	<ul style="list-style-type: none"> 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 (2015). "Quality management systems — Requirements", ISO standard ISO 9001:2015.	4.1.2 Documentation
ISO/CD 24089 (20XX). "Road vehicles — Software update engineering", ISO standard ISO/CD 24089.	4.4.3 Implementation of Updates
ISO/IEC/IEEE 15288 (2015). "System and Software Engineering – System Life Cycle Processes", ISO standard ISO/IEC/IEEE 15288.	4.2.4 Architecture
ISO/IEC/IEEE 42010 (2011). "Systems and software engineering – Architecture description", ISO standard ISO/IEC/IEEE 42010.	4.2.4 Architecture
ISO/PAS 21448 (2019). "Road vehicles — Safety of the intended functionality", ISO standard ISO/PAS 21448:2019.	<ul style="list-style-type: none"> 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 (2020). "Road vehicles — Safety and cybersecurity for automated driving systems — Design, verification and validation", ISO standard ISO/PRF TR 4804.	<ul style="list-style-type: none"> 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

Reference	Relevant topics in CoP-ADF
ISO/PWI 34505 (20XX) "Road vehicles — Evaluation of test scenarios for automated driving systems", ISO Proposed Work Item.	4.3.4 Ethics & Other Traffic-Related Aspects
ISO/SAE 21434 (2021). "Road vehicles – Cybersecurity engineering", ISO standard under preparation.	4.1.3 Existing Standards 4.4.2 Cybersecurity 4.4.3 Implementation of Updates
ISO/WD 34501 (20XX) "Road vehicles — Terms and definitions of test scenarios for automated driving systems", ISO Working Document.	4.1.4 Testing 4.3.4 Ethics & Other Traffic-Related Aspects
ISO/WD 34502 (20XX) "Road vehicles — Engineering framework and process of scenario-based safety evaluation", ISO Working Document.	4.3.4 Ethics & Other Traffic-Related Aspects
ISO/WD 34503 (20XX). "Road vehicles — Taxonomy for operational design domain for automated driving systems", ISO Working Document.	4.2.1 Requirements 4.3.4 Ethics & Other Traffic-Related Aspects
ISO/WD 34504 (20XX) "Road vehicles — Scenario attributes and categorization", ISO Working Document.	4.3.4 Ethics & Other Traffic-Related Aspects
ISO/WD 34505 (20XX) "Road vehicles — Evaluation of test scenarios for automated driving systems" ISO Working Document.	4.3.4 Ethics & Other Traffic-Related Aspects
Japan Automobile Manufacturers Association (JAMA) (2004). "Guidelines for In-vehicle Display Systems — Version 3.0", Report.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse
Kelsch, J., Dziennus, M., Schieben, A., Schömig, N., et al. (2017). "Final functional Human Factors recommendations", AdaptIVe Deliverable D3.3.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse
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.	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

Reference	Relevant topics in CoP-ADF
Makoto, I., (2017). Effects of system information on drivers' behaviour. SIP-adus Workshop 2017, Tokyo.	4.5.3 Driver Monitoring
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.	4.3.3 Traffic Simulation
Maurer, M., Gerdes, J.C., Lenz, Winner, H. (2016). "Autonomous Driving - Technical, Legal and Social Aspects" Springer.	4.3.3 Traffic Simulation
Ministry of Land, Infrastructure, Transport and Tourism (MIT) (2018). "Guideline regarding Safety Technology for Automated Vehicles in Japan", Presentation, 1st Meeting of working party on automated/autonomous and connected vehicles (GRVA).	4.4.4 Safety of the Intended Functionality
National Transport Commission (NTC) (2017). "Guidelines for trials of automated vehicles in Australia", Report, ISBN: 978-0-6480156-2-8.	4.1.4 Testing
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.	4.5.1 Guidelines for HVI
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.	4.5.4 Controllability & Customer Clinics
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.	4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse

Reference	Relevant topics in CoP-ADF
<p>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.</p>	<p>4.5.1 Guidelines for HVI 4.5.2 Mode Awareness, Trust & Misuse 4.5.4 Controllability & Customer Clinics</p>
<p>Naujoks, F., Wiedemann, K., Schömig, N., Jarosch, O., & Gold, C. (2018-2). Expert-based controllability assessment of control transitions from automated to manual driving. MethodsX, 5, 579-592.</p>	<p>4.5.4 Controllability & Customer Clinics</p>
<p>PEGASUS Project (2019). "PEGASUS method – an overview", Report of the PEGASUS research project funded by the federal ministry of economic affairs and energy.</p>	<p>4.1.4 Testing 4.2.2 Scenarios and Limitations 4.3.4 Ethics & Other Traffic-Related Aspects</p>
<p>Post, K., Davey, C. (2019) "Integrating SOTIF and Agile Systems Engineering", SAE Technical Paper 2019-01-0141.</p>	<p>4.4.4 Safety of the Intended Functionality</p>
<p>Prokop, G. (2001). "Modelling human vehicle driving by model predictive online optimization", Vehicle System Dynamics, 35, pp. 19–53.</p>	<p>4.3.3 Traffic Simulation</p>
<p>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, pp. 794-807.</p>	<p>4.3.3 Traffic Simulation</p>
<p>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.</p>	<p>4.5.3 Driver Monitoring</p>
<p>Riedmaier et al. (2018). Validation of X-in-the-Loop Approaches for Virtual Homologation of Automated Driving Functions, 11th FRAZ Symposium virtual vehicle.</p>	<p>4.3.3 Traffic Simulation</p>

Reference	Relevant topics in CoP-ADF
SAE International (2018). "Taxonomy and Definition for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016)", J3016 Revision June 2018.	4.2.2 Scenarios and Limitations 4.2.4 Architecture
SAE International (2016). "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems (J3061)", J3061 2016.	4.1.3 Existing Standards 4.4.2 Cybersecurity 4.4.3 Implementation of Updates
SAE International (2012). "Automated Driving Reference Architecture (J3131)", J3131 2012.	4.2.4 Architecture
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).	4.3.4 Ethics & Other Traffic-Related Aspects
Sato, T. (2017). Driver distraction and inattention in the realm of automated driving. SIP-adus Workshop 2017, Tokyo.	4.5.3 Driver Monitoring
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.	4.4.3 Implementation of Updates
SIP-adus (2017). "SIP-adus Workshop 2017 Summary Report", Conference report.	4.5.3 Driver Monitoring 4.5.5 Driver Training & Variability of Users
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].	4.1.4 Testing
SVA Simulation of Autonomous Vehicle Safety (2020). (https://www.irt-systemx.fr/en/projets/sva/).	4.3.4 Ethics & Other Traffic-Related Aspects
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.	4.4.2 Cybersecurity

Reference	Relevant topics in CoP-ADF
Thorn, E., Kimmel, S., Chaka, M. (2018). "A Framework for Automated Driving System Testable Cases and Scenarios", DOT HS 812 623.	4.3.1 Automated Driving
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).	4.1.4 Testing
UNECE (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.	4.1.1 Minimal Risk Manoeuvre 4.1.2 Documentaiton 4.1.3 Existing Standards 4.1.4 Testing 4.3.3 Traffic Simulatin 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
UNECE (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.	4.1.3 Existing Standards 4.4.2 Cybersecurity
UNECE (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.	4.1.3 Existing Standards 4.4.3 Implementation of Updates
UN Task Force on Cybersecurity and Over-the-Air issues (UNTF) (2018). "Draft Recommendation on Software Updates of the Task Force on Cybersecurity and Over-the-air issues of UNECE WP.29 GRVA", Internal Document.	4.4.3 Implementation of Updates
UN (2019). Framework document on automated/ autonomous vehicles. United Nations World Forum for Harmonization of Vehicle Regulations (WP.29).	4.1.3 Existing Standards

Reference	Relevant topics in CoP-ADF
US Department of Transport (USDOT) (2018). "Preparing for the future of transport – Automated vehicles 3.0" Report of the US Department of Transport.	4.3.2 V2X Interaction
UTO-ISAC (2016). "Auto-ISAC Best Practices", Report.	4.4.2 Cybersecurity
VV Methoden Project (VVM-Projekt). (https://www.vvm-projekt.de/en/).	4.2.2 Scenarios and Limits
Wann, J. P., Wilkie, R. M. (2004). "How do we control high speed steering?" in <i>Optic Flow and Beyond</i> , pp. 371– 389.	4.3.3 Traffic Simulation
Waymo (2018). "On the Road to Fully Self-Driving – Waymo Safety Report", Waymo Reprot.	4.3.3 Traffic Simulation
Winner, H., Wachenfeld, W. (2013). "Absicherung automatischen Fahrens" 6. FAS Tagung, Munich.	4.1.4 Testing
Wood, M., Knobel, C., Garbacik, N., et al. (2019). "Safety first for automated driving", Report of different companies.	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
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.	4.5.2 Mode Awareness, Trust & Misuse 4.5.3 Driver Monitoring
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.	4.5.3 Driver Monitoring

Glossary

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 death.
Attack Vector	A path or route used by the adversary to gain access to the target (asset).
Automated Driving Function	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 Scenario	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.

Term	Definition
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.
Event	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 an 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. For example, 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 that changes the foreseeable action (speed, direction) of the vehicle.
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 brings 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 minimising 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.

Term	Definition
Object and Event Detection and Response	The subtasks of the dynamic driving task (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).
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 her / 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.
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 a system against intentional subversion or forced failure.
Sensor	A device that responds to a physical stimulus (such as heat, light, sound, pressure, magnetism or a particular motion) and transmits a resulting impulse that can be interpreted as a measure by an instrument / observer.

Term	Definition
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 the final objective of transitioning it to the user. One scale to describe or rate the maturity is the technology readiness level.
Test Scenario	The test setup in which a scenario is 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, organisation or individual.
Triggering Event	Specific condition of a driving scenario that serves 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 is 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 determining whether the system has the required functionalities and whether these functionalities are working as intended, without errors, considering certain constraints.

Term	Definition
Vulnerability	A weakness of an asset or a 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 motorcyclists and persons with disabilities or reduced mobility and orientation.

List of Abbreviations and Acronyms

Abbreviation	Meaning
AD	Automated Driving
ADAS	Advanced Driver Assistance Systems
ADF	Automated Driving Function
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

Abbreviation	Meaning
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
OEM	Original Equipment Manufacturer
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)

www.L3Pilot.eu
Twitter @_L3Pilot_
LinkedIn L3Pilot



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



Supported by the European Council
for Automotive R&D