Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Guidelines and recommendations for ADS safety requirements, assessments and test methods to inform regulatory development

Section 1. Introduction

In 2015, the World Forum for Harmonization of Vehicle Regulations (WP.29) established a programme under the Intelligent Transport Systems (ITS) informal working group to focus on automated driving (ITS/AD).

During its 174th (March 2018) session, WP.29 approved a proposal from the ITS/AD informal group for a "Reference document with definitions of Automated Driving under WP.29 and the General Principles for developing a UN Regulation on automated vehicles".[1]

In March 2018, ITS/AD established a Task Force on Automated Vehicle Testing (TFAV) "to develop a regulatory testing regime that assesses a vehicle's automated systems so as to realise the potential road safety and associated benefits under real life traffic conditions".[2]

TFAV established subgroups to consider AV assessment methods:

- Physical certification tests and audit
- Real-world test drive.

In October 2018, TFAV proposed creating an informal working group on Validation Methods for Automated Driving (VMAD) "to develop methods to assess the safety of driving performance of automated driving systems including safe responses to the environment as well as safe behaviour towards other road users":

- In a controlled environment,
- Via audit of OEM processes,
- Under simulation and virtual testing, and
- Under real-world conditions.

During its 178th (June 2019) session, WP.29 approved a Framework Document on Automated/Autonomous Vehicles.[3]

The Framework Document provides "guidance to WP.29 subsidiary Working Parties (GRs) by identifying key principles for the safety and security of automated/autonomous vehicles of levels 3 and higher."[4]

[1] ECE/TRANS/WP.29/2018/2 as amended by paragraph 31 of the session report ECE/TRANS/WP.29/1137 and consolidated in ECE/TRANS/WP.29/1140.

[2] TFAV-02-12

[3] ECE/TRANS/WP.29/2019/34/Rev.2 and ECE/TRANS/WP.29/1147 Annexes V and VI.

[4] The Framework Document refers back to the Automated Driving definitions provided in the reference document ECE/TRANS/WP.29/1140 noted in para. 1.2. The reference document cites SAE J3016:2016 as its source for establishing levels of driving automation (1-5).

The Framework Document established a safety vision and identified key issues and principles for work under WP.29:

- System safety
- Failsafe response
- Human Machine Interface/operator information
- Object and Event Detection and Response
- Operational Design Domain
- Validation for System Safety
- Cyber security
- Software updates
- Event Data Recorder and Data Storage System for Automated Driving.

The Framework Document identified three additional issues not listed in the agreed WP.29 priorities:

- Remote operation
- Safety of in-use vehicles
- Consumer education and training

Table 1 of the Framework Document allocated work on these WP.29 priorities across several informal working groups:

- Functional Requirements for Automated Vehicles (FRAV)
- Validation Methods for Automated Driving (VMAD)
- Cyber Security and Over-the-Air Software Updates (CS/OTA)
- Event Data Recorders/Data Storage Systems for Automated Driving (EDR/DSSAD).

Terms of reference mandated FRAV to develop functional (performance) requirements for automated vehicles, addressing:

- System safety
- Failsafe Response
- HMI /Operator information
- OEDR (functional requirements).[5]

Terms of reference mandated VMAD to develop a new assessment/test method (NATM) "to validate the safety of automated systems based on a multi-pillar approach" including:

- Scenarios
- Audit
- Simulation/virtual testing
- Test track
- Real-world testing.[6]

[5] ECE/TRANS/WP.29/1147/Annex V.

[6] ECE/TRANS/WP.29/1147/Annex VI.

During its June 2021 session, WP.29 endorsed a draft "New Assessment/Test Method for Automated Driving (NATM) - Master Document" submitted by GRVA that proposed a multi-pillar approach comprised of:

- A scenario catalogue
- Simulation/virtual testing
- Track testing
- Real world testing
- Audit/assessment procedures
- In-service monitoring and reporting.[7]

Through subsequent revisions to Table 1 of the Framework Document, WP.29 directed FRAV and VMAD to deliver, respectively, for its June 2023 session:

- Guidelines for regulatory requirements and for verifiable criteria for ADS safety validation, and
- Guidelines for NATM.[8]

WP.29 further directed FRAV and VMAD to collaborate and deliver a consolidated FRAV/VMAD submission (requirements and assessment methods) for its June 2024 session.

During the June 2023 session, WP.29 reviewed and endorsed documents submitted by GRVA presenting the guidelines prepared by FRAV and VMAD (per para. 1.13).[9]

Between 2019 and 2023, some 200 experts participated in nearly 80 FRAV and VMAD sessions to develop this document.

Section 2. Scope and purpose

This document aims to fulfil the FRAV and VMAD mandates and deliver the consolidated deliverable per the Framework Document described above.

The document proposes guidelines and recommendations for the establishment of safety requirements and assessment methods applicable to ADS vehicles as defined in Section 3.

These guidelines cover ADS vehicles which operate on publicly accessible roadways (including parking areas and private areas that permit public access) that collectively serve all road users (if allowed by the road characteristics), including cyclists, pedestrians, and users of vehicles with and without driving automation features.

The diversity of ADS vehicle configurations and the characteristics and constraints of their ODD present challenges in establishing harmonized requirements for worldwide use. These guidelines recommend the establishment of high-level requirements to cope

[7] ECE/TRANS/WP.29/2021/61 (ECE/TRANS/WP.29/1159)

[8] ECE/TRANS/WP.29/2019/34/Rev.2, ECE/TRANS/WP.29/2021/151, ECE/TRANS/WP.29/2023/43.

[9] WP.29-190-08 later superseded by WP.29-191-07 in November 2023 (FRAV safety recommendations) and WP.29/2023/44/Rev.1 (VMAD guidelines).

with this diversity. The guidelines propose a framework for applying these high-level requirements to individual ADS use cases.

The complexity of driving also presents challenges to the assessment of ADS performance across the diversity of possible ODD. These guidelines recommend a multi-pillar approach to ensure comprehensive and efficient validation of ADS safety. The guidelines recommend the future development of a scenario catalogue for use across five validation pillars:

- Audit and safety-by-design assessment
- Simulation/virtual testing
- Track testing
- Real-world testing
- In-service monitoring and reporting.

These guidelines and recommendations are intended to support future initiatives that WP.29 may decide to initiate under the 1958, 1997, and/or 1998 Agreements.

Usage of the verbal forms “shall” (indicating an obligatory provision) and “may” (indicating a permissive provision) in this document should be understood within the context of providing such recommendations.

The guidelines recommend technology-neutral and evidence-based requirements and methods for objective, repeatable, and reproducible assessments within a framework that can adapt to technological progress.

Section 3. Terms and definitions

This section defines terms used in this document. Use of these terms and their definitions is recommended in the development of legal requirements related to ADS and ADS vehicles.

“Abstraction” means a process of selecting relevant aspects of a source or referent system to be represented in a model or simulation.[10]

“Automated Driving System (ADS)” means the vehicle hardware and software that are collectively capable of performing the entire Dynamic Driving Task (DDT) on a sustained basis.[11]

[10] Any modelling abstraction carries with it the assumption that it should not significantly affect the intended uses of the simulation tool.

[11] This definition is based on SAE J3016 and ISO/PAS 22736 (Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles). These standards define levels of driving automation based on the functionality of the driving automation system feature as determined by an allocation of roles in DDT and DDT fallback performance between that feature and the (human) user (if any). The term “Automated Driving System” is used specifically to describe a Level 3, 4, or 5 driving automation system.

"ADS feature" means an application of an ADS designed specifically for use within an Operational Design Domain (ODD).

"(ADS) function" means an ADS hardware and software capability designed to perform a specific portion of the DDT.

"ADS vehicle" means a vehicle equipped with an ADS.

"Behavioural competency" means an expected and verifiable capability of an ADS feature to operate a vehicle within the ODD of the feature.

"Closed-loop testing" means testing in an environment in which actions of the ADS hardware, software, or other element(s) in the loop influence the actions of other objects in the simulation.[12]

"Open-loop testing" means testing in an environment in which the actions of the ADS hardware, software, or other element(s) in the loop do not affect the actions of other objects in the simulation.[13]

"Stochastic" means a process involving or containing a random variable or variables pertaining to chance or probability.

"Driver" means a human user who performs in real time part or all of the DDT and/or DDT fallback for a particular vehicle.

"Dynamic Driving Task (DDT)" means the real-time operational and tactical functions required to operate the vehicle.

When the ADS is in operation, the DDT is always performed in its entirety by the ADS which means the whole of the tactical and operational functions necessary to operate the vehicle (i.e., the ADS performs "the entire DDT" as stated in the definition of an "Automated Driving System" under para. 3.2.). These functions can be grouped into three interdependent categories: sensing and perception, planning and decision, and control.

Sensing and perception include:

- Monitoring the driving environment via object and event detection, recognition, and classification.
- Perceiving other vehicles and road users, the roadway and its fixtures, objects in the vehicle's driving environment and relevant environmental conditions.
- Sensing the ODD boundaries, if any, of the ADS feature.
- Positional awareness.

Planning and decision include:

- Predicting actions of other road users.
- Response preparation.
- Manoeuvre planning.

[12] For example, evaluating ADS interactions with other objects that respond to the actions of the ADS within a traffic model.

[13] For example, evaluating ADS interaction with a recorded traffic situation.

Control includes:

- Object and event response execution.
- Lateral vehicle motion control.
- Longitudinal vehicle motion control.
- Enhancing conspicuity via lighting and signalling.

The DDT excludes strategic functions.

“Strategic function” means a capability to issue commands, instructions, or guidance for execution by an ADS.[14]

“Tactical function” means a capability to perceive the vehicle environment and control real-time planning, decision, and execution of manoeuvres, including conspicuity of the vehicle and its motion.[15]

“Operational function” means a capability to control the real-time motion of the vehicle.[16]

“Edge Case” means a low-frequency occurrence that might arise within the ODD of an ADS and warrants specific design attention due to the potential severity of outcomes that might result from encountering such a situation or condition across a full-scale deployed fleet of such ADS vehicles.[17]

“ADS fallback response” means a system-initiated deactivation of the ADS or an ADS-controlled procedure to place the vehicle in a minimal risk condition.

“Fallback user” means a user designated to perform the DDT pursuant to an ADS fallback response.

“Minimal Risk Condition (MRC)” means a stable and stopped state of the vehicle that reduces the risk of a crash.

“Model” means a description or representation of a system, entity, phenomenon, or process.

“Model calibration” means a process of adjusting numerical or modelling parameters in a model to improve agreement with a referent.

“Model parameter” means a numerical value inferred from real-world data and used to characterise a system functionality.

“*Occurrence*” means a safety-relevant event involving an ADS vehicle.

[14] Examples include setting the starting point, destination, route, and way points to be used by an ADS during a trip.

[15] Examples include deciding whether to overtake a vehicle or change lanes, signalling intended manoeuvres, deciding when to initiate the manoeuvre, choosing the proper speed, and executing the manoeuvre.

[16] Operational functions involve executing micro-changes in steering, braking, and accelerating to maintain lane position or proper vehicle separation and immediate responsive actions to avoid crashes in critical driving situations.

[17] Examples include a unique road sign or an unusual animal type in the roadway.

"*Non-critical Occurrence*" means an operational interruption, defect, fault, or other circumstance that influenced or may have influenced ADS safety but did not result in a collision or serious incident.[18]

"Critical Occurrence" means an occurrence during which at least one of the following criteria is fulfilled:

(a) at least one person suffers an injury that requires medical attention or dies as a result of being in the vehicle or being involved in the event.

(b) the ADS vehicle, other vehicles or stationary objects sustain physical damage that exceeds a certain threshold.

(c) any vehicle involved in the event experiences an airbag deployment.

"*Operational Design Domain (ODD)*" means the operating conditions under which an ADS feature is specifically designed to function.

"*ODD exit*" means:

(a) the presence of one or more ODD conditions outside the limits defined for use of the ADS feature, and/or

(b) the absence of one or more conditions required to fulfil the ODD conditions of the ADS feature.[19]

"Other road user (ORU)" means any entity making use of publicly accessible road infrastructure.

"Priority vehicle" means a vehicle subject to exemptions, authorizations, and/or right-of-way under traffic laws while performing a specified function.

"Proving ground" and "*Test track*" mean a facility closed to public traffic and designed to enable physical assessment of an ADS and/or ADS vehicle performance, e.g., via sensor stimulation and/or the use of dummy devices.

"Real time" means the actual time during which a process or event occurs.

"Road-safety agent" means a human being engaged in directing traffic, enforcing traffic laws, maintaining/constructing roadways, and/or responding to traffic incidents.

"Safety case" means a structured argument supported by a body of evidence that provides a compelling, comprehensible, and valid case that the ADS is or will be free from unreasonable risk for a given application in a given environment.

[18] Examples include minor incidents, safety degradation not preventing normal operation, emergency/complex manoeuvres to prevent a collision, and more generally all occurrences relevant to the safety performance of the in-service ADS (like transfer of control, interaction with remote operator, etc.).

[19] ODD conditions are distinct from ADS capabilities. An ADS may be designed to manage transient changes in the operating environment where such transient changes do not represent an ODD exit.

“Safety concept” means a description of the measures designed into the ADS so that it operates in such a way that it is free of unreasonable safety risks to the ADS vehicle user(s) and other road users in every operating condition relevant to the ODD.

“Sensor Stimulation” means a technique whereby artificially generated signals are provided to trigger the element under testing in order to produce the result required for evaluation of the element.

“Simulation” means the imitation of the operation of a real-world process or system over time.

“Simulation toolchain” means a combination of simulation tools that are used to support the validation of an ADS.

“Test case specification” means the detailed specifications of what must be done by the tester to prepare for the test.

“Test method” means a structured approach to consistently derive knowledge about the ADS by means of executing tests.[20]

“Traffic scenario” means a description of a sequence of driving situations that may occur during a given trip.[21]

“Nominal scenario” means a traffic scenario representing usual and/or expected objects, object behaviours and/or road conditions.

“Critical scenario” means a traffic scenario representing unusual and/or unexpected objects, object behaviours, and/or road conditions.

“Failure scenario” means a traffic scenario representing a system failure that compromises the capability of the ADS to perform the entire DDT.

“Functional scenario” means a basic traffic scenario describing a situation and its corresponding elements at the highest level of abstraction in natural, non-technical language.[22]

“Abstract scenario” means a formalized, declarative description of a scenario derived from a functional scenario.[23] The specification on the abstract level enables highlighting of the relevant aspects of the scenario while focusing on efficient description of relations (cause-effect).

[20] For example, virtual testing in simulated environments, physical, structured testing in controlled test-facility environments, and real-world on-road conditions.

[21] Scenarios include a driving manoeuvre or sequence of driving manoeuvres. Scenarios can also involve a wide range of elements, such as some or all portions of the DDT, different roadway layouts, different types of road users and objects exhibiting static or diverse dynamic behaviours, and diverse environmental conditions (among many other factors).

[22] For example, a description of the ego vehicle’s actions, the interactions of the ego vehicle with other road users and objects, and other elements that compose the scenario such as environmental conditions.

[23] Declarative descriptions can include structured natural language, programming language or other forms of languages that meet the required criteria (formalized and declarative).

"Logical scenario" means a traffic scenario elaborated at a lower level of abstraction to include value ranges or probability distributions for each element of the corresponding functional scenario.[24]

"Concrete scenario" means a traffic scenario at a level of abstraction in which specific values have been selected for each element from the continuous ranges as may be defined in the corresponding logical scenario.

"Complex scenario" means a traffic scenario containing one or more situations that involve a large number of other road users, unlikely road infrastructure, or abnormal geographic/environmental conditions.

System-initiated deactivation of the ADS means a procedure by which the ADS initiates the transfer of performance of the DDT from the ADS to a vehicle user.

User-initiated deactivation of the ADS means a procedure by which the user initiates the transfer of performance of the DDT from the ADS to a vehicle user.

"(ADS) User" means a human user of an ADS vehicle.

"Useful life (of an ADS vehicle)" means the duration during which an ADS vehicle is in an operational state under which it may be driven on public roads regardless of the operational state of the ADS.

"Validation of the simulation model" means the process of determining the degree to which a simulation model is an accurate representation of the real world from the perspective of the intended uses of the tool.

"Verification of the simulation model" means the process of determining the extent to which a simulation model or a virtual testing tool is compliant with its requirements and specifications as detailed in its conceptual models, mathematical models, or other constructs.

"Virtual testing" means the process of testing a system using one or more simulation models.

"Driver-In-the-Loop" *(DIL*) means a driving simulator with components to enable the driver to operate in and communicate with the virtual environment and used to assess the human-automation interaction design.

"*Hardware-In-the-Loop*" (HIL) means the hardware of a specific vehicle subsystem running the software with input and output connected to a simulation environment to replicate sensors, actuators, and/or mechanical components in a way that connects all the I/O of the Electronic Control Units (ECU) before the final system is integrated.

"Model-In-the-Loop" (MIL) means high-level-of-abstraction software frameworks running on general-purpose computing systems to enable quick algorithmic development without involving dedicated hardware.

[24] For example, elaborating the lane element to cover possible lane widths.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

“Software-In-the-Loop” (SIL) means a methodology where executable code such as algorithms, an entire controller strategy, or a complete software implementation is assessed within a modelling environment on general-purpose computing systems.

“Vehicle -In-the-Loop” (VIL) means a fusion of real-world and virtual environments to assess the dynamics of a physical ADS vehicle on a vehicle test bed or a test track at the same level as real-world testing.

Section 4. Overview of ADS safety requirements, assessment, and validation

These recommendations concern the assessment and validation of ADS safety within a regulatory context. This section summarizes key aspects of the guidelines and their application to produce an efficient, comprehensive, and coherent assessment.

Driving can be viewed as an exercise in risk management within the context of achieving strategic goals. An ADS must demonstrate the competency to operate the vehicle safely, to respond to external conditions, and to manage internal failures.

Moreover, the ADS must be designed to ensure safe use and the safety of its users throughout the useful life of the vehicle.

These guidelines address the conditions an ADS might be expected to encounter via a framework for the development of traffic scenarios under which an ADS should be assessed. Establishment of scenarios depends primarily on analysis of the Operational Design Domain(s) (ODD) within which the ADS will operate (see Annex 3).

The framework differentiates among nominal, critical, and failure scenarios. Nominal scenarios enable assessment of the ADS competency to operate the vehicle safely. Critical scenarios enable assessment of the ADS competency to manage conflicts and mitigate external risks. Failure scenarios enable assessment of the ADS competency to manage and respond to system failures.

This framework focuses on subjecting the ADS to these scenarios and assessing the behavioural competencies demonstrated by the ADS under each scenario against requirements for performance of the Dynamic Driving Task (DDT). These requirements focus on desired driving capabilities and outcomes. The requirements intentionally avoid technical specifications and performance limits because each traffic situation requires a response appropriate to its combination of elements, risks, and available options.

Under nominal scenarios, an ADS is expected to demonstrate behavioural competencies consistent with the requirements for DDT performance. For example, one of those competencies would be the ability to minimise risks of getting into critical situations through the exercise of competent and careful driving.

However, defining performance criteria in critical scenarios might prove difficult, especially under conditions where requirements must be prioritised. In these cases, the framework proposes the use of appropriate safety models to enable assessment of ADS performance within the limits of the safety model(s).[25] For example, it is recognised that an ADS might not be able to avoid a collision, so the ADS performance needs to be compared with safety-model performance to set the threshold where avoidance is required and that where avoidance is not feasible, and if mitigation may be possible.

[25] These guidelines refer to some illustrative models but do not specify which may be appropriate or seek to limit the use of appropriate safety models.

In cases where the behavioural competency demonstrated by the ADS involves such exceptions, the framework relies on safety models to determine whether the exceptions are justified. For example, an ADS might violate a lane restriction in order to avoid a collision. The safety model enables determinations on the collision risk, the ADS response, and the necessity of the traffic-rule violation.

Failure scenarios address situations where the ADS performance of the DDT has been compromised by a system fault. Unless a fallback user manages the response to the fault, the ADS is expected to bring the vehicle to a safe, stopped condition (i.e., a minimal risk condition). However, depending on the severity of the fault, the safety requirements allow the ADS to adapt its performance of the DDT to the nature of the fault. This tolerance permits an ADS where possible to mitigate risks while reaching a safe location to stop the vehicle.

The guidelines recommend consolidation of these scenarios into a scenario catalogue that may be used under the NATM to systematically validate the safety of an ADS.

These guidelines address the safety of ADS vehicle users via sets of requirements aligned with the relationships that users might have with a given ADS during use of the ADS vehicle. These relationships can vary depending on whether a user is located inside or outside the ADS vehicle, the degree(s) of control that a user may exercise over the vehicle during a trip, and whether a user has a one-to-one relationship with a single vehicle or may be performing functions relative to multiple vehicles.

Regardless of any assistance systems, drivers perform the DDT until they activate an ADS feature. An ADS feature is specific to an ODD. Activation of an ADS feature initiates ADS performance of the tactical and operational functions required to perform the entire DDT within the ODD of the feature. In the context of the driver relationship, the vehicle is moving (i.e., the user is driving the vehicle) and the activation involves a transition of control over vehicle operation from the driver to the ADS.

Upon activation of a feature, the ADS performs the entire DDT necessary to operate the vehicle within the ODD of the feature. The driver, therefore, shifts to the role of fallback user or passenger. Some ADS designs may initiate a system-initiated deactivation of the ADS (i.e., fall back to the user) in the event that the ADS can no longer perform the DDT (e.g., prior to reaching the boundary of the ODD of the feature in use).

A passenger has no capabilities to perform the DDT. Nonetheless, passengers require means to select destinations, routes, and stops and therefore have necessary interactions with the ADS.

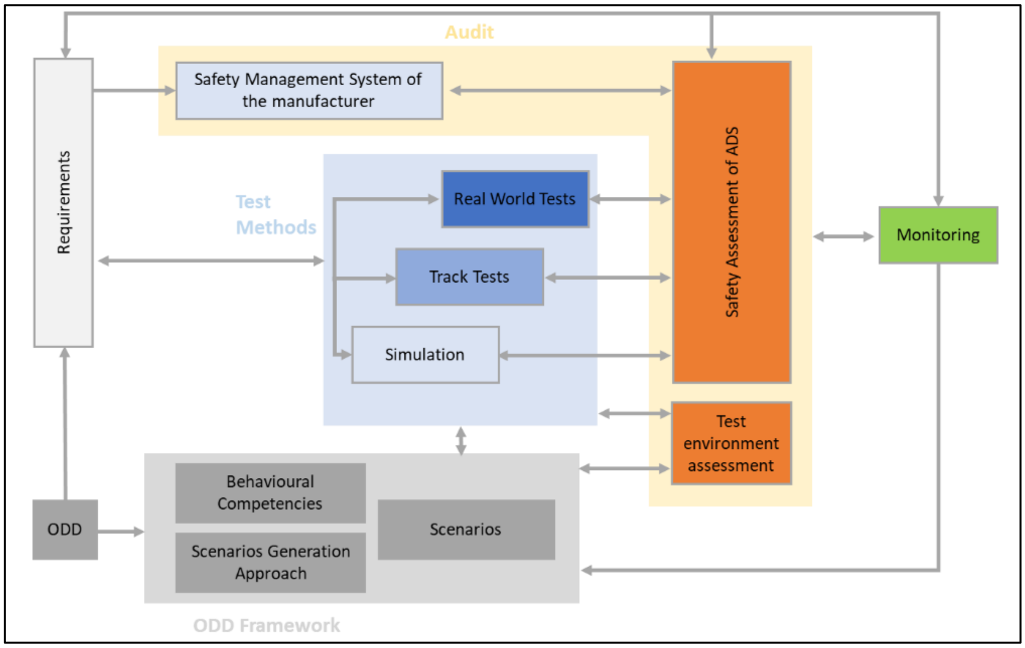
These guidelines propose principles and specifications to ensure the safety of users and their use of ADS vehicles across these relationships. The guidelines recognise that additional relationships might need consideration in the further development of such safety requirements.

The assessment of an ADS for compliance with these safety recommendations rests on five validation pillars:

1. Documentation and audit
2. Virtual testing
3. Track testing
4. Real-world testing
5. In-service monitoring and reporting.

These pillars are intended for use in combination(s) to produce an efficient, comprehensive, and coherent assessment of ADS compliance with the guidelines on safety performance. Each of the testing methodologies possesses its own strengths and limitations, such as differing levels of environmental control, environmental fidelity, scalability, and cost, which should be considered. In some cases, the application of more than one method could be necessary to assess the capability of an ADS to cope with range of situations that can arise in real-world traffic. The use of multiple methods allows for flexibility in the composition, sequencing, and application of testing across the diversity of ADS while avoiding unnecessary redundancies and overlaps. Figure 1 below illustrates relationships across the ADS safety requirements, ODD analysis and scenario generation, and the validation pillars.

Figure 1. Relationships across safety requirements, ODD analysis and scenario generation, and validation pillars



The pillars concern Audit, Test Methods, and In-Service Monitoring and Reporting.

Audit

ADS technologies generate diverse vehicle configurations, intended uses, and limitations on use across operating environments. Therefore, the assessment of an ADS vehicle must be based on a clear understanding of the ADS to be evaluated.

Under these guidelines, the manufacturer is required to furnish documentation covering:

- The ODD of each ADS feature
- Traffic scenarios relevant to each ODD
- Manufacturer’s validation of the ADS
- ADS design safety
- Manufacturer’s ADS safety management system

The Audit pillar concerns the evaluation of this documentation to verify the robustness of the manufacturer’s development and validation of the ADS and capabilities to assure ADS safety after deployment.

Test Methods

Virtual testing provides means to assess ADS performance across a wide range of traffic scenarios efficiently. These guidelines recommend procedures for evaluating the reliability of the manufacturer’s virtual testing tool chains and methodologies. This credibility assessment enables confidence in applying these tools and methods, and the evidence they generate, to the assessment of ADS safety (see Annex 5).

Virtual testing uses different types of simulation toolchains to assess compliance of an ADS with safety requirements across a wide range of traffic scenarios, including some of which would be difficult (if not impossible) to reproduce in physical settings.

The toolchain methodologies include (but are not necessarily limited to):

- Model in the Loop (MIL)
- Software in the Loop (SIL)
- Hardware in the Loop (HIL)
- Vehicle in the Loop (VIL)
- Driver in the Loop (DIL)

Virtual testing enables efficient assessment across nominal, critical, and failure scenarios and ranges of parameters within scenarios relevant to the ADS configuration, intended uses, and limitations on use, including determination of the boundaries between collision avoidance and crash mitigation. Virtual testing also enables assessment of compliance with safety requirements relevant to user interactions, especially through DIL and similar “user in the loop” methodologies.

Virtual testing may be more suitable when there is a need to vary test parameters and a large number of tests need to be carried out to support efficient scenario coverage (e.g., for path planning and control, or assessing perception quality with prerecorded sensor data).

Virtual testing enables identification of scenarios that result in exceptions to nominal DDT performance requirements (e.g., deviation from traffic rules, evasive manoeuvres, collision outcomes) for assessment based on safety models.

Methods of randomization of parameters and scenario composition enable ADS performance assessments under critical scenarios, including low probability events.

Virtual testing enables the identification of high-value scenarios that can be applied to track testing. After ADS deployment, virtual testing can contribute to the analysis of ADS behaviours inconsistent with behavioural competencies demonstrated during the original assessment.

Track testing concerns the physical assessment of ADS performance under controlled conditions on closed-access grounds. For these reasons, track testing may be best suited to assessment of ADS performance under scenarios that entail significant safety risks in case of failure to meet the requirements, where performance can be assessed through a discrete number of physical tests, and where testing benefits from the capacity to control conditions (e.g., for HMI and fallback responses, under critical scenarios).

Having determined performance boundaries and identified situations involving ADS responses to manage conflicts and mitigate risks under the virtual testing, concrete test scenarios can be defined for track testing based on the parameters of the corresponding virtual scenarios. Comparison of performance between a virtual test and a track test when executing the same scenario enables assessment of the accuracy of the virtual testing toolchain.

Real-world testing assesses the capability of the ADS to perform the DDT and its interactions with its user(s) while in operation on public roads under real-world traffic conditions. Real-world testing may be more suitable to ensure a level of fidelity that might not be represented virtually or on a test track (e.g., interactions with other road-users and perception capabilities).

The primary aim is to verify compliance with safety requirements for DDT performance under normal operational and road conditions and for nominal ADS interactions with its user(s).

While this method provides a high degree of environmental fidelity for testing an ADS, constraints on time, cost, controllability, reproducibility, and safety assurance limit the feasibility of covering traffic scenarios in the strict sense.

Therefore, this method requires attention to designing test routes that capture predictable aspects of the ODD (e.g., road types and geometries), elements found in the related nominal scenarios (e.g., other road users, signs, and signals), and typical dynamic conditions (e.g., high/low traffic densities). The test routes should also enable verification of nominal requirements for the safety of user interactions, including prior to, at the time of, and after entering and exiting the ODD of an ADS feature.

To the extent that an ADS encounters critical or failure situations during a real-world test drive, the response of the ADS, including exceptions to the nominal performance requirements, should be considered in conjunction with the outcomes of track and virtual testing.

In-Service Monitoring and Reporting

In addition to initial assessments of ADS safety, the guidelines also recommend post-deployment assessment of ADS performance under an In-Service Monitoring and Reporting (ISMR) pillar.

The guidelines recommend that manufacturers monitor the performance of their in-service ADS vehicles and report safety-relevant information to the safety authority.

The monitoring requires manufacturers to collect and analyse information representative of in-service ADS performance to:

(a) Identify safety concerns, including predictive monitoring for trends indicative of emerging risks,

(b) Identify instances of ADS performance inconsistent with the safety requirements and/or behavioural competencies demonstrated during the original assessment, and

(c) Characterise beneficial and adverse occurrences.

(d) Ongoing validation of the safety concept.

The reporting requires manufacturers to inform the safety authority in the short-term and periodically concerning the above in order to:

(a) Ensure the implementation of remedial actions to address the identified safety concerns,

(b) Assess the impact of ADS use on road safety,

(c) Improve ADS safety assessments, including addition of new traffic scenarios, and

(d) Efficiently disseminate information to enable continuous improvement of ADS safety performance.

As noted above, the manufacturer must evidence its capability to perform this monitoring of its ADS vehicles in use during the Audit assessment.

Section 5. Audit, Safety Assessment, and Manufacturer’s System Documentation

Introduction

An audit of the ADS manufacturer’s safety management system and a safety assessment of the ADS manufacturer’s safety case, including its safety-by-design concept, referred to hereafter as the “safety concept” (see definition above), are important validation pillars. To enable this audit and safety assessment, the ADS manufacturer might be required to provide certain documentation. In some jurisdictions, the audit and safety assessment will be performed directly by an approval authority, while in other jurisdictions, the relevant authority may enlist an independent entity to conduct these functions.

Purpose and Elements of the Audit Pillar

The purpose of the audit pillar is to facilitate a determination that:

- The manufacturer has the right processes to ensure operational and functional safety during the vehicle lifecycle, and
- The vehicle’s ADS is safe by design and that the design has been sufficiently validated before market introduction.

Therefore, this pillar is composed of two main components: the audit of the manufacturer processes established through a safety management system and the evaluation (i.e., safety assessment) of the safety case provided by the manufacturer, including the safety of the ADS design.

It is recommended that the manufacturer be required to demonstrate that:

(a) Robust processes are in place to ensure safety throughout the vehicle's lifecycle (development, production, operation, and decommissioning). This shall include taking the right measures to monitor the vehicle during the in-service operation and to take appropriate (corrective or preventive) action to address any issues,

(b) The hazards and risks of the ADS have been identified and it is clear that the manufacturer's safety concept exists and had been applied to mitigate them through a safety-by-design approach, and

(c) The risk assessment and the safety concept have been validated, through testing, by the manufacturer and show that the vehicle meets the safety requirements before market introduction. The vehicle should be free of unreasonable safety risks to the broader transport ecosystem, and in particular, to the ADS vehicle user(s) and other road users. Based on the evidence provided by the manufacturer in its safety case and confirmatory tests conducted by or for the safety authority, authorities will be able to assess whether the processes, the risk assessment, the design, and the validation are robust enough with regard functional and operational safety.

Documentation to be provided

To facilitate the approval authority's audit and safety assessment, the ADS manufacturer should provide certain specific documentation.

It is recommended that the documentation package shows that the ADS:

(a) Is designed and was developed to operate in such a way that it is free from unreasonable risks for the ADS vehicle user(s) and other road users within the declared ODD.

(b) Respects any applicable performance requirements concerning performance of the DDT and interaction with ADS users.

(c) Was developed according to the development process/method declared by the manufacturer.

Documentation should be made available in three parts:

(a) An information document which is submitted to the authority and should contain a brief overview of the separate documents provided.

(b) For the purpose of conducting the audit, a complete description of the manufacturer's Safety Management System.

(c) For the purpose of conducting the safety assessment, a complete safety case[26] for the ADS and its features, including a description of the design processes used to implement the safety concept, and a structured presentation demonstrating through a body of evidence that the ADS and its feature have undergone sufficient safety validation to ensure an absence of unreasonable risk in the ADS's performance.

Rather than including such information in the documentation submitted to the approval authority, additional confidential material and analysis data (intellectual property) should be retained by the manufacturer but made open for inspection (e.g. on-site in the engineering facilities of the manufacturer) at the time of the product assessment / process audit.

The manufacturer should ensure that this material and analysis data remains available for a period of 10 years counted from the time when production of the ADS is discontinued. Any changes to ADS safety design should be communicated as required to the relevant authority.

Safety Management System

The purpose of the audit of the manufacturer's safety management system is to confirm that the manufacturer has robust processes to manage safety risks and to ensure safety throughout the ADS lifecycle (development, production, operation and decommissioning). It should include taking appropriate measures to monitor the vehicle during the in-service operation and to take the corrective remedial action when necessary.

An SMS is a systematic approach to managing safety, which encompasses and integrates organizational, human and technical factors:

(a) Human component ensuring the ADS lifecycle is monitored by personnel with appropriate skills, training, and understanding to identify risks and appropriate mitigation measures,

(b) Organisational component procedures and methods that help to manage the identified risks, understand their relationships and interactions with other risks and mitigation measures, and help to ensure that there are no unforeseen consequences.

(c) Technical component using appropriate tools and equipment.

An adequate SMS will incorporate all three factors to monitor and improve safety and help to control the identified risks. The SMS evaluation is based on automotive (or

[26] Although a manufacturer's safety case entails documentation of the manufacturer's own assessment of its processes, design, production, and validation testing to ensure the safety of the ADS, this document uses "safety assessment" to describe the evaluation of the safety case by the authority.

other industry) engineering standards, guidebooks, and best practice documents relevant to safety.

Safety Policy

It is recommended that a safety policy be included in the SMS to outline the aims and objectives that the organisation will use to achieve the desired safety outcomes. The policy should declare the principles and philosophies that lay the foundation for the organisation’s safety culture and be communicated to all staff throughout the organisation. The creation of a positive safety culture begins with clear, unequivocal safety governance.

The processes and activities that are recommended to be documented by the manufacturer include:

(a) Safety policies and principles (in line with the concept stated in ISO 21434, para. 5.4.1 and ISO 9001 Automotive 5.2,)

(b) Organisation safety objectives and the process for creating safety performance indicators used in the safety case

(c) Appropriate structure for SMS, taking into account regulation, standards, best practice guidance and the use-case of the vehicle and mapping its organisation structure, processes, and work products onto the SMS.

(d) Safety culture (ISO 26262-2, para. 5.4.2)

(e) Safety Governance elements including: (i) Management commitment (in line with the concept stated in ISO 21434, para. 5.4.1 and ISO 9001 Automotive 5.1 (ii) Roles and responsibilities (ISO 26262-2, para. 6.4.2, this relates to the organizational and project dependent activities)

(f) Effective communications within the organization on safety issues (ISO 26262-2, para. 5.4.2.3)

(g) Information sharing outside of the organization (in line with the concept stated in ISO 21434, para. 5.4.5 and ISO 9001, but from a safety perspective)

(h) Quality Management System (e.g., as per IATF 16949 or ISO 9001 or equivalent) to support safety engineering, including change management, configuration management, requirement management, tool management etc.

Risk Management

It is recommended to include in the SMS a Safety risk management process to identify and assess the risks associated to the three SMS factors described above (i.e., human, organizational, and technical). Any operational risk identified in the product should, where appropriate, have mitigations implemented during the Design and Development phase. The ADS manufacturer should then be able to show the link between the overall risk management process, the mitigations, and the resulting operational risks.

Examples of risk management processes and activities that are recommended to be documented by the manufacturer:

(a) Risk identification (in line with ISO 31000 para. 6.4.2 standard or equivalent)

(b) Risk analysis (in line with ISO 31000 para. 6.4.3 standard or equivalent)

(c) Risk evaluation (in line with ISO 31000 para. 6.4.4 standard or equivalent)

(d) Risk treatment (in line with ISO 31000 para. 6.4.5 standard or equivalent),

(e) Processes for keeping the risk assessments up to date, 14

(f) Review of safety performance of the organization and effectiveness of safety risk controls.

Design and Development Process

It is recommended that the design and development process is well established and documented in the SMS. It should include risk management, requirements management, requirements' implementation, testing, failure tracking, remedial actions, and release management. Examples of processes and activities that should be considered to assure that responsibilities are properly discharged:

(a) Roles and responsibilities of the people involved during the design and development phase.

(b) Qualifications and experience of persons responsible for making decisions that affect safety.

(c) Coordination of roles, responsibilities and information transfer between design and production activities.

Examples of processes and activities that should be documented to ensure the robustness of the design and development phase:

(a) A general description of how the organization performs all the design and development activities.

(b) Vehicle/system development, integration, and implementation.

(i) Requirements management (e.g. Requirement capture and validation).

(ii) Validation strategies, including but not limited to:

a. Assessment of the physical testing environment

b. Credibility assessment for virtual tool chain

c. System integration

d. Software

e. Hardware

(iii) Management of functional Safety and operational safety, including the ongoing evaluation and update of risk assessments and interactions.

(iv) Management of Human Factors (e.g. Human-centred design processes).

(c) Design and change management, including but not limited to:

(i) The major design decisions,

(ii) The relevant design modifications to the ADS

(iii) The personnel involved in the design

(iv) The tools and thresholds adopted for the ADS safety verification.

It is recommended that the manufacturer institutes and maintains effective communication channels between the departments responsible for functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.

Production and Deployment Process

It is recommended that the production process is well established and documented in the SMS. Examples of processes and activities that are recommended to be documented to ensure the robustness of the development and the production phase include:

(a) Quality Management System accreditation (e.g., as per IATF 16949 or ISO 9001 or equivalent).

(b) A description of the way in which the organisation performs all the production functions including management of working conditions, working environment, equipment and tools.

Examples of processes and activities to be documented to assure robustness of development and distributed production:

(a) Liaison between the vehicle and/or ADS manufacturer and all other organisations (partners or subcontractors) involved.

(b) Criteria for the acceptability of “subsystem/components” manufactured by other partners or subcontractors. (i.e., deployment of production assurance requirements to supply chain).

It is recommended that the manufacturer demonstrate that periodic independent internal audits and external audits are carried out to ensure that the processes established for the Safety Management System are implemented consistently.

It is recommended that the SMS include a robust process to ensure that post-deployment software updates are properly validated and distributed and downloading is confirmed.

It is recommended that the manufacturer put in place suitable arrangements (e.g., contractual arrangements, clear interfaces, quality management system) with any organization involved in the development, manufacturing, or in-use deployment of its vehicles (e.g., contracted suppliers, service providers, or manufacturers’ sub-organizations) to ensure that their approaches to safety management related to the committed activities comply with the recommendations of the present guidelines. Examples of processes and activities that are recommended to be documented:

(a) Organizational policy for supply chain.

(b) Incorporation of risks originating from supply chain.

(c) Evaluation of supplier SMS capability and corresponding audits.

(d) Processes to establish contracts, agreements for ensuring safety across the phases of development, production, and post-production.

(e) Processes for distributed safety activities.

SMS documentation shall be regularly updated in line with any relevant changes to the SMS processes. It is recommended that gap analysis should be used when auditing and updating the SMS, examining the current safety culture before formulating new and more appropriate SMS processes to ensure issues are adequately resolved. The SMS shall be subject to a process of continual improvement (e.g. "Plan, Do, Check, Act" as described in ISO 9001). Any changes to SMS documentation should be communicated as required to the relevant authority.

It is recommended that the SMS address measures to be taken to ensure ADS safety in the event of discontinued production, support, or maintenance of the ADS.

It is recommended that the manufacturer has processes for:

(a) Assuring that all practices and activities documented as part of the SMS are followed.

(b) Assuring that an independent check of compliance with the applicable requirements is performed. (i.e., not from person creating the compliance data).

(c) Assuring the continued evaluation of the Safety Management System so that it remains effective.

Link with the in-service monitoring/reporting pillar

It is recommended that a manufacturer include in the SMS processes to monitor safety-relevant incidents/ crashes/collisions caused by the ADS. The manufactures should also have a process to manage potential safety-relevant gaps during the in-service operation phase (possibly identified by in-service monitoring) and a process to update those vehicles.

The manufacturer should have processes to report safety relevant occurrences (e.g. collision with another road users and potential safety-relevant gaps, see the In-service Monitoring and Reporting Pillar) to the relevant authority when they occur.

The manufacturers should set up processes for the operational phase to confirm of compliance with the defined safety case. It should include early detection of new unknown situations (in line with SOTIF safety development goal to minimize the unknown scenarios area), event investigation, to share lessons derived from incidents and near-miss analysis to allow the whole community to learn from operational feedback and to contribute to the continuous improvement of automotive safety. Example of guiding principles: Is there a document describing the appropriate procedure of reporting incidents to the management? Is there evidence that the company is complying with that procedure? Is there a document describing the appropriate procedure of investigation and documentation of incidents? Is there evidence that the company is complying with that procedure?

Safety Assessment of the ADS

The purpose of the safety assessment of the ADS is for the safety authority to determine that hazards and risks relevant to the ADS have been identified by the manufacturer and a consistent safety concept has been implemented to mitigate these risks. The ADS safety case should explain the manufacturer’s safety concept and how it has been implemented to ensure safety by design and should demonstrate, through structured argumentation and evidence, that the risk assessment and the design have been validated by the manufacturer through testing and that, before the ADS-equipped vehicle is placed on the market, the ADS meets the relevant safety requirements. The safety case should provide sufficient evidence that the ADS is free of unreasonable safety risks to the broader transport ecosystem and in particular to the ADS vehicle user(s) and other road users. The safety case should address the following subjects.

ADS General Description

It is recommended that the safety case provided by the ADS manufacturer include a description of the ADS configuration and the intended uses and limitations on the use of its features, which gives a simple explanation of the operational characteristics of the ADS and ADS features:

(a) Operational Design Domain (e.g., road speed limits, road type and roadway characteristics, country, environment, road conditions, etc.) and including the ODD conditions and boundaries of each ADS feature in measurable and/or verifiable terms.

(b) Basic performance (e.g. Object and Event Detection and Response (OEDR), etc.).

(c) Interactions with other road users.

(d) Main conditions for achievement of a minimal risk condition.

(e) Interaction with the driver (if relevant) including the transition of control procedures, ADS notifications and fallback user responses.

(f) Supervision centre (if relevant).

(g) The method of activating, overriding, or deactivating the ADS by any or all of the ADS user (where relevant), the human supervision centre (where relevant), passengers (where relevant) or other road users (where relevant).

Description of the functions of the ADS

A description should be provided which gives a clear explanation of all the functions including control strategies of the ADS and the methods employed to perform the dynamic driving tasks within the ODD and the boundaries under which the ADS is designed to operate, including a statement of the mechanism(s) by which control is exercised. It is recommended that a list of all input and sensed variables is provided and the working range of these defined, along with a description of how each variable affects system behaviour. A list of all output variables which are controlled by the ADS should be provided and an explanation given, in each case, of whether the control is direct or via another vehicle system. The range of control exercised on each variable should be defined.

ADS Layout and Schematics

(a) Inventory of components

A list should be provided, including all the units of the ADS and mentioning the other vehicle systems which are needed to achieve the control function in question. An outline schematic showing these units and their relationships should be provided, with both the equipment distribution and the interconnections made clear. It is recommended that the outline includes: (i) Perception and objects detection including mapping and positioning (ii) Characterization of decision-making (iii) Remote supervision and remote monitoring by a remote supervision centre (if applicable). (iv) Information display/user interface (v) The data storage system (e.g., DSSAD).

(b) Functions of the units

The function of each unit of the ADS should be outlined and the signals linking it with other units or with other vehicle systems should be shown. This may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram. It is recommended that interconnections within the ADS should be shown by a circuit diagram for the electric transmission links, by a piping diagram for pneumatic or hydraulic transmission equipment and by a simplified diagrammatic layout for mechanical linkages. The transmission links both to and from other systems should also be shown. There should be a clear correspondence between transmission links and the signals carried between units. Priorities of signals on multiplexed data paths should be stated wherever priority may be an issue affecting performance or safety.

(c) Identification of units

Each unit should be clearly and unambiguously identifiable (e.g. by marking for hardware, and by marking or software identification for software content). This should provide a clear method for identifying the hardware and software in the associated documentation. Where the software version can be changed without requiring replacement of the marking or component, the software identification must be updated by means of the newly released software. It is recommended that where functions are combined within a single control unit or indeed within a single computer, but shown in multiple blocks in the diagram, then for clarity and ease of explanation, only a single hardware identification marking should be used. The identification defines the hardware and software version and, where the software changes and alters the function of the unit, the identifier associated with that software should also be changed.

(d) Installation of sensing system components

The manufacturer should provide information regarding the installation options that will be employed for the individual components that comprise the sensing system. These options should include, but are not limited to, the location of the component in/on the vehicle, the material(s) surrounding the component, the dimensioning and geometry of the material surrounding the component, and the surface finish of the materials surrounding the component, once installed in the vehicle. The information should also include installation specifications that are critical to the ADS's performance, e.g., tolerances on installation angle. Any changes to the individual components of the sensing system, or the installation options, should be updated in the documentation.

(e) ADS specifications

(i) Description of ADS specifications in nominal, critical, and failure situations, acceptance criteria and the demonstration of compliance with those criteria. (ii) List of applied regulations, codes, and standards.

(f) Maintenance and repair interface; protection against unauthorized access

(i) The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons.

(ii) The ADS shall be designed to protect against unauthorized access to and modification of the ADS functions.

(iii) The measures ensuring protection from unauthorized access should be provided in alignment with engineering best practices.

Safety Concept and Validation of the Safety Concept by the Manufacturer

The manufacturer should provide a safety case that affirms and provides evidence to demonstrate that the ADS is free from unreasonable risks for the ADS vehicle user(s) and other road users. Part of the safety case is the safety concept, which describes measures designed into the ADS to achieve the goal of avoidance of unreasonable risk with regard to functional and operational safety. In addition to this descriptive documentation, the safety case also includes a structured demonstration supported by evidence, including validation tests, that the ADS will be free from unreasonable risk. In respect of software employed in the ADS, the outline architecture should be explained and the design methods and tools used should be identified. The manufacturer should show evidence of how the ADS capabilities were realized and checked during the design and development process.

It is recommended that the safety concept element of the safety case should provide an explanation of the design provisions built into the ADS to ensure functional and operational safety. Possible design provisions in the ADS include:

(a) Fallback (or fail safe) operation using a partial system.

(b) Redundancy using separate systems.

(c) A list of the potential faults identifiable by the diagnostic system(s) of the ADS.

(d) Removal of some or all automated driving function(s). If a chosen provision utilizes a partial performance mode of operation under certain fault conditions (e.g. in case of severe failures), then these conditions should be stated (e.g. type of failure). The resulting ADS behaviour and capabilities should be defined (e.g. achievement of a minimal risk condition immediately) as well as the warning strategy to the driver/remote supervision centre (if applicable). If the chosen provision selects a second (back-up) means to realize the performance of the dynamic driving task, it is recommended that the principles of the change-over mechanism, the logic and level of redundancy and any built-in back-up checking features be explained and the resulting limits of back-up effectiveness defined. If the chosen provision selects the removal of an automated driving function, it is recommended that this is done in compliance with the relevant provisions of this regulation. All the corresponding output control signals associated with this function should be inhibited.

The documentation should be supported, by an analysis which shows how the ADS will behave to mitigate or avoid hazards which can have a bearing on the safety of the ADS vehicle user(s) and other road users. It should show how unknown hazardous scenarios will be managed by the manufacturer to keep the residual risk level under control. The chosen analytical approach(es) should be established by the manufacturer and made available for assessment to the relevant authority before market introduction.

The auditor should perform an assessment of the application of these analytical approaches, including:

(a) Inspection of the safety approach at the concept (vehicle) level.

(b) It is recommended that this approach be based on a Hazard / Risk analysis appropriate to system safety.

(c) Inspection of the safety approach at the ADS level including a top down (from possible hazard to design) and bottom-up approach (from design to possible hazards). The safety assessment may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) and a System-Theoretic Process Analysis (STPA) or any similar process appropriate to system functional and operational safety.

(d) Inspection of the documentation that should demonstrate the validation/verification plans and results including appropriate acceptance criteria. It should include testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, testing with real end users, or any other testing appropriate for validation/verification. The auditor/assessor should perform an assessment of the physical testing (proving ground and/or public road) environment and should assess the documentation of the virtual tool chain provided by the manufacturer. The auditor/assessor may decide to carry out tests of the complete integrated tool to assess the credibility of the virtual tool chain. Results of validation and verification may be assessed by analysing coverage of the different tests and setting minimal coverage thresholds for various metrics. [insert cross-reference to credibility assessment appendix from SG2]

It is recommended that the documentation confirms that at least each of the following items are covered where applicable:

(a) Issues linked to interactions with other vehicle systems (e.g., braking, steering).

(b) Failures of the automated driving system and the resulting risk mitigation strategy.

(c) Situations within the ODD when a system may create unreasonable safety risks to the ADS vehicle user(s) and other road users due to operational disturbances, for instance: • lack of or wrong comprehension of the vehicle environment; • lack of understanding of the reaction from the driver the ADS vehicle user(s) or other road users; • inadequate control; • challenging scenarios.

(d) Identification of the relevant scenarios within the ODD boundaries and the methodology used to select scenarios and choose the validation methodology and approach.

(e) Decision-making process for the performance of the dynamic driving tasks (e.g. emergency manoeuvres), the interaction with other road users and the compliance with traffic rules.

(f) Cyber-attacks that may have an impact on the safety of the vehicle.

(g) Reasonably foreseeable misuse by the driver (if applicable) (e.g., the use of a driver availability recognition system and an explanation on how the availability criteria were established), mistakes or misunderstanding by the driver if applicable (e.g., unintentional override) and intentional tampering of the ADS.

The safety case should include arguments and evidence supporting the implementation of the safety concept that is understandable and logical and cover all the different functions of the ADS. The documentation should also demonstrate that validation measures are robust enough to demonstrate safety (e.g., reasonable coverage of chosen scenarios as part of the validation methodology chosen) and have been completed.

It is recommended that the documentation provides evidence that the vehicle is free from unreasonable risks to the ADS vehicle user(s) and other road users in the operational design domain. This could be achieved through:

(a) Overall validation targets (i.e., validation acceptance criteria) supported by validation results, demonstrating that at entry into service of the ADS will not increase the overall level of risk to the ADS vehicle user(s) and other road users compared to a manually driven vehicles within the ODD, and

(b) A scenario-specific approach showing that the ADS will not increase the overall level of risk to the ADS vehicle user(s) and other road users compared to a manually driven vehicles within the ODD for each of the safety relevant scenarios.

The safety case should provide documentation sufficient to allow the relevant authority to verify through assessment of the case and possible testing by the authority that the manufacturer has successfully implemented the safety concept applicable to the ADS. It is recommended that the documentation itemizes the parameters being monitored on the vehicle and should set out evidence supporting the argument that applicable safety requirements have been met. This documentation should also describe the measures in place to ensure the ADS is free from unreasonable risks to the ADS user(s) and other road users when the performance of the ADS is affected by environmental conditions (e.g., climatic, temperature, dust ingress, water ingress, ice packing).

Data Storage System

It is recommended that the documentation describe: (a) Storage location and crash survivability (b) Data recorded during vehicle operation and occurrences (c) Data security and protection against unauthorized access or use (d) Means and tools to carry out authorized access to data.

Cyber Security and Software Update Management

The documentation should describe: (a) Cyber security and software update management, (b) Identification of risks, mitigation measures, (c) Secondary risks and assessment of residual risks, (d) Software update procedure and management put in place to comply with legislative requirements.

Information Provision to Users (as appropriate: owners, users, operators, etc.)

For the ADS users, documentation should facilitate user understanding of the functionality and operation of the system covering at least:

- An operational description of the ADS features, capabilities, and limitations (the information should also refer to specific scenarios and/or ODD).

- Terms for the correct use of the ADS and its feature(s).

- Instructions for the activation and deactivation of the ADS, with clear explanations of the distinctions between user-initiated deactivation and system-initiated deactivation.
- A description of the roles and responsibilities of the driver/user and ADS when an ADS (feature) is active.
- Information on ADS responses to ADS vehicle user interventions in the dynamic control of the vehicle.
- A description of the permitted transitions of roles and the procedure for those transitions.
- A general overview of non-driving-related activities (NDRA) allowed when an ADS feature is active.
- Safety precautions and safety-relevant information for the user.
- Information related to the HMI's indications:
    - Visual tell-tales, icons.
    - Auditory signals.
    - Haptic signals.
- Safety measures to be taken in the event of malfunctioning of the ADS.
- Extent, timing and frequency of maintenance operations.
- Means to enable a periodical technical inspection.
- Documents and templates for maintenance, repair and periodical technical inspection.
- Precautionary statements in the sense of compliance with limit values for the technical functions.
- Data protection and data security functionalities.

Section 6. Requirements for ADS Performance of the DDT

Introduction

The following subsections recommend criteria for validating the safety of ADS and/or ADS vehicles. Annex 2 contains a matrix linking these criteria with recommended test methods.

As a general concept, the safety level of ADS shall be at least to the level at which a competent and careful human driver could minimize the unreasonable safety risks to the ADS vehicle user(s) and other road users. The subsections below concern ADS performance of the DDT. The recommended requirements have been drafted for worldwide application. These requirements, therefore, do not specify technical performance limits due to the diversity of ODD-specific conditions and requirements that may influence safe performance of the DDT.

Scenario generation and behavioural competencies

Driving involves real-time risk management under prevailing traffic conditions. Therefore, safe ADS performance of the DDT depends upon the conditions presented under each individual scenario.

Annex 3 provides a recommended approach to scenario generation and to the establishment of ADS behavioural competencies to be demonstrated under these scenarios. Each scenario is associated with one or more behavioural competencies.

The ODD-based approach to scenario generation provides analytical methods to ensure that the scenarios cover the ODD of the ADS feature(s). These scenarios address nominal, critical, and failure situations to enable assessments in accordance with the WP.29 Framework Document on Automated Vehicles (FDAV). The behavioural competencies define ADS responses that comply with the following global requirements (Subsections 6.3-6.6) within the bounds of a relevant safety model quantifying dimensions for assessment of ADS performance (as described in Annex X). The behavioural competencies align with the layer of abstraction of the scenario to provide verifiable criteria at the functional layer down to measurable criteria at the concrete layer of abstraction.

Compliance with the recommended requirements under the following subsections is determined by verifying that the ADS demonstrates the behavioural competencies associated with the scenarios relevant to the ODD of its features. These requirements shall be applied in the definition of behavioural competencies to be demonstrated under traffic scenarios.

ADS Performance of the DDT under Nominal Traffic Scenarios

The following recommendations address the Framework document on automated/autonomous vehicles (ECE/TRANS/WP.29/2019/34/Rev.2) guidance that ADS vehicles shall not cause traffic accidents or disrupt traffic. Compliance with this broad objective can be verified by subjecting the ADS and/or ADS vehicle to nominal traffic scenarios representing usual and expected traffic conditions and behaviours. By minimizing risk factors outside the ADS nominal performance of the DDT, the impact of the ADS driving behaviour on other road users and the flow of traffic can be isolated. This section recommends requirements for assessing ADS performance of the DDT under normal operational and driving conditions.

- The ADS shall be capable of performing the entire Dynamic Driving Task (DDT) within the ODD of its feature(s).
- The ADS shall operate the vehicle at safe speeds.
- The ADS shall maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle.

- The ADS shall adapt its driving behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic).
- The ADS shall adapt its driving behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).
- The ADS shall detect and respond to objects and events relevant to its performance of the DDT.
- The ADS shall detect and respond to priority vehicles in service in accordance with the relevant traffic law(s).
- Under nominal traffic scenarios, the driving behaviour of the ADS shall not force other road users to take evasive action to avoid a collision with the ADS vehicle.
- Under nominal traffic scenarios, the driving behaviour of the ADS shall not cause a collision.
- The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation.
- The ADS shall interact safely with other road users.
- The ADS shall avoid collisions with safety-relevant objects where possible.
- The ADS shall signal intended changes of direction.
- The ADS shall signal its operational status in accordance with national rules.
- Pursuant to a passenger request, the ADS shall bring the vehicle to a safe stop.

ADS Performance of the DDT under Critical Traffic Scenarios

The following recommendations address the Framework document on automated/autonomous vehicles (ECE/TRANS/WP.29/2019/34/Rev.2) guidance that ADS vehicles shall not cause any traffic accidents resulting in injury or death that are reasonably foreseeable and preventable. Compliance with this broad objective can be verified by subjecting the ADS and/or ADS vehicle to critical traffic scenarios representing unusual or unexpected traffic conditions, objects, and/or object behaviours that elevate road safety risks. By introducing foreseeable external risk factors into scenarios, the capability of the ADS to manage safety-critical events that may arise within its ODD can be assessed.

- The requirements for DDT performance under nominal scenarios shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.

- In the event of a collision, the ADS shall stop the vehicle in an MRC and/or in accordance with applicable traffic laws.[27]
- The ADS shall not resume travel until the safe operational state of the ADS vehicle has been verified.
- The ADS may resume the trip where permissible under the applicable traffic rule(s) and other safety considerations.

ADS Performance of the DDT under Failure Scenarios

The following recommendations address the Framework document on automated/autonomous vehicles (ECE/TRANS/WP.29/2019/34/Rev.2) guidance regarding the assurance of system safety and responses to system failures that compromise the capability of the ADS to perform the entire DDT.

- The requirements for DDT performance under nominal scenarios shall continue to apply during failure scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.
- The ADS shall detect faults, malfunctions, and abnormalities that compromise its capability to perform the entire DDT within the ODD of its feature(s) per the manufacturer's documentation under Section 5 above.
- The ADS may continue to operate in the presence of faults that do not prevent that ADS from fulfilling the safety requirements applicable to the ADS.
- In response to a fault, the ADS may permit activation and use of a feature impacted by the fault provided that the ADS continues to provide the functions necessary to perform the entire DDT.
- The ADS shall adapt its performance of the DDT in accordance with the severity of the fault to ensure road safety.
- The ADS shall prohibit activation of an ADS feature in the presence of a fault in an ADS function that compromises the ADS capability to perform the entire DDT within the ODD of the feature.
- The limited operation of the ADS should comply with the normally applicable safety requirements.
- Remote termination of individual or multiple ADS or feature(s) by the manufacturer and/or service operator shall be possible when requested by Authorities.
- Remote termination for an ADS performing the DDT shall be capable of triggering an ADS fallback response.

[27] This provision requires further consideration regarding the threshold for collisions that would require the fallback to an MRC.

- Remote termination of an ADS or ADS feature(s) shall render them unable to be activated by user.

ADS Performance of the DDT at ODD Boundaries

- The ADS shall recognise the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's description of the ODD as described under Section 5.
- The ADS shall be able to determine when the conditions are met for activation of each feature.
- The ADS shall prevent activation of a feature unless the ODD conditions of the feature are met.
- The ADS shall execute a fallback response when one or more ODD conditions of the feature in use are no longer met.
- The ADS shall be able to anticipate foreseeable exits from the ODD of each feature.

Minimal Risk Condition Requirements

- The ADS shall signal its intention to place the vehicle in an MRC.
- The ADS shall execute a fallback response in the event of a failure in the ADS and/or other vehicle system that prevents the ADS from performing the DDT.
- In the absence of a fallback-ready user, the ADS shall fall back directly to an MRC.
- If the ADS is designed to request and enable intervention by a human driver, the ADS should execute a fallback to an MRC in the event of a failure in the transition of control to the user.
- Upon completion of a fallback to an MRC, a user may be permitted to assume control of the vehicle.

Considerations for specific testing requirements

See Annex 2 for the matrix giving a mapping of each requirement to the relevant validation pillars.

Application of the validation pillars to nominal traffic scenario requirements

Most of the requirements for DDT performance under nominal scenarios can be validated with any of the test methods; however, complex scenarios with high levels of traffic can be potentially difficult to implement on a test track.

Application of the validation pillars to critical traffic scenario requirements

The requirements for DDT performance under critical scenarios cover difficult and/or unsafe scenarios that would be dangerous to be sought out amongst naïve traffic in the real world. Some critical scenarios can be recreated on test tracks in controlled conditions, but virtual testing is recommended for testing the most dangerous situations.

Application of the validation pillars to failure scenario requirements

The requirements for DDT performance under failure scenarios cover scenarios where system failures compromise the capability of the ADS to perform the entire DDT. Considerations must be made for how to manually trigger a failure through either hardware or software mechanisms. Purposefully degrading the performance of the ADS in the real world amongst naïve traffic would be dangerous except in very specific low traffic situations. Testing failures is safer and more applicable on test tracks and via virtual testing.

Application of the validation pillars to ODD boundary requirements

The requirements for DDT performance at ODD boundaries cover situations where the ADS interacts with the boundaries of its ODD. Some of these boundaries can be validated on a test track provided that track testing is conducted on a testing ground that is part of, or suitably represents, the ODD of the ADS. However, certain boundaries such as performance at the edge of geofenced ODD boundaries will only be possible to validate via real world or virtual testing.

Application of the validation pillars to Minimal Risk Condition requirements

The Minimal Risk Condition requirements are related to the ADS achieving a MRC. Depending on the design of the ADS, this MRC may not necessarily be desirable on a real world road e.g. stopping in lane. As such, testing fallbacks to an MRC in real-world traffic could be dangerous depending on the nature of the fallback. Testing MRC may then be safer and more applicable on test tracks and via virtual testing.

Section 7. Requirements for safe interactions between Users and ADS

The following subsections provide safety-related recommendations to support user interactions with ADS. It is noted that the recommendations vary depending on user role, system design, and tasks to be performed by the user during the use of the ADS equipped vehicle.

For a safe use of the ADS by users who may need to take over control of the driving task from the ADS, it is necessary to provide correct information on the capabilities of the ADS to ensure that the user can develop a mental model that correctly reflects these capabilities. This information should be provided before and during driving with an ADS vehicle.

To further detail some of the recommendations it is recommended to draw on Human Factors knowledge, which is an established multidisciplinary science that applies knowledge of human abilities and limitations to the design and evaluation of technology for improved safety and usability.

It has to be noted that knowledge on testing the interaction between user and ADS including pass/fail criteria partly still needs to be developed. It also relevant to aim for a certain level of 'commonality' in the user interactions with the ADS for all brands and models. This will help users to develop and apply a single mental model and will also help to reduce the risk of user confusion (e.g., mode confusion) when changing between vehicles with ADS from different manufacturers. Such commonality cannot be defined now, but it is vital to establish it as a goal of future design.

This section provides recommendations on the design of the ADS user interactions between users and ADS vehicles to obtain safe operation of ADS vehicles. These recommendations do not apply to ADS vehicles and ADS features designed without accommodations for a user. The types of ADS users considered in this document are driver, fallback user, passenger.

General recommendations

- The ADS shall signal the presence of any failure that limits the operation of an available feature.
- The ADS shall signal its intention to place the vehicle in an MRC to the ADS user(s).
- An ADS that controls the operation of doors shall provide an emergency override to the user.
- The ADS HMI shall provide safety relevant information and signals clearly noticeable to the target user(s) under all operating conditions, multimodal (e.g., optical, acoustic, haptic) if needed, simply and unambiguously.

ADS features that allow a user to take over manual control of the DDT

General recommendations

- When the ADS is active, the vehicle driving controls, indicators, tell-tales, and DDT-related warnings may be disabled, suppressed, de-activated, inhibited or by other means made unavailable, as needed to mitigate the risk of errors in operation, misuse and reduce ambiguous states of vehicle control.
- The ADS shall be designed to prevent misuse and errors in operation by the user.
- The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions.[28]
- While an ADS feature is active, it shall inform the user on:

[28] Through size, form, location, colour, type, action, spacing and/or control shape. The provision aims to promote correct use and is not intended to prohibit multifunction controls.

(a) ADS status information.

(b) The role of the fallback user, if applicable.

(c) Any failure of the ADS that limits the operation of an available feature.

- The ADS shall indicate the availability of a feature for activation.

Recommendations on ADS feature activation

- The ADS shall ensure a safe ADS feature activation.

(a) The ADS shall provide prompt feedback to indicate success or failure when the user attempts to enable an ADS feature.

(b) The feature activation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.

(c) An ADS feature activation resulting in a user becoming a fallback user shall inform the fallback user of the consequent expectations on them.

Recommendations on ADS feature deactivation to manual driving

- The ADS shall have a monitoring system to support safe and appropriate engagement of the user as necessary.
- At the completion of the deactivation process, lateral and longitudinal control shall be returned to the driver without any continuous control assistance active.[29]

Features that allow a user-initiated system deactivation of the ADS

The ADS shall be designed to ensure a safe user-initiated system deactivation process.

(a) The ADS shall only allow the user to initiate a system deactivation process if the ADS can verify that the user is in a position to resume the role of the driver.

(b) ADS feature deactivation may be delayed if it is assessed by the ADS that the situation is unsuitable for the subsequent mode of vehicle operation. (e.g., due to the current situation being unsuitable or unsafe for the subsequent mode of operation).

(c) The user-initiated system deactivation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.

(d) The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process.

(e) The ADS shall provide a specific indication of the completion of the deactivation of the ADS.

[29] This provision may be changed pursuant to evidence from manufacturers demonstrating assurance of the safety of continuous control assistance pursuant to ADS deactivation.

(f) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.

(g) If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.

Features that have a system-initiated deactivation of the ADS

The ADS shall ensure a safe system-initiated deactivation to a fallback user.

(a) A system-initiated deactivation in nominal situations should be indicated in a timely manner to support the fallback user re-engaging to the driving task.

(b) The system-initiated deactivation to manual driving process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.

(c) The ADS shall:

(i) Continuously assess whether the fallback user is available for a system-initiated deactivation.

(ii) Provide effective procedures for re-engaging the fallback user who has been detected not to be available.

(iii) Trigger a fallback to an MRC where it has not been possible, feasible and/or safe to re-engage the fallback user.

(iv) Where appropriate, adapt the system-initiated deactivation process (e.g., timing, levels of warnings) according to the current circumstances (e.g., the engagement of the fallback user, the status of the ADS and vehicle, the current traffic situation).

(d) The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process.

(e) The ADS shall remain active until the system initiated deactivation process has been completed or the ADS vehicle reaches a minimal risk condition.

(f) The ADS shall provide a specific indication of the completion of the deactivation of the ADS.

(g) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.

(h) If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.

ADS features that do not allow a user to take manual control of the DDT

- The ADS shall provide the passenger(s) with means to request to stop the vehicle.
- The ADS vehicle shall provide safety-related information to the passengers.

- The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated.
- The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress).
- Controls provided for manual driving (e.g., steering, service brake, parking brake, accelerator, lighting) shall be designed to prevent any effect on the DDT whilst the ADS is performing the DDT, or reasonable safeguards shall be put in place to prevent access to controls.

Testing for compliance with user interaction requirements

See Annex 2 for the matrix giving a mapping of each user requirement to the relevant validation pillars.

Many HMI requirements relate to the design of the system, whilst the effects of these design can be tested in practice using simulation, test track and real world tests, the audit pillar would be most applicable for determining if the design requirements are followed.

DIL virtual testing can be helpful to support the assessment of this category of safety requirement by analysing the interaction between the driver and the ADS in a safe and controlled environment.

Track tests may be well suited for when the performance of an ADS can be assessed in a discrete number of physical tests, and the assessment would benefit from higher levels of fidelity for HMI related tests or those testing the ADS fall back response.

Utilising the information on ADS performance under real-world conditions could help to enhance or modify track tests. Furthermore, ISMR concerning user-interaction metrics could provide information useful for improving the HMI of an ADS, its usability, and driver education.

As with the DDT requirements, user requirements in failure scenarios such as for signalling a failure to a user require consideration of how to manually trigger a failure through either hardware or software mechanisms. Intentionally degrading ADS performance of the DDT in real-world traffic could present unreasonable safety risks; therefore, testing performance under failure scenarios would be safer via track and/or virtual testing.

Testing for failure signals, emergency user overrides, and system-initiated fallbacks to a user or an MRC might lead to the ADS achieving a MRC. Depending on the design of the ADS, this MRC might not necessarily be desirable on a real world road (e.g. stopping in lane). As such, testing fallbacks to an MRC in real-world traffic could be dangerous depending on the design of the MRC. Testing fallbacks to an MRC might then be safer and more applicable on test tracks and via virtual testing.

Systems that rely on the presence of a fallback user must fulfil requirements related to detecting the presence of this fallback user. To fully test such a requirement the fallback user must not be present/available when required. The system should be able to cope with this eventuality, but this aspect should still be tested on a controlled test track to avoid potential safety risks in real-world traffic should the ADS not meet the requirement.

Virtual testing covers both traffic simulation and vehicle simulators. For most requirements, one of those will cover the requirement; however, some cases such as evaluating user engagement prior to ADS deactivation of DDT performance require assessment of both the ADS and a human driver which may be challenging on a simulator test.

Section 8. In-Service Monitoring and Reporting

Introduction

In-Service Monitoring and Reporting (ISMR) is a validation methodology which is part of the multi pillar approach. It addresses the in-service safety of automated vehicles after market introduction.

In principle, ISMR is not a pre-deployment validation tool like the others, but it can still (especially the monitoring part) be used to validate ADS requirements . ISMR is mainly designed to provide evidence of in-service safety performance of the ADS, to identify a drift or deviation from the demonstrated performance and to find areas where ADS fails, and not provide evidence that the requirement itself is validated pre-deployment as demonstrated by simulation, track testing and real-world testing.

In practice, the application of the other pillars of the NATM guidelines will assess whether the ADS is safe, according to the existing criteria, for market introduction; whereas the in-service monitoring and reporting will gather additional evidence from its in-service operation to demonstrate that the ADS continues to be safe after market introduction, i.e., that use of the ADS does not present an unreasonable safety risk.

This pillar describes how to monitor the dynamic nature of the in-service operational use and then to provide feedback to ensure that there is continuous improvement of the safety of the ADS.

It relies on the collection of fleet data in the field to assess whether the ADS continues to be safe when operated on the road. This data collection can also provide information to help develop new scenarios or variations of existing scenarios for the scenarios catalogue allowing the whole ADS community to learn from major ADS accidents/incidents.

ISMR requires ADS manufacturers to collect and analyse the safety-relevant information related to their in-service ADS' operation and report data on safety related concerns, occurrences and performance metrics to the relevant authority.

The ADS's safety performance remains the responsibility of the manufacturer throughout the lifetime of the ADS.

ISMR is a mechanism to provide safety authorities with information about a manufacturer’s ADS that complements information that may be gathered from other sources.

It is recommended that a feedback loop (fleet monitoring) is put in place to confirm the safety argument and confirm the validation carried out by the manufacturer before market introduction.

ISMR enables the identification of unreasonable risks related to the use of an ADS on public roads and the evaluation of its safety performance during real-world operation.

Objectives

The aim of ISMR is to contribute to the improvement of road safety by ensuring that relevant information on safety is collected, processed, and disseminated.

The ISMR aims to fulfil three main objectives:

- Identify safety risks related to ADS performance that need to be addressed, including instances of non-compliance with ADS safety requirements (objective 1).
- Support the development of testable traffic scenarios through capturing information when the ADS does not perform safely in unanticipated situations (objective 2).
- Share information and recommendations to promote continuous improvement of ADS safety performance (objective 3).

The actual level of safety will only be confirmed once there are enough ADS vehicles in-service that have encountered a sufficient range of traffic and environmental conditions. It is therefore essential that a feedback loop, facilitated by ISMR, is in place.

This data will be used to assess and review the ADS manufacturer’s safety case and to validate the information that was used to enable market introduction.

The operational experience feedback from ISMR will allow ex-post evaluation of the regulatory requirements and validation methods, providing an indication of any issues and consequently the need for any modification to the requirements.

Unanticipated situations, risks, and hazards might be identified during real-world ADS operation, and this information could be used to develop new scenarios for a future scenario catalogue.

In the early phase of market introduction of ADS vehicles, it is essential that the whole community learns from safety-critical situations involving an ADS. It is important therefore that there is a mechanism that allows information from the ISMR and recommendations from its analysis to be shared with the ADS community. This will allow others to react and should lead to developments that reduce or prevent that situation from occurring in another ADS.

However, the ISMR has a more extensive application. For example, utilising the information on ADS performance under real-world conditions could help to enhance or modify track tests. Furthermore, ISMR concerning user-interaction metrics could provide information useful for improving an ADS' HMI, its usability, and driver education.

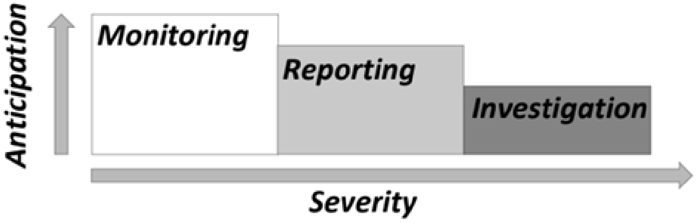
Collection, processing and dissemination of information related to ADS safety performance from the ISMR will also help to evaluate the impact of ADS on the safety of the road network. The information collected thanks to the ISMR can also be used to share the safety benefits of ADS.

Monitoring, Reporting, and Investigation

Monitoring refers to the overall data collection and analysis conducted by the manufacturers with aim at extracting safety related information from data. It mainly concerns the collection of relevant data elements during normal ADS operation to have a proactive approach to provide evidence of the in-service safety performance of the ADS.

Reporting applies to occurrences which endanger or which, if not corrected, would endanger a vehicle, its occupants or any other person, and in more terms the reporting of all occurrences relevant to the safety performance of the ADS. The reporting constitutes an event-based data collection methodology that is triggered by the happening of the set of occurrences.

It is expected that the ISMR will be complemented by safety investigations of (at least) critical occurrences conducted by an independent body.



ISMR Processes

Before the deployment of the ADS, the manufacturer should establish processes to demonstrate its capabilities to execute an effective ISMR. These processes should be part of the SMS of the manufacturer.

The processes for ISMR should demonstrate the capabilities:

- To monitor critical and non-critical occurrences caused by the ADS.
- To manage potential safety-relevant gaps during the in-service operation phase.
- To report safety-relevant occurrences to the authority when they occur.
- To confirm the compliance with the defined safety case.

- To share learnings derived from incidents and near-miss analysis.
- To contribute to the continuous improvement of automotive safety.

The manufacturer should define appropriate Key Performance Indicators (KPI) to measure the effectiveness of ISMR activities for the ADS operations.

The processes put in place by the manufacturer to manage safety of the ADS during in-service operation, e.g. to manage changes in the traffic rules and in the infrastructure, fall outside this pillar and are assessed with the audit pillar.

ISMR Implementation

In-Service Monitoring

The manufacturer and (where applicable) the fleet operator should set up a monitoring program aimed at collecting and analysing vehicle data, and data from other sources. It should provide evidence of the in-service safety performance of the ADS and confirmatory evidence of the audit results of the Safety Management System requirements established by the Audit Pillar. (Note: The in-service monitoring is intended to be applicable to all individual ADS types, not to a subset selected by the manufacturer or where applicable, by the fleet operator).

The monitoring program should include a data acquisition strategy, data retention strategy, data access, security and protection policy.

The data acquisition strategy ensure a representative collection of data to monitor the ADS in service performance.

The retention strategy should ensure that the dataset is retained until the corrective action and review processes are complete. In addition, the strategy should ensure the retention of the data for longer-term trend analysis (i.e. subset of the collected data).

The data access, security and protection policies should ensure that information access is allowed only to authorised persons and contains safeguards to ensure the security and protection of the data.

The data monitoring program should allow the manufacture and (where applicable) the fleet operator to:

- Identify areas of operational risk and quantify current safety margins (e.g. in service safety performance monitoring).
- Identify when the ADS prevents incidents/accidents (e.g., MRC fallbacks, collision avoidance, emergency manoeuvres).
- Identify and quantify operational risks by collecting data to characterize and analyse occurrences.
- Use metrics and thresholds to assess safety risks and discover trends that suggest the emergence of unacceptable risks if that trend continues.

- Put in place procedures for remedial action when an unacceptable risk is discovered or predicted by trends.
- Confirm the in-service safety level and effectiveness of any remedial action.

The data monitoring program should ensure that the data analysis is performed with sufficient frequency so that remedial action can be taken promptly and in line with reporting requirements.

The analysis techniques should comprise the following:

- Routine measurements: a selection of parameters should be collected to characterise each trip and to allow a comparative analysis. These measurements should aim at identifying and monitoring emerging trends and tendencies before the trigger levels associated with exceedances are reached. (e.g. vehicle performance monitoring).
- Exceedance detection: a set of core ”value” should be selected to cover the main areas of interest for the ADS operation with aim at searching for deviations from vehicle performance and limits. Typically, the main areas of interest are derived from the assessment of the most significant risks before the market introduction. However, they should be continuously reviewed to reflect the current operations. (e.g., speed limits exceedance, near misses, harsh braking, etc.).
- Occurrence analysis: recorded data should be able to characterize and investigate all the occurrences listed in the Annex 8.
- Statistics: Data Series should be collected to support the analysis process with additional information. These data should provide information to generate rate and trends. (e.g. driven km, operating hours).

The data monitoring programme should identify KPIs to assure that the monitoring is performing at an optimal level, and address any issues affecting the effectiveness of the monitoring program (e.g., data corruption or loss, or result in delayed or degraded event detection). Examples of KPIs for monitoring are trip collection rate, i.e. time between actual safety occurrence and detection of the occurrence (Date of detection of the occurrence by the In-service Monitoring – Date of the actual occurrence of the event).

The subsection below on “Monitoring of Performance” describes the relationship between ADS requirements and ISMR activities through a cross-reference matrix that specifies which requirements are suitable for monitoring.

Vehicle data collection

There is regulatory work to introduce Event Data Recorder (EDR) and Data Storage System for Automated Driving (DSSAD) requirements. Until those requirements have been defined this section is only suggesting the data elements that should be collected and uploaded by the manufacturer from ADS vehicles for aggregation and processing to allow reporting of the metrics defined in the Reporting section. Additionally, access to EDR data might be subject to data privacy issues, because the data is generally owned by the vehicle owner which raises the need for dedicated data collection provisions for the ISMR use case.

Other manufacturer-accessible sources of data indicative of ADS performance

Manufacturers may be expected to collect data relevant to typical operations such as dealer reports, customer reports, etc.

Monitoring of Performance

The monitoring of the ADS performance is intended:

- To provide evidence of in-service safety performance of the ADS.
- To identify a drift or deviation from the demonstrated performance including the ones that end in an occurrence.

Following the results obtained from the monitoring, the manufacturer should evaluate:

- In-service safety performance.
- The adequacy of the metrics and thresholds.
- Any remedial actions.

Annex 7 contains the matrix which links the ADS requirements to ISMR activities.

In-Service Reporting

The main purpose of occurrence reporting is to identify possible improvement for the ADS safety performance, and not to attribute blame or liability.

Recommended reporting by the manufacturer

The manufacturer should report, as required by the Authority, in accordance with this section and the subsections below on “Occurrence reporting” and “Tools for reporting”. It is expected that two types of reports on the in-service safety performance will be produced. These are short-term and periodic.

Short term reporting of occurrences and safety concerns is required for matters of such safety importance that they may require the manufacturer to take remedial action, including:

- Indications of failure to meet safety requirements.
- Critical occurrence where the ADS was involved known to the ADS manufacturer or OEM.
- Other safety-relevant performance issues.

At National level, there may be further requirements for immediate reporting/notification to the authority in the event the ADS manufacturer becomes aware of a failure /defect which poses an immediate risk to public safety.

The manufacturer should also undertake periodic reporting of performance metrics and occurrences to the safety authority.

The periodic report should provide evidence of the in-service ADS safety performance. In particular, it should demonstrate that:

- No inconsistencies have been detected compared to the ADS safety performance declared prior to market introduction.
- The ADS fulfils the performance requirements and as evaluated in the test methods.
- Any newly discovered significant ADS safety performance issues that pose an unreasonable risk to safety have been adequately addressed and how this was achieved.

The subsection on “Occurrence reporting” below provides a list of critical and non-critical occurrences aligned with safety requirements. This represents the generic areas of interest to be defined in greater detail considering both the usefulness of each suggested reporting element to the safety authorities, their capacity to review the volume of data reported, and the feasibility of storing, collecting and reporting the various elements.

During the investigation, the authority should be informed about the data processing (for example: filtering and conditioning) procedure and agree on the steps undertaken to deliver the data supporting the report.

Where feasible, a harmonized approach to the reporting should be developed by contracting parties, and their relevant domestic authorities.

The authority, where necessary, may verify the information provided and, if needed, may make recommendations to the enforcement authority and/or to the ADS manufacturer to remedy any detected conditions constituting an unreasonable risk to safety.

If a serious safety risk is identified, the safety authority may recommend temporary safety measures, including immediately restricting or suspending the relevant operations, and require actions to restore an acceptable level of safety.

Reporting from other sources

The effectiveness of the ISMR pillar is determined by the availability of data on ADS safety performance. Limiting the reporting to manufacturers would also restrict the type of occurrences that may be identified by ISMR, and consequently the level of safety improvement achievable through operational experience feedback will be limited.

It is recommended that Contracting Parties consider extending the operational reporting mechanism to other sources (e.g. drivers, operators, users, managers, road traffic authorities …), following best practices already adopted in other transport sectors.

Occurrence reporting

The short term and periodic reports should be made available, as required by the Authority, in two parts:

- A report (according to Annex 8), that contains a summary and the information relevant to the requirements for reporting.
- The data underpinning the report, exchanged with the authority by means of an agreed data exchange file.

Short term reporting is expected to be submitted for each critical occurrence.

Short term reporting is due within one month of the manufacturer's knowledge of the matter. Short term reporting is needed to provide awareness of situations in which the ADS may be or is posing an unreasonable risk to safety in-service.

Manufacturers are required to notify such concerns promptly upon their identification and to issue a report within 30 days form the knowledge of the matter.

The reporting scheme applies to automated vehicle features of an ADS which was active during a critical occurrence or up to 30 seconds prior to the critical occurrence.

Periodic reporting should be submitted regularly, at least every year, in the form of aggregated data (e.g., per hour of operation and distance driven) for ADS-vehicle type and related to ADS operation (i.e., when ADS is activated).

The occurrences have been subdivided into four categories:

1) Occurrences related to ADS performance of the DDT.
2) Occurrences related to ADS interaction with ADS vehicle users.
3) Occurrences related to ADS technical conditions, including maintenance and repair.
4) Occurrences related to the identification of new safety-relevant scenarios.

The following is a list of occurrences that have been derived from the ADS safety requirements. It is recommended that these form the basis of the reporting requirements. For each occurrence, its relevance to the short-term and/or periodic reporting has been flagged in the table below.

Occurrence	*Short-term reporting* *[1 Month]*	*Periodic Reporting [1 Year]*
1) Occurrence related to ADS performance of the DDT		

1.a. Safety critical occurrences known to the ADS manufacturer or OEM	X	X
1.b. Occurrences related to ADS operation outside its ODD	X	X
1.c. ADS failure to achieve a minimal risk condition when necessary	X	X
1.d. Communication-related occurrences		X
1.e. Cybersecurity-related occurrences		X
1.f. Interaction with remote operator if applicable Propose to delete		X
2) Occurrences related to ADS interaction with ADS vehicle users		
2.a. Driver unavailability (where applicable) and other user-related occurrences		X
2.b. Occurrences related to Transfer of Control failure		X
2.c. Prevention of takeover under unsafe conditions		X
3.a. Occurrences related ADS failure		X
3.b. Maintenance and repair problems		X
3.c. Occurrences related to unauthorized modifications		X
3.d. Modifications made by the ADS manufacturer or OEM to address an identified and significant ADS safety issue	X (if the issue presented an unreasonable risk to safety)	X
4. Occurrences related to the identification of new safety-relevant scenarios	(already covered under 1.a, 1.b, 1.c and 3,d)	X

Tools for reporting

The reporting templates aim at assuring the harmonization of the information to be reported and facilitating the information sharing.

The reporting templates aim at ensuring that a consistent and comprehensive set of information is delivered to the safety authority to foster an effective application of reporting scheme. Further granularity of the information can be considered depending on the ADS use cases.

The reporting shall be carried out according to the laws applicable in each contracting party and according to the information available to the reporting actors (manufacturers and/or operators).

The short term template (Annex 8) provides a list of information with corresponding specifications that should be made available to the authority following the occurrence of an event flagged under the “Short term reporting”.

In particular, the short-term reporting provisions shall contribute to identify:

a) Safety-relevant occurrences caused by an ADS.

b) Traffic situations unforeseen in the original validation that resulted in ADS behaviors inconsistent with the expected behavioral competencies.

c) ADS noncompliance with the ADS safety requirements.

d) Safety concerns in need of remedy.

It shall also be noticed that information reported in the short term template will remain confidential.

The periodic reporting template (Annex 8) provides a list of information with corresponding specifications that should be made available to the authority on a yearly basis in accordance with the occurrences under the “Periodic reporting”.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

ANNEXES

Annex 1: Background on development of ADS safety requirements

This annex provides background information concerning the deliberations on safety requirements for Automated Driving Systems (ADS).

The development of these recommendations involved extensive consideration of what an ADS is and how ADS relate to human roles in driving. Accordingly, the definition of ADS is central to these recommendations. Two leading international standards bodies (SAE and ISO) define ADS as: "The hardware and software that are collectively capable of performing the entire DDT (Dynamic Driving Task) on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD)."[30]

ADS present challenges to the safety regulator that require new concepts, tools, and methodologies in addition to those historically used for previous vehicle technologies and systems.

This section explains the considerations behind the recommendations for ensuring ADS safety presented in this document.

Driving

Driving is a complex activity with traffic laws and codes of behaviour based upon human cognitive strengths and weaknesses.

Driving involves three behavioural levels: strategic, tactical, and operational.

The strategic level concerns general trip planning such as determination of trip goals, the route to be used, the modal choice, and evaluation costs and risks associated with these decisions.

The tactical level involves manoeuvring the vehicle in traffic during a trip, including perceiving and assessing of the driving environment, deciding and planning on a specific manoeuvre (e.g., on whether and when to overtake another vehicle), and executing the manoeuvre.

The operational level concerns vehicle-stabilisation capabilities (e.g., making micro-corrections to steering, braking, and accelerating to maintain lane position in traffic).

For example, a decision to drive from home to a workplace involves a strategic assessment of the current conditions, the risks involved in driving under those conditions, and the probability for arriving at work on time. While driving, the driver makes tactical decisions based on conditions encountered along the way such as to change lanes or turn onto another street. In changing lanes, the driver makes a tactical

[30] This term is used specifically to describe a Level 3, 4, or 5 driving automation system These aspects of DDT, ODD, and the "hardware and software" capabilities are addressed in these recommendations, including their interplay in defining applications of ADS technologies and assurance of their safe deployment.

assessment that the lane change is feasible, actuates the direction indicators and steers the vehicle while maintaining an appropriate speed, often with continuous adjustments on the operational level.

These behavioural levels relate to perception, information processing, and decision making under uncertainty. Driving can be considered an exercise in risk management within the context of achieving strategic goals. Drivers assess and respond in real time to perceived risks (including the behaviours of other road users) in the road environment.

The real-time tactical and operational functions required to operate a vehicle in on-road traffic are collectively known as the Dynamic Driving Task (DDT). As noted above, these functions may be performed within the context of strategic goals, but the DDT itself excludes such strategic functions. These functions may overlap or operate in combination such as in a tactical decision in response to road conditions to deviate from the original strategy to follow a particular route. Strategic decisions nonetheless may be made during a trip (for example, a decision to leave the motorway for lesser roads).

Although the DDT comprises several subtasks (sensing, cognitive processing, action), the DDT itself refers to performing the whole driving task within its Operational Design Domain (ODD). Within the ODD, the ADS or the driver performs the DDT. A system that cannot perform the entire DDT can only assist the driver's performance of the DDT.

Tactical functions include but are not limited to manoeuvre planning and execution, enhancing conspicuity (lighting, signalling, gesturing, etc.), and managing interactions with other road users. Tactical functions generally occur over a period of seconds.

Operational functions include but are not limited to lateral vehicle motion control (steering) and longitudinal vehicle motion control (acceleration and deceleration). This operational effort involves split-second reactions, such as making micro-corrections while driving.

The DDT cannot be apportioned between a driver and a driving system because these functions are interdependent and operate as a whole. Operational and tactical functions are inherent in monitoring the driving environment (object and event detection, recognition, classification, and response preparation) and in object and event response execution.

Automated driving

While the previous section concerns driving in general, human and automated driving have notable differences.

Unlike human drivers broadly licensed to operate a vehicle on all roadways under all conditions, ADS may be designed for specific purposes and to operate under specific conditions.

The diversity of ADS and ADS vehicle configurations requires attention to the roles, if any, that a vehicle user may play in the use of the vehicle. ADS vehicles may, or may not, be designed to carry human occupants. They may, or may not, be designed to be driven by a human being. They may permit or prohibit driver activation of the ADS while the vehicle is moving.

Safety requirements must account for the role(s) a user may have in the use of the ADS and/or ADS vehicle such as driver or passenger. These human-user roles may involve vehicle occupants, or they may be external to the vehicle.

Roles may change during the course of a trip. For example, in some configurations, a driver may activate the ADS while the vehicle is moving such that the ADS becomes the sole vehicle operator (i.e., performing the DDT within the ODD of the activated feature) and the driver shifts to the role of fallback user. For safety reasons, this fallback-user role might entail an obligation to remain receptive and responsive to ADS requests to assume control over the vehicle (i.e., to return to the role of driver). In other configurations, human occupants might not be expected to play any DDT-relevant role during the course of an entire trip.

The requirements recommended in this document address misuse prevention and the safety of user interactions such as transitions of vehicle control.

The conditions under which an ADS is designed to operate are known as the Operational Design Domain (ODD), which include but are not limited to aspects such as roadway speed limits, road designs (surface, geometry, infrastructure, etc.), weather conditions, and traffic densities. The ODD may include constraints or limitations on ADS use such as maximum vehicle speed, maximum rate of rainfall, or road type.

The ADS requirements must address the diversity of driving conditions that may arise singly and in combination within the ODD.

In addition, the requirements must address ADS that may be designed to operate in more than one ODD. As long as the ADS safely performs the DDT within each ODD, there is no reason to limit the definition of sets of ADS capabilities designed to operate the vehicle under separate sets of ODD conditions.

For an ADS, the operational and tactical functions of the DDT can be logically grouped under three general categories:

- Sensing and Perception
  ADS sensing and perception functions include monitoring the driving environment to achieve object and event detection, recognition, and classification. These functions include perceiving other vehicles and road users, the roadway and its fixtures, objects in the vehicle's driving environment, and relevant environmental conditions, including sensing ODD boundaries, if any, of the ADS feature and positional awareness relative to driving conditions.

- Planning and Decision

  Planning and decision include anticipation and prediction of actions that other road users may take, response preparation, and manoeuvre planning.

- Control

Control refers to lateral and/or longitudinal motion control and enhancing vehicle conspicuity via lighting and signalling.

Automated Driving Systems

Based on the above, ADS need to be described in terms that cover the DDT (tactical and operational functions required to operate the vehicle in traffic) and the ODD (conditions under which such ADS capabilities are made available to a user).

An ADS consists of hardware and software that are collectively capable of performing the entire DDT on a sustained basis within one or more ODD.

Driving automation systems that require human intervention to perform aspects of the DDT fall below the level of an ADS.

In order to cover the diversity of ADS configurations, uses, and limitations on use, these recommendations define ADS in terms of functions and features.

ADS functions: DDT Performance Capabilities

ADS integrate subsets of hardware and software (i.e., functions) designed to perform one or more aspects of the DDT.

ADS functions, in general, correspond to system-level capabilities integrated into the ADS design.

A function enables the ADS to perform one or more elements of the DDT (e.g., sensing the environment).

Functions represent the first level of safety that an ADS must fulfil. These functions correspond to essential capabilities without which an ADS cannot be deemed safe for use in traffic.

However, functions that enable performance of the DDT and capabilities that ensure safe use, including the safety of user interactions, have distinctly different objectives and requirements.

Safe ADS performance of the DDT

Requirements to ensure safe ADS performance of the DDT address the functional and behavioural objectives described by the WP.29 Framework Document on Automated Vehicles: ADS operation shall not cause any traffic accidents resulting in property damage, injury, or death that are reasonably foreseeable and preventable.

The requirements recommended in this document aim to ensure that each ADS is capable of performing the entire DDT to the extent necessary to operate the vehicle within the ODD of the ADS feature(s). Because the performance of tactical and operational functions is dependent on the prevailing traffic conditions, these DDT requirements specify that the ADS must demonstrate behavioural competencies across traffic scenarios covering its ODD. The behavioural competencies inherently require functional capabilities to perform the DDT.

These recommendations intentionally omit specifications for individual DDT functions. For example, the recommendations do not in general prescribe technical specifications for lateral or longitudinal control. As noted above, performance of the DDT is dependent on traffic conditions where such functions cannot be limited to representative specifications. For example, it is not possible to specify a particular measure of lateral control that would be appropriate in all circumstances. ADS safety involves real time tactical and operational adaptation to dynamic road conditions in the ODD. Tactical and operational functions are interdependent where the complexity of their interactions needs to be assessed under diverse traffic conditions.

By ensuring that an ADS will be subjected to traffic scenarios representative of what the ADS is reasonably likely to encounter in its ODD, the assessment of the behavioural competencies demonstrated by the ADS under those scenarios verifies the capability of the ADS to perform the entire DDT necessary to navigate its ODD.

Additional ADS Capabilities: Safe use of ADS and ADS vehicles

In addition to DDT-specific functions, an ADS may require capabilities that contribute to ensuring the safe operational state of the ADS and/or preventing use when the ADS is not in a safe operational state.

ADS functions might also ensure the correct use of the ADS and safe interactions with a user such as in transitions of control.

Ensuring the safety of interactions between ADS and their users demands a human-centred focus on user needs, strengths, and weaknesses.

Trust often determines automation usage. Operators may not use a reliable automated system if they believe it to be untrustworthy. Conversely, they may continue to rely on automation even when it malfunctions. ADS should be designed to foster a level of trust that is aligned with their capabilities and limitations to ensure proper use.

These recommendations address user understanding of the ADS configuration, intended uses, and limitations on use, simplicity in defining and communicating user roles and responsibilities, clarity and commonality across ADS controls, requests, and feedback, and both misuse prevention as well as safeguards in the event of misuse.

The recommendations encourage Safety Management Systems that integrate Human-Centred Design Processes to ensure safe interactions between ADS and their users.

These human-centred processes should include analyses by qualified personnel of user needs and risk, setting safety and usability objectives, specifying user requirements and ensuring user understanding and context to produce design solutions that meet the requirements.

ADS should be evaluated, particularly under real-world testing on real users (i.e., not the people who are developing the products).

ADS performance should be monitored in the field and this information should be used to set future design targets and evaluate designs against these requirements.

These recommendations for user safety align with this human-centred approach to identify functions that must be integrated into ADS designs to ensure safe interactions and prevent misuse.

ADS features

An ADS feature refers to an application of ADS capabilities designed for use within a defined ODD. In the case of an ADS designed to operate within a single ODD, the ADS and the ADS feature are synonymous. Examples of ADS features are highway-only driving and automated parking.

Although an ADS performs the entire DDT on a sustained basis, an ADS may be designed to operate within more than one ODD.

Each set of ODD-specific capabilities has a unique set of constraints defining the conditions under which the ADS may be used.

ADS functions enable each ADS feature to operate the vehicle within the ODD of the feature. ADS functions may be used by more than one ADS feature and ADS features may use some or all of the ADS functions.

This document recommends a feature-based assessment of ADS. In cases where an ADS has more than one feature (i.e., is designed to operate in more than one ODD), each feature should be assessed to ensure that the ADS provides the functions necessary for performance of the entire DDT within the ODD of each feature.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 2: Matrix of DDT and User requirements with applicable test pillars

This annex contains a matrix which provides guidance linking the DDT and user requirements to the applicable pre-deployment validation pillars.

The matrix is aimed at approval testing after the manufacturer has already undergone their own internal development testing which is covered under the audit pillar. However, the matrix can also be used to provide guidance to manufacturers during their own internal development testing.

The matrix indicates which pillars are possible to test, not which should be tested or the priority/order of testing as this will be use case specific.

The matrix uses a green, orange, red, white colour scheme to indicate the relative applicability of the pillars.

- Green is broadly applicable to the requirement, can test most aspects of the requirement e.g. could test the ability to perceive any individual priority vehicle.
- Orange is only applicable to the requirement a limited way e.g. some ODD boundaries could be tested on a test track but many will not be possible.
- Red is largely not applicable to the requirement e.g. It would be dangerous to try and create a critical scenario in a road test with naïve traffic.
- White represents a requirement related to the design of the system, which should be assessed via the Audit pillar.

If a pillar is green, then a test using that pillar doesn’t necessarily fully validate the requirement but demonstrates an aspect of it i.e. a spot check.

Although certain pillars are currently rated as having limited applicability (orange or red), technological advances could change this assessment in the future.

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
ADS Performance of the DDT under Nominal Traffic Scenarios			
The ADS shall operate the vehicle at safe speeds.	🟩	🟩	🟩
The ADS shall maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle.	🟩	🟩	🟩
The ADS shall adapt its driving behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic).	🟩	🟩	🟩

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
The ADS shall adapt its driving behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).	🟩	🟩	🟩
The ADS shall detect and respond to objects and events relevant to its performance of the DDT.	🟩	🟩	🟩
The ADS shall detect and respond to priority vehicles in service in accordance with the relevant traffic law(s).	🟩	🟩	🟩
Under nominal traffic scenarios, the driving behaviour of the ADS shall not force other road users to take evasive action to avoid a collision with the ADS vehicle.	🟩	🟧	🟩
Under nominal traffic scenarios, the driving behaviour of the ADS shall not cause a collision.	🟩	🟩	🟩
The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation.	🟩	🟩	🟩
The ADS shall interact safely with other road users.	🟩	🟩	🟩
The ADS shall avoid collisions with safety-relevant objects where possible.	🟩	🟩	🟩
The ADS shall signal intended changes of direction.	🟩	🟩	🟩
The ADS shall signal its operational status in accordance with national rules.	🟩	🟩	🟩
Pursuant to a passenger request under para. 7.4.1., the ADS shall bring the vehicle to a safe stop.	🟩	🟩	🟩
ADS Performance of the DDT under Critical Traffic Scenarios	⬛	⬛	⬛
The requirements for performance of the DDT under nominal scenarios shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.	🟩	🟩	🟥
In the event of a collision, the ADS shall stop the vehicle in an MRC and/or in accordance with applicable traffic laws.	🟩	🟩	🟥
The ADS shall not resume travel until the safe operational state of the ADS vehicle has been verified.	🟩	🟩	🟥
The ADS may resume the trip where permissible under the applicable traffic rule(s) and other safety considerations.	🟩	🟩	🟥
ADS Performance of the DDT under Failure Scenarios	⬛	⬛	⬛

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
The requirements for performance of the DDT under nominal scenarios shall continue to apply during failure scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.	🟩	🟩	🟥
The ADS shall detect faults, malfunctions, and abnormalities that compromise its capability to perform the entire DDT within the ODD of its feature(s) per the manufacturer's documentation.	🟩	🟩	🟥
The ADS may continue to operate in the presence of faults that do not prevent that ADS from fulfilling the safety requirements applicable to the ADS.	🟩	🟩	🟥
In response to a fault, the ADS may permit activation and use of a feature impacted by the fault provided that the ADS continues to provide the functions necessary to perform the entire DDT.	🟩	🟩	🟥
The ADS shall adapt its performance of the DDT in accordance with the severity of the fault to ensure road safety.	🟩	🟩	🟥
The ADS shall prohibit activation of an ADS feature in the presence of a fault in an ADS function that compromises the ADS capability to perform the entire DDT within the ODD of the feature.	🟩	🟩	🟥
The limited operation of the ADS should comply to the normally applicable safety requirements.	🟩	🟩	🟥
Remote termination of individual or multiple ADS or feature(s) by the manufacturer and/or service operator shall be possible when requested by Authorities.	🟩	🟩	🟧
Remote termination for an ADS performing the DDT shall be capable of triggering an ADS fallback response.	🟩	🟩	🟧
Remote termination of an ADS or ADS feature(s) shall render them unable to be activated by user.	🟩	🟩	🟩
ADS Performance of the DDT at ODD Boundaries	⬛	⬛	⬛
The ADS shall recognise the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration.	🟩	🟧	🟩
The ADS shall be able to determine when the conditions are met for activation of each feature.	🟩	🟧	🟩
The ADS shall prevent activation of a feature unless the ODD conditions of the feature are met.	🟩	🟧	🟩

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
The ADS shall execute a fallback response when one or more ODD conditions of the feature in use are no longer met.	🟩	🟧	🟩
The ADS shall be able to anticipate foreseeable exits from the ODD of each feature.	🟩	🟧	🟩
Minimal Risk Condition Requirements			
The ADS shall signal its intention to place the vehicle in an MRC.	🟩	🟩	🟧
The ADS shall execute a fallback response in the event of a failure in the ADS and/or other vehicle system that prevents the ADS from performing the DDT.	🟩	🟩	🟧
In the absence of a fallback-ready user, the ADS shall fall back directly to an MRC.	🟩	🟩	🟧
If the ADS is designed to request and enable intervention by a human driver, the ADS should execute a fallback to an MRC in the event of a failure in the transition of control to the user.	🟩	🟩	🟧
Upon completion of a fallback to an MRC, a user may be permitted to assume control of the vehicle.	🟩	🟩	🟧

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
Recommendations for safe interactions between Users and ADS.			
The ADS shall signal the presence of any failure that limits the operation of an available feature.	🟩	🟩	🟥
The ADS shall signal its intention to place the vehicle in an MRC to the ADS user(s).	🟩	🟩	🟧
An ADS that controls the operation of doors shall provide an emergency override to the user.	🟩	🟩	🟧
The ADS HMI shall provide safety relevant information and signals clearly noticeable to the target user(s) under all operating conditions, multimodal (e.g., optical, acoustic, haptic) if needed, simply and unambiguously.	🟩	🟩	🟩

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
ADS features that allow a user to take over manual control of the DDT.	⬛	⬛	⬛
When the ADS is active, the vehicle driving controls, indicators, tell-tales, and DDT-related warnings may be disabled, suppressed, de-activated, inhibited or by other means made unavailable, as needed to mitigate the risk of errors in operation, misuse and reduce ambiguous states of vehicle control.	🟩	🟩	🟩
The ADS shall be designed to prevent misuse and errors in operation by the user.	Audit		
The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions.	Audit		
While an ADS feature is active, it shall inform the user on:	⬛	⬛	⬛
ADS status information.	🟩	🟩	🟩
the role of the fallback user, if applicable.	🟩	🟩	🟩
Any failure of the ADS that limits the operation of an available feature.	🟩	🟩	🟥
The ADS shall indicate the availability of a feature for activation.	🟩	🟩	🟩
Recommendations on the ADS feature activation.	⬛	⬛	⬛
The ADS shall ensure a safe ADS feature activation.	⬛	⬛	⬛
The ADS shall provide prompt feedback to indicate success or failure when the user attempts to enable an ADS feature.	🟩	🟩	🟩
The feature activation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.	Audit		
An ADS feature activation resulting in a user becoming a fallback user shall inform the fallback user of the consequent expectations on them.	🟩	🟩	🟩
Recommendations on ADS feature deactivation to manual driving.	⬛	⬛	⬛
The ADS shall have a monitoring system to support safe and appropriate engagement of the user as necessary.	Audit		

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
At the completion of the deactivation process, lateral and longitudinal control shall be returned to the driver without any continuous control assistance active.	🟩	🟩	🟩
ADS features that allow a user-initiated system deactivation to manual driving.	⬛	⬛	⬛
The ADS shall be designed to ensure a safe user-initiated system deactivation process.	⬛	⬛	⬛
The ADS shall only allow the user to initiate a system deactivation process if the ADS can verify that the user is in a position to resume the role of the driver.	🟩	🟩	🟧
ADS feature deactivation may be delayed if it is assessed by the ADS that the situation is unsuitable for the subsequent mode of vehicle operation. (e.g., due to the current situation being unsuitable or unsafe for the subsequent mode of operation).	🟩	🟧	🟥
The user-initiated system deactivation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.	Audit		
The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process.	🟧	🟩	🟩
The ADS shall provide a specific indication of the completion of the deactivation of the ADS.	🟩	🟩	🟩
If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.	🟩	🟩	🟩
If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.	🟩	🟩	🟩
ADS features that have a system-initiated deactivation to manual driving.	⬛	⬛	⬛
The ADS shall ensure a safe system-initiated deactivation to a fallback user.	⬛	⬛	⬛
A system-initiated deactivation in nominal situations should be indicated in a timely manner to support the fallback user re-engaging to the driving task.	🟩	🟩	🟩

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
The system-initiated deactivation to manual driving process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.	Audit		
The ADS shall:	⬛	⬛	⬛
Continuously assess whether the fallback user is available for a system-initiated deactivation.	🟩	🟩	🟥
Provide effective procedures for re-engaging the fallback user who has been detected not to be available.	🟩	🟩	🟥
Trigger an MRM where it has not been possible, feasible and/or safe to re-engage the fallback user.	🟩	🟩	🟥
Where appropriate, adapt the system-initiated deactivation process (e.g., timing, levels of warnings) according to the current circumstances (e.g., the engagement of the fallback user, the status of the ADS and vehicle, the current traffic situation).	🟩	🟩	🟩
The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process.	🟥	🟩	🟩
The ADS shall remain active until the system initiated deactivation process has been completed or the ADS vehicle reaches a minimal risk condition.	🟩	🟩	🟥
The ADS shall provide a specific indication of the completion of the deactivation of the ADS.	🟩	🟩	🟩
If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.	🟩	🟩	🟩
If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.	🟩	🟩	🟩
ADS features that do not allow a user to take manual control of the DDT.	⬛	⬛	⬛
The ADS shall provide the passenger(s) with means to request to stop the vehicle.	Audit		
The ADS vehicle shall provide safety-related information to the passengers.	🟩	🟩	🟩
The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated.	🟩	🟩	🟩

Requirement	Test Pillars		
Text	Virtual	Track	Real-world
The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress).	🟩	🟩	🟩
Controls provided for manual driving (e.g., steering, service brake, parking brake, accelerator, lighting) shall be designed to prevent any effect on the DDT whilst the ADS is performing the DDT, or reasonable safeguards shall be put in place to prevent access to controls.	Audit		

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 3: Approach to derive verifiable performance criteria

This annex provides an overview on an approach that may be used to derive verifiable performance criteria for the certification or, as relevant, for self-certification of ADS, based on the manufacturer/ ADS developer’s description of the Operational Design Domain (ODD) of the ADS. Such criteria would be developed by identifying behavioural competencies that embody and correspond to specific ADS safety requirements and relevant scenarios that may be used to validate the ADS’s competencies.

The suggested approach includes a description of how such competencies can be classified into nominal, critical and failure categories and mapped to the relevant scenarios, selected either from existing databases or identified through the application of knowledge and data-based approaches.

Different approaches may exist to perform such an activity; therefore, the approach herein presented should be considered as a guideline for both manufacturers and authorities.

Introduction and approach

Operational Design Domain

Operational design domain (ODD) refers to:

> Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics. (SAE J3016)

Given a specific ODD, it is crucial for the ADS to ensure that:

- it can operate safely within its ODD under conditions reasonably expected in the ODD
- it will be used only within its ODD
- it can monitor whether it is inside/outside its ODD and respond appropriately.

The conditions constituting the ODD in which the ADS was designed to operate will help determine which ADS competencies are required. For example, if an ADS has an ODD which comprises of roads with non-signalised junctions, one of the required behaviour competencies for the ADS in that ODD could potentially be “unprotected left or right turn”. However, the same behaviour competency may not be required if the ODD of an ADS is limited to motorways or highways with signalised junctions.

Behavioural competencies

The concept of “behavioural competencies” is useful in determining the safety of the performance of the Dynamic Driving Task (DDT) by an Automated Driving System (ADS):

- Behaviour: Specific goal-oriented actions directed by an engaged ADS in the process of completing the DDT or DDT fallback within the ODD (if applicable) at a variety of timescales.
- Behavioural Competency: Expected and verifiable capability of an ADS to operate a vehicle within the ODD of its feature(s).

Behavioural competencies can be described with different abstraction levels, similarly to functional, logical, and concrete scenarios. Refinement of the competencies from a functional to a more concrete level is possible by following the approach proposed in these guidelines.

Such competencies track the three broad categories of driving situations that may be encountered in performance of the DDT: nominal, critical, and failure.

Nominal driving situations are those in which behaviour of other road users and the operating conditions of the given ODD are reasonably foreseeable (e.g., other traffic participants operating in line with traffic regulations) and no failures occur that are relevant to the ADS's performance of the DDT.

Critical driving situations are those in which the behaviour of one or more road users (e.g., violating traffic regulations) and/or a sudden and not reasonably foreseeable change of the operating conditions of the given ODD (e.g., sudden storm, damaged road infrastructure) creates a situation that may result in an immediate risk of collision. In this case, as it is recognised that in some cases the ADS may not be able to avoid a collision, the ADS performance are compared with safety model performance to set the threshold between where avoidance is required and where it is not feasible, but mitigation may be possible.

Failure situations involve those in which the ADS or another vehicle system experiences a fault or failure that removes or reduces the ADS's ability to perform the DDT, such as sensor or computer failure or a failed propulsion system.

Concrete performance requirements depend on the specific situations the ADS encounters, on a reference behaviour that is deemed appropriate for a human driver or a technical system, and on assumptions (e.g. friction values, reaction times) about the behaviour of the vehicle and other road users. Since it is virtually impossible to write a regulation that sets out verifiable criteria for every combination of these variables, this document aims at providing a set of different reference behaviours or safety models together with an overview of the characteristics and required assumptions that can be useful in deriving verifiable performance criteria in some situations. The aim is then to assist those who develop concrete regulations with the selection and parameterization of functions or selection of scalars as pass/fail criteria.

For this, the following is needed:

- An overview of reasonable expectations (which might occur in different ODDs),
- An overview of reference behaviours / safety models that define the boundary between avoidable accidents and mitigation (note that these reference

behaviours will not be used for anything else than providing this boundary as a performance criterion).

- A matrix combining suggested reference behaviours / safety models with driving situations.

Behavioural Competencies Identification

The approach suggests a series of analytical frameworks that could help to derive measurable criteria appropriate for the specific application. These frameworks are divided into:

- ODD Analysis
- Driving Situation Analysis
- OEDR Analysis.

ODD analysis

This analysis represents the first step with the aim to identify the characteristics of the ODD. An ODD may consist of stationary physical elements (e.g., physical infrastructure), environmental conditions, dynamic elements (e.g., reasonably expected traffic level and composition, vulnerable road users) and operational constraints to the specific ADS application. Various sources provide useful guidance for precisely determining the elements of a particular ODD and their format definition.[31,32, 33, 34]

As part of this activity, the level of detail of the ODD definition using the ODD attributes will also need to be established.

Driving situation analysis

In the driving situation analysis, the behaviours of other road users that are reasonably expected and presence of roadway characteristics in the ODD are explored in more detail by mapping actors with appropriate properties and defining interactions between the objects.

An example of this analysis is given in Table 1, where static and dynamic behaviours of other objects (including other road users) that the ADS is reasonably expected to encounter within the ODD are described. In the case of vehicles, this includes behaviours such as “acceleration”, “deceleration”, “cut-in”; for pedestrians, examples of dynamic behaviours include “crossing road”, “walking on sidewalk”, etc. Some of these behaviours may involve nominal situations (e.g., lead vehicle deceleration at a

[31]; E.g., *AVSC Best Practice for Describing an Operational Design Domain: Conceptual Framework and Lexicon*; and *A Framework for Automated Driving System Testable Cases and Scenarios* (NHTSA).

[32] *E.g. BSI PAS 1883:2020 Operational Design Domain (ODD) taxonomy for an automated driving system (ADS) - Specification*

[33] ASAM OpenODD

[34] Road Vehicles — Test scenarios for automated driving systems — Taxonomy for operational design domain

rate reasonably expected in light of traffic and other circumstances within the bounds of physical limitations[35]) while others may involve critical situations (e.g., sudden cut-ins or unpredictable pedestrian or cyclist behaviour, including behaviours that may violate local traffic laws such as crossing a road outside a designated cross walk).

The behaviour of other road users and the condition of physical objects within the ODD may fall at any point along a continuum of likelihood. For example, deceleration by other vehicles may range from what is expected and reasonable in the traffic circumstances, to unreasonable but somewhat likely rapid deceleration, to extremely unlikely (e.g., a sudden cut-in combined with full braking on a clear high-speed road). The analysis of the ODD and reasonably expected driving situations within the ODD should make distinctions that include an estimate of the likelihood of situations to ensure that the ADS's performance is evaluated based on response to reasonably likely occurrences involving nominal, critical and failure situations but not on the expectation that the ADS will avoid or mitigate the most extremely unlikely occurrences.

Table 1. Static / Dynamic elements and their properties

Objects	Events/Interactions
Vehicles (e.g. cars, light trucks, heavy trucks, buses, motorcycles)	Lead vehicle decelerating, Lead vehicle stopped, Lead vehicle accelerating, Changing lanes, Cutting in, Turning, Encroaching opposite vehicle, Encroaching adjacent vehicle, Entering roadway, Cutting out, …
Pedestrians	Crossing road -inside crosswalk, Crossing Road – outside crosswalk, Walking on sidewalk / shoulder
Cyclists	Riding in lane, Riding in adjacent lane, Riding in dedicated lane, Riding on sidewalk/shoulder, Crossing road – inside/outside crosswalk, …
Animals	Static in lane, Moving into/out of lane, Static/Moving in adjacent lane, Static/Moving on shoulder, …
Debris	Statis in lane
Other dynamic objects (e.g. shopping carts)	Static in lane, Moving into/out of lane,

[35] Deceleration of road vehicles is limited by tire-road friction and separating fluid, if any (e.g. wet, ice). It is only in some rare circumstances limited by brake capacity, specifically if the brake torque fades due to hot brakes.

	…
Traffic signs	Stop, Yield, Speed limit, Crosswalk, Railroad crossing School zone, …
Vehicle signals	Turn signals

Object and Event Detection and Response (OEDR) Analysis: Behavioural competency identification

Once the objects and their reasonably expected behaviours have been identified, it is possible to map the appropriate ADS response, which can be expressed as a behavioural competency. The detailed response is derived from more general and applicable functional requirements. The acceptable ADS response will vary depending on whether the driving situation involves nominal, critical, or failure characteristics.

The outcome of the analysis is a set of behaviour competencies that can be applied to the events characterizing the ODD. Table 2 provides a qualitative example of a matching event – response.

Table 2. Example of elementary behavioural competencies for given events.

Event	Response
Lead vehicle decelerating	Follow vehicle, decelerate, stop
Lead vehicle stopped	Decelerate, stop
Lead vehicle accelerating	Accelerate, follow vehicle
Lead vehicle turning	Decelerate, stop
Vehicle changing lanes	Yield, decelerate, follow vehicle
Vehicle cutting in	Yield, decelerate, stop, follow vehicle
Opposite vehicle encroaching	Decelerate, stop, shift within lane, shift outside lane
Adjacent vehicle encroaching	Yield, decelerate, stop
Lead vehicle cutting out	Accelerate, decelerate, stop
Pedestrian crossing road	Yield, decelerate, stop
Cyclist riding in lane	Yield, follow
Cyclist crossing road	Yield, decelerate, stop

The combination of objects, events, and their potential interaction, as a function of the ODD, constitute the set of nominal or critical situations pertinent to the ADS under analysis.

Nominal Situation Competencies

In these situations, ADS competencies can often be derived by applying traffic laws of the country where the ADS is intended to operate, as well as by applying general safe driving principles for situations not addressed adequately by current traffic laws for human drivers. Examples of such competencies may include adherence to legal requirements to maintain a safe distance from vehicles ahead, provide pedestrians the right of way, obey traffic signs and signals, etc. Of course, some nominal competencies (e.g., safe merging, safely proceeding around road hazards) may not be explicitly articulated or mandated by traffic laws. In some instances, traffic laws may provide wide discretion for the driver to determine the safest response to a particular situation (for example, how to respond to adverse weather conditions). As such not all traffic laws are stated with sufficient specificity to provide a clear basis for defining a competency.

Therefore, an approach to codify rules of the road to provide additional specificity was developed (see Appendix 1). Additionally, application of models involving safe driving behaviour may be needed in addition to reference to codified rules of the road in developing behavioural competencies for nominal driving situations.

Critical Situation Competencies

The development of these competencies requires analysis of (1) what constitutes such unreasonable behaviour by ORUs and/or a sudden change of the operating conditions that are not reasonably foreseeable and (2) what constitutes an appropriate ADS response to avoid or mitigate the imminent crash. Additionally, it is also important to identify the occurrence of unplanned emergent behaviour in critical situations.

Analysis of the first type may be based on a variety of methodologies, including e.g. IEEE 2846-2022 (which offers guidance on what behaviours by other road users are reasonably foreseeable) and other models of reasonable driving behaviour. Analysis of the second factor may be based on various models of acceptable human driving behaviour in crash imminent situations.

Hazard identification methods (e.g. STPA as mentioned in SAE J3187) which analyse the system design for functional and operational insufficiencies can help identify the occurrence of emergent behaviour which may lead to critical situations.

Development of behavioural competencies for critical driving situations faces several challenges. No general consensus exists on the appropriate models for the behaviour of ORUs or appropriate responses by the ADS to unreasonable ORU behaviours that make a crash imminent.

Failure Situation Competencies

The ADS safety requirements include management of various failure modes. As noted above, failure situations involve those in which the ADS or another vehicle system experiences a fault or failure that removes or reduces the ADS's ability to perform the DDT, such as sensor or computer failure or a failed propulsion system.

In developing the behavioural competencies appropriate for failure situations, the objective is to describe the ability of the ADS to detect and respond safely to specific types of faults and failures. Depending upon the nature and extent of the fault or failure, the responses can include identifying a minor fault for immediate repair after trip completion, responding to a significant fault with restrictions (such as limp-home mode) for the remainder of the trip, or responding to major failures by achieving a minimal risk condition. Communication of the fault or failure condition to vehicle users may also be a desirable ADS behavioural competency.

Scenario Identification

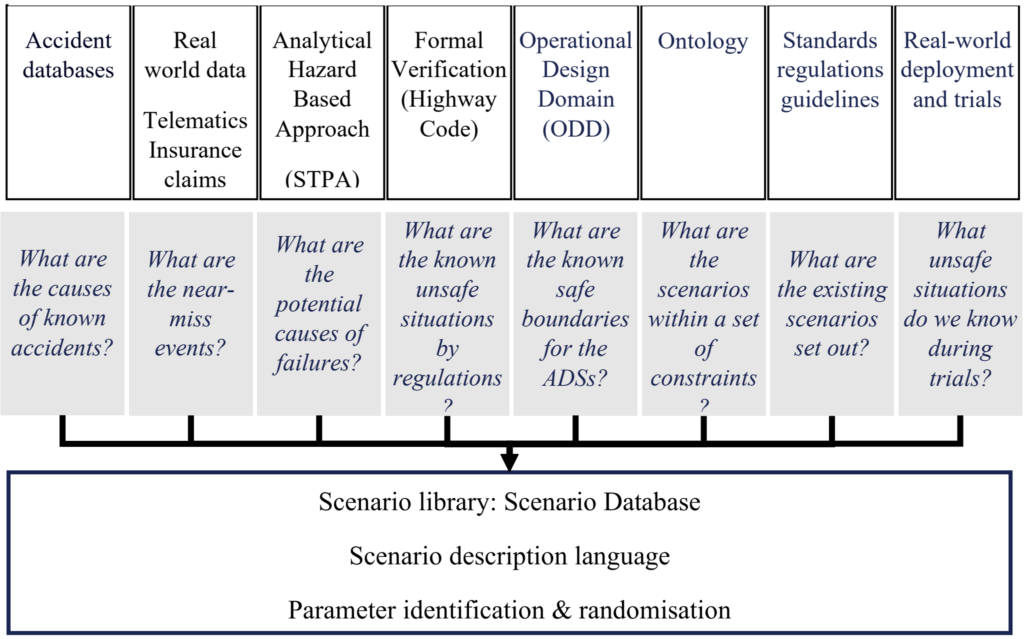
To ensure that the behavioural competences identified in the previous paragraphs are ready to be assessed through the application of simulations or physical testing, ODD-relevant scenarios must be developed. Scenario creation involves use of assumptions concerning the actions of road users that incorporate realistic parameters.

This approach suggests two complementary methodologies to derive reasonably expectable situations which might occur for a given ODD:

- Knowledge-based (e.g. goal-based)
- Data-based.

A knowledge-driven scenario generation approach utilizes domain specific (or expert) knowledge to identify hazardous events systematically and create scenarios. A data driven approach utilizes the available data (e.g. accident databases, insurance records) to identify and classify occurring scenarios. Figure 1 illustrates various data-based and knowledge-based scenario generation methods.

Figure 2. Data-based and knowledge-based scenario generation methods.


Accident databases
Real world data
Telematics Insurance claims
Analytical Hazard Based Approach
(STPA)
Formal Verification (Highway Code)
Operational Design Domain (ODD)
Ontology
Standards regulations guidelines
Real-world deployment and trials
What are the causes of known accidents?
What are the near-miss events?
What are the potential causes of failures?
What are the known unsafe situations by regulations ?
What are the known safe boundaries for the ADSs?
What are the scenarios within a set of constraints ?
What are the existing scenarios set out?
What unsafe situations do we know during trials?
Scenario library: Scenario Database
Scenario description language
Parameter identification & randomisation

Accident datasets and field data can be analysed to identify accident hotspots and scenario parameters which contribute to causation of accidents carrying high levels of severity.

Knowledge based methods, or other formal techniques can be used to analyse the characteristics of the ADS architecture and identify system failures and hazardous situations [see SAE J3187]. The analysis is then converted into a set of abstract/logical scenarios together with their corresponding pass/fail criteria.

Other knowledge-based methods include the formal analysis approach with the highway code rules for scenario generation. Each of the highway code rules describes a hypothetical driving scenario with the corresponding behaviour and ODD elements. The ODD is a specification set out by the manufacturer of an ADS and it defines the operating conditions within which the ADS can operate safely. Formal models are generated via a model template to create the mathematical representations of those scenarios, collecting the combinations of ODD and behaviour parameters. The analysis reports the manoeuvre parameters that are close of violating the pass criteria and produce scenarios that represent these set of violations. Other knowledge-based methods use formal representation of the ODD and behaviour competencies of the ADS for scenario generation.

Furthermore, the existing scenarios already defined in the standards, regulations or guidelines (Option 6 - KB) can also be utilized for the testing of ADSs, for example the scenarios set out in ISO22737 and NCAP. ISO22737 has been developed for low-speed automated driving systems (LSAD) and the NCAP provides a set of testing scenarios for the safety assurance of vehicles. Option 7 (DB) includes the scenarios that occur during real world trials and deployments. Such scenarios might have not been considered pre-deployment but are key learnings.

Assumptions: Logical to concrete scenarios

Assumptions concerning the actions of other road users may need to account for cultural differences in driving styles in different geolocations, making it impracticable to harmonise these assumptions across different domains. Therefore, evidence should be provided to support the assumptions made. Existing standards e.g. IEEE 2846-2022 provide a set of assumptions to be considered by ADS safety-related models for an initial set of driving situations. Additionally, several other tools including data collection campaigns performed during the development phase, real-world accident analysis and realistic driving behaviour evaluations, constraint randomisation, Bayesian optimisation besides others can be used to inform values for such assumptions.

Application of Rules of Road as Pass criteria and requirements

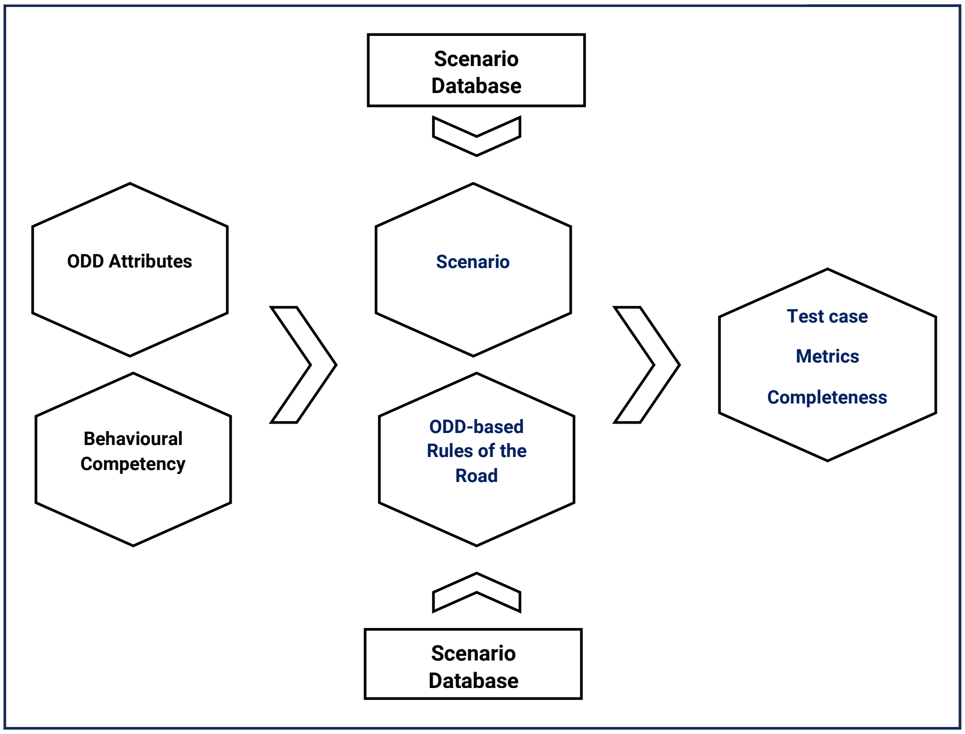
An approach to define an acceptance criterion related to nominal driving situations is to evaluate the ADS performance against the rules of the road. Furthermore, ADS safety requirements state that *"The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation."* It is challenging to test against this requirement in the absence of codified rules of the road.

Appendix 1 of this annex provides a framework for codifying the rules of the road that govern the behaviour of ADS. The approach may be used to define "good behaviour" to inform validation and verification processes (including for scenario-based testing) for nominal scenarios.

Using rules of the road as pass criteria

Figure 3 illustrates the use of codified rules of the road as a pass criterion for scenario-based testing activities. Every test scenario definition will have ODD and behaviour competency attributes defined. Every rule of the road will also have ODD and behaviour competency attributes as part of its definition. Therefore, it is possible to map every scenario to a corresponding rule(s) of the road using ODD and behaviour tags or labels in a scenario catalogue.

Figure 3. Rules of the road as pass/fail criteria.



This approach would allow the test engineer to map each scenario to a corresponding rule (or set of rules). These rules can then serve as the pass criteria during the scenario-based testing approach. This approach can thus enable engineers and authorities to show/assess compliance to traffic rules by making the rules of the road verifiable.

Application of Safety Models to Derive Verifiable Performance Requirements for Accident Avoidance

Despite the fact that behavioural competencies will help the automated vehicle to not cause accidents or drive defensively to stay away from conflicts, there are situations where automated vehicles have to react to unexpected situations, e.g. where other traffic participants cause situations which can end up in accidents. It is the task of the automated driving system – like it is the task for human drivers – to perform evasive actions, whether it is possible and reasonable in order to minimize any human harm.

One important question is – to what extent and depending on what circumstances is collision avoidance possible? This question will have to be answered when developing concrete new regulations (UN regulations and/or Global Technical Regulations) for automated driving systems.

For this, simple logic models, the so-called safety models, are introduced. They provide assumptions how traffic rule violations and misbehaviour by other traffic participants could be dealt with and use physical properties and fundamental driving dynamics to further detail conditions for accident avoidance.

The purpose of this document is to define a process as to how concrete performance criteria for future ADS regulations could be developed.

The set of safety models described in this document should be regarded as a set of tools, whereas selecting the right tool (the right safety model) depends on the boundary conditions and should be the task of groups dedicated to writing concrete regulations. Hence in this document, there exists no preference for any of the safety models being depictured.

Two important points to consider: safety models are a methodology to derive a threshold vector to separate between collisions that have to be avoided and those where only mitigation is required. The aim is NOT to prescribe a specific behaviour of the ADS in any given critical situation. This is only about the expected outcome. However, the safety model selected need to fit the use case. E.g. a steer-around model cannot be selected for cases without a second lane.

Also, the characteristics for typical/generic vehicles given below should not be used to calculate accident avoidance for the specific vehicle in the approval process, but for typical/generic vehicles. The reason for this is that low required accident-avoidance capabilities could be a wrong incentive in the vehicle design process.

In a mathematical & logical sense, for any given situation, there will be a function depending on variables that partly describe a scenario, delivering a Boolean "true" or "false" for whether the collision needs to be avoided, and vice versa for whether mitigation is acceptable:

$$Avoidance[0;1] = f_{safetymodel}(scenario\ variable\ 1, scenario\ variable\ 2, \dots),$$

$$Mitigation[0;1] = 1 - f_{safetymodel}(scenario\ variable\ 1, scenario\ variable\ 2, \dots).$$

It is envisioned that concrete ADS regulations, (being) built by using the guidelines as specified here, may contain either a concrete scalar threshold (example: avoid accidents for a driving speed below 42 km/h, see UN R152), or formulate a concrete fsafetymodel where all parameters are specified (simplified example from UN R157: when cut-ins of other vehicles occur before a specific TTC, the collision needs to be avoided, the resulting function as given in the regulation would be:

$$f_{\text{safetymodel}} = [1 \text{ for } TTC_{LaneIntrusion} > (v_{rel}/(2 \cdot 6\text{m/s}^2) + 0.35s);\ 0 \text{ otherwise}].$$

Choosing appropriate model(s) depends, amongst others, on:

- the balance between risk to the ADS itself vs. risk towards the accident partner (e.g. for pedestrians, it would very likely be acceptable to have a slightly increased risk for the typically belted ADS occupants when the risk for the pedestrian would be significantly reduced, e.g. by earlier or stronger brake intervention; for unmanned ADS similar risk balance considerations have to be done),

- the assumed anticipation level (e.g. is it feasible to anticipate actions of other traffic parameters and start countermeasures earlier, or will it be a simple reaction to faults),
- the environmental condition parameters. (e.g. what level of friction is typically available where the ADS are travelling),
- the balance between efficiency and acceptable remaining risk (e.g. passing a pedestrian with no acceptable risk would be possible only with very low speeds, which would render the current sidewalk close to streets infrastructure useless for automation).

These factors will be different for different situations, or in other words: there would be different fsafetymodel,i for different critical situations anticipated to occur in the operational domain of the concrete ADS regulation in pseudo-code:

```
Example Regulation XXX =
{Situation / parameter range 1, avoidance = fsafetymodel,1(parameters a,b,c);
        # address pedestrian accidents in urban areas
Situation / parameter range 2, avoidance = fsafetymodel,2(parameters d,e,f);
        # address car-car accidents with cut-in on motorways…}.
```

The safety models can be grouped into models for the performance in accident avoidance and behaviour models for conflict avoidance, see Table 3. The difference between those two is that the accident avoidance models can be used to understand to what extent accident situations – caused by other traffic - are unavoidable, while conflict avoidance models formalize strategies for the behaviour of an ADS to not come into conflict. Conflict avoidance models are better suited being integrated into the document on the dynamic driving task.

*Table 3. Overview of Safety Models**

Model	*Explanation*
Performance Requirements for Accident Avoidance	
Last Point to Steer	Estimate avoidance and mitigation in longitudinal traffic, typically used for driver assistance & active safety
Safety Zone	Estimate avoidance and mitigation in cross-traffic accidents with VRU
Careful and Competent Human Driver	Estimate avoidance and mitigation in longitudinal traffic cut-in situations, using reaction characteristics of good human driver
Fuzzy Surrogate Safety Model	Estimate avoidance and mitigation in longitudinal traffic cut-in situations, taking anticipation of other vehicle behaviour into account

*Models discussed during guidelines development and not intended as exhaustive list.

These guidelines recommend the development of regulatory provisions to permit the use of safety models, including but not necessarily limited to the approaches described in this annex, to generate verifiable criteria for the assessment of ADS performance with regard to collision avoidance under critical traffic scenarios.

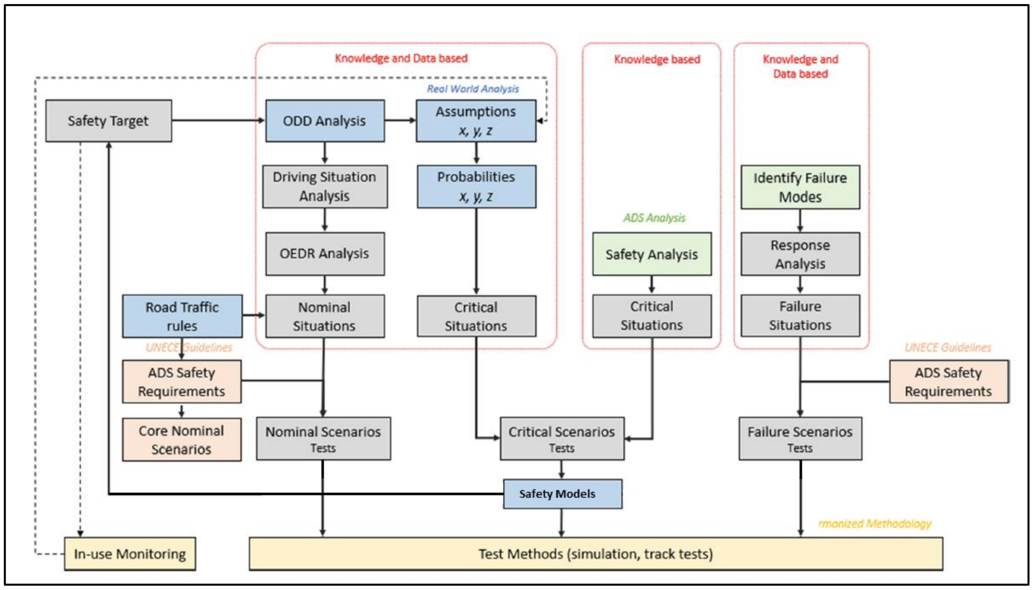
Performance Evaluation and Targets

As previously highlighted, nominal situations are considered reasonably foreseeable and preventable for a given ODD and therefore it is expected that the ADS would be capable of handling them without any resulting collision.

On the other hand, failure situations are performed to assess the ADS ability to recognise faults/failures in the system.

For the purpose of defining performance criteria in critical situations, those where others are at fault, behaving unforeseeably, and the collision might potentially not be prevented have to be analysed further. In these situations, it is proposed that safety models are used to explore and compare the ADS performance with mathematical formulations to derive what is deemed as preventable or where mitigation strategy is needed.

Figure 4. Approaches to derive verifiable performance criteria



Annex 1—Appendix 1

Codification methodology for rules of the road

Current rules of the road (for human drivers) have three components:

Rule of road
(for human drivers) = *Operating condition + Behaviour competency + Assumptions (implicit)*

Operating conditions include both ODD aspects and vehicle states (e.g., system failures, hardware failures etc.). Every set of traffic laws or behaviour rules (for human drivers) defined in any country are based on an understanding of the expected behaviours of human drivers. As a result, they do not explicitly define all aspects of the expected driving behaviour but can be argued to include "implicit assumptions" based on this understanding.

Following the process (illustrated in section 8.1), a "codified" rule of the road for an automated driving system, will also have three components:

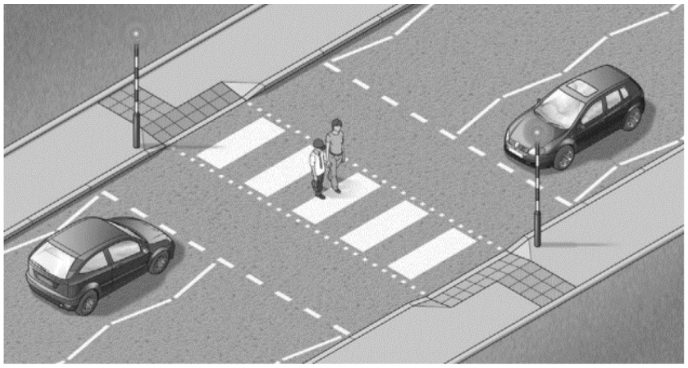
Codified Rule of road = Operating condition + Behaviour competency + Driving decisions

The process of codification helps identify where "implicit assumptions" about driving behaviour are present in the rules for human drivers. The codified rules of the road help to turn "undefined" attributes in the rules of the road (for human drivers) to "defined" attributes in the codified "rules of the road".

Taking an example of the UK road rules where behaviour (for human drivers) is governed by the Highway Code (HC), the methodology is further explained. UK's Highway Code Rule 195 states (Zebra crossing):

> *Rule 195: "As you approach a zebra crossing: look out for pedestrians waiting to cross and be ready to slow down or stop to let them cross; you MUST give way when a pedestrian has moved onto a crossing."*

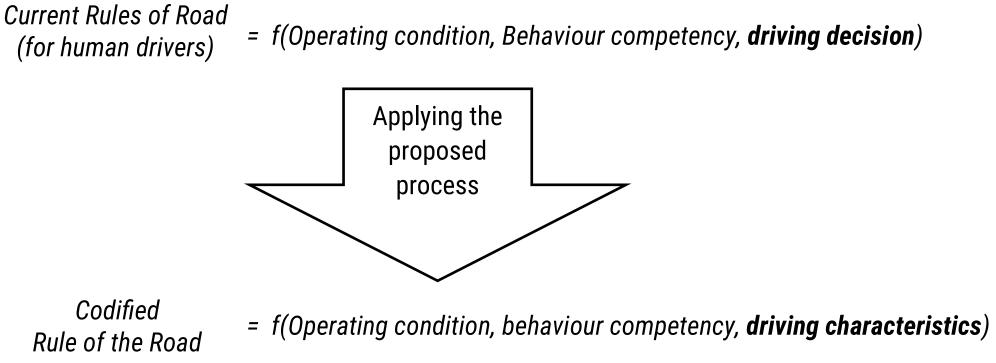
Figure 3: Example of zebra crossing from UK's Highway Code:
Source: https://www.gov.uk/guidance/the-highway-code/rules-for-pedestrians-1-to-35#rule19



From this rule, one can extract the "operating condition or ODD" variables, as well as the behaviour competencies. "Zebra crossing" and "pedestrian" define the operating condition; and "slow down or stop" defines the behaviour competency. However, the rule doesn't mention for how long the vehicle should be stopped, or when it is considered safe to proceed again. There is an "implicit assumption" made based on typical human (the driver behaviour), and it is not considered necessary for the rule to define this. However, for an ADS, such assumptions how long the vehicle is stopped for, and when it moves off again will be determined by the automated driving system and its analysis of the relevant parameters specific to that situation and will need to be specified. For every concrete scenario being tested, the driving decisions exhibited by ADS will need to be explainable.

Figure 4 illustrates this process. After following the codification process of defining the "rules of the road", there will be no underlying "assumptions" (see Codification methodology below).

Table 4. Converting current rules of the road (for human drivers) to codified rules for ADS.



Current Rules of Road (for human drivers) = f(Operating condition, Behaviour competency, ***driving decision****)*

Applying the proposed process

Codified Rule of the Road = f(Operating condition, behaviour competency, ***driving characteristics****)*

Furthermore, for all areas or jurisdiction or country, there will be a minimum set of behaviour code rules which will have consistent "driving characteristics" – the base or common set of rules of the road (for ADS).

Codification methodology

The codification methodology is a four-step process:

- Step 1: Identify terms and construct a vocabulary: The natural language text of the rule is analysed and words that are associated with the ODD or behaviour of actors in the rule are identified. These terms taken together are used to identify the component of the rule that can be codified.
- Step 2: Identify unspecified terms: Some terms are unclear because they are not unequivocal or absolute and therefore require clarification. In some cases, these terms are codified as is, when a meaning can be inferred, while in others, comments are provided to highlight why the terms are not defined, and how they may be elaborated.
- Step 3: Query / Update/ Add ODD and Behaviour terms: Terms defining predicates (representing facts whose truth may be evaluated) and functions (representing non-Boolean properties – such as ADS attributes, action labels) are identified. The codified rule will consist of these predicates and functions. The outcome of Step 3 is an intermediate rule that is in its minimal form.
- Step 4: Express rule in first order logic: For each rule of the road, a single codified rule, or a set of rules are written. The predicates and functions identified in Step 3, together with the structure of constraints from Step 1 are used to construct the rule(s). The output of Step 2 provides insights concerning the rule and gaps that exist in its codification. Step 4 uses the vocabulary to identify which sub-rules are to be converted to First Order Logic and then perform the conversion.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Vienna Convention codification example

The Vienna convention rule is stated below (Chapter 2 – Rules of the Road – Article 11 (Overtaking – 11)).

Vienna Convention Rule Text:

> *A vehicle shall not overtake another vehicle which is approaching a pedestrian crossing marked on the carriageway or signposted as such, or which is stopped immediately before the crossing, otherwise than at a speed low enough to enable it to stop immediately if a pedestrian is on the crossing.*

The following sections take this rule through each step, explaining how each component of the codification process works.

Step 1: Identify Terms and Construct a Vocabulary

The rule is re-stated below highlighting important terms:

> A vehicle **shall not overtake another vehicle** which is **approaching** a **pedestrian crossing** marked **on** the **carriageway or signposted** as such, **or** which is **stopped immediately before** the **crossing**, **otherwise** than at a **speed low enough** to **enable** it to stop immediately **if** a **pedestrian** is **on** the **crossing**.

Terms that are ODD and behaviour related are in bold and underline, while other terms that are relevant to giving the rule meaning are in bold.

Step 2: Identify Unspecified Terms

From the example above, the terms that remain underspecified are as follows:

Term	Specification Required
Immediately	How is immediately defined? A *distance* may be used to define this.
Low enough	What speed is considered low enough? This could be a function of distance to the pedestrian, or an absolute threshold.
**Overtaking is an action that is applicable to vehicles that are ahead of the ego*	This is an assumption that is understood by a human reader.

Step 3: Identify Predicates and Functions

The non-highlighted terms are removed and only terms that are important to the meaning of the rule are kept.

Shall not overtake another vehicle

- **approaching pedestrian crossing on carriageway or signposted,**

- **or stopped immediately before crossing**,

otherwise speed low enough enable stop immediately if pedestrian on crossing.

The terms identified are converted into predicates. For the VC Rule, we construct the following predicates:

Predicate	Description
isEgo(x)	x is the Ego
canOvertake(x,y)	x can overtake y
isApproaching(x,y)	x is approaching y
isPedestrianCrossing(x)	x is a pedestrian crossing
isCarriageway(x)	x is a carriageway
isSignposted(x)	x is signposted
isStopped(x)	x is stopped
isAhead(x,y)	x is ahead of y
hasSpeed(x,y)	x has speed y
isLowEnoughSpeed(x,y)	x is a low enough speed for action y

Step 4: Express Rule in First Order Logic

The rule determines overtaking behaviour for a vehicle that is close to a pedestrian crossing. The rule contains conditions that would prevent a vehicle from overtaking another, but simultaneously provides an exception, that of being slow enough to stop. Further, the ability of the vehicle to stop is independent of whether there is an actor (such as a pedestrian) on the crossing. The rule makes references to the vehicle having a slow enough speed to stop immediately, which has been identified as an ambiguous phrase and represented as a predicate in Step 3. To represent the action of stopping immediately, we use the constant “STOP_IMM”.

For ease of understanding, the rule may be broken down into four logical statements, that are logically related, with the relationship being stated as the last rule. The predicates that were produced as an outcome of Step 1 are used to construct the logic specification for the rule.

The parameters for the rules: the ego vehicle (x), the other actor (y), the pedestrian crossing (w), the carriageway (c), the speed of the ego (s).

The rules are as follows:

Rule (a):	isEgo(x) ∧ isOtherRoadUser(y)	x is the ego and y is the other vehicle

Rule (b):	isPedestrianCrossing(w) Λ (isCarriageway(c) V isSignposted(w))	w is a pedestrian crossing and (c is a carriageway or w is signposted)
Rule (c):	isApproaching(y,w) V isAhead(w,y)	y is approaching w, or w is ahead of y
Rule (d):	hasSpeed(x,s) Λ ¬isLowEnoughSpeed(s,STOP_IMM)	x has speed s, and s is not a low enough speed to stop immediately.
The Rule	*(a) Λ (b) Λ (c) Λ (d) → ¬canOvertake(x,z)*	

The symbol "¬" when used as a prefix to a predicate indicates the negation of the predicate. In this context, in English, the rule may be read as: If "a" is true, and "b" is true, and "c" is true, and "d" is true, then x cannot overtake z. Note that the exception condition, that of being slow, is used in its negative form to assert that the vehicle cannot overtake, since this is explicit in the rule. It is left to interpretation if a positive rule, specifically allowing the vehicle to overtake is necessary. If so, a new rule that allows a vehicle to overtake must be written. This would depend on the interpretation of the rule.

Annex 4: Traffic Scenarios

At this relatively early stage in the development of ADS, much of the existing literature that assesses the current state of ADS development uses metrics such as miles/kilometres travelled in real-world test situations with the absence of a collision, a legal infraction, or a disengagement by the vehicle's ADS.

Metrics such as kilometres travelled without a collision, legal infraction, or disengagement can be helpful for informing public dialogue about the general progress being made to develop ADS. Such measurements on their own, however, do not provide sufficient evidence to the international regulatory community that an ADS will be able to safely navigate the vast array of different situations a vehicle could reasonably be expected to encounter.

Furthermore, validation through real world testing alone would be time and cost prohibitive, potentially requiring an ADS to drive billions of kilometres without incident to prove that it has significantly better safety performance than a human driver. It would also not be feasible to replicate this testing later if there was a change to the system that needed to be re-validated.

With these considerations in mind, it is recommended that a scenarios-based approach be used to systematically organize safety validation activities in an efficient, objective, repeatable, and scalable manner.

Scenarios based validation consists of reproducing specific situations that exercise and challenge the capabilities of an ADS-equipped vehicle to operate safely.

It is recommended that future work will establish a catalogue of scenarios that can be used by the various NATM pillars to validate the functional safety requirements established by FRAV. The section below shows some initial examples of how such a catalogue could be formed focusing on the highway use case.

What is a traffic scenario?

A scenario is a description of one or more driving situations that may occur during a given trip[36]. Scenarios can involve many elements, such as roadway layout, types of road users, objects exhibiting static or diverse dynamic behaviours, and diverse environmental conditions (among other factors).

Ensuring adequate scenario coverage

It is recommended that the scenarios-based validation methods include adequate coverage of relevant, nominal, failure, critical, and complex scenarios to effectively validate an ADS. To note: "Coverage" refers to the degree to which scenarios sufficiently incorporates driving situations in order to validate the relevant requirements defined by FRAV. Sufficient coverage is essential to the overall effectiveness and credibility of this methodology as a validation approach. Sufficient

[36] A trip is a traversal of an entire travel pathway by a vehicle from the point of origin to a destination.

coverage should be with respect the ADS feature or ODD. Coverage can be measured across different domains, and metrics can be used to determine sufficiency.

When validating the safety of an ADS, it is recommended that each scenario selected to test the ADS precisely reflects the particular conditions (e.g., road configurations, direction of traffic in a given lane, etc.) that constitute the ODD in which the ADS is designed to operate. Scenarios should be relevant to the ADS feature being validated. For example, an ADS feature intended only for highway use would not be subject to a scenario involving turns at intersections with the exception of testing outside its ODD

Because an ADS will need to be responsive to actions by other road users, which may make a crash unavoidable, it is recommended that scenarios are not limited to those that are deemed preventable by the ADS. Unsafe behaviours of other road users (e.g. vehicle travelling in the wrong direction, sudden unsignalled lane changes, and exceeding the speed limit) —if reasonably foreseeable within the appropriate ODD— should be included as part of validation testing.

Consideration should be given to the many approaches that can be used to identify scenarios for safety validation purposes, including:

(a) Analysing human driver behaviour, including evaluating naturalistic driving data;

(b) Analysing collision data, such as law enforcement and insurance companies' crash databases;

(c) Analysing traffic patterns in specific ODD (e.g., by recording and analysing a road user behaviour at intersections);

(d) Analysing data collected from ADS' sensors (e.g., accelerometer, camera, radar, and global positioning systems);

(e) Using a specially configured measurement vehicle, onsite monitoring equipment, drone measurements, etc. for collecting various traffic data (including other road users);

(f) Knowledge/experience acquired during ADS development;

(g) Synthetically generated scenarios from key parameter variations;

(h) Engineered scenarios based on functional safety requirements and safety of intended functionality;

(i) composing complex scenario from existing catalogues of basic scenarios; and

(j) Random variations of all scenario parameters, both for the ADS an ORUs.

A scenario catalogue would not necessarily be exhaustive and authorities may need to consider additional scenarios as necessary to support safety validation of an ADS feature.

Classifying scenarios

The amount of information that is included in a scenario can be extensive. For example, the description of a scenario could contain information specifying a wide range of different actions, characteristics and elements[37], such as objects (e.g., vehicles, pedestrians), roadways, and environments, as well as pre-planned courses of action and major events that should occur during the scenario. Therefore, it is critical that a standardized and structured language for describing scenarios is established so that ADS stakeholders understand the intention of a scenario, each other's objectives, and the capabilities of an ADS. One tool for establishing uniform language for describing a scenario is a template, which ensures that the information to be included in the scenario is consistent and minimizes the possibility of confusion in its interpretation.

It is recommended that a uniform language be used to describe a scenario to ensure that the information included is consistent and minimizes the possibility of confusion in its interpretation.

It is recommended to describe scenarios by different levels of abstraction. Abstraction supplies the ability to focus the scenario description on specific aspects, while leaving other details for further processing as needed. Some Industries and researches are proposing 3 or 4 levels of scenario abstraction: Functional, Abstract, Logical, and Concrete. The essence of these levels is described below. The 3 or 4 levels do not imply nor mandate any specific implementation or translation flow from one level to the other.

(a) Functional Scenario: A scenario described in natural language on a conceptional level, in general without specific physical values. These are scenarios with the highest level of abstraction, outlining the core concept of the scenario, such as a basic description of the ego vehicle's actions; the interactions of the ego vehicle with other road users and objects; and other elements that compose the scenario (e.g. environmental conditions etc.). This approach uses accessible language to describe the situation and its corresponding elements.

(b) Abstract Scenario: A formalized, declarative description of the scenario derived from functional scenario.[38] The specification on the abstract level enables highlighting of the relevant aspects of the scenario while focusing on efficient description of relations (Cause-effect).

(c) Logical Scenario: A scenario described with the inclusion of parameters, where the values of some of the parameters are defined as ranges. For example, building off the elements identified within the functional scenario, developers generate a logical scenario by selecting value ranges or probability

[37] Traffic scenarios are derived by combining a number of relevant elements describing the scenario space systematically.

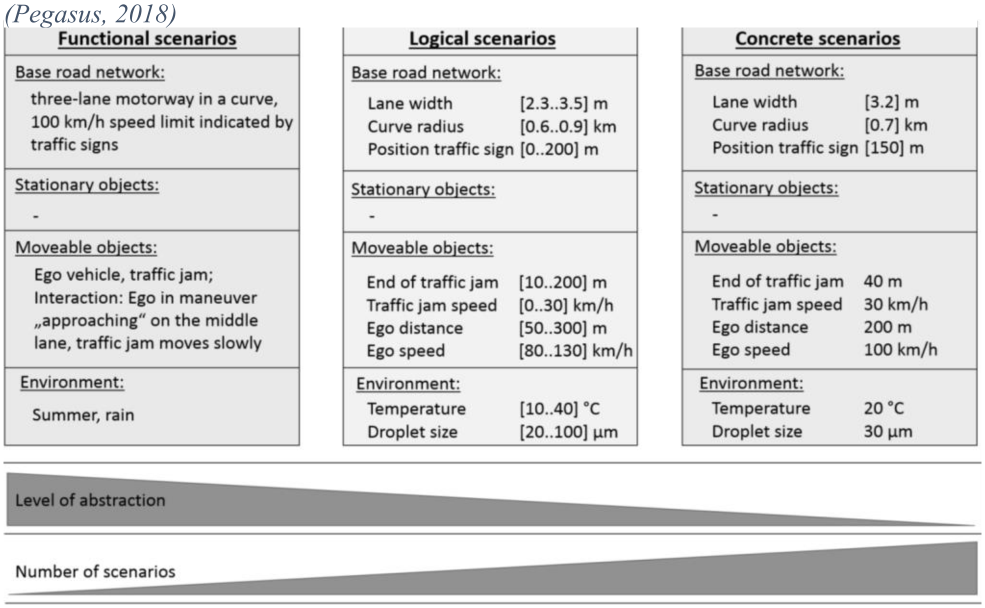
[38] Declarative description can include structured natural language, programming language or other forms of languages that meet the required criteria (formalized and declarative).

distributions for each element within a scenario (e.g., the possible width of a lane in meters).

(d) Concrete Scenarios: A scenario depicted with explicit parameters values, describing physical attributes. Concrete scenarios are established by selecting specific values for each element. This step ensures that a specific test scenario is reproducible. In addition, for each logical scenario with continuous ranges, any number of concrete scenarios can be developed, helping to ensure a vehicle is exposed to a wide variety of situations.

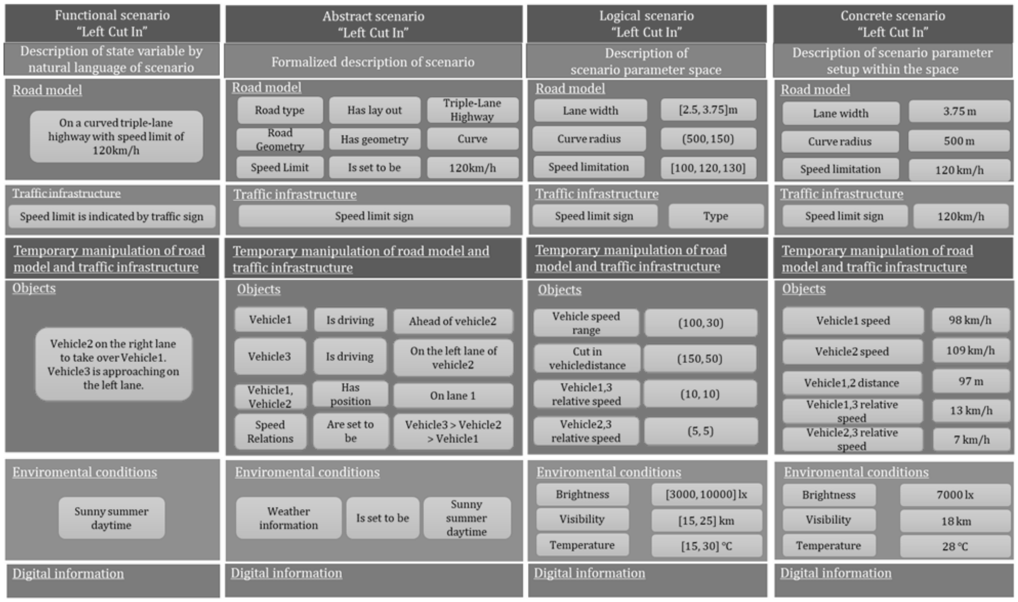
The following figures represents different options of using the levels of abstractions in order to derive concrete scenarios, other implementations are also possible.

Figure 5. Examples of a scenario using functional, logical, and concrete categorizations (Pegasus, 2018)



Functional scenarios	Logical scenarios	Concrete scenarios
Base road network: three-lane motorway in a curve, 100 km/h speed limit indicated by traffic signs	Base road network: Lane width [2.3..3.5] m Curve radius [0.6..0.9] km Position traffic sign [0..200] m	Base road network: Lane width [3.2] m Curve radius [0.7] km Position traffic sign [150] m
Stationary objects: -	Stationary objects: -	Stationary objects: -
Moveable objects: Ego vehicle, traffic jam; Interaction: Ego in maneuver „approaching“ on the middle lane, traffic jam moves slowly	Moveable objects: End of traffic jam [10..200] m Traffic jam speed [0..30] km/h Ego distance [50..300] m Ego speed [80..130] km/h	Moveable objects: End of traffic jam 40 m Traffic jam speed 30 km/h Ego distance 200 m Ego speed 100 km/h
Environment: Summer, rain	Environment: Temperature [10..40] °C Droplet size [20..100] µm	Environment: Temperature 20 °C Droplet size 30 µm

Figure 6. Examples of the relationship of functional scenario, abstract scenario, logical scenario and concrete scenario (ISO 34501)



Functional scenario "Left Cut In"	Abstract scenario "Left Cut In"	Logical scenario "Left Cut In"	Concrete scenario "Left Cut In"
Description of state variable by natural language of scenario	Formalized description of scenario	Description of scenario parameter space	Description of scenario parameter setup within the space
Road model On a curved triple-lane highway with speed limit of 120km/h	Road model Road type – Has lay out – Triple-Lane Highway Road Geometry – Has geometry – Curve Speed Limit – Is set to be – 120km/h	Road model Lane width – [2.5, 3.75]m Curve radius – (500, 150) Speed limitation – [100, 120, 130]	Road model Lane width – 3.75 m Curve radius – 500 m Speed limitation – 120 km/h
Traffic infrastructure Speed limit is indicated by traffic sign	Traffic infrastructure Speed limit sign	Traffic infrastructure Speed limit sign – Type	Traffic infrastructure Speed limit sign – 120km/h
Temporary manipulation of road model and traffic infrastructure	Temporary manipulation of road model and traffic infrastructure	Temporary manipulation of road model and traffic infrastructure	Temporary manipulation of road model and traffic infrastructure
Objects Vehicle2 on the right lane to take over Vehicle1. Vehicle3 is approaching on the left lane.	Objects Vehicle1 – Is driving – Ahead of vehicle2 Vehicle3 – Is driving – On the left lane of vehicle2 Vehicle1, Vehicle2 – Has position – On lane 1 Speed Relations – Are set to be – Vehicle3 > Vehicle2 > Vehicle1	Objects Vehicle speed range – (100, 30) Cut in vehicledistance – (150, 50) Vehicle1,3 relative speed – (10, 10) Vehicle2,3 relative speed – (5, 5)	Objects Vehicle1 speed – 98 km/h Vehicle2 speed – 109 km/h Vehicle1,2 distance – 97 m Vehicle1,3 relative speed – 13 km/h Vehicle2,3 relative speed – 7 km/h
Enviromental conditions Sunny summer daytime	Enviromental conditions Weather information – Is set to be – Sunny summer daytime	Enviromental conditions Brightness – [3000, 10000] lx Visibility – [15, 25] km Temperature – [15, 30] ℃	Enviromental conditions Brightness – 7000 lx Visibility – 18 km Temperature – 28 ℃
Digital information	Digital information	Digital information	Digital information

Scenario usage

The use of scenarios can be applied to different testing methodologies, such as virtual/simulation, test track, and real-world testing. Together, these methodologies provide a multifaceted testing architecture, with each methodology possessing specific strengths and weaknesses. Therefore, some scenarios may be more appropriately tested using certain test methodologies over others.

It is recommended that sampling techniques be used when selecting parameters to be used in creating logical and concrete scenarios for ADS validation for a particular ADS and its ODD to avoid the ADS being optimized for a set of known test cases. Using a maxim number of random samples is clearly preferable from a credibility perspective, it is recognized that this can place a greater burden on manufacturers and the relevant authority (e.g. technical service). This should be considered when determining the volume of tests to be conducted when using the random sampling. It is assumed that for simulation/virtual testing the burden of random sampling is less and therefore maximizing the number of random samples for this facet of the testing is more feasible.

Scenario template

It is recommended that scenarios included within a possible future scenario catalogue should follow a common template to ease comparison of scenarios and aid authorities in determining which scenarios are appropriate for testing a particular ADS.

a) Scenario Name

A title describing the scenario.

b) Scenario ID

Unique identifying number.

c) Contributed by

Which organisation contributed the scenario.

d) Scenario source

What is the source of this scenario (e.g., ISMR, synthetic scenario, other regulation, accident database etc)? This includes the geographical location of an original incident (if applicable))

e) Version

Version of the scenario to track updates, contains date of submission.

f) Graphic

A graphic describing the scenario, movements may be represented as well by arrows or other graphics means. This graphic may be 2D or 3D.

g) Functional Scenario Description

A section with textual description of the scenario. This may include some specific testing and safety evaluation goals. This description could be either structured or unstructured natural language.

h) ODD Tags[39] [40]

Scenery elements (road details, buildings etc.),
Environmental conditions,
Dynamic elements (elements in motion)

i) Behaviour Tags[3]

Ego vehicle behaviour and actions during the scenario. It may also indicate expected responses.
Behaviours for all other active actors in the scenario.

j) Type of scenario

Nominal, Critical, or Failure

These scenario types are defined by the external conditions rather than the ADS, further work is required in order to determine classification for the catalogue. At the functional level more than one option may be appropriate.

[39] There are many standards of tags used for ODD and Behaviour, they may be used to create a list of common tags to be used in the catalogue.

[40] ODD tags in the scenario template are not to be interpreted as “scenario ODD”, but rather refer to the tags of the ODD of the ADS to be tested using the scenario. This is to aid the user of the catalogue to search for scenarios relevant to the ODD of the ADS to be tested. ODD is a design artefact of the subject vehicle and is determined by the ADS developer.

k) Range of applicability

Range and/or parameter constraints on usage of the scenario

l) Abstract Scenario (Optional)

A formalized, declarative description of the scenario[41] derived from the functional scenario. The specification on the abstract level enables highlighting of the relevant aspects of the scenario while focusing on efficient description of relations (cause-effect).

Annex 4—Appendix 1

This appendix provides a synthesis of various elaborations of traffic scenarios with the designated purpose to create a functional scenario list for ADS in motorway use-cases. ODD range: Highways with up to 130 km/h and lane changes allowed.

Building blocks of functional scenarios

Functional scenarios can cover several aspects (e.g., road geometry at different abstraction levels, environmental conditions, ego-vehicle behaviour, moving/stable objects).

Additional aspects that are not covered by functional scenarios (e.g., absolute speeds, accelerations, positions, failures, miscommunications, road geometries at more detailed levels) should be covered by logical scenario.

Since classification of aspects to functional and logical scenarios (i.e., “which aspects should be considered in functional scenarios” and “which aspects should be considered in logical scenarios”) has not yet been discussed and agreed, the classification in this document is an initial version and should be updated through discussion.

Coverage

Collisions always occur with other vehicles/objects (assuming that they can operate properly when there are no other vehicles/objects). Interaction with other vehicles under nominal driving can cover all interactions between other vehicles/objects and ego vehicle. These scenarios can cover collision with other vehicles/objects appropriately.

As described above., factors not covered in the proposed functional scenarios (e.g. initial speed of ego vehicle, size, initial position, initial speed, acceleration of other vehicles/objects), some perception factor (e.g. brightness, blind spot, false positive

[41] Declarative description can include structured natural language, programming language or other forms of languages that meet the required criteria (formalized and declarative).

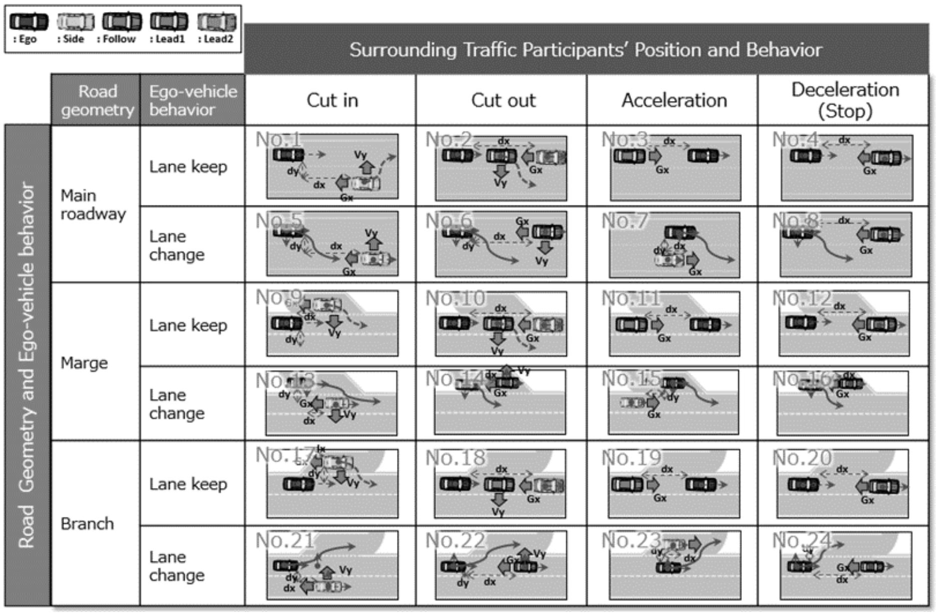
factor, blinkers of other vehicles) and vehicle stability factors (e.g. details of curve, slope, road surface μ, wind, etc.) can be described with parameters in logical scenarios.

Approach for scenario family identification

Scenario families will generally have some combination of road layout configuration and ego-vehicle and other vehicle behaviour. Figure 1, illustrates some of these combinations for a motorway use case with road geometry and ego behaviour on the y-axis and surrounding traffic vehicle behaviour on the x-axis.

The 24 scenario families in Figure 1 can cover the interaction with other vehicles driving in the same direction on the same or adjacent lanes.

Figure 7. Example of scenario families



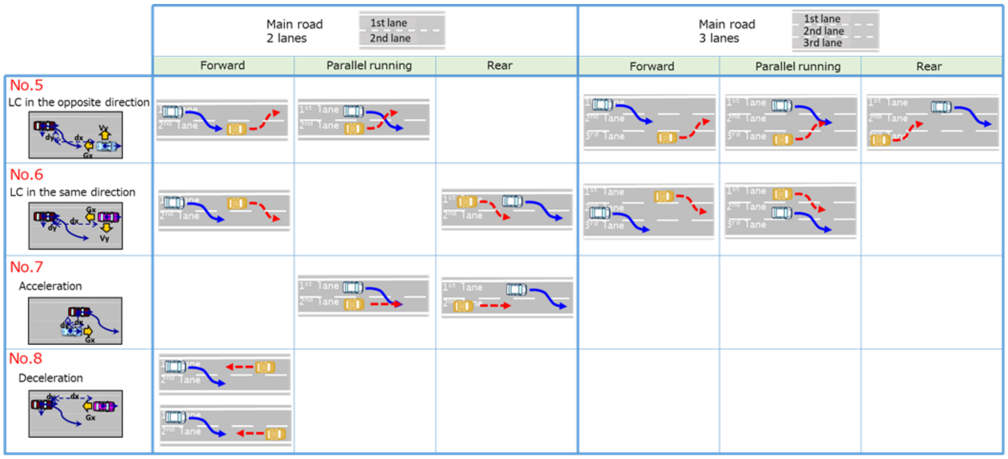
Road Geometry and Ego-vehicle behavior		Surrounding Traffic Participants' Position and Behavior			
Road geometry	Ego-vehicle behavior	Cut in	Cut out	Acceleration	Deceleration (Stop)
Main roadway	Lane keep	No.1	No.2	No.3	No.4
	Lane change	No.5	No.6	No.7	No.8
Marge	Lane keep	No.9	No.10	No.11	No.12
	Lane change	No.13	No.14	No.15	No.16
Branch	Lane keep	No.17	No.18	No.19	No.20
	Lane change	No.21	No.22	No.23	No.24

In the 12 scenarios in which the ego vehicle performs lane change, the vehicle closest to the ego vehicle may not be necessarily in the same lane or an adjacent lane to the ego vehicle. It may be 2 lanes over from the ego vehicle, and even in such cases, the vehicle has to be detected by the ego vehicle because they can interact with one another if both change lanes. To describe these cases in the 12 scenarios properly, some parameters should be included at the logical scenario level such as “number of lanes”, “lane of ego vehicle” and “relative position between ego and other vehicle”. The examples of “main road case” are shown below. Other cases in “merged road” and “branched road” should be considered too.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

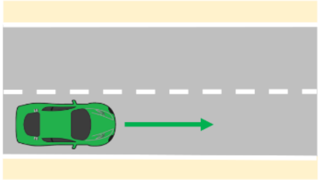
Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

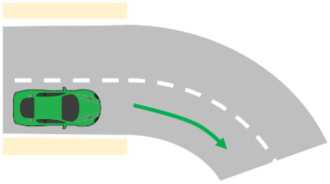
Figure 8. Examples of lane-change scenarios

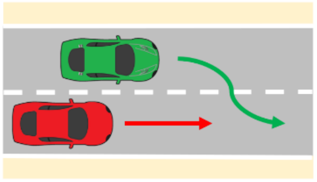


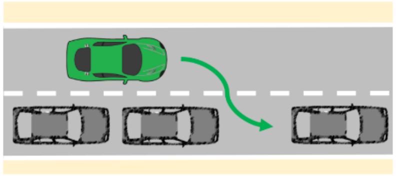
List of example scenarios for the highway use case

The following scenarios have been formatted to use the template described above.

Scenario Name	**Driving straight**
Scenario ID	S.1.1.a
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is driving on a straight road. The aim of this scenario is to test the lane keeping ability of the vehicle under normal or demanding conditions and parameters.
ODD Tags	Straight road
Behaviour Tags	Lane keeping Speed control
Type of scenario (nominal / critical / failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional) For 1-1 a) b) With LV	Standard used: BSI Flex 1889 Link : https://www.bsigroup.com/en-GB/CAV/bsi-flex-1889/ There is no junction present. There is 1 road, Road R1. Road R1 is a straight A road. There are 2 vehicles, vehicle ego and vehicle V1. Vehicle ego is at Road R1. Vehicle V1 is at Road R1. When vehicle V1 is driving, vehicle ego drives at the same pace vehicle V1 at its rear with a normal distance, at a normal speed of 60 to 70 'mph'. The scenario takes place between 09:00 to 21:00 under a lighting condition of 100.0 to 25000.0 'lx', and a cloud condition of 0 to 8 'oktas'.

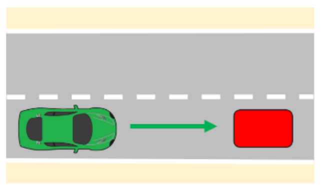
Scenario Name	**manoeuvring a bend**
Scenario ID	S.1.1.b
Contributed by	[contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is driving on a curved road. The aim of this scenario is to test if the vehicle is able to handle the road curvatures specified as part of the ODD.
ODD Tags	Curved road
Behaviour Tags	Lane keeping Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	Standard used: BSI Flex 1889 Link : https://www.bsigroup.com/en-GB/CAV/bsi-flex-1889/ There is no junction present. There is 1 road, Road R1. Road R1 is a curved A road, with a moderate curvature. There are 2 lanes on Road R1, Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the opposite. There is 1 vehicle, vehicle ego. Vehicle ego is at Road R1 and Lane 1. The scenario takes place between 09:00 to 21:00 under a lighting condition of 100.0 to 25000.0 'lx', and a cloud condition of 0 to 8 'oktas'.

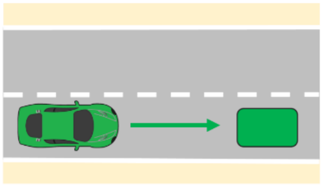
Scenario Name	**Ego vehicle performing lane change with vehicle behind**
Scenario ID	S.2.1.A
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	In an adjacent lane, another vehicle (red) is driving in the same direction as the ego vehicle (green). The intention of the ego vehicle is, to perform a lane change to the lane in which the other vehicle is driving
ODD Tags	Straight road
Behaviour Tags	Lane change Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	Standard used: ASAM OpenSCENARIO® DSL Link: https://www.foretellix.com/openscenario-2-0/ scenario sut.ego_cut_in: other_vehicle: vehicle other_vehicle_side: av_side do serial(): # Starting positions start_scenario_cut_in: parallel(overlap:equal, duration: [duration_range]second): ego.car.drive() with: keep_lane() other_vehicle.drive() with: position(time: [time_ahead_range]s, behind: ego.car, at: start) lane(side_of: ego.car, side: other_vehicle_side, at: start) # Cut in vehicle tries to cut in in front of Ego and leads the Ego same_as_other_vehicle: parallel(overlap:equal, duration:[cut_in_duration_range]second): ego.car.drive() with: lane(same_as:other_vehicle, at: end) other_vehicle.drive() with: position(time: [post_cut_in_range]s, behind: ego.car, at: end)

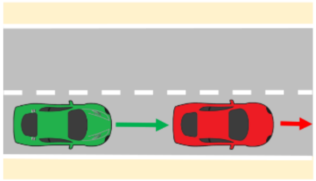
Scenario Name	**Merging into an occupied lane**
Scenario ID	S.2.1.D
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	Other vehicles (grey) occupy the lane adjacent to the ego lane. The ego vehicle (green) intends to perform. a lane change to the lane in which the other vehicles are driving [1-4]. According to road. geometry, speed, number and layout of other vehicles, the difficulty of the scenario changes.
ODD Tags	Straight road Any Environmental conditions Occupied lane
Behaviour Tags	Lane change Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations

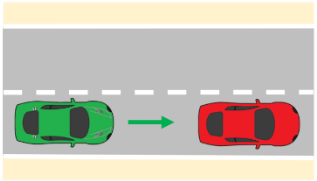
Abstract Scenario (optional)	Standard used: ASAM OpenSCENARIO® DSL
	Link: https://www.foretellix.com/openscenario-2-0/
	scenario sut.ego_with_adjacent_vehicle_group:
	  adjacent_vehicle_group: single_lane_vehicle_group
	  for vehicles in adjacent_vehicle_group.cars:
	    keep(vehicles.initial_bm == behavioural_model)
	    keep(vehicles.tau == [time_range_between_vehicles]s)
	  do serial():
	    # Starting positions
	    initial_placement: parallel(overlap:equal, duration: [duration_range]second):
	      ego.car.drive() with:
	        keep_lane()
	      adjacent_vehicle_group.drive() with:
	        lane(side_of: ego.car, at: all)
	  # change the lane and merge with the group
	    ego_changed_lane_same_as_adjacent_vehicles: parallel(overlap: equal, duration[change_lane_duration_range]second):

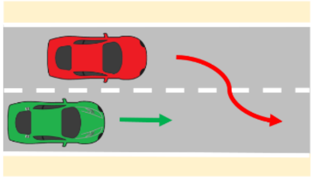
	ego.car.drive() with:
	lane(same_as: adjacent_vehicle_group,at: end)
	adjacent_vehicle_group.drive() with:
	keep_lane()

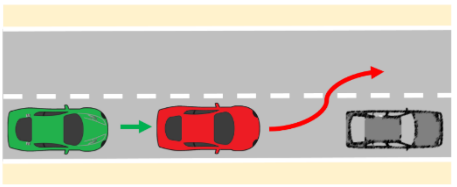
Scenario Name	**Impassable object on intended path**
Scenario ID	S.2.2.e
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is driving on a road with an impassable object in the ego lane (red). The objective of the ego vehicle is to continue driving straight. The ego vehicle needs to react. Depending on the velocity of the ego vehicle, the severity of the scenario is changing
ODD Tags	Straight road Any Environmental conditions Impassable object in road
Behaviour Tags	Lane change Speed control Passing object in road
Type of scenario (nominal/critical/failure)	Nominal/Critical
Range of applicability	No limitations
Abstract Scenario (optional)	Standard used: ASAM OpenSCENARIO® DSL Link: https://www.foretellix.com/openscenario-2-0/ scenario sut.ego_with_impassable_stationary_object: # define the impassable object red_box_pose: pose_3d # which has lon and lat defined red_box_pose.position[lat_range_as_per_ego] red_box_pos.position[lon_range] # Add constraints for fields of green_box_pose red_box: stationary_object red_box.physical.passable = false red_box.location(green_box_pose) # drive ahead do ego.car.drive(duration:[duration_range]) with: lane(1, curb, at: start)

Scenario Name	**Passable object on intended path**
Scenario ID	S.2.2.f
Contributed by	[contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is driving on a road with a passable object (green box) in the ego lane, e.g., a manhole lid or a small branch. The objective of the ego vehicle is to continue driving straight. The ego vehicle needs to react. Depending on the velocity of the ego vehicle, the difficulty of the scenario is changing. *Tested parameters*: reaction of ego (false positive, lane change/braking), distance to object, lateral velocity of ego (if changing lane), etc.
ODD Tags	Straight road Any Environmental conditions Passable object in road
Behaviour Tags	Passing object in road Speed control
Type of scenario (nominal critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

Scenario Name	**Lead vehicle braking**
Scenario ID	S.2.2.g
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is following a LV (red). The LV brakes, the ego vehicle has to adapt its speed in order to stay at a safe distance from the lead vehicle. *Tested parameters*: distance between ego and LV, reaction to other vehicles in adjacent lanes, etc.
ODD Tags	Straight road Any Environmental conditions
Behaviour Tags	Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

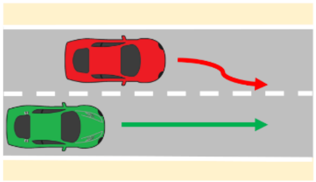
Scenario Name	**Approaching slower/stopped LV**
Scenario ID	S.2.2.h
Contributed by	[contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	LV (red) is driving in front of the ego vehicle (green) at a slower speed. The ego vehicle might brake or perform a lane change to avoid a collision. According to the speed of the LV and ego vehicle, the severity of this scenario can be assessed. *Emphasized scenario parameters*: ego velocity (road rules), LV speed profile (deceleration), layout and speed profile of other vehicles (if present). *Tested parameters*: distance between ego and LV, reaction to other vehicles in adjacent lanes, etc.
ODD Tags	Straight road Any Environmental conditions
Behaviour Tags	Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

Scenario Name	**Cut-in in front of the ego vehicle**
Scenario ID	S.2.2.I
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	Another vehicle (red) is driving in the same direction as the ego vehicle (green) in an adjacent lane. The other vehicle makes a lane change, such that is becomes the LV from the ego vehicle’s perspective. Depending on the distance and lateral velocity of the LV, the severity of the cut-in manoeuvre changes. *Emphasized scenario parameters*: LV lateral speed, distance to LV, ego velocity, lane width, layout and speed profile of other vehicles (if present). *Tested parameters*: distance between ego and LV, distance to other vehicles, etc.
ODD Tags	Straight road Any Environmental conditions
Behaviour Tags	Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

Scenario Name	**Cut-out in front of the ego vehicle**
Scenario ID	S.2.2.J
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	LV (red) is driving in the same direction as the ego vehicle (green) in front of the ego vehicle. The LV makes a lane change, such that it will no longer be the ego vehicle's LV. In order to test the behaviour of the ego vehicle, an obstacle is present (grey) in the ego lane in front of the ego vehicle. Depending on the velocity of the ego vehicle and the lateral velocity of the LV, the difficulty of this scenario changes. *Emphasized scenario parameters*: LV lateral speed, distance to LV, ego velocity, lane width, layout and speed profile of other vehicles (if present). *Tested parameters*: distance between ego and obstacle, distance to other vehicles etc.
ODD Tags	Straight road Any Environmental conditions
Behaviour Tags	Speed control
Type of scenario (nominal/critical/failure)	Nominal/Critical
Range of applicability	No limitations

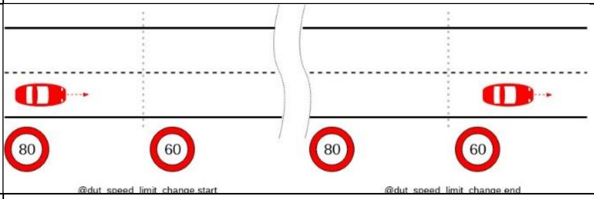
Abstract Scenario (optional)	Standard used: ASAM OpenSCENARIO® DSL
	Link: https://www.foretellix.com/openscenario-2-0/
	
	scenario sut.vehicle_cut_out:
	  car1: vehicle # The "cut-out" car
	  do serial():
	    # Starting poisitions
	    start_scenario_cut_out: parallel(overlap:equal, duration:[duration_range]second):
	      ego.car.drive() with:
	        keep_lane()
	      car1.drive() with:
	         position(time: [time_ahead_range]s, ahead_of: ego.car, at: start)
	         lane(same_as: ego.car, at: start)
	    # lead vehicle cut out to a lane on the side
	    side_of_ego_lane: parallel(overlap:equal, duration:[cut_out_duration_range]second):
	      ego.car.drive() with:
	        keep_lane()

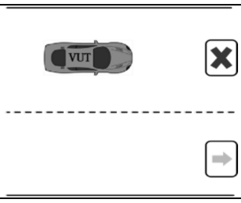
	car1.drive() with: lane(side_of:ego.car, at: all)

Scenario Name	**Detect and respond to swerving vehicles**
Scenario ID	S.2.2.K
Contributed by	[contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	Another vehicle (red) is driving in the same direction as the ego vehicle (green) in an adjacent lane. The other vehicle swerves towards the ego vehicle's lane
ODD Tags	Straight road Any Environmental conditions
Behaviour Tags	Speed control
Type of scenario (nominal/critical/failure)	Nominal/Critical
Range of applicability	No limitations
Abstract Scenario (optional)	Standard used: BSI Flex 1889 Link : https://www.bsigroup.com/en-GB/CAV/bsi-flex-1889/ There is no junction present. There is 1 road, Road R1. Road R1 is a straight A road. There are 2 lanes on Road R1, Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the same. There are 2 vehicles, vehicle ego and vehicle V1. Vehicle ego is at Road R1 and Lane 1, Vehicle V1 is at front left of Vehicle ego with an unsafe distance. When Vehicle ego is driving, Vehicle V1 changes lane right cut-in towards vehicle ego at its front left with a critical distance. The scenario takes place between 09:00 to 21:00 under a lighting condition of 100.0 to 25000.0 'lx', and a cloud condition of 0 to 8 'oktas'.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

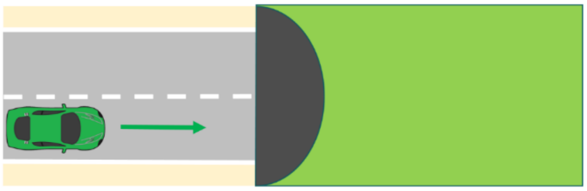
Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

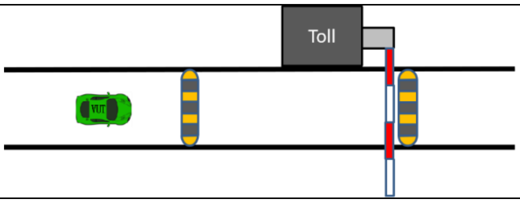
Scenario Name	**Speed limit change**
Scenario ID	S.3.A
Contributed by	[Contributor] SAFE/Foretellix
Scenario source	Synthetic scenario
Version	1.0
Figure	 80 60 80 60 @dut_speed_limit_change.start @dut_speed_limit_change.end
Functional Scenario Description	The ego vehicle (red) is driving on a straight road with a speed limit change. The objective of the ego vehicle is to respond appropriately to speed limit change by decelerating when entering a lower speed zone. *Environmental requirements*: A straight road that has at least one change in the speed limit. *Ego vehicle behaviour*: The ego vehicle drives straight on the road, adapting its speed to the changing limitations. *Emphasized scenario parameters*: The layout and speed profile of other vehicles (if present), ego velocity. *Tested parameters:* Longitudinal control of ego (braking/accelerating), perception capability of the Ego.
ODD Tags	Straight road Any Environmental conditions Speed limit sign
Behaviour Tags	Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

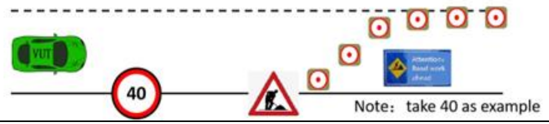
Scenario Name	**Signal lights**
Scenario ID	S.3.B
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The test road consists of at least two lanes. The lanes of the test road feature smart lane signage set above the road. The ego vehicle (grey)is positioned in a lane which is indicated as closed, and the signal lights of adjacent lanes are kept in an open state. The objective of the ego vehicle is to respond appropriately to the signal lights by changing lanes when the signal about the occupied lane indicates that it is closed. *Environmental requirements*: A road that has at least two lanes, and smart signalling to indicate the status of the lane (open/closed). *Ego vehicle behaviour*: The ego vehicle drives on the road, changing lanes as necessary, in accordance with the signal lights. *Emphasized scenario parameters*: Layout and speed profile of other vehicles (if present), ego velocity. *Tested parameters:* reaction of ego (lane change/braking), lateral velocity of ego (if changing lane) etc.
ODD Tags	Straight road Smart lane signage Variable lane signage Any Environmental conditions Signal lights
Behaviour Tags	Lane change
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

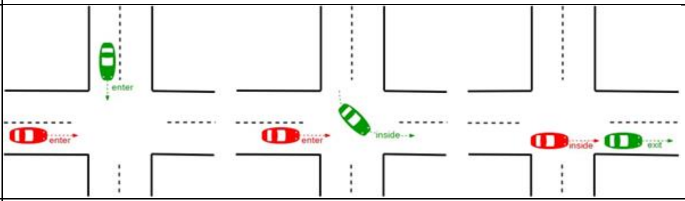
Scenario Name	**Drive through tunnel**
Scenario ID	S.3.C
Contributed by	[contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is driving through a tunnel (lack of GPS signals and natural light). The vehicle needs to adapt to the quickly changing light parameters and lack of global positioning. Depending on the speed of the ego vehicle, the difference between the light conditions outside and inside the tunnel and the length of the tunnel, the difficulty of the scenario is changing
ODD Tags	Any Environmental conditions Tunnel Limited GPS Limited Connectivity
Behaviour Tags	Lane keeping Speed control
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	Standard used: BSI Flex 1889 Link : https://www.bsigroup.com/en-GB/CAV/bsi-flex-1889/ There is no junction present. There is 1 road, Road R1. Road R1 is a straight A road. There are 2 lanes on Road R1, Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the same. There is a tunnel as Structure T1 at 50 to 60 'm' on Road 1. There is 1 vehicle, vehicle ego. Vehicle ego is at Road R1 and Lane 1. The scenario takes place between 09:00 to 21:00 under a lighting condition of 100.0 to 25000.0 'lx', and a cloud condition of 0 to 8 'oktas'.

Scenario Name	**Toll**
Scenario ID	S.3.D
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	The ego vehicle (green) is driving on a long straight road with at least one lane. A toll station is positioned on this road, and toll station signs, speed limit signs and speed bumps are set in front of the toll station. The objective of the ego vehicle is to safely drive in and out of the toll station, slowing down and/or stopping where necessary. *Emphasized scenario parameters*: road layout (location of speed bumps and toll booth etc.), layout and speed profile of other vehicles (if present), ego velocity. *Tested parameters:* reaction of ego (slowing down and/or stopping).
ODD Tags	Straight road Any Environmental conditions Toll booth Speed limit signs Speed bumps
Behaviour Tags	Speed control Safe stopping
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

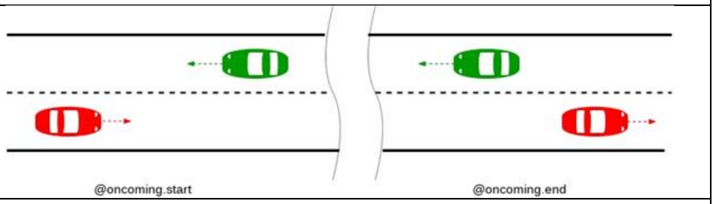
Scenario Name	**Conventional obstacles**
Scenario ID	S.3.E
Contributed by	[Contributor]
Scenario source	Synthetic scenario
Version	1.0
Figure	 Note： take 40 as example
Functional Scenario Description	The ego vehicle (green) is driving on a long straight road containing at least two lanes, and the middle lane line is a white dashed line. Within the lanes, conical traffic signs and traffic markings are placed according to the traffic control requirements of the road maintenance operation. The objective of the ego vehicle is to safely navigate these obstacles, and change lanes where necessary. *Emphasized scenario parameters*: road layout (visibility of the obstacles on the path), layout and speed profile of other vehicles (if present), ego velocity. *Tested parameters:* reaction of ego (lane change/braking), lateral velocity of ego (if changing lane) etc.
ODD Tags	Straight road Multiple lanes Any Environmental conditions Obstacles in road
Behaviour Tags	Passing objects in road Speed control Lane change
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Scenario Name	**Interceptor junction**
Scenario ID	S.4.a
Contributed by	SAFE/Foretellix
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	For the ego vehicle (green), junctions present a challenge due to the increased likelihood of conflicts with other actors. In this scenario, the ego vehicle traverses an intersection simultaneously with another car (red) - the interceptor. This scenario tests the ego vehicle's behaviour when on a collision course with another car in an intersection, possibly with signs, signals, or traffic lights. The ego vehicle should be able to safely manoeuvre through the intersection and avoid or mitigate a collision.
ODD Tags	Crossroad (4-way junction) Any Environmental conditions Signs Signals Traffic lights
Behaviour Tags	Turning left Speed control Path planning
Type of scenario (nominal/critical/failure)	Nominal
Range of applicability	No limitations
Abstract Scenario (optional)	Standard used: BSI Flex 1889 Link : https://www.bsigroup.com/en-GB/CAV/bsi-flex-1889/ There is a crossroad, Junction C1, which has road connections with Road 1, Road 2, Road 3 and Road 4. Road 1 to Road 2 is straight ahead, Road 1 to Road 3 is to the right, Road 3 to Road 4 is straight ahead. There are 4 roads, Road 1, Road 2, Road 3 and Road 4. Road 1 is a straight A road. There are 2 lanes on Road 1, Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the opposite. There are 2 lanes on Road 2, Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the opposite. There are 2 lanes on Road 3, Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the opposite. There are 2 lanes on Road 4,

	Lane 1 and Lane 2. The travel direction between Lane 1 and Lane 2 is the opposite. There are 2 vehicles, vehicle ego and vehicle interceptor. Vehicle ego is at Road 1 and Lane 1, Vehicle interceptor is at Road 3 and Lane 2. When Vehicle ego is turning left, at the same time Vehicle V1 drives towards vehicle ego at its rear with a critical distance. The scenario takes place between 09:00 to 21:00 under a lighting condition of 100.0 to 25000.0 'lx', and a cloud condition of 0 to 8 'oktas'.

Scenario Name	**Wrong way driver**
Scenario ID	S.5.a
Contributed by	SAFE/Foretellix
Scenario source	Synthetic scenario
Version	1.0
Figure	
Functional Scenario Description	Oncoming is a scenario in which a car (red) approaches the ego vehicle (green) from the opposite direction and drives past the ego vehicle.
ODD Tags	Straight road Unidirectional road (one-way road) Broken centre line Any Environmental conditions
Behaviour Tags	Wrong way driver Speed control
Type of scenario (nominal/critical/failure)	Critical
Range of applicability	No limitations

Abstract Scenario (optional)	Standard used: ASAM OpenSCENARIO® DSL
	Link: https://www.foretellix.com/openscenario-2-0/
	
	scenario sut.oncoming_vehicle:
	    car1: vehicle
	
	    do oncoming: parallel(overlap:equal):
	        car1.drive()
	        ego.car.drive() with:
	            oncoming(ref_car: car1, distance: [distance_range]meter, at:all)

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 5: Virtual testing and credibility assessment

Types of simulation toolchain approaches

The simulation toolchain used for virtual testing may result in the combination of different approaches. In particular, there are many ways that tests can be performed:

(a) Entirely inside a computer (referred to as Model or Software in the Loop testing, MIL/SIL), with the model of the elements involved (e.g., a simple representation of the control logic of an ADS) interacting in a simulated environment; and/or

(b) With a sensor, a subsystem, or the whole vehicle interacting with a virtual environment (Hardware or Vehicle in the Loop testing, HIL/VIL). For VIL testing, the vehicle can either be in:

(i) A laboratory where the vehicle would be standing still or moving on a chassis dynamometer or on a powertrain test bed and is connected to the environment model by wire or by direct stimulation of its sensors; or

(ii) A proving ground where the vehicle would be connected to an environment model and would interact with virtual objects by physically moving on the test-track.

(c) With a subsystem interacting with a real driver (Driver in the Loop testing, DIL).

Interaction between the system and the environment

The interaction between the system under the test and the environment can either be an open- or closed-loop.

In open-loop virtual testing a data provision unit provides input stimuli to an ADS. The data provision unit can provide data that was collected from a real-world drive or from a different data source. For example, data can be generated during a test using an environment simulator. In any case, the provided data establishes an environment for the ADS. Compared to closed-loop testing there is no feedback between the data provision unit and the ADS. As a common use case is the re-computation of recorded drives, open-loop testing is sometimes referred to as re-compute, replay or re-simulation. A useful property of open-loop testing is the inherent small gap between a virtual test and a corresponding collected real-world situation, as the open-loop test can be as realistic as the used collection mechanism allowed for, with, under ideal circumstances, no additional error introduced by the open-loop approach. Potential applications of open-loop testing include:

- Regression tests for previously resolved issues as well as tests for newly introduced ADS features.
- Re-validation of previously validated features, e.g., as part of the validation of an improved ADS, especially for features that have no associated functional change.

- The testing of non-functional properties of the ADS. For example, evaluating scheduling or timing behavior of executables.

In shadow mode testing, an ADS that is subject to testing is connected to a data provision unit. However, the ADS tested is not controlling the vehicle itself. Indeed, it has no effect on the state or behavior of the controlling unit of the vehicle. This approach enables realistic large-scale testing with a fleet of vehicles as test platforms. Since the ADS that is subject to testing has no effect on the vehicle, using a shadow mode can be categorized as open-loop testing.

Closed-loop virtual tests include a feedback loop that continuously sends information from the “closed-loop” controller back to the ADS when the ADS takes an action. Within these test systems, the digital objects in the environment could react in different ways depending on the action of the system under test.

Selecting an open- or closed-loop test could depend on factors such as the objectives of the virtual testing activity and the status of development of the system under test.

The flexibility of simulation makes it a standard test method during a vehicle’s design and the development of this pillar will also make it part of the ADS validation process. For an ADS, it will be impossible to test the vehicle’s behaviour in the real world for all possible situations as well as for any subsequent change in the ADS’ driving logic. Virtual testing will therefore become an indispensable tool to verify the capability of the automated system to deal with a wide variety of possible scenarios. In addition, virtual testing can be beneficial in replacing real world and proving ground testing where there are concerns over safety-critical traffic scenarios. It is recommended therefore that virtual testing be used to test the ADS under safety critical scenarios that would be difficult and/or unsafe to reproduce on test tracks or public roads.

Virtual tests used for ADS validation can achieve different objectives depending on the overall validation strategy and the accuracy of the underlying simulation and models.

(a) Provide qualitative confidence in the safety of the full system.

(b) Contribute directly to statistical confidence in the safety of the full system (caveats apply).

(c) Provide qualitative or statistical confidence in the performance of specific subsystems or components.

(d) Discover challenging scenarios that can be tested in the real world.

In contrast to all its potential benefits, a limitation, of this approach, is in its intrinsic limited fidelity. As models provide a representation of the reality, the suitability of a model to satisfactorily replace the real world for validating the safety of an ADS has to be carefully assessed. Therefore, the validation of the simulation and models used in virtual testing is essential to determine the quality and reliability of the results compared to real-world performance.

It is recommended that a virtual test of the ADS’ performance is compared with its performance in the real world when executing the same scenario. This will provide the opportunity to assess the accuracy of the virtual testing toolchain that is used. Given the high number of scenarios that virtual testing can perform compared to track testing, the validation will probably need to be performed on a smaller but still sufficiently representative subset of the relevant scenarios in order to substantiate any extrapolation beyond the scenarios used for the validation.

In the short-term, virtual testing might only be conducted using simulation toolchains developed and maintained by the ADS manufacturer. Since their design depends on the validation and verification strategies implemented by the manufacturer, it is recommended that simulation toolchains are not subject to regulation or standardization at this time. Rather, simulation toolchains should be explained and documented by the ADS manufacturer and its suitability assessed during the certification process. For this reason, the output of the NATM related to virtual testing ensures that documentation and data provided by the manufacturer is appropriate. Furthermore, virtual testing using modelling and simulation should be credible enough for an assessor to make sound decisions. Credibility is discussed further below.

It is recommended that when validating the safety of the ADS, particular attention should be placed on the interaction between virtual testing and the other test methods. Virtual testing will have strong relationships with all the pillars of the NATM guidelines. In particular:

(a) Virtual testing supplements physical testing to account for the quantity and diversity of ADS configurations, intended uses and limitations on use. One of the strengths of virtual testing is its capacity to assess the ADS performance across multiple scenarios and across ranges of parameters within scenarios in a cost-effective manner. Virtual testing enables results of limited physical tests to be supplemented by verifiable data covering numerous instances of the test scenario, by varying parameters. Using this approach, virtual testing can demonstrate ADS coverage of safety-critical scenarios, and hence provide evidence that an ADS will perform as intended for that type of scenario in the real world. These advantages reduce the burden on physical tests (offsetting their weaknesses) and help to improve the efficiency of the overall assessment process across the pillars. Virtual testing can also be effectively used to identify and cover edge cases and other low-probability scenarios to increase confidence on the ADS' likely performances.

(b) Virtual testing can play an important role in the development of traffic scenarios.

(c) Virtual testing enables assessment of ADS performance boundaries, enabling precise definition of the boundaries between collision avoidance and crash mitigation. Through methods of randomization and scenario compositions, virtual testing enables the developer or the assessor to challenge the ADS and increase confidence in its performance when challenged with low probability events.

(d) Virtual testing will be a key element in the audit assessment. Results of virtual testing carried out both during vehicle development and in the verification and validation phase will provide valuable evidence supporting the safety audit. The manufacturers will need to provide evidence and documentation about how the virtual testing is carried out and how the underlying simulation toolchain has been validated.

(e) Results from real-world tests can improve the accuracy of simulation and models.

(f) Virtual testing can play an important role in responding to concerns identified through in-use monitoring of ADS performance. Virtual testing provides a quick and flexible approach to analyse ADS performance based on real-world events. It allows manufacturers to understand and verify the ADS behaviour and to understand why an issue may have occurred. It may identify an untested scenario, or a set of untried parameters. It may also identify the "scale" of any issue. If the virtual testing does identify unsafe behaviour it can then also help to assess the efficacy of modifications to the ADS and ultimately to improve the overall ADS performance. Where appropriate, the information and scenario descriptions can be shared and integrated into scenarios and testing regimes worldwide.

It is recognised that specific regulatory functional safety requirements are still under development. Virtual testing however, using a validated simulation toolchain, shows promise for assessing the following general safety requirements that are currently under consideration:

(a) The ADS should drive safely and manage safety critical situations. These are the requirements where virtual testing can play a prominent role. MIL/SIL, HIL and VIL virtual testing can all be used to assess these requirements at different stages of vehicle verification and validation.

(b) The ADS should interact safely with the user. DIL virtual testing can be helpful to support the assessment of this category of safety requirement by analysing the interaction between the driver and the ADS in a safe and controlled environment.

(c) The ADS should safely manage failure modes and ADS should ensure a safe operational state. The use of virtual testing in these two categories is also very promising but would probably require further research work. SIL virtual testing could include simulated failures and maintenance requests. HIL and VIL virtual testing could be used to assess how the system would react to the occurrence of a malfunctioning induced into the real system.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Appendix 1: Credibility assessment for using virtual toolchain in ADS validation

Introduction, motivation, and scope

The use of Modelling and Simulation (M&S) is becoming widespread thanks to the increasing computational capabilities, accuracy, usability, and availability of M&S software packages. M&S can be beneficial for ADS safety validation because it provides an opportunity to overcome some of the limitations of real testing and to increase the number of testing scenarios. Nonetheless, M&S can also lead to erroneous/seemingly correct results, especially in relation to complex simulations not adequately supported by robust practices addressing all M&S aspects beyond pure validation. Therefore, higher confidence in M&S credibility is needed so that virtual testing can be used instead of and in conjunction with the other pillars. In other words, M&S can be used for virtual testing if an assessor is able to consider the simulation results credible enough to make sound decisions taking into account the potential uncertainties of M&S.

If M&S is to be credible it needs to be validated. Validating the models and the simulation tools and process that make up M&S toolchain is difficult and there are limitations, which include the limited scope of the validation tests and the difficulty in gathering data to support the validation procedures. The use of M&S requires attention to all the factors influencing the quality and validity of M&S toolchain and all its separate components. The aim is to:

(a) Identify a common framework to determine, justify, assess and report the overall credibility of the M&S toolchain.

(b) Identify a way to indicate the levels of confidence in the results when a validation assessment takes place and also to determine the associated domains of applicability for the toolchain.

This framework should be general enough to be used for different M&S types and applications. Unfortunately, the goal is further complicated by the range and differences of ADS features and the variety of simulation tools and toolchains that are used. These considerations lead to the decision to use an (risk-based/informed) credibility assessment framework that can be applied to all M&S applications.

The proposed credibility assessment framework provides a general description of the main aspects needed for assessing the credibility of an M&S solution together with guidelines of the role played by the relevant assessor in the validation process with respect to credibility. The assessor should investigate the documentation and evidence supporting credibility during the audit phase. It is understood that the actual validation tests will take place once there is sufficient evidence that a simulation tool or toolchain produces credible results.

The outcome of the current credibility assessment will define the envelope in which the virtual tool can be used to support the ADS assessment.

Components of the credibility assessment framework

It is recommended that the M&S toolchain could be used for virtual testing if its credibility is established by evaluating its fitness for the intended purpose. It is recommended that credibility is achieved by investigating and assessing five M&S properties:

(a) Capability – what the M&S can do, and what are the associated risks.

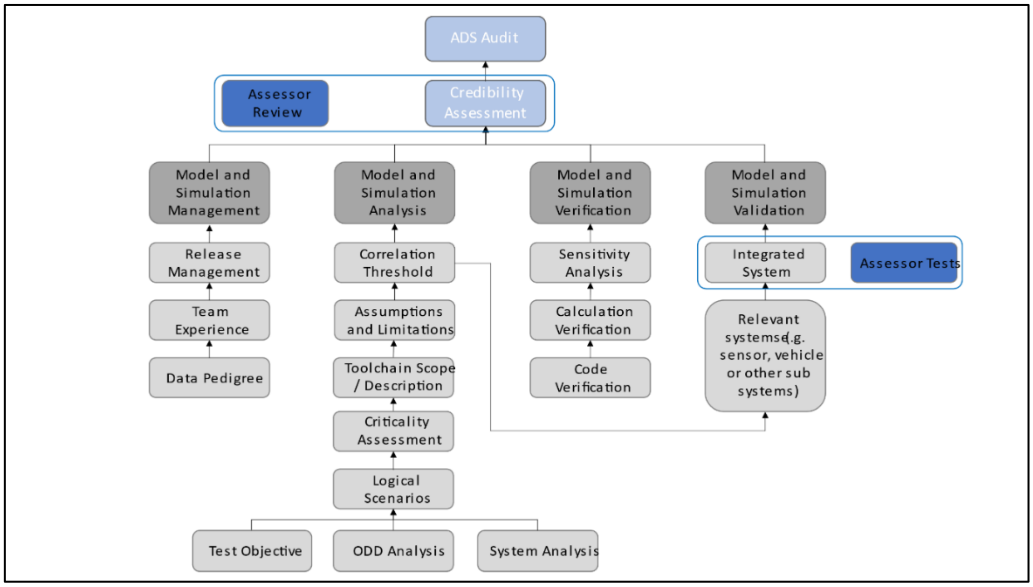
(b) Accuracy – how well M&S does reproduce the target data.

(c) Correctness – how sound & robust is the M&S data and the algorithms in the tools.

(d) Usability – what training and experience is needed and what is the quality of the process that manage its use.

(e) Fit for Purpose – how suitable is the M&S toolchain for the assessment of the ADS within its ODD.

Figure 9. Graphical representation of the relationships between the components of the credibility assessment framework



Therefore, credibility requires a unified method to investigate these properties and get confidence in the M&S results. The Credibility Assessment framework introduces a way to assess and report the credibility of M&S based on quality assurance criteria that allow an indication of the levels of confidence in results. In other words, the credibility is established by evaluating the key influencing factors that are the main contributors to the behaviour of the models and simulation tools and therefore affect the overall M&S toolchain credibility: The following all have an influence on the overall M&S credibility; organizational management of the M&S activity, team's experience and expertise, the analysis and description of the chosen M&S toolset, the pedigree of the data and inputs, verification, validation, uncertainty characterization. How well each of these factors is addressed indicates the level of quality achieved by M&S toolchain, and the comparison between the obtained levels and the required levels provides a qualitative measure of the M&S credibility and fitness for its use in virtual testing. A graphical representation of the relationship among the components of the credibility assessment framework is reported in Figure 9.

Models and Simulation Management

The M&S lifecycle is a dynamic process with frequent releases that should be monitored and documented. As a result, it is recommended that management activities should be established to support the M&S through typical product management processes. Relevant information on the following aspects should be included in this section.

It is recommended that this part should:

(a) Describe the modifications within the M&S toolchain releases.

(b) Designate the corresponding software (e.g., specific software product and version) and hardware arrangement (e.g., XiL configuration).

(c) Record the internal review processes that accepted the new releases.

(d) Be supported throughout the full duration of the virtual testing utilization.

Releases management

It is recommended that any toolchain’s version used to release data for certification purposes should be stored. The virtual models constituting the testing tool should be documented in terms of the corresponding validation methods and acceptance thresholds to support the overall credibility of the toolchain. The developer should establish and enforce a method to trace generated data to the corresponding toolchain version.

Quality check of virtual data. Data completeness, accuracy, and consistency are ensured throughout the releases and lifetime of a tool or toolchain to support the verification and validation procedures.

Team's Experience and Expertise.

Even though Experience and Expertise (E&E) are already covered in a general sense within an organization, it is important to establish the basis for confidence on the specific experience and expertise for M&S activities.

In fact, the credibility of M&S depends not only on the quality of the simulation models but also on the E&E of the personnel involved in the validation and usage of the M&S. For instance, a proper understanding of the limitations and validation domain will prevent possible misuse of the M&S or misinterpretation of its results.

It is important to establish the basis for the ADS manufacturer’s confidence in the experience and expertise of:

(a) The teams that will internally assess and validate the M&S toolchain and,

(b) The teams that will use the validated simulation for the execution of virtual testing with the purpose of validating the ADS.

Thus, if a team's E&E is good it increases the level of confidence and hence the credibility of M&S and its results by ensuring that the human elements underpinning the M&S activity are taken into consideration and risks from the human aspect of the activity can be controlled, through its Management System.

If the ADS manufacturer's toolchain incorporates or relies upon inputs from organizations or products outside of the manufacturer's own team, it is recommended that the ADS manufacturer includes an explanation of measures it has taken to manage and develop confidence in the quality and integrity of those inputs.

The team's Experience and Expertise include two aspects:

1. Organizational level

   The credibility is established by setting up processes and procedures to identify and maintain the skills, knowledge, and experience to perform M&S activities. The following processes should be established, maintained and documented:

   (a) Process to identify and evaluate the individual's competence and skills.

   (b) Process for training personnel to be competent to perform M&S-related duties.

2. Team level:

   Once a toolchain has been finalized, its credibility is mainly dictated by the skills and knowledge of the teams that will first validate the M&S and then use it for the validation of ADS. The credibility is established by documenting that these teams have received adequate training to fulfil their duties.

   The ADS manufacturer should:

   (a) Provide the basis for the ADS manufacturer's confidence in the Experience and Expertise of the individual/team that validates the M&S toolchain.

   (b) Provide the basis for the ADS manufacturer's confidence in the Experience and Expertise of the individual/team that uses the simulation to execute virtual testing with the purpose of validating the ADS.

The ADS manufacturer should demonstrate of how it applies the principles of its Management Systems, e.g. ISO 9001 or a similar best practice or standard, with regard to the competence of its M&S organization and the individuals in that organization and the basis for this determination. It is recommended that the assessor not substitute its judgment for that of the ADS manufacturer regarding the experience and expertise of the organization or its members.

Data/input pedigree

The pedigree and traceability of the data and inputs used in the validation of the M&S is important. The manufacturer should have a record of these that allows the assessor to verify their quality and appropriateness.

1. Description of the data used for the M&S validation

   (a) The ADS manufacturer should document the data used to validate the models included in the tool or toolchain and note important quality characteristics;

   (b) The ADS manufacturer should provide documentation showing that the data used to validate the models covers the intended functionalities that the toolchain aims at virtualizing;

   (c) The ADS manufacturer should document the calibration procedures employed to fit the virtual models' parameters to the collected input data.

2. Effect of the data quality (e.g. data coverage, signal to noise ratio, and sensors' uncertainty/bias/sampling rate) on model parameters uncertainty

   The quality of the data used to develop the model will have an impact on model parameters' estimation and calibration. Uncertainty in model parameters will be another important aspect in the final uncertainty analysis.

Data/output pedigree

The pedigree of the output data is important. The manufacturer should keep a record of the outputs of the M&S toolchain and ensure that it is traceable to the inputs and the M&S toolchain that produced it. This will form part of the evidence trail for the ADS validation.

1. Description of the data generated by the M&S

   (a) The ADS manufacturer should provide information on any data and scenarios used for virtual testing toolchain validation.

   (b) The ADS manufacturer should document the exported data and note important quality characteristics e.g. using the correlation methodologies as defined Annex II.

   (c) The ADS manufacturer should trace M&S outputs to the corresponding M&S setup:

      (i) Effect of the data quality M&S credibility

      - The M&S output data should be sufficient to ensure the correct execution of the validation exercise. The data should sufficiently reflect the ODD relevant to the virtual assessment of the ADS.

      - The output data should allow consistency/sanity check of the virtual models, possibly by exploiting redundant information.

(ii) Managing stochastic models

- Stochastic models should be characterized in terms of their variance.
- The use of a stochastic models should not prohibit the possibility of deterministic re-execution.

M&S Analysis and Description

The M&S analysis and description aim to define the whole toolchain and identify the parameter space that can be assessed via virtual testing. It defines the scope and limitations of the models and simulation tools and the uncertainty sources that can affect its results.

General description

The ADS manufacturer should provide a description of the complete toolchain along with how the M&S data will be used to support the ADS validation strategy.

The ADS manufacturer should provide a clear description of the test objective.

Assumptions, known limitations, and uncertainty sources

The ADS manufacturer should motivate the modelling assumptions which guided the design of the M&S toolchain. The ADS manufacturer should provide evidence on:

- How the manufacturer-defined assumptions play a role in defining the limitations of the toolchain.
- The level of fidelity required for the simulation models.

The ADS manufacturer should provide justification that the tolerance for M&S versus real-world correlation is acceptable for the test objective

Finally, this section should include information about the sources of uncertainty in the model. This will represent an important input to final uncertainty analysis, which will define how the M&S toolchain outputs can be affected by the different sources of uncertainty of the M&S toolchain used.

Scope (what is the model for?). It defines how the M&S is used in the ADS validation.

The credibility of virtual tool should be enforced by a clearly defined scope for the utilization of the developed M&S toolchains.

The mature M&S should allow a virtualization of the physical phenomena to a degree of accuracy which matches the fidelity level required for certification. Thus, the M&S environment will act as a “virtual proving ground” for ADS testing.

M&S toolchains need dedicated scenarios and metrics for validation. The scenario selection used for validation should be sufficient such that there is confidence that the toolchain will perform in the same manner in scenarios that were not included in the validation scope.

ADS manufacturers should provide a list of validation scenarios together with the corresponding parameter description limitations.

ODD analysis is a crucial input to derive requirements, scope and the effects that the M&S toolchain must consider supporting ADS validation.

Parameters generated for the scenarios will define extrinsic and intrinsic data for the toolchain and the simulation models.

Criticality assessment

The simulation models and the simulation tools used in the overall toolchain should be investigated in terms of their impact in case of a safety error in the final product. The proposed approach for criticality analysis is derived from ISO 26262, which requires qualification for some of the tools used in the development process. In order to derive how critical the simulated data is, the criticality assessment considers the following parameters:

(a) The consequences on human safety e.g. severity classes in ISO 26262.

(b) The degree in which the M&S toolchain results influence's the ADS.

The table below provides an example criticality assessment matrix to demonstrate this analysis. ADS manufacturers may adjust this matrix to their particular use case.

Table 5. Criticality assessment matrix

Influence on ADS	Significant	N/A			
	Moderate				
	Minor				
	Negligible			N/A	
		Negligible	Minor	Moderate	Significant
		Decision consequence			

From the perspective of the criticality assessment, the three possible cases for assessment are:

1. Those models or tools that are clear candidates for following a full credibility assessment.
2. Those models or tools that may or may not be candidates for following the full credibility assessment at the discretion of the assessor.

3. Those models or tools that are not required to follow the credibility assessment.

Verification

The verification of M&S deals with the analysis of the correct implementation of the conceptual/mathematical models that create and build up the overall toolchain. Verification contributes to the M&S's credibility via providing assurance that the individual tools will not exhibit unrealistic behaviour for a set of inputs which cannot be tested. The procedure is grounded in a multi-step approach described below, which includes code verification, calculation verification and sensitivity analysis.

Code verification

Code verification is concerned with the execution of testing that demonstrates that no numerical/logical flaws affect the virtual models.

The ADS manufacturer should document the execution of proper code verification techniques, e.g. static/dynamic code verification, convergence analysis and comparison with exact solutions if applicable

The ADS manufacturer should provide documentation showing that the exploration in the domain of the input parameters was sufficiently wide to identify parameter combinations for which the M&S tools show unstable or unrealistic behaviour. Coverage metrics of parameters combinations may be used to demonstrate the required exploration of the model's behaviours.

The ADS manufacturer should adopt sanity/consistency checking procedures whenever data allows

Calculation verification

Calculation verification deals with the estimation of numerical errors affecting the M&S. The ADS manufacturer should document numerical error estimates (e.g. discretization error, rounding error, iterative procedures convergence). The numerical errors should be kept sufficiently bounded to not affect validation.

Sensitivity analysis

Sensitivity analysis aims at quantifying how model output values are affected by changes in the model input values and thus identifying the parameters having the greatest impact on the simulation model results. The sensitivity study also provides the opportunity to determine the extent to which the simulation model satisfies the validation thresholds when it is subjected to small variations of the parameters, thus it plays a fundamental role to support the credibility of the simulation results.

The ADS manufacturer should provide supporting documentation demonstrating that the most critical parameters influencing the simulation output have been identified by means of sensitivity analysis techniques such as by perturbing the model's parameters;

The ADS manufacturer should demonstrate that robust calibration procedures have been adopted and that this has identified and calibrated the most critical parameters leading to an increase in the credibility of the developed toolchain.

Ultimately, the sensitivity analysis results will also help to define the inputs and parameters whose uncertainty characterization needs particular attention to characterize the uncertainty of the simulation results.

Validation

The quantitative process of determining the degree to which a model or a simulation is an accurate representation of the real world from the perspective of the intended uses of the M&S. It is recommended that the following items be considered when assessing the validity of a model or simulation:

(a) Measures of Performance (metrics)

The Measures of Performance are metrics that are used to compare the ADS's performance within a virtual test with its performance in the real world. The Measures of Performance are defined during the M&S analysis. Metrics for validation may include:

- Discrete value analysis e.g. detection rate, firing rate;
- Time evolution e.g. positions, speeds, acceleration;
- Analysis of state changes e.g. distance/speed calculations, TTC calculation, brake initiation.

(b) Goodness of Fit measures

The analytical frameworks used to compare real world and simulation metrics are generally derived as Key Performance Indicators (KPIs) indicating the statistical comparability between two sets of data. The validation should show that these KPIs are met.

(c) Validation methodology

The ADS manufacturer should define the logical scenarios used for virtual testing toolchain validation. They should be able to cover, to the maximum possible extent, the ODD of virtual testing for ADS validation. The exact methodology depends on the structure and purpose of the toolchain. The validation may consist of one or more of the following:

- Validate subsystem models e.g. environment model (road network, weather conditions, road user interaction), sensor models (Radio Detection And Ranging (RADAR), Light Detection And Ranging (LiDARs), Camera), vehicle model (steering, braking, powertrain).
- Validate vehicle system (vehicle dynamics model together with the environment model).

- Validate sensor system (sensor model together with the environment model).
- Validate integrated system (sensor model + environment model with influences form vehicle model).

(d) Accuracy requirement

Requirement for the correlation threshold is defined during the M&S analysis. The validation should show that these KPIs are met. e.g. using the correlation methodologies as defined in Annex II.

(e) Validation scope (what part of the toolchain to be validated)

A toolchain consists of multiple tools, and each tool will use several models. The validation scope includes all tools and their relevant models.

(f) Internal validation results

The documentation should not only provide evidence of the M&S validation but also should provide sufficient information related to the processes and products that demonstrate the overall credibility of the toolchain used. Documentation/results may be carried over from previous credibility assessments.

(g) Independent Validation of Results

The assessor should audit the documentation provided by the manufacturer and may carry out tests of the complete integrated tool. If the output of the virtual tests does not sufficiently replicate the output of physical tests, the assessor may request that the virtual and/or physical tests to be repeated. The outcome of the tests will be reviewed and any deviation in the results should be reviewed with the manufacturer. Sufficient explanation is required to justify why the test configuration caused deviation in results.

(h) Uncertainty characterisation

This section is concerned with characterizing the expected variability of the virtual toolchain results. The assessment should be made up of two phases. In a first phase the information collected from the "M&S Analysis and Description" section and the "Data/Input Pedigree" are used to characterise the uncertainty in the input data, in the model parameters and in the modelling structure. Then, by propagating all of the uncertainties through the virtual toolchain, the uncertainty of the model results is quantified. Depending on the uncertainty of the model results, proper safety margins will need to be introduced by the ADS manufacturer in the use of virtual testing as part of the ADS validation.

(i) Characterization of the uncertainty in the input data

The ADS manufacturer should demonstrate they have estimated the model's critical inputs by means of robust techniques such as providing multiple repetitions for their assessment.

(ii) Characterization of the uncertainty in the model parameters (following calibration).

The ADS manufacturer should demonstrate that when a model's critical parameters cannot be fully determined they are characterized by means of a distribution and/or confidence intervals.

(iii) Characterization of the uncertainty in the M&S structure

The ADS manufacturer should provide evidence that the modelling assumptions are given a quantitative characterization by assessing the generated uncertainty (e.g. comparing the output of different modelling approaches whenever possible).);

(iv) Characterization of aleatory vs. epistemic uncertainty

The ADS manufacturer should aim to distinguish between the aleatory component of the uncertainty (which can only be estimated but not reduced) and the epistemic uncertainty deriving from the lack of knowledge in the virtualization of the process.

Appendix 2: Documentation structure

This section will define how the aforementioned information will be collected and organized in the documentation provided by the ADS manufacturer to the relevant authority.

The ADS manufacturer should produce a document (a "simulation handbook") structured using this outline to provide evidence for the topics presented.

The documentation should be delivered together with the corresponding release of the toolchain and appropriate supporting data.

The ADS manufacturer should provide clear reference that allows tracing the documentation to the corresponding parts of the toolchain and the data.

The documentation should be maintained throughout the whole lifecycle of the toolchain utilization. The assessor may audit the ADS manufacturer through assessment of their documentation and/or by conducting physical tests.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 6: Track and real-world testing

This annex proposes test matrices to support track and real-world testing of ADS and ADS vehicles. This approach recommends the use of one general matrix for physical testing complemented by test matrices designed respectively for track testing and real world testing.

The general matrix for physical testing provides an overview of how the ADS safety requirements could be assessed using track testing, real world testing, or both. The test matrices for track testing and real world testing would differ in design in order to take into account the different settings in which the tests are conducted and to ensure that the strengths of each testing method can be utilized.

The test matrices set out in this annex are illustrative and include indicative rather than definitive criteria.

General matrix for physical testing

The general matrix overviews the type(s) of physical tests suitable for assessing compliance with the ADS safety requirements. The following table illustrates the concept for listing requirements alongside the indication of whether track and/or real-world testing might be suitable for assessment of compliance. The listed requirements are indicative and would be replaced by verifable criteria defined for the ADS under assessment (see Annex 3 for an approach to defining these criteria based on the high-level ADS safety requirements).

Table 6. Example of the General Matrix for Physical Testing

ADS Safety Requirement	*Track*	*Real World*
1. The ADS should perform the entire Dynamic Driving Task.	Yes	Yes
2. The ADS should control the longitudinal and lateral motion of the vehicle.	Yes	Yes
(…)		
7. The ADS should adapt its behaviour in line with safety risks.	Yes	If encountered
8. The ADS should adapt its behaviour to the surrounding traffic conditions.		Yes
(…)		
30. The ADS should safely manage short-duration ODD exits.	Yes	Yes
31. Pursuant to a collision, the ADS should stop the vehicle and deactivate.	Yes	If encountered
(…)		

One very important consideration in applying this matrix is that an ADS (except one at SAE Level 5) is designed to perform the DDT only within its ODD. Except for momentary situations where an ODD element is missing (e.g., an ADS reliant on lane markngs encounters a short stretch of road with obscured markings), an ADS will not perform the DDT outside of its ODD and for safety reasons should not do so. Therefore, track and real world testing of an ADS must occur in a test environment within the ODD of the ADS or one that sufficiently replicates the relevant ODD elements.

‘If encountered’ as used in the table above would indicate that real-world testing would not seek to assess the particular requirement but would do so if it occurred during a test. Some situations are clearly undesirable from a safety perspective on public roads. However, given that real-world testing inherently involves uncontrolled parameters, critical traffic situations could organically occur and in this case, the performance with regard to the specific requirement should be assessed. Safety during testing on public roads should also be taken into account, and the assessor or the driver should ensure they can take over the driving task if needed.

Instead of “Yes” or “If encountered”, the table might also be structured to provide more information on the intended objective(s) of the test. For example:

Table 7. Example of alternative structure for the general matrix

ADS Safety Requirement	*Track*	*Real World*
The ADS should respond safely to the cut-in of another vehicle.	Verification of the ADS crash-avoidance response to a dangerous cut in.	Nominal verification that the ADS adapts the vehicle positioning in response to the cut in. Verification of the ADS crash-avoidance response to a dangerous cut in, if encountered.

Matrix for track testing

The following table illustrates an approach combining traffic scenarios, performance requirements, and test specifications into a matrix for conducting track tests. The “scenario” column would cross-reference the testing with the scenario upon which the testing is based, covering the traffic situation, infrastructure elements, objects, ODD elements, etc. The “safety requirement(s)” column would cross-reference the specifications established for ADS performance under the scenario. The “additional test specification” column would allow for conditions or parameters not described in either the traffic scenario or the safety requirement(s), but are necessary to conduct the track test (e.g. minimum duration of the test).

Table 8. Example of a test matrix for track test

Traffic Scenario	*Safety Requirement(s)*	*Additional Test Specifications*	*Assessment Specification*
Unobstructed travel on a straight path	Safe lateral positioning in a lane of travel	A minimum test duration of 5 minutes	The test shall verify that the ADS does not leave its lane and maintains a stable position inside its ego lane across the speed range within its system boundaries.
Unobstructed travel along a curve	Safe lateral positioning in a lane of travel Adapt to road conditions	A minimum test duration of 5 minutes	The test shall demonstrate that the ADS does not leave its lane and maintains a stable position inside its ego lane across the speed range and different curvatures within its system boundaries.
Cut-in by another vehicle while traveling on a straight path	Respond safely to the cut-in Safe longitudinal positioning relative to a lead vehicle	Scenario with selected parameters to verify the ADS crash-avoidance response to a dangerous cut in per the safety requirements[42]	The test shall demonstrate that the ADS is capable of avoiding a collision with a vehicle cutting into the lane of the ADS vehicle up to a certain criticality of the cut-in manoeuvre.
ODD exit scenario	ADS detection of ODD boundary Automated response (failed fallback user response or no fallback user)	Test for failed fallback user response	The test shall demonstrate that the ADS is capable of bringing the vehicle to a safe stop, in case of a failed fallback user response.

Matrix for real world testing

The following table illustrates an approach combining performance requirements and traffic situations into a matrix for conducting real-world testing. The “safety requirements” column would specify the verifiable performance requirement(s).

The top rows on the right side set out traffic situations to be encountered during real-world testing. The matrix intentionally uses the term “traffic situation” rather than “traffic scenario” given that real-world traffic cannot be controlled to reproduce

[42] This inclusion assumes the traffic scenario does not prescribe the range of parameters to be selected for the occurrence of a safety-critical situation. If that were to be included in the scenario, this field could be empty.

predefined scenarios in all cases. The test route(s) should be designed to ensure exposure of the ADS to situations under which the ADS can demonstrate compliance with the safety requirements.

The remaining fields of the matrix describe behavioural competencies defined for the traffic situations per Annex 3. Each behavioural competency summarizes the desired performance in one sentence with a more detailed description to be set out in the testing protocols accompanying the test matrix where necessary. The behavioural competencies correspond to the safety requirement(s) applicable to each traffic situation.

As discussed under the general matrix, the real-world testing matrix allows for “if encountered” assessments. Real-world testing requires assessment of nominal performance but allows for conditional assessment of critical and/or failure performance should such situations occur during the testing. Real-world testing includes assessment of the ADS competency to mitigate safety risks due to external conditions and behaviours of other road users. For example, row 2.1. notes ADS responses to a nominal cut-in by another vehicle as well as the possibility of a dangerous cut-in occurring during the testing.

Aspects related to routing (e.g. minimum duration, minimum frequency of a given traffic situation encountered during testing, etc.) would be set out in the accompanying test protocols.

Table 9. Example of a test matrix for real world testing: motorway application

		Traffic Situations				
	Safety Requirements	*Driving on the motorway*	*Merging*	*Lane Change*	*Overtaking*	*Exiting Motorway*
1.1.	Safe lateral positioning in a lane of travel	The ADS demonstrates it does not leave its lane and maintains a stable position inside its ego lane across the speed range within its system boundaries.	The ADS demonstrates it achieves a stable position inside the target lane upon completion of the lane change procedure.	The ADS demonstrates stable positioning inside the target lane upon completion of the lane change procedure.	The ADS demonstrates it achieves a stable position inside the target lane upon completion of the lane change procedure.	The ADS demonstrates it maintains a stable position in the off-ramp lane.
2.1.	Respond safely to the cut-in of another vehicle	The ADS adapts the vehicle positioning in response to the (nominal) cut in. The ADS responds appropriately[43] to a dangerous cut in, if applicable.[44]				
2.2.	Safe longitudinal positioning relative to a lead vehicle	The ADS demonstrates it maintains a safe longitudinal position relative to a lead vehicle.	The ADS demonstrates it maintains a safe longitudinal position relative to a lead vehicle during and upon the completion of the lane change procedure.	The ADS demonstrates it maintains a safe longitudinal position relative to a lead vehicle prior and during the lane change procedure. The ADS demonstrates it maintains a safe longitudinal position relative to a lead vehicle upon the completion of the lane change procedure, if applicable.	The ADS demonstrates it maintains a safe longitudinal position relative to a lead vehicle prior and during the lane change procedure.	The ADS demonstrates it maintains a safe longitudinal position relative to a lead vehicle, if applicable.

[43] What constitutes an ‘appropriate response’ would then be set out in the testing protocols that accompany the test matrix, sourced from FRAV.

[44] To be determined whether ‘If encountered’ situations should be included in the matrix itself. Included here, as well as in other parts of the table, as an illustration.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 7: ISMR and safety requirements matrix

The following matrix indicates which requirements are suitable for ISMR activities

The matrix is aimed at providing guidance for manufacturer and authorities in regard to the monitoring of ADS operations.

The matrix uses a green, orange, red colour scheme to indicate the relative applicability of the pillars.

- Green is broadly applicable to the requirement, can monitor most aspects of the requirement
- Orange is only applicable to the requirement a limited way.
- Red is largely not applicable to the requirement.

If a pillar is green, then applying the ISMR pillar does not necessarily mean fully monitoring the requirement but potentially only an aspect of it

Although certain pillars are currently rated as having limited applicability (orange or red), technological advances could change this assessment in the future.

Requirements	Comments
ADS Performance of the DDT under Nominal Traffic Scenarios	
The ADS shall operate the vehicle at safe speeds.	1) it can be monitored, but it is difficult to define what safe speed is 2) Speed-limit compliance suitable for periodic reporting. However, it is difficult to report, because it can require data from other sources
The ADS shall maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle.	Appropriate distance can be monitored via SPIs (e.g., Longitudinal and lateral distance)
The ADS shall adapt its driving behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic).	Simple kinematic metrics or similar metrics could be monitored (e.g., TTC, THW)
The ADS shall adapt its driving behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).	Simple kinematic metrics and similar metrics could be monitored (e.g., TTC, THW)
The ADS shall detect and respond to objects and events relevant to its performance of the DDT.	It can be monitored via SPIs (e.g., OEDR reaction time) Failure respond to OEDR could result in short-term (i.e. covered by EDR requirements)

The ADS shall detect and respond to priority vehicles in service in accordance with the relevant traffic law(s).	There may be cases where the ADS cannot detect an emergency vehicle and consequently has no way of monitoring the event. In this case, third-party data are needed to monitor and report the event Notes: it could be a triggering condition for DSSAD
Under nominal traffic scenarios, the driving behaviour of the ADS shall not force other road users to take evasive action to avoid a collision with the ADS vehicle.	There may be cases where the ADS cannot detect an emergency vehicle and consequently has no way of monitoring the event. In this case, third-party data are needed to monitor and report the event
Under nominal traffic scenarios, the driving behaviour of the ADS shall not cause a collision.	1) To be monitored 2) Short-term reporting in case of a collision which fall into the critical occurrence category 3) Periodic reporting of aggregated metrics Note: Any collision requires a proper investigation to identify the root cause.
The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation.	There may be cases where the compliance to the traffic rules requires third party data.
The ADS shall interact safely with other road users.	It can be monitored via dedicated SPIs
The ADS shall avoid collisions with safety-relevant objects where possible.	It can be monitored via dedicated SPIs
The ADS shall signal intended changes of direction.	It could be monitored, but It is a signaling requirement, mainly related to the Design.
The ADS shall signal its operational status in accordance with national rules.	It could be monitored, but It is a signaling requirement, mainly related to the Design.
Pursuant to a passenger request, the ADS shall bring the vehicle to a safe stop.	It can be monitored
ADS Performance of the DDT under Critical Traffic Scenarios	
The requirements for DDT performance under nominal scenarios shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.	
In the event of a collision, the ADS shall stop the vehicle in an MRC and/or in accordance with applicable traffic laws	1) To be monitored 2) Post-collision behaviors to be reported in short-term

The ADS shall not resume travel until the safe operational state of the ADS vehicle has been verified.	1) It can be monitored. However, only selfcheck carried out by the ADS vehicle itself is possible via monitoring. Third parties information can be needed 2) Post-collision behavior to be reported in short-term
The ADS may resume the trip where permissible under the applicable traffic rule(s) and other safety considerations.	1) It can be monitored 2) Post-collision behavior to be reported in short-term
ADS Performance of the DDT under Failure Scenarios	
The requirements for DDT performance under nominal scenarios shall continue to apply during failure scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.	
The ADS shall detect faults, malfunctions, and abnormalities that compromise its capability to perform the entire DDT within the ODD of its feature(s) per the manufacturer's documentation.	1) To be monitored 2) ADS faults to be reported through periodic reporting.
The ADS may continue to operate in the presence of faults that do not prevent that ADS from fulfilling the safety requirements applicable to the ADS.	1) It can be monitored 2) ADS faults to be reported through periodic reporting, but it is missing a dedicated provision for the reporting of normal operations in fault conditions
In response to a fault, the ADS may permit activation and use of a feature impacted by the fault provided that the ADS continues to provide the functions necessary to perform the entire DDT.	1) It can be monitored 2) ADS faults to be reported through periodic reporting, but it is missing a dedicated provision for the reporting of operations in fault conditions
The ADS shall adapt its performance of the DDT in accordance with the severity of the fault to ensure road safety	it can be monitored
The ADS shall prohibit activation of an ADS feature in the presence of a fault in an ADS function that compromises the ADS capability to perform the entire DDT within the ODD of the feature.	It could be monitored to some extent.
The limited operation of the ADS should comply to the normally applicable safety requirements.	1) It can be monitored 2) same considerations of the "normally applicable requirements" apply
Remote termination of individual or multiple ADS or feature(s) by the manufacturer and/or service operator	1) it could be monitored bt it is mainly a design requirement. 2) The remote termination could be a potential occurrence to be reported.

shall be possible when requested by Authorities.	
Remote termination for an ADS performing the DDT shall be capable of triggering an ADS fallback response.	1) it can be monitored. 2) The remote termination could be a potential occurrence to be reported.
Remote termination of an ADS or ADS feature(s) shall render them unable to be activated by user.	1) it could be monitored bt it is mainly a design requirement. 2) The remote termination could be a potential occurrence to be reported.
ADS Performance of the DDT at ODD Boundaries	
The ADS shall recognise the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration.	1) To be monitored according to section 8. 2) ADS operation outside its ODD should be reported via short-term and at aggregated level via periodic-term according to the Occurrence list in section 8
The ADS shall be able to determine when the conditions are met for activation of each feature.	It can be monitored
The ADS shall prevent activation of a feature unless the ODD conditions of the feature are met.	1) It can be monitored to some extent(indirectly) but, It is mainly a design requirement. 2) ADS operation outside its ODD should be reported via short-term and at aggregated level via periodic-term
The ADS shall execute a fallback response when one or more ODD conditions of the feature in use are no longer met.	1) It can be monitored 2) ADS operation outside its ODD should be reported via short-term and at aggregated level via periodic-term 3) Transfer of control failure in periodic reporting 4) Failure to achieve MRC in short term and periodic reporting
The ADS shall be able to anticipate foreseeable exits from the ODD of each feature.	It can be monitored, Notes: it could be a triggering condition for DSSAD.
Minimal Risk Condition Requirements	
The ADS shall signal its intention to place the vehicle in an MRC.	It can be monitored. It is a Safety Critical information
The ADS shall execute a fallback response in the event of a failure in the ADS and/or other vehicle system that prevents the ADS from performing the DDT.	1) it can be monitored 2) ADS failure to achieve a minimal risk condition in short term and periodic reporting
In the absence of a fallback-ready user, the ADS shall fall back directly to an MRC.	1) it can be monitored

	2) ADS failure to achieve a minimal risk condition in short term and periodic reporting
If the ADS is designed to request and enable intervention by a human driver, the ADS should execute a fallback to an MRC in the event of a failure in the transition of control to the user.	1) It can be monitored 2) Transfer of control failure in the periodic reporting
Upon completion of a fallback to an MRC, a user may be permitted to assume control of the vehicle.	1) it could be monitored to some extent but, it ia mainly a Design requirement. 2) post MRC behavior can be monitored 3) Reporting provisions for MRC failures
Recommendations for safe interactions between Users and ADS.	
The ADS shall signal the presence of any failure that limits the operation of an available feature.	1) It could be monitored to some extent 2) ADS faults to be reported through periodic reporting
The ADS shall signal its intention to place the vehicle in an MRC to the ADS user(s).	It could be monitored to some extent
An ADS that controls the operation of doors shall provide an emergency override to the user.	1) Design requirement
The ADS HMI shall provide safety relevant information and signals clearly noticeable to the target user(s) under all operating conditions, multimodal (e.g., optical, acoustic, haptic) if needed, simply and unambiguously.	1) Design requirement
ADS features that allow a user to take over manual control of the DDT.	
When the ADS is active, the vehicle driving controls, indicators, tell-tales, and DDT-related warnings may be disabled, suppressed, de-activated, inhibited or by other means made unavailable, as needed to mitigate the risk of errors in operation, misuse and reduce ambiguous states of vehicle control.	1) Design requirement
The ADS shall be designed to prevent misuse and errors in operation by the user.	1) Design requirement
The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions.[1]	

While an ADS feature is active, it shall inform the user on: (a) ADS status information. (b) the role of the fallback user, if applicable. € Any failure of the ADS that limits the operation of an available feature.	1) Design requirement
The ADS shall indicate the availability of a feature for activation.	1) Design requirement
Recommendations on the ADS feature activation.	
The ADS shall ensure a safe ADS feature activation. (a) The ADS shall provide prompt feedback to indicate success or failure when the user attempts to enable an ADS feature. (b) The feature activation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards. € An ADS feature activation resulting in a user becoming a fallback user shall inform the fallback user of the consequent expectations on them.	1) Design requirement
Recommendations on ADS feature deactivation to manual driving.	
The ADS shall have a monitoring system to support safe and appropriate engagement of the user as necessary.	1) Design requirement
At the completion of the deactivation process, lateral and longitudinal control shall be returned to the driver without any continuous control assistance active.[2]	1) Design requirement
ADS features that allow a user-initiated system deactivation to manual driving.	
The ADS shall be designed to ensure a safe user-initiated system deactivation process. (a) The ADS shall only allow the user to initiate a system deactivation process if the ADS can verify that the user is in a position to resume the role of the driver. (b) ADS feature deactivation may be delayed if it is assessed by the ADS that the situation is unsuitable for the subsequent mode of vehicle	1) It could be monitored to some extent. However, most of the points are not suitable for ISMR. The point a) and b) can be monitored. 2) Prevention of takeover under unsafe conditions to be reported according to NATM occurrence list 3) Driver unavailability (where applicable) and other user related occurrences to be reported according to section 8 occurrence list

operation. (e.g., due to the current situation being unsuitable or unsafe for the subsequent mode of operation). € The user-initiated system deactivation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards. (d) The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process. € The ADS shall provide a specific indication of the completion of the deactivation of the ADS. (f) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving. (g) If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.	
ADS features that have a system-initiated deactivation to manual driving.	
The ADS shall ensure a safe system-initiated deactivation to a fallback user. (a) A system-initiated deactivation in nominal situations should be indicated in a timely manner to support the fallback user re-engaging to the driving task. (b) The system-initiated deactivation to manual driving process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards. € The ADS shall: (i) Continuously assess whether the fallback user is available for a system-initiated deactivation. (ii) Provide effective procedures for re-engaging the fallback user who has been detected not to be available. (iii) Trigger an MRM where it has not been possible, feasible and/or safe to re-engage the fallback user.	1) It could be monitored to some extent. However, most of the points are not suitable for ISMR. The point c) can be monitored. 2) Occurrences related to Transfer of Control failure and Driver unavailability already included in the occurrence list of section 8

(iv) Where appropriate, adapt the system-initiated deactivation process (e.g., timing, levels of warnings) according to the current circumstances (e.g., the engagement of the fallback user, the status of the ADS and vehicle, the current traffic situation). (d) The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process. € The ADS shall remain active until the system initiated deactivation process has been completed or the ADS vehicle reaches a minimal risk condition. (f) The ADS shall provide a specific indication of the completion of the deactivation of the ADS. (g) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving. (h) If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.	
ADS features that do not allow a user to take manual control of the DDT.	
The ADS shall provide the passenger(s) with means to request to stop the vehicle.	1) Design requirement
The ADS vehicle shall provide safety-related information to the passengers.	It can be monitored
The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated.	1) Design requirement
The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress).	1) Design requirement
Controls provided for manual driving (e.g., steering, service brake, parking brake, accelerator, lighting) shall be designed to prevent any effect on the DDT whilst the ADS is performing the DDT, or reasonable safeguards shall be	1) Design requirement

put in place to prevent access to controls.	
Safety throughout the Useful Life of the ADS and its Features	
The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons.	1) Design requirement
The ADS shall be designed to protect against unauthorized access to and modification of the ADS functions.	1) to be monitored 2) Unauthorized access to and modification of the ADS functions to be reported
The measures ensuring protection from unauthorized access should be provided in alignment with engineering best practices.	1) Design requirement
ADS safety shall be ensured in the event of discontinued production, support, and/or maintenance.	1) Design requirement
Note: Critical occurrences to be reported as short-term report can be the result of non-compliance with ADS safety requirements.	

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 8: ISMR reporting templates

This Annex provides guidance to help ADS manufacturers and ADS operators with the implementation of the short-term and periodic reporting scheme.

Short term reporting

The first topic of the reporting form (“WHAT”) is a short description of the event aimed at providing a brief summary of the occurrence. A list of example circumstances can be found in the insurance report templates and in the NHTSA ADS standing order.

WHAT		
Entry name	Field to be filled	Type/size
Headline		Text(200)

Secondly, the occurrence is classified according to a list of possible classes. Currently, this document only provides a distinction between critical and non-critical occurrences. Those categories might be refined to include additional classes, e.g. referring to the classification of conflict type.

OCCURRENCE CLASSIFICATION		
Occurrence class		Text(50)
Occurrence type		Text(200)

The reporting form shall be filled with weather detail and other information, as available which might help identify the safety relevance of the occurrence (speed, acceleration, and mass, existence and behaviour of other road users, volatile infrastructure characteristics). Additionally, if supporting vehicle telematics and/or media (e.g. camera/LiDAR recordings) are provided they shall be stated in the following section.

OCCURRENCE DETAILS		
Weather conditions		Text(20)
Lighting conditions		Text(20)
ADS vehicle pre-occurrence speed		Number(3) – [km/h]
ADS vehicle post-occurrence max deceleration		Number(3) – [m/s^2]
ADS vehicle estimated pre-occurrence mass		Number(5) – [kg]
ADS vehicle telematics provided		[Y/N]
ADS vehicle EDR data provided		[Y/N]

ADS vehicle DSSAD data provided		[Y/N]
ADS vehicle media provided		[Y/N]
Third-party sources media/telematics provided		[Y/N]
Occurrence reported to the police		[Y/N]
Police report available		[Y/N]
Autonomy level at occurrence		Text(50)
Driver/remote operator available at occurrence		[Y/N]
Driver/remote operator attempted takeover		[Y/N]

The reporting form should be filled with time information, both local and UTC.

WHEN		
UTC date		[YYYY/MM/DD]
UTC time		[HH:mm]
Local date		[YYYY/MM/DD]
Local time		[HH:mm]

The reporting form should be filled with the complete specification of the occurrence location and a brief description of the local scenery.

WHERE		
Country		Text(50)
State/Province		Text(50)
City		Text(50)
ZIP code		Number(10)
Street/Intersection		Text(50)
GNSS coordinates		[longitude, latitude] [Decimal degree]
Scenario within ODD		[Y/N]
Speed limit at location		Number(3) – [km/h]
Roadway type		Text(50)
Roadway surface		Text(50)
Roadway description		Text(100)

The reporting template shouldbe filled with the levels and details of the damages recorded for both the ADS vehicle and other traffic participants/objects. A practical indication of the damage level is found in the aviation practice:

(a) destroyed: the damage makes it inadvisable to restore the vehicle;

(b) substantial: the vehicle sustained damage of structural failure requiring major replacement;

€ minor: the vehicle can be rendered operational by simple repairs/replacement;

(d) none: the vehicle sustained no damage;

€ unknown: the damage level is unknown.

In addition, the Collision Deformation Classification (CDC) or the Vehicle Damage Index (VDI) should be provided if applicable.

DAMAGE		
Highest damage		Text(20)
ADS vehicle damage level		Text(20)
ADS vehicle damage location		Text(20)
Highest damage to other object		Text(20)
Object damaged (level)		Text(50)
		Text(50)
		Text(50)
		Text(50)

The reporting form should be filled with details regarding the injury level for the ADS vehicle occupants and each other road user being involved and stated to be injured. Examples from the CADaS taxonomy are:

(a) fatal: death within 30 days of the accident and as a result of the accident;

(b) critical: injured (although not killed) in the road accident & injured person in very serious condition, may need surgery or a long hospital stay to survive;

€ serious: injured (although not killed) in the road accident and hospitalized for at least 24 hours;

(d) minor: Injured in road accident but no hospitalization required, only first aid;

€ none: nobody was injured during the occurrence;

(f) unknown: injured in the road accident but the injury level is unknown.

If possible, the additional use of Abbreviated Injury Scheme (AIS) injury classification is recommended, either on single injuries or at the person level, reporting MAIS.[45]

[45] Additional examples include Canada National Collision Database (NCDB).

INJURY		
Injury level		Text(50)
Total fatalities ADS vehicle		Number(3)
Total fatalities other road user		Number(3)
Road user type		Text(50)
Total serious injuries ADS vehicle		Number(3)
Total serious injuries other road user		Number(3)
Road user type		Text(50)
Total minor injuries ADS vehicle		Number(3)
Total minor injuries other road user		Number(3)
Road user type		Text(50)
Total unknown injuries ADS vehicle		Number(3)
Total unknown injuries other road user		Number(3)

The reporting form shall be filled with details concerning the ADS vehicle.

VEHICLE		
Vehicle Identification Number		Text(17)
Serial number		Text(50)
License plate		Text(10)
State/Country/Province of registry		Text(50)
Vehicle category		Text(50)
Manufacturer		Text(50)
Model		Text(50)
Model Year		Number(4)
Mileage		Number(9)
ADS version		Text(50)
ADS licensing		Text(50)
Operator (if any)		Text(50)
Autonomy level		Text(50)

The reporting form should be filled with an exhaustive narrative concerning the occurrence. A schematic representation similar to the insurance report might be provided to help with the occurrence understanding. The pre-crash scenario assessment may be carried out according to the NHTSA scenario crash scenario topology where applicable . Moreover, this section shall be filled with the post-crash behaviour of the ADS vehicle. If possible digital reconstruction files shall be provided (e.g. PC CRASH files, etc.).

NARRATIVE	
Description of the event	
Post-crash behaviour	

The report shall include a preliminary root cause analysis, including risk assessment, and the corresponding corrective implementing action (if any) procedure enforced by the reporting authority after the same has become aware of the occurrence.

ANALYSIS	
Root cause analysis	
Corrective implementing action	

The report shall include management details including the reporting entity that provided the report and the reporting status. A few options are provided for the reporting status:

(a) preliminary: the communication used for the prompt dissemination of data obtained in the early stages of the investigation. More data is expected;

(b) initial notification: record is based on, or contains information corresponding to the level of information in the initial notification of an accident or incident (ICAO Annex 13, Chapter 4);

€ factual: the handling of the occurrence has not yet been completed, but there is sufficient information to analyse and code the occurrence;

(d) closed on issue: report closed by the reporting organisation on first its issuance;

€ closed: no further information is expected.

REPORT MANAGEMENT		
Reporting entity		Text(100)

Report ID		Text(240)
Report version		Number(10)
Report status		Text(100)
Report data		[YYYY/MM/DD]
Parties informed		Text(100)

Periodic reporting

The first set of entries covers general information about the ADS identification and usage in terms of distance/time travelled. This set of information has the main aim of providing the authority with the possibility of occurrences normalization with respect to the effective ADS operation.

ADS IDENTIFICATION		
Entry name	Field to be filled	Type/size
ADS manufacturer		Text(50)
ADS licensing authority		Text(50)
ADS version		Text(50)
Autonomy level		Text(50)
Vehicle model		Text(50)
Model year		Text(50)

ADS OPERATION INFORMATION		
Number of vehicles featuring ADS		Number(10)
Cumulative distance travelled by ADS in operation		Number(10)
Cumulative time travelled by ADS in operation		Number(10)
Average ADS time engagement		Number(10)

The second list of entries covers the set of occurrences which remained unexplored from short term reporting as of the occurrence table coupled with the safety outcome of such events. Eventually, by combining the ADS operation with the list occurrences, the authority and manufacturer should agree on the Metrics and Safety Performance Indicators to confirm the safety level stated by the ADS manufacturer.

OCCURRENCES ASSESSMENT		
Cumulative number of occurrences		Number(10)
Occurrences covered under the short-term reporting provisions		Number(10)

Safety critical occurrences known to the ADS manufacturer or OEM		Number(10)
Occurrences related to ADS operation outside its ODD		Number(10)
ADS failure to achieve a minimal risk condition when necessary		Number(10)
Modifications made by the ADS manufacturer or OEM to address an identified and significant ADS safety issue		Number(10)
Occurrences covered under the periodic reporting provisions		Number(10)
Communication-related occurrences		Number(10)
Cybersecurity-related occurrences		Number(10)
Interaction with remote operator if applicable		Number(10)
Driver unavailability (where applicable) and other user-related occurrences		Number(10)
Occurrences related to Transfer of Control failure		Number(10)
Prevention of takeover under unsafe conditions		Number(10)
Occurrences related ADS failure		Number(10)
Maintenance and repair problems		Number(10)
Occurrences related to unauthorized modifications		Number(10)
Occurrences related to the identification of new safety-relevant scenarios		Number(10)
Other occurrences		Number(10)

Thirdly, the safety outcome associated with the occurrences shall be reported together with aggregate data about other traffic participants involved in the occurrences.

OCCURRENCES SAFETY OUTCOME		
Fatalities		Number(10)
ADS vehicle occupants		Number(10)
Other road users		Number(10)
Serious injures		Number(10)
ADS vehicle occupants		Number(10)
Other road users		Number(10)
Minor injures		Number(10)
ADS vehicle occupants		Number(10)

Other road users		Number(10)
Unknown injures		Number(10)
ADS vehicle occupants		Number(10)
Other road users		Number(10)
Accident and serious incidents		Number(10)
Minor incidents		Number(10)

OCCURRENCES AGGREGATE DESCRIPTION		
Collision with:		-
• Passenger car		Number(10)
• VAN		Number(10)
• Truck		Number(10)
• Bus		Number(10)
• Other: Vehicle		Number(10)
• Motorcycle		Number(10)
• Cyclist		Number(10)
• Pedestrian		Number(10)
• Other: VRU		Number(10)
• Animal		Number(10)
• Fixed object		Number(10)
• Unknown		Number(10)
• ADS vehicle damage level		-
• Destroyed		Number(10)
• Substantial		Number(10)
• Minor		Number(10)
• Unknown		Number(10)
ADS vehicle damaged area		-
• Front		Number(10)
• Front-left		Number(10)
• Front-right		Number(10)
• Rear		Number(10)
• Rear-left		Number(10)
• Rear-right		Number(10)
• Left		Number(10)

• Right		Number(10)
• Top		Number(10)
• Bottom		Number(10)
• Unknown		Number(10)

The fourth set of entries covers modifications (if any) made to the ADS in case of safety gaps.

ADS SAFETY GAP		
ADS discovered safety gaps		Number(10)
Gap #1:		Text(500)
Gap #2:		Text(500)
ADS addressed safety gaps (if any)		Number(10)
Gap #1:		Text(500)
Gap #2:		Text(500)
ADS safety gap are addressed and how		Number(10)
Gap #1:		Text(500)
Gap #2:		Text(500)

Eventually, the report shall include management details including the reporting entity that provided the report and the reporting status. A few options are provided for the reporting status:

- preliminary: the communication used for the prompt dissemination of data obtained in the early stages of the investigation. More data is expected;
- initial notification: record is based on, or contains information corresponding to the level of information in the initial notification of an accident or incident (ICAO Annex 13, Chapter 4);
- factual: the handling of the occurrence has not yet been completed, but there is sufficient information to analyse and code the occurrence;
- closed on issue: report closed by the reporting organisation on first its issuance;
- closed: no further information is expected.

REPORT MANAGEMENT		
Reporting entity		Text(100)
Report ID		Text(240)
Report version		Number(10)
Report status		Text(100)
Report data		[YYYY/MM/DD]

Parties informed		Text(100)

Annex 9: Additional recommendations for effective in-service monitoring

Voluntary Reporting

At the national level, Safety Authorities may put in place a system of voluntary reporting to collect and analyse information on observed ADS behaviours which are not required to be reported under the system of occurrences reporting set in this document, but which are perceived by the reporter as an actual or potential hazard.

Collection and storage of information

It is recommended that a mandatory reporting system is established at national level by means of a national database and at international level by means of a harmonized Common Central Repository.

Data quality and consistency should be ensured both at national and international level by establishing checking processes.

a) National level

To implement the ISMR framework, Contracting Parties are recommended to designate one or more competent authorities to put in place a mechanism to collect, evaluate, process and store occurrences reported in accordance with ISMR principles.

The safety authority/ies at national level should be responsible for collecting and assessing the data and for deriving and sharing safety recommendations. It (They) should manage the safety-related information stored in the national database and share that information with other competent authorities. These safety authorities are also in charge of issuing an annual report summarizing the level of ADS safety and providing an overall safety assessment and action plan. The annual report should be submitted to WP29.

Short term and periodic reports should be stored within the common national database. Safety recommendations should also be stored in the common national database and made accessible to the relevant stakeholders.

Safety authorities should transfer safety recommendations and annual reports to the Common Central Repository.

b) International level

WP29 provides a suitable international context for exchanges between Contracting Parties and for defining the guiding principles on the ISMR framework implementation.

It is recommended that WP.29 establishes a proper management system of the Common Central Repository. It should cover accessibility and dissemination of information, data protection where needed, data evaluation and annual reporting. The technical protocols for transferring all safety recommendations to the Common Central Repository should also be established.

Clear guidance on the standardized approach to ISMR, including the harmonisation of the data entry process, should be organized by WP.29 at international level by providing guidelines, workshops and appropriate training.

Occurrences Investigations

It is recommended that each Contracting Party designates at national level one competent body responsible for conducting the investigations of accidents, incidents and any other relevant event in their countries according to its investigation mandate. The body may be an existing transportation safety investigative agency responsible for investigating transportation accidents.

It is desirable for this body to be independent in its organisation, legal structure and decision-making from any interested party, including other entitled regulatory body, other national bodies in charge of investigating liability aspects of crashes or in charge of the collection and storage of information reported by manufacturers.

In case of accidents/incidents an investigation report should be produced. It should be produced and made available in the shortest possible time after the date of the occurrence to all parties involved. It should where appropriate, contain safety recommendations.

A periodic report should be produced and shared regularly at least every year, or more frequently if relevant. It should provide information about the investigations carried out in the preceding year and the safety recommendations that were issued.

Exchange of Information

It is recommended that WP29 promotes and facilitates a broader exchange of information and the dissemination of safety recommendations among the Contracting Parties with the aim of improving safety.

Safety Authorities should participate regularly in the exchange and analysis of information contained in the Common Central Repository.

It is recommended that Safety Authorities participate in an exchange of information by making all relevant safety-related information available to the other competent authorities.

The exchange of relevant information among involved Contracting Parties / Authorities should be required in case of accidents/incidents investigations.

The dissemination of information should be limited to what is strictly required for the purpose of its users, in order to ensure appropriate confidentiality of that information.

Protection of information

Given the sensitive nature of safety-related information, the protection of its source and the confidence and trust of the reporters should be guaranteed to the extent legally possible. To protect the sensitivity of the information, it is recommended that it is only used for safety related activities and not for any other purpose.

Security measures need to be in place to protect the confidentiality of information that is shared. For example, the security measures and protocols should ensure that no personal details are ever recorded in the databases either at national or international level and that relevant protections for trade secrets and confidential business information be observed.

Without prejudice to the applicable national law, it is recommended that Safety Authorities refrain from instituting proceedings in respect of unpremeditated or inadvertent infringements of the law that come to their attention only because they have been reported under the ISMR occurrence-reporting scheme, except in cases of gross negligence.

In accordance with the procedures defined in their national laws and practices, Safety Authorities should ensure that employees who report incidents of which they may have knowledge are not subjected to any prejudice by their employer.

Submitted by the co-chairs of the
FRAV and VMAD Informal Working Groups

Informal Document GRVA-18-xx
18th GRVA session
22-26 January 2024

Annex 10: Further considerations for future work

This annex notes topics for further consideration raised during the work on these guidelines. These items are offered for future consideration…

- Relationships between the Safety Management System concept and regulations concerning cyber security and software update management.
- Procedures for the establishment of objective behavioural competencies for DDT performance based on the safety requirements and their application to scenarios and test methods.
- Relationship between In-Service Monitoring and Reporting (ISMR) and the behavioural competencies demonstrated during the original ADS assessment.
- Procedures for establishing the validity of safety models used to assess ADS performance under critical scenarios with regard to avoidable/unavoidable outcomes.
- Further consideration of approaches to developing safety models, including their applicability to assess aspects of ADS performance, and covering FRAV discussions on methodologies such as "state of the art", "careful and competent driver", and "safety envelope" concepts.
- Consideration of a common catalogue or database of traffic scenarios for regulatory use.
- Consideration of data recording under ISMR and the activities of the EDR/DSSAD informal group.
- Development of procedures for establishing track and real-world testing matrices and protocols.
- Consideration of "remote operation" of ADS vehicles.
- Selection of fallback user (e.g., untrained, professional, level of experience) under physical test procedures and consideration of the term "on-board operator" in lieu of "fallback user".
- Responsibility for civil liability during real-world testing (WP.29, WP.1?).
- Determination of pass/fail criteria under real-world testing.
- Reconciliation of track testing and ODD coverage.
- Protocols for designing real-world tests (e.g., scenarios, engineered test routes).
- Consideration of user monitoring with regard to safe use of ADS.
- Consideration of less subjective definitions for nominal and critical traffic scenarios and procedures for classification of traffic scenarios within the context of assessing compliance with safety requirements.

- Consideration of “interpretation materials” to support Safety Management System guidelines.
- Development of harmonised provisions to ensure reasonable uniformity across ODD descriptions.
- Measures to address risks of mode confusion.
- Consideration of ISMR templates and reporting from other stakeholders.