

1. Introduction

- 1.1. 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).
- 1.2. 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
- 1.3. 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
- 1.4. TFAV established subgroups to consider AV assessment methods:
 - Physical certification tests and audit
 - Real-world test drive.
- 1.5. 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.
- 1.6. During its 178th (June 2019) session, WP.29 approved a Framework Document on Automated/ Autonomous Vehicles.³
- 1.6.1. 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
- 1.7. 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

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).

- Operational Design Domain
 - Validation for System Safety
 - Cyber security
 - Software updates
 - Event Data Recorder and Data Storage System for Automated Driving.
- 1.8. 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
- 1.9. 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).
- 1.10. 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
- 1.11. 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
- 1.12. 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

⁵ ECE/TRANS/WP.29/1147/Annex V.

⁶ ECE/TRANS/WP.29/1147/Annex VI.

⁷ ECE/TRANS/WP.29/2021/61 ([ECE/TRANS/WP.29/1159](https://www.unece.org/transport/automated/automated-vehicles-and-systems/wp29_2021_61.html))

- 1.13. 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
- 1.14. 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.
- 1.15. 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
- 1.16. Between 2019 and 2023, some 200 experts participated in nearly 80 FRAV and VMAD sessions to develop this document.

2. Scope and purpose.

- 2.1. This document aims to fulfil the FRAV and VMAD mandates and deliver the consolidated deliverable per the Framework Document described above.
- 2.2. The document proposes guidelines and recommendations for the establishment of safety requirements and assessment methods applicable to ADS vehicles as defined in Section 3.
- 2.3. The diversity of ADS vehicle configurations and the characteristics and constraints of their ODD present challenges in establishing harmonized requirements for worldwide use.
 - 2.3.1. These guidelines recommend the establishment of high-level requirements to cope with this diversity.
 - 2.3.2. The guidelines propose a framework for applying these high-level requirements to individual ADS use cases.
- 2.4. The complexity of driving also presents challenges to the assessment of ADS performance across the diversity of possible ODD.
 - 2.4.1. These guidelines recommend a multi-pillar approach to ensure comprehensive and efficient validation of ADS safety.
 - 2.4.2. The guidelines recommend the development of a scenario catalogue for use across five validation pillars:
 - Audit and safety-by-design assessment
 - Simulation/virtual testing

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 (FRAV draft guidelines with pending open issues) and WP.29/2023/44/Rev.1 (VMAD guidelines)

- Track testing
 - Real-world testing
 - In-service monitoring and reporting.
- 2.5. 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.
- 2.6. 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.
- 2.7. 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.

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.

- 3.1. “*Abstraction*” means a process of selecting relevant aspects of a source or referent system to be represented in a model or simulation.¹⁰
- 3.2. “*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
- 3.3. “*ADS feature*” means an ADS functionality designed specifically for use within an Operational Design Domain (ODD).
- 3.4. “*(ADS) function*” means an ADS hardware and software capability designed to perform a specific portion of the DDT.
- 3.5. “*ADS vehicle*” means a vehicle equipped with an ADS.
- 3.6. “*Behavioural competency*” means an expected and verifiable capability of an ADS feature to operate a vehicle within the ODD of the feature.

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.

- 3.7. *“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
- 3.8. *“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
- 3.9. *“Stochastic”* means a process involving or containing a random variable or variables pertaining to chance or probability.
- 3.10. *“Driver”* means a human user who performs in real time part or all of the DDT and/or DDT fallback for a particular vehicle.
- 3.11. *“Dynamic Driving Task (DDT)”* means the real-time operational and tactical functions required to operate the vehicle in on-road traffic.
- 3.11.1. The DDT is always performed in its entirety by the ADS in operation (“the entire DDT” as stated in the definition of an “Automated Driving System” under para. 3.2.) which means the whole of the tactical and operational functions necessary to operate the vehicle. These functions can be grouped into three interdependent categories: sensing and perception, planning and decision, and control.
- 3.11.1.1. 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.
- 3.11.1.2. Planning and decision include:
- Predicting actions of other road users.
 - Response preparation.
 - Manoeuvre planning.
- 3.11.1.3. Control includes:
- Object and event response execution.
 - Lateral vehicle motion control.
 - Longitudinal vehicle motion control.
 - Enhancing conspicuity via lighting and signalling.
- 3.11.1.4. The DDT excludes strategic functions.

¹²For 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.

- 3.11.2. “*Strategic function*” means a capability to issue commands, instructions, or guidance for execution by an ADS.¹⁴
- 3.11.3. “*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
- 3.11.4. “*Operational function*” means a capability to control the real-time motion of the vehicle.¹⁶
- 3.12. “*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
- 3.13. “*ADS fallback response*” means an ADS-initiated transition of control or an ADS-controlled procedure to place the vehicle in a minimal risk condition.
- 3.14. “*DDT fallback*” means a response by the user to either perform the DDT or to achieve a minimal risk condition or a response by an ADS to achieve a minimal risk condition **in situations that include:**
 - (1) after the occurrence of one or more DDT performance-relevant system failures, or
 - (2) upon an ODD exit.
- 3.15. “*Fallback user*” means a user expected to perform the DDT pursuant to a transition of control.
- 3.16. “*Minimal Risk Condition (MRC)*” means a stable and stopped state of the vehicle that reduces the risk of a crash.
- 3.17. “*Model*” means a description or representation of a system, entity, phenomenon, or process.
- 3.18. “*Model calibration*” means a process of adjusting numerical or modelling parameters in a model to improve agreement with a referent.
- 3.19. “*Model parameter*” means a numerical value inferred from real-world data and used to characterise a system functionality.
- 3.20. “*Occurrence*” means a safety-relevant event involving an ADS vehicle.

Commented [DS1]: SAE/ISO JWG is considering expanding this definition to include at least crashes, as it now seems to narrowly confined to just two situations.

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.

- 3.21. *“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
- 3.22. *“Critical Occurrence”* means an occurrence during which the ADS is performing the DDT and:
- (a) at least one person suffers an injury that requires medical attention 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.
- 3.23. *“Operational Design Domain (ODD)”* means the operating conditions under which an ADS feature is specifically designed to function.¹⁹
- 3.24. *“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.²⁰
- 3.25. *“Other road user (ORU)”* means an entity in the ADS vehicle environment capable of motion and of coordinated interaction with the ADS vehicle.
- 3.26. *“Priority vehicle”* means a vehicle subject to exemptions, authorizations, and/or right-of-way under traffic laws while performing a specified function.
- 3.27. *“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, including via sensor stimulation and/or the use of dummy devices.
- 3.28. *“Real time”* means the actual time during which a process or event occurs.
- 3.29. *“Road-safety agent”* means a human being engaged in directing traffic, enforcing traffic laws, maintaining/constructing roadways, and/or responding to traffic incidents.

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 Examples include but are not limited to environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.

²⁰ 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.

- 3.30. "Safety case" means a compelling, comprehensible, and valid argument, supported by a body of evidence, documenting that a system is, or will be, adequately safe for a given application in a given environment. structured argument, supported by a body of evidence that provides a compelling, comprehensible, and valid case that a system is or will be adequately safe for a given application in a given environment.²¹
- 3.31. "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.
- 3.32. "Simulation" means the imitation of the operation of a real-world process or system over time.
- 3.33. "Simulation toolchain" means a combination of simulation tools that are used to support the validation of an ADS.
- 3.34. "Test case specification" means the detailed specifications of what must be done by the tester to prepare for the test.
- 3.35. "Test method" means a structured approach to consistently derive knowledge about the ADS by means of executing tests.²²
- 3.36. "Traffic scenario" means a description of one or more real-world driving situations that may occur during a given trip.²³
- 3.36.1. "Nominal scenario" means a traffic scenario representing usual and/or expected objects, object behaviours and/or road conditions.
- 3.36.2. "Critical scenario" means a traffic scenario representing unusual and/or unexpected objects, object behaviours, and/or road conditions.
- 3.36.3. "Failure scenario" means a traffic scenario representing a system failure that compromises the capability of the ADS to perform the entire DDT.
- 3.36.4. "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.²⁴
- 3.36.5. "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.²⁵

Commented [DS2]: OICA/CLEPA has recommended deletion of some of the definition we have been using due to what it considers the subjectivity of "compelling, comprehensible, and valid". I've suggested using NASA's definition, which contains those same words but applies them to the "case" and notes that the argument is "structured." I've cited the NASA source. If those adjectives suffice to define a safety case for aerospace systems they should also suffice in this context.

²¹ [NASA System Safety Handbook, NASA/SP-2014-612 Version 1.0 November 2014, at 16.](#)

²² For example, virtual testing in simulated environments, physical, structured testing in controlled test-facility environments, and real-world on-road conditions.

²³ 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).

²⁴ 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.

²⁵ For example, elaborating the lane element to cover possible lane widths.

Formatted: English (United States)

- 3.36.6. *"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.
- 3.36.7. *"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.
- 3.37. *"Transition of control (TOC)"* means a procedure by which the ADS transfers performance of the DDT to an ADS vehicle user.
- 3.38. *"TOC request"* means an alert issued by an ADS to an ADS vehicle user prompting the user to intervene in performance of the DDT.²⁶
- 3.39. *"TOC response"* means an ADS vehicle user intervention in performance of the DDT pursuant to a TOC request.
- 3.40. *"(ADS) User"* means a human user of an ADS vehicle.
- 3.41. *"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.
- 3.42. *"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.
- 3.43. *"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.
- 3.44. *"Virtual testing"* means the process of testing a system using one or more simulation models.
- 3.45. *"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.
- 3.46. *"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 mechanical components in a way that connects all the I/O of the Electronic Control Units (ECU) before the final system is integrated.
- 3.47. *"Model-In-the-Loop" (MIL)* means high-level-of-abstraction software frameworks running on general-purpose computing systems to

²⁶ The TOC request, depending on the ADS design and reason for initiation of the transition of control, may aim to engage the user in performing the DDT (i.e., to the role of driver manually operating the vehicle) or to achieve an MRC.

- enable quick algorithmic development without involving dedicated hardware.
- 3.48. *“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.
- 3.49. *“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.

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 *chapter/annex*).

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.

However, critical scenarios may present conditions where requirements must be prioritised and exceptions to requirements may be necessary. In these cases, the framework proposes safety models to enable assessment of ADS performance within the limits of the safety model(s). For example, an ADS might execute an evasive manoeuvre to avoid a collision or might not be able to avoid a collision given scenario parameters. The ADS performance can be evaluated against one or more safety models that establish the feasibility of collision avoidance and thresholds for prioritising avoidance over other requirements.

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 (*chapter/annex*). 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 (*chapter/annex*). 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.

These guidelines specifically address one-to-one vehicle relationships of users located inside an ADS vehicle (i.e., driver, fallback user, and passenger). The recommendations for user safety differentiate among these user relationships and therefore, differentiate applications of ADS technologies across vehicle designs.

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. The ADS may transition control back to this user (i.e., fall back upon this 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.

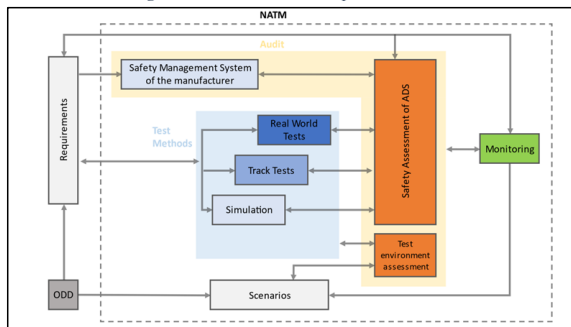
These guidelines propose principles and specifications to ensure the safety of users and their use of ADS vehicles across these relationships. The guidelines recognise that additional relationships may need consideration in the further development of such safety requirements.

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. 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 (*chapter/annex*).

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 (*chapter/annex*).

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 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.

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 (see credibility assessment)

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.

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, may 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 validation of ADS performance under an In-Service Monitoring and Reporting (ISMR) pillar (see Section 8).

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.

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.

DRAFT (October 15, 2023)

Except as indicated by different color text or strikeouts, the text comes directly from FRAV and VMAD documents

5. Audit and Manufacturer’s System Documentation

5.1 Introduction

[An audit of the ADS manufacturer’s safety assessment of the ADS design and safety management system is an] important validation pillar that VMAD has explained in detail. FRAV recommends certain documentation requirements that in many ways correlate directly with the documentation that the audit pillar would require that manufacturers submit to the approval authority. This section fully explains and synthesizes the elements of the audit pillar and the FRAV documentation recommendations.]

Commented [GU3]: Espedito: I suggest not referring to VMAD because this is a stand alone document

Commented [da4R3]: I don't understand. This intro explains how the VMAD and FRAV docs are being integrated on these subjects.

Commented [GU5]: Espedito: I suggest to delete "manufaturer's safety processes" because the SMS already includes the safety processes

Commented [da6R5]: OK. I've done that.

Commented [GU7]: Would it be possible to remove references to VMAD and FRAV? If this combined document is read from an external party they may not be familiar. Maybe reference some of those items that are contained in annexes?

Commented [da8R7]: The intro to the doc explains what FRAV and VMAD are and what they have done.

Commented [GU9]: Espedito: the introduction should also refer to the assessment which is mainly correlated with the FRAV documentation

Commented [da10R9]: OK, I added a reference to safety assessment in the intro.

5.2 **FRAV Documentation Requirements**

[FRAV guidelines recommend that ADS manufactures provide] documentation on several specific points, set out below:

[requirements 4.1 through 4.9 from [GRVA-16-29, Rev. 1](#)] and 4.10 to 4.11 from [FRAV-43-04-rev4](#)]

~~4. ADS Documentation This section concerns the availability and/or provision of information regarding an ADS and its features and/or ADS vehicle. Unless otherwise specified, "documentation" should be understood as agnostic regarding the form or format for substantiation of such information. 4.1.~~

- The manufacturer shall provide written information on the ADS configuration and the intended uses and limitations on the use of its feature(s). [\[See 5.51\]](#)
- The manufacturer shall describe the information and approach to be made available to the public to promote a correct understanding of the intended uses and limitations on the use of the ADS and its feature(s). [\[See 5.57\]](#)
- The manufacturer shall establish terms for the correct use of the ADS and its feature(s). [\[See 5.57\]](#)
- The manufacturer shall provide written information on the roles and responsibilities of the ADS vehicle user(s), including on permissible user activities while the ADS is performing the DDT. [\[See 5.57\]](#)
- The manufacturer shall provide written instructions for the activation and deactivation of the ADS. [\[See 5.57\]](#)
- The manufacturer shall provide written information on ADS responses to ADS vehicle user interventions in the dynamic control of the vehicle. [\[See 5.57\]](#)
- The manufacturer shall provide written descriptions of the transition of control procedures, including ADS notifications and fallback user responses. [\[See 5.57\]](#)
- The manufacturer shall list the potential faults identifiable by the diagnostic system(s) of the ADS. [\[See 5.52 and 5.54\]](#)
- The manufacturer shall establish the ODD conditions and boundaries of each ADS feature in measurable and/or verifiable terms ~~[in accordance with Appendix A]~~. [\[See 5.51 and 5.54\]](#)
- For the ADS users, the ADS shall be supported by documentation and tools to facilitate user understanding of the functionality and operation of the system covering at least: [\[See 5.57\]](#)
 - An operational description of the ADS features, capabilities, and limitations (the information should also refer to specific scenarios and/or ODD).
 - A description of the roles and responsibilities of the driver/user and ADS when an ADS (feature) is active.
 - 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.
- The ADS manufacturer / vehicle manufacturer (as appropriate) shall provide documentation available for audit on: [\[see 5.51 and 5.54\]](#)
 - The details of their user-centred design process.
 - Its intended educational approach for theoretical and practical training.
 - Human-Factors related standards used in the design process.

Commented [GU11]: "Suggested Documentation Requirements" (ie remove reference to FRAV and be more broad)

Commented [da12R11]: Not for now. I'd like to retain all of the references to FRAV and VMAD so that reviewers understand the sources. If we later decide to remove them when we are near completion of the integrated doc, that's the time to do so.

Commented [GU13]: Espedito: If possible, we should combine FRAV documentation requirements with the similar recommendations coming from VMAD. Note: Recommendations in VMAD use "Should".

Commented [da14R13]: The bottom line of this FRAV section notes that all of FRAV's documentation requirements are covered by the audit pillar. Pulling the FRAV wording into the VMAD section would seem unnecessary and would contravene the chairpersons' wishes to retain original text as much as possible.

Commented [da15R13]: Also, the bullets here come directly from the GRAV doc, which uses "shall." If we are changing that to "should" in the more current doc, we can change it here, too.

Commented [GU16]: "ADS manufacturers should provide ..." removal of reference to FRAV and broadening of text

Commented [da17R16]: Again, I'm retaining all of these references until FRAV and VMAD have finished their review.

Commented [pe18]: These are the additional requirements from the September FRAV Document

Additionally [in accordance with Appendix A] has been removed as well

4.10. For the ADS users, the ADS shall be supported by documentation and tools to facilitate user understanding of the functionality and operation of the system covering at least:

- (a) An operational description of the ADS features, capabilities, and limitations (the information should also refer to specific scenarios and/or ODD).
- (b) A description of the roles and responsibilities of the driver/user and ADS when an ADS (feature) is active.
- (c) A description of the permitted transitions of roles and the procedure for those transitions.
- (d) A general overview of non-driving-related activities (NDRA) allowed when an ADS feature is active.

4.11. The ADS manufacturer / vehicle manufacturer (as appropriate) shall provide documentation available for audit on:

- (a) The details of their user-centred design process.
- (b) Its intended educational approach for theoretical and practical training.
- (c) Human-Factors related standards used in the design process.

[The audit pillar, as described below, generally addresses all of the FRAV documentation requirements as part of the safety assessment, either in the portion of the assessment that requires a comprehensive system description or the portion that requires provision of information to users. [Therefore, [FRAV’s] documentation requirements are largely subsumed by the documentation aspects of the audit pillar, which addresses the same subjects in far greater detail but the FRAV requirements are in some cases more detailed than relevant language in the audit pillar.]

[NOTE: The FRAV documentation requirements above in some cases contain more detail than the related VMAD audit pillar contents below. This seems particularly true with regard to issues related to providing information to ADS users. We have attempted to show the relationships between the FRAV and VMAD language by showing in brackets after each FRAV requirement above the portions below of the VMAD audit pillar that is relevant. However, we should consider whether the final integrated document will blend the FRAV documentation requirements into the audit pillar language. Also, in that case, swe should consider whether the FRAV documentation requirements should be simplified into a single requirement that requires all documentation necessary to fulfill the audit pillar.]

5.3 Purpose and Elements of the Audit Pillar

(section IX of [GRVA-16-39](#))

[from paragraphs 58 to 60 of GRVA doc]

The purpose of the audit pillar is to assess/demonstrate that:

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

Therefore, this pillar is composed of two main components: ~~one is~~ the audit of the manufacturer processes established through a safety management system, and the ~~other consists- audit~~ of the safety assessment 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 a “safety-by-design” approach exists and had been applied to mitigate them; and
- (c) The risk assessment and the safety-by-design approach 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 driver, passengers and other road users. Based on the evidence provided by the manufacturer and including the tests,

- Commented [GU19]: "these requirements ..." -
- Commented [da20R19]: No. Maybe after FRAV and VMAD review.
- Commented [GU21]: the
- Commented [da22R21]: Did I omit "the"? If so, yes, it should be added.
- Commented [GU23]: In this case, would it be just a case of coordinating between FRAV/VMAD and removing the extra requirements? Should flag this so it is in one, integrated location
- Commented [da24R23]: Maybe in a subsequent draft after review by FRAV and VMAD
- Commented [GU25]: Espedito. In my opinion, this document should not refer to VMAD and FRAV but it should merge similare contents
- Commented [da26R25]: Same as above.

- Commented [GA27]: A question: wouldn't it be better to introduce the purpose before the previous chapter (FRAV documentation requirements ?)
- Commented [da28R27]: The entire rest of this section deals with the audit pillar from VMAD. Putting this before the small portion on FRAV documentation would seem confusing since this introduces all that comes after it.
- Commented [GU29]: Espedito: VMAD uses the word Audit for the SMS (i.e., for the processes), while Assessment is used for the product (i.e., investigation of the safety by design)
- Commented [da30R29]: Not sure I understand. Are you suggesting that we delete "audit of the" here? The question is whether the authority is auditing the manufacturer's safety assessment of the ADS design or is conducting its own safety assessment of the design.
- Formatted: Font colour: Accent 5

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.

~~A. General guidance on the audit of the manufacturer safety management system~~

5.4 Safety Management System

[from paragraphs 61 to 75 and paragraph 80 of the GRVA doc]

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.

~~The documentation provided by a manufacturer should demonstrate that their safety management system has effective processes, methodologies and tools. It should be up to date and also clear that it is being used within the organization. It should show how the organization intends to manage safety and to demonstrate continued compliance throughout the product lifecycle (design, development, production, operation and decommissioning). [repetitious of the preceding paragraph]~~

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 ~~leveraged upon~~ 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~~ ~~helping~~ to ensure that there are no unforeseen consequences.
- (c) Technical component using appropriate tools and equipment.

An adequate SMS will incorporate, ~~monitor and improve~~ all three factors to monitor and improve safety and help to control the identified risks. The SMS evaluation is based on automotive (or other industry) engineering standards, guidebooks, and best practice documents relevant to safety.

5.4.1 Safety Policy

It is recommended that a safety policy ~~is~~ be established 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.

~~Examples of~~ 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, ~~but from a safety perspective~~)

Commented [GU31]: Espedito: not sure why only monitored?

Commented [da32R31]: What would be a better word? "Leveraged upon" was the original and that didn't make sense.

Formatted: Indent: Left: 0.5"

(b) Organisation safety objectives and the process for creating safety performance indicators used in the safety case [Note use of “safety case”; intended to refer to “safety concept”? should safety case be used instead and defined?]

(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, but from safety perspective) (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.

5.4.2 Risk Management

It is recommended to establish a Safety risk management process to identify and assess the risks associated to the three SMS factors described in the point 63) 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 Management:

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

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

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

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

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

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

5.4.3 Design and Development Process

It is recommended that the design and development process is well established and documented. It should include risk management, requirements management, requirements' implementation,

Formatted: Font: Bold, Font colour: Accent 5

Submitted by the expert from SAE

FRAV-VMAD-01-09
1st FRAV/VMAD session
29-30 November 2023

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 with InService Safety
 - (iv) Management of Human Factors (e.g. Human centered design processes)
- (c) Design and change management, including but not limited;
 - (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.

The following are examples of processes and activities that should be documented to assure independent design audit and assessment:

- (a) assurance that all practices and procedures applied during the vehicle\system development are followed;

- (b) assurance that there is an independent check of compliance with the applicable requirements and regulations is performed. (i.e., not from person creating the compliance data);
- (c) process to assure the continuing evaluation of the Safety Management System to ensure that it remains effective.

5.4.4 Production and Deployment Process

It is recommended that the Production process is well established and documented. 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 audit are carried out to ensure that the processes established for the Safety Management System are implemented consistently. (UN R157, para. 3.5.5, ISO 26262-2, para. 6.4.11)

Suggestion; add recommendation for a robust process to ensure software updates are properly validated and distributed and downloading is confirmed

It is recommended that a manufacturer puts 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 their vehicles (e.g. contracted suppliers, service providers or manufacturers’ sub-organizations) to ensure that their approach to safety management related to the committed activities complies 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 postproduction
- (e) Processes for distributed safety activities

Formatted: Font: Bold, Font colour: Accent 5

Commented [GU33]: Espedito: I think the validation is covered in the development part

Commented [da34R33]: I don't see this level of detail anywhere else other than general references to change management. If I were still a regulator I would want to know the manufacturer had this process in its SMS.

Commented [er35R33]: Espedito: I agree. we could introduce more a precise text in the 5.4.3 (b)

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.

5.4.5 Safety throughout the Useful Life of the ADS and its Features

This section addresses the safe use of an ADS and its feature(s) during the useful life of the ADS vehicle. It is recommended that the Safety Management System ensure that:

- (a) The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons.
- (b) The ADS shall be designed to protect against unauthorized access to and modification of the ADS functions.
- (c) The measures ensuring protection from unauthorized access should be provided in alignment with engineering best practices.
- (d) ADS safety shall be ensured in the event of discontinued production, support, and/or maintenance.

Commented [DS36]: This subsection covers FRAV requirements 5.14 through 5.14.4. The SMS seemed the logical place to insert these because the SMS is intended to address risks throughout the lifecycle of the ADS all the way to decommissioning.

Commented [DS37R36]:

Formatted: Font: Bold

Formatted: List Paragraph, Numbered + Level: 1 + Numbering Style: a, b, c, ... + Start at: 1 + Alignment: Left + Aligned at: 0.25" + Indent at: 0.5"

5.4.6 Link with the in-service monitoring/reporting pillar

[from paragraphs 76-79 of the GRVA doc]

It is recommended that a manufacturer has 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. [Here again, "safety case" is used. Does it refer to "safety concept"? Should one term or the other be used throughout?] 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 learnings 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?

Formatted: Font: Bold

Formatted: Level 3, Indent: First line: 0.5"

5.5 Safety Assessment of the ADS

[from paragraphs ~~81~~ 121 of GRVA doc]

Commented [GU38]: paragraphs 80-81 are skipped, not sure if relevant to the doc, just noting

Commented [da39R38]: 80 is addressed in section 5.4; see the very top of that section in brackets. It was out of order in the VMAD doc. Not sure why I dropped 81, which I have now inserted here. Thanks.

The purpose of the audit of the safety by design concept of the ADS is to demonstrate that hazards and risks relevant to the ADS have been identified by the manufacturer and a consistent safety-by-design concept has been implemented to mitigate these risks. In addition, it should demonstrate that the risk assessment and the design have been validated by the manufacturer through testing. This should demonstrate that, before the vehicle is placed on the market, it meets the relevant safety requirements. This means it is free of unreasonable safety risks to the broader transport ecosystem and in particular to the driver, passengers and other road users.

5.5.1 ADS General Description

It is recommended that a description should be provided, which gives a simple explanation of the operational characteristics of the ADS and ADS features:

- (a) Operational Design Domain (Road Speed limits, road type, country, Environment, Road conditions, etc.);
- (b) Basic performance (e.g. Object and Event Detection and Response (OEDR), etc.)
- (c) Interaction with other road users
- (d) Main conditions for Minimum Risk Manoeuvres.
- (e) Interaction with the driver (if relevant)
- (f) Supervision centre (if relevant)
- (g) The method of activating, overriding or deactivating the ADS by any or all of the driver (where relevant), the human supervision centre (where relevant), passengers (where relevant) or other road users (where relevant).

5.5.2 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

Formatted: Font: Bold

5.5.3 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.

Formatted: Font: Bold

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 ~~Normal and Emergency Conditions~~nominal, critical, and failure situations, acceptance criteria and the demonstration of compliance with those criteria. (ii) List of applied regulations, codes, and standards

5.5.4 Safety Concept [Case?] and Validation of the Safety Concept [Case?] by the Manufacturer

The manufacturer should provide a statement which affirms that the ADS is free from unreasonable risks for the driver (if applicable), passengers and other road users. 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 manufacturer 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:

Formatted: Font: Bold
Formatted: Font: Bold
Formatted: Font: Bold

- (a) Fall-back (or fail safe) operation using a partial system.
- (b) Redundancy using separate systems.
- (c) 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. initiation of a minimum risk manoeuvre 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 driver (if applicable), passengers 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 approach(es), 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 ~~approach~~ 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 for the driver (if applicable), passengers 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 (if applicable), passenger 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 documentation should have arguments supporting the safety concept [\[case?\]](#) that is understandable and logical and cover all the different functions of the ADS. The documentation should also demonstrate that validation plans 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 for the driver (if applicable); vehicle occupants and other road users in the operational design domain. This could be achieved through:

- (a) ~~An~~ 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 for the driver (if applicable), vehicle occupants, 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 for the driver (if applicable), passengers and other road users compared to a manually driven vehicles [within the ODD](#) for each of the safety relevant scenarios.

The documentation should allow the relevant authority to test and verify the safety concept [\[case?\]](#). It is recommended that the documentation itemizes the parameters being monitored on the vehicle and should set out, for each failure condition of the type defined in accordance with 84.6. of this annex [\[need to find this reference and insert it here\]](#), the warning signal to be given to the driver (if applicable) /vehicle occupants/other road users and/or to service/technical inspection personnel. This documentation should also describe the measures in place to ensure the ADS is free from unreasonable risks for the driver (if applicable), vehicle occupants, 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.

5.5.5 Data Storage System

Formatted: Font: Bold

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.

5.5.6 Cybersecurity and Software Update Management

Formatted: Font: Bold

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.

5.5.7 Information Provision to Users

Formatted: Font: Bold

It is recommended that the documentation includes:

- (a) The distinction between maintenance and an operational manual,
- (b) A safety precaution manual that includes safety-relevant information for the user,
- (c) A briefing on the user's role and how it might change during the vehicle operation, including when the user is responsible for the safety and control of the vehicle,
- (d) Information on how to use the ADS, o Transition of Control (ToC), where applicable o Take over o ADS activation o ODD o Role of the user after regaining control
- (e) System Description and functional limitations
- (f) Operational description (e.g., implications of switching off the ADS)
- (g) Nominal Operations
- (h) Emergency Operations
- (i) Role of the user within the ADS' ODD 21
- (j) Information related to the HMI's indications o Visual tell-tales, icons o Auditory signs o Haptic signs
- (k) Means to deactivate the automated driving mode (take-over)
- (l) Safety measures to be taken in the event of malfunctioning of the ADS
- (m) Extent, timing and frequency of maintenance operations
- (n) Means to enable a periodical technical inspection
- (o) Documents and templates for maintenance, repair and periodical technical inspection
- (p) Precautionary statements in the sense of compliance with limit values for the technical functions
- (q) Data protection and data security functionalities
- (r) List of system fault codes

~~(j) Safety management system—The manufacturer should have a valid Safety Management System relevant to the specific ADS and should inform the authority of any change that will affect the Safety Management System for the specific ADS.~~

5.5.8 Type of Documentation to be Provided

Formatted: Font: Bold

Documentation should be brief yet provide evidence that the design and development has had the benefit of expertise from all the ADS fields which are involved.

- (a) A documentation package which gives access to the basic design of the ADS and how it is linked to other vehicle systems or by which it directly controls output variables.
- (b) Documentation explaining the function(s) of the ADS, including the control strategies and the safety concept.
- (c) For periodic technical inspections, the documentation should describe how the current operational status of the ADS can be checked
- (d) Documentation about how the software version(s) and the failure warning signal status can be readable in a standardized way via the use of an electronic communication interface (i.e., using a standard interface, such as the OBD port).

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 driver (if applicable), passengers and other road users within the declared ODD;
- (b) Is capable of recognizing its boundaries;
- (c) Respects any performance requirements specified by FRAV;
- (d) 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 brief information on all the items.
- (b) The formal documentation package annexed to the information document, which should be supplied to the Authority for the purpose of conducting the safety assessment.
- (c) Additional confidential material and analysis data (intellectual property) which 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.

6. Requirements for ADS Performance of the DDT

6.1. Introduction

GRVA 17-33e 5.1 – 5.3

The following subsections recommend criteria for validating the safety of ADS and/or ADS vehicles. [Annex 4 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 drivers and other road users. Subsections 6.3-6.6 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.

6.2 Scenario generation and behavioural competencies

GRVA 17-33e 5.4 – 5.9

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 X](#) 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 Subsections 6.3-6.6. 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.

6.3 ADS Performance of the DDT under Nominal Traffic Scenarios

GRVA 17-33e 5.10 – 5.10.18 not including 5.10.5 – 5.10.7 as these are in the ODD boundary section and 5.10.16 as it is in the MRC section.

Commented [PE40]: This is the FRAV annex reference which will be included as an annex

Commented [PE41]: To be discussed with FRAV: Does this refer to "coverage" or "correctly reflect"

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.

- 6.3.1 The ADS shall be capable of performing the entire Dynamic Driving Task (DDT) within the ODD of its feature(s).
- 6.3.1.1 The ADS shall operate the vehicle at safe speeds.
- 6.3.1.2 The ADS shall maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle.
- 6.3.1.3 The ADS shall adapt its driving behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic).
- 6.3.1.4 The ADS shall adapt its driving behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).
- 6.3.2 The ADS shall detect and respond to objects and events relevant to its performance of the DDT.
- 6.3.3 The ADS shall detect and respond to priority vehicles in service in accordance with the relevant traffic law(s).
- 6.3.4 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.
- 6.3.5 Under nominal traffic scenarios, the driving behaviour of the ADS shall not cause a collision.
- 6.3.6 The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation.
- 6.3.7 The ADS shall interact safely with other road users.
- 6.3.8 The ADS shall avoid collisions with safety-relevant objects where possible.
- 6.3.9 The ADS shall signal intended changes of direction.
- 6.3.10 The ADS shall signal its operational status in accordance with national rules.
- 6.3.11 Pursuant to a passenger request under para. 7.4.1., the ADS shall bring the vehicle to a safe stop.

6.4 ADS Performance of the DDT under Critical Traffic Scenarios

GRVA 17-33e 5.11 – 5.11.4.2

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.

- 6.4.1 The requirements of section 6.3. shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.
- 6.4.2 In the event of a collision, the ADS shall stop the vehicle in an MRC and/or in accordance with applicable traffic laws.²⁷
 - 6.4.2.1 The ADS shall not resume travel until the safe operational state of the ADS vehicle has been verified.
 - 6.4.2.2 The ADS may resume the trip where permissible under the applicable traffic rule(s) and other safety considerations.

6.5 ADS Performance of the DDT under Failure Scenarios

GRVA 17-33e 5.12 – 5.12.3

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.

- 6.5.1 The requirements of section 6.3 shall continue to apply during failure scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.
- 6.5.2 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 45](#).
 - 6.5.2.1 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.
 - 6.5.2.2 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.
 - 6.5.2.3 The ADS shall adapt its performance of the DDT in accordance with the severity of the fault to ensure road safety.

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

6.5.2.4 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.

6.5.2.4.1 The limited operation of the ADS should comply to the normally applicable safety requirements.

6.5.3 Remote termination of individual or multiple ADS or feature(s) by the manufacturer and/or service operator shall be possible when requested by Authorities.

6.5.3.1 Remote termination for an ADS performing the DDT shall be capable of triggering an ADS fallback response.

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

6.6 ADS Performance of the DDT at ODD Boundaries

GRVA 17-33e 5.10.5 – 5.10.7

6.6.1 The ADS shall recognise the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under [paragraph 4.9.5.2.](#)

6.6.2 The ADS shall be able to determine when the conditions are met for activation of each feature.

6.6.2.1 The ADS shall prevent activation of a feature unless the ODD conditions of the feature are met.

6.6.2.2 The ADS shall execute a fallback response when one or more ODD conditions of the feature in use are no longer met.

6.6.3 The ADS shall be able to anticipate foreseeable exits from the ODD of each feature.

Commented [PE42]: Change to appropriate reference in new document

6.7 [Minimum Risk Condition Requirements](#)

GRVA 17-33e 5.10.16, 5.12.4- 5.12.4.2.1.

6.7.1 The ADS shall signal its intention to place the vehicle in an MRC.

6.7.2 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.

6.7.2.1 In the absence of a fallback-ready user, the ADS shall fall back directly to an MRC.

6.7.2.2 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.

Commented [PE43]: New section for MRC requirements as these will not always be failure scenarios, also prevents 5.10.16 being a lone MRC requirement in the nominal section.

- 6.7.2.2.1 Upon completion of a fallback to an MRC, a user may be permitted to assume control of the vehicle.

6.8 Multi pillar approach

GRVA-16-39e (192 – 199) Not including 196 and 197e

- 6.8.1 As previously noted, the multi-pillar approach recognizes that the safety of an ADS cannot be reliably assessed/validated using only one of the pillars. Each of the aforementioned testing methodologies possesses its own strengths and limitations, such as differing levels of environmental control, environmental fidelity, and scalability, which should be considered accordingly.
- 6.8.2 It is important to note that a single assessment or test method may not be enough to assess whether the ADS is able to cope with all occurrences that may be encountered in the real world.
- 6.8.3 For instance, while real-world testing provides a high degree of environmental fidelity, a scenario-based testing methodology using only real-world testing could be costly, time-consuming, difficult to replicate, and pose safety risks. Consequently, track testing may be more appropriate methods to run higher risk scenarios without exposing other road users to potential harm. Further, test scenarios can also be more easily replicated in a closed track environment compared to the real-world. That said, test track scenarios can be potentially difficult to develop and implement, especially if there are numerous or complex scenarios, involving a variety of scenario elements.
- 6.8.4 ~~Consideration should be given to the fact that~~ Simulation/virtual testing, by contrast, can be more scalable, cost-effective, safe, and efficient compared to track or real-world testing, allowing a test administrator to safely and easily create a wide range of scenarios, including complex scenarios, where a diverse range of elements are examined. However, simulations may be of a lower fidelity than the other methodologies. Simulation software may also vary in quality and tests could be difficult to replicate across different simulation platforms.
- 6.8.5 In addition to the respective strengths and weakness of each test pillar, the nature of the safety requirements being assessed will also inform what pillars are used:
- 6.8.5.1 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).
- 6.8.5.2 Track tests may be best 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 (e.g., for HMI or fall back, critical traffic situations).
- 6.8.5.3 Real-world testing may be more suitable where the scenario may not be precisely represented virtually or on a test track (e.g., interactions with other road-users and perception quality may be assessed through real world evaluation).

Commented [PE44]: Germany: This seems like a requirement and should be removed

6.8.6 Given these considerations, it should be noted that the sequence and composition of test pillars used to assess each safety requirement may vary. While some testing might follow a logical sequence from simulation to track and then to real world testing, there may be deviations depending on the specific safety requirement being tested.

6.8.7 It is therefore necessary for the NATM pillars to be used together to produce an efficient, comprehensive, and cohesive process, considering their strengths and limitations. The methods should complement one another, avoiding excessive overlaps or redundancy to ensure an efficient and effective validation strategy.

6.9 Considerations for specific requirements

[See Annex \[\] for the matrix giving a mapping of each requirement to the relevant validation pillars.](#)

6.9.1 Application of the validation pillars to nominal traffic scenario requirements

New text

[Most of the requirements of section 6.3 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.](#)

6.9.2 Application of the validation pillars to critical traffic scenario requirements

New text

[The requirements of section 6.4 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.](#)

6.9.3 Application of the validation pillars to failure scenario requirements

New text

[The requirements of section 6.5 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.](#)

6.9.4 Application of the validation pillars to ODD boundary requirements

New text (part of GRVA16-39e 45a)

[The requirements of section 6.6 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.](#)

6.9.5 Application of the validation pillars to Minimum Risk Condition requirements

New text

The requirements of section 6.7 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 MRC in the real world amongst naïve traffic could be dangerous depending on the design of the MRC. Testing MRC may then be safer and more applicable on test tracks and via virtual testing.

7. Requirements for safe interactions between Users and ADS.

New text Introduction and GRVA 17-33e 15.3-15.3.4.5 for requirements

7.1. Introduction

7.1.1 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.

7.1.2

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.

7.2. General recommendations

- 7.2.1. The ADS shall signal the presence of any failure that limits the operation of an available feature.
- 7.2.2. The ADS shall signal its intention to place the vehicle in an MRC to the ADS user(s).
- 7.2.3. An ADS that controls the operation of doors shall provide an emergency override to the user.
- 7.2.4. 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.

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

7.3.1. General recommendations.

- 7.3.1.1. 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.
- 7.3.1.2. The ADS shall be designed to prevent misuse and errors in operation by the user.
 - 7.3.1.2.1. The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions.²⁸
 - 7.3.1.2.2. 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.
 - (c) Any failure of the ADS that limits the operation of an available feature.
 - 7.3.1.2.3. The ADS shall indicate the availability of a feature for activation.

7.3.2. Recommendations on the ADS feature activation.

- 7.3.2.1. The ADS shall ensure a safe ADS feature activation.

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) 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.

7.3.3. Recommendations on ADS feature deactivation to manual driving.

7.3.3.1.1 The ADS shall have a monitoring system to support safe and appropriate engagement of the user as necessary.

7.3.3.1.2 At the completion of the deactivation process, lateral and longitudinal control shall be returned to the driver without any continuous control assistance active.²⁹

7.3.4 ADS features that allow a user-initiated system deactivation to manual driving.³⁰

7.3.4.1. 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.
- (f) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.

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

³⁰ An ADS that may “suggest” the user takes control (e.g., when approaching the end of its ODD) and that is not designed to require a fallback user to continuously be ready to take control should be considered as a user-initiated system deactivation with regard to the requirements of this section.

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

7.3.5. ADS features that have a system-initiated deactivation to manual driving.

7.3.5.1. 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 an MRM 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.

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

- 7.4.1. The ADS shall provide the passenger(s) with means to request to stop the vehicle.
- 7.4.2. The ADS vehicle shall provide safety-related information to the passengers.
- 7.4.3. The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated.
- 7.4.4. The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress).
- 7.4.5. 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.

7.5 Testing User interaction requirements

See [Annex 4 for the matrix giving a mapping of each user requirement to the relevant validation pillars.](#)

7.5.1. [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.](#)

7.5.2 **VMAD 42 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.

7.5.3 **VMAD 197 c (c)** ~~Track tests may be well best 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 (e.g., for HMI related tests or those testing the ADS fall back response-critical traffic situations).~~

7.5.4 **VMAD 137** ~~For example, U~~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.

7.5.5 [As with the DDT requirements user requirements in failure scenarios such as 7.2.1, and 7.3.1.2.2 c require 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 therefore safer and more applicable on test tracks and via virtual testing.

7.5.6 Requirements 7.2.2, 7.2.3., 7.3.5.1. c.iii. and 7.3.5.1. e., may lead 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 MRC in the real world amongst naïve traffic could be dangerous depending on the design of the MRC. Testing MRC may then be safer and more applicable on test tracks and via virtual testing.

7.5.5 Systems that rely on the presence of a fallback user must fulfill 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 putting naïve traffic participants at risk should the ADS not meet the requirement.

7.5.6 Virtual testing covers both traffic simulation and vehicle simulators, for most requirements one of those will cover the requirement, however some cases such as 7.3.5.1 d require assessment of both the ADS and a human driver which may be challenging on a simulator test.

Colour Scheme Description

| | |
|---|--|
|  | Copy and paste from the reference (No modification) |
|  | Adaptation of the text from the reference (NO change of the meaning) |
|  | New text (to clarify some concepts) |

Notes for the readers

The following colour scheme is applied in this document:

The following documents are used as reference:

Submitted by the expert from SAE

FRAV-VMAD-01-09
1st FRAV/VMAD session
29-30 November 2023

- GRVA-16-39e, June 2023 - New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS)
- GRVA 17-33e, September 2023 - Guidelines for Regulatory Requirements and Verifiable Criteria for ADS Safety Validation

The relevant Annexes of the section 8 are included at the end of this document for readability purpose and to facilitate the crosscheck.

8. In Service Monitoring and Reporting

8.1. Introduction

- 8.1.1. In-Service Monitoring and Reporting (ISMR) is a validation methodology which is part of the multi pillar approach [GRVA-16-39e point 6]. It addresses the in-service safety of automated vehicles after market introduction [GRVA-16-39e point 6 & 122].
- 8.1.2. 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 [New, based on points 122, 124, 126, 127].
- 8.1.3. In practice, the application of the other pillars of the NATM guidelines³¹ 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 [GRVA-16-39e point 122].
- 8.1.4. 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 [GRVA-16-39e point 122].
- 8.1.5. 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 [GRVA-16-39e point 13.f and 123].
- 8.1.6. 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 [GRVA-16-39e point 131].
- 8.1.7. The ADS' safety performance remains the responsibility of the manufacturer throughout its lifetime [GRVA-16-39e point 132].
- 8.1.8. 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 [GRVA-16-39e point 133].
- 8.1.9. 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 [GRVA-16-39e point 126].
- 8.1.10. 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. [GRVA-16-39e point 130].

1.

8.2. Objectives

- 8.2.1. 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 [GRVA-16-39e point 134].
- 8.2.2. The ISMR aims to fulfil three main objectives:
 - 8.2.2.1. Identify safety risks related to ADS performance that need to be addressed, including instances of non-compliance with ADS safety requirements (objective 1);

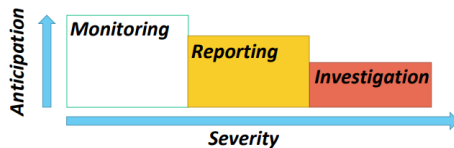
³¹ GRVA-16-39e, June 2023 - New Assessment/Test Method for Automated Driving (NATM) Guidelines for Validating Automated Driving System (ADS)

- 8.2.2.2. Support the development of the Scenario Catalogue through capturing information when the ADS does not perform safely in unanticipated situations (objective 2);
- 8.2.2.3. Share information and recommendations to promote continuous improvement of ADS safety performance (objective 3) [GRVA-16-39e point 135].
- 8.2.3. 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 [GRVA-16-39e point 126 and 136].
- 8.2.4. 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 [GRVA-16-39e point 136].
- 8.2.5. 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 [GRVA-16-39e point 136].
- 8.2.6. Unanticipated situations, risks and hazards might be identified during real-world ADS operation, and this information could be used to develop new scenarios for the common scenario catalogue [GRVA-16-39e point 138].
- 8.2.7. 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 [GRVA-16-39e point 139].
- 8.2.8. However, the ISMR has a more extensive application [New]. 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 [GRVA-16-39e point 137].
- 8.2.9. 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 [New] [GRVA-16-39e point 140].

2.
3.
4.

8.3. Monitoring, Reporting and Investigation

- 8.3.1. Monitoring refers to the overall data collection and analysis conducted by the manufacturers with aim at extracting safety related information from data [GRVA-16-39e point 129]. 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. [New]
- 8.3.2. 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 [GRVA-16-39e point 129]. The reporting constitutes an event-based data collection methodology that is triggered by the happening of the set of occurrences [New].
- 8.3.3. It is expected that the ISMR will be complemented by safety investigations of (at least) critical occurrences conducted by an independent body [GRVA-16-39e point 129].



5.

8.4. ISMR Processes

- 8.4.1. 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 [New].
- 8.4.2. 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 [GRVA-16-39e point 76-78].
- 8.4.3. The Manufacturer should define appropriate:
- 8.4.3.1. Key Performance Indicators (KPIs) to measure the effectiveness of ISMR activities for the ADS operations [GRVA-16-39e point 149].
- 8.4.4. 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 [GRVA-16-39e point 125].

6.

8.5. ISMR Implementation

8.5.1. In Service Monitoring

- 8.5.1.1. 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) [GRVA-16-39e point 141].
- 8.5.1.2. The monitoring program should include a data acquisition strategy, data retention strategy, data access, security and protection policy [GRVA-16-39e point 142].
- 8.5.1.3. The data acquisition strategy ensure a representative collection of data to monitor the ADS in service performance [GRVA-16-39e point 143].
- 8.5.1.4. 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) [GRVA-16-39e point 144].
- 8.5.1.5. 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 [GRVA-16-39e point 145].
- 8.5.1.6. The data monitoring program should allow the manufacture and (where applicable) the fleet operator to:
- 8.5.1.6.1. identify areas of operational risk and quantify current safety margins (e.g. in service safety performance monitoring),
 - 8.5.1.6.2. identify when the ADS prevents incidents/accidents (e.g. MRM, EM),
 - 8.5.1.6.3. identify and quantify operational risks by collecting data to characterize and analyse occurrences,
 - 8.5.1.6.4. use metrics and thresholds to assess safety risks and discover trends that suggest the emergence of unacceptable risks if that trend continues,
 - 8.5.1.6.5. put in place procedures for remedial action when an unacceptable risk is discovered or predicted by trends,
 - 8.5.1.6.6. confirm the in-service safety level and effectiveness of any remedial action [GRVA-16-39e point 146].

- 8.5.1.7. 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 **[GRVA-16-39e point 147]**.
- 8.5.1.8. The analysis techniques should comprise the following:
 - 8.5.1.8.1. 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)
 - 8.5.1.8.2. 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.)
 - 8.5.1.8.3. Occurrence analysis: recorded data should be able to characterize and investigate all the occurrences listed in the annex IV.
 - 8.5.1.8.4. 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) **[GRVA-16-39e point 148]**.
- 8.5.1.9. 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) **[GRVA-16-39e point 149]**.
- 8.5.1.10. Section 8.5.2 describes the relationship between ADS requirements and ISMR activities through a cross reference matrix (reported in the Annex II) that specifies which requirements are suitable for monitoring [New].

7.
8.

a) Vehicle data collection

- 8.5.1.11. 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 **[GRVA-16-39e point 150]**.

b) Other manufacturer-accessible sources of data indicative of ADS performance

- 8.5.1.12. Manufacturers may be expected to collect data relevant to typical operations such as dealer reports, customer reports, etc **[GRVA-16-39e point 150]**.

8.5.2. Monitoring of Performance

- 8.5.2.1. The monitoring of the ADS performance is intended:
 - 8.5.2.1.1. to provide evidence of in-service safety performance of the ADS
 - 8.5.2.1.2. to identify a drift or deviation from the demonstrated performance including the ones that end in an occurrence [New].
- 8.5.2.2. Following the results obtained from the monitoring, the Manufacturer should evaluate:
 - 8.5.2.2.1. is service safety performance

- 8.5.2.2.2. the adequacy of the metrics and thresholds
- 8.5.2.2.3. any mitigation actions. [New].
- 8.5.2.3. Annex 2 contains the matrix which links the ADS requirements to ISMR activities. [New].

8.5.3. In Service Reporting

8.5.3.1. The main purpose of occurrence reporting is to identify possible improvement for the ADS safety performance, and not to attribute blame or liability *[GRVA-16-39e point 152]*.

a) Recommended reporting by the manufacturer

8.5.3.2. The manufacturer should report, as required by the Authority, in accordance with this section and the section 8.5.4 and 8.5.5. It is expected that two types of reports on the in-service safety performance will be produced. These are short-term and periodic *[GRVA-16-39e point 153]*.

8.5.3.3. 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:

8.5.3.3.1. indications of failure to meet safety requirements

8.5.3.3.2. critical occurrence where the ADS was involved known to the ADS manufacturer or OEM

8.5.3.3.3. other safety-relevant performance issues *[GRVA-16-39e point 154]*.

8.5.3.4. 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 *[GRVA-16-39e point 156]*.

8.5.3.5. The manufacturer should also undertake periodic reporting of performance metrics and occurrences to the safety authority *[GRVA-16-39e point 157]*.

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

8.5.3.6.1. no inconsistencies have been detected compared to the ADS safety performance declared prior to market introduction;

8.5.3.6.2. the ADS fulfils the performance requirements and as evaluated in the test methods;

8.5.3.6.3. any newly discovered significant ADS safety performance issues that pose an unreasonable risk to safety have been adequately addressed and how this was achieved *[GRVA-16-39e point 158]*

8.5.3.7. Section 8.5.4 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 *[GRVA-16-39e point 159]*.

8.5.3.8. 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-*[GRVA-16-39e point 161]*.

8.5.3.9. Where feasible, a harmonized approach to the reporting should be developed by contracting parties, and their relevant domestic authorities *[GRVA-16-39e point 162]*.

8.5.3.10. 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 *[GRVA-16-39e point 163]*.

8.5.3.11. 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 *[GRVA-16-39e point 164]*.

b) Reporting from other sources

- 8.5.3.12. 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 [GRVA-16-39e point 165].
- 8.5.3.13. It is recommended that CPs 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 [GRVA-16-39e point 166].

9.

8.5.4. Occurrence reporting

- 8.5.4.1. The short term and periodic reports should be made available, as required by the Authority, in two parts:
 - 8.5.4.1.1. A report (according to Annex III), that contains a summary and the information relevant to the requirements for reporting,
 - 8.5.4.1.2. The data underpinning the report, exchanged with the authority by means of an agreed data exchange file [GRVA-16-39e point 160].
- 8.5.4.2. Short term reporting is expected to be submitted for each critical occurrence [GRVA-16-39e Annex IV].
- 8.5.4.3. 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 [GRVA-16-39e point 155].
- 8.5.4.4. 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 [GRVA-16-39e Annex IV].
- 8.5.4.5. The reporting scheme applies to automated vehicles features of an ADS which was active, at least, 30 seconds before the critical occurrence [GRVA-16-39e Annex IV].
- 8.5.4.6. 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) [GRVA-16-39e Annex IV].
- 8.5.4.7. 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
- 10. 8.5.4.8. 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. [GRVA-16-39e Annex IV].

| Occurrence | Short-term reporting [1 Month] | Periodic Reporting [1 Year] |
|---|-----------------------------------|-----------------------------|
| 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 | | X |
| 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 |

8.5.5. Tools for reporting

- 8.5.5.1. The reporting templates aim at assuring the harmonization of the information to be reported and facilitating the information sharing. *[GRVA-16-39e Annex IV]*.
- 8.5.5.2. The reporting templates aims at ensuring that a conannexsistent 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. *[GRVA-16-39e Annex IV]*.
- 8.5.5.3. 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). *[GRVA-16-39e Annex IV]*.
- 8.5.5.4. The short term template (Annex 3) 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 the Section 8.5.4 *[GRVA-16-39e Annex IV]*.
- 8.5.5.5. In particular, the short-term reporting provisions shall contribute to identify:
- Safety-relevant occurrences caused by an ADS.
 - Traffic situations unforeseen in the original validation that resulted in ADS behaviors inconsistent with the expected behavioral competencies.
 - ADS noncompliance with the ADS safety requirements.
 - Safety concerns in need of remedy. *[GRVA-16-39e Annex IV]*.
- 8.5.5.6. It shall also be noticed that information reported in the short term template will remain confidential *[GRVA-16-39e Annex IV]*.
- 8.5.5.7. The periodic reporting template (Annex 3) 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” in the Section 8.5.4. *[GRVA-16-39e Annex IV]*.

Submitted by the expert from SAE

FRAV-VMAD-01-09
1st FRAV/VMAD session
29-30 November 2023

Annex 1 - Additional recommendations for an effective monitoring

11.

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 [GRVA-16-39e point 167].

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 [GRVA-16-39e point 168].

Data quality and consistency should be ensured both at national and international level by establishing checking processes [GRVA-16-39e point 169].

a) National level

12. 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 [GRVA-16-39e point 170].
- 13.
14. 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 [GRVA-16-39e point 171].
- 15.
16. 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 [GRVA-16-39e point 172].
- 17.
18. Safety authorities should transfer safety recommendations and annual reports to the Common Central Repository [GRVA-16-39e point 173].

b) International level

- 19.
20. WP29 provides a suitable international context for exchanges between Contracting Parties and for defining the guiding principles on the ISMR framework implementation [GRVA-16-39e point 173].
- 21.
22. 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 [GRVA-16-39e point 174].
- 23.
24. 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 [GRVA-16-39e point 175].

Occurrences Investigations

- 25.
26. 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 *[GRVA-16-39e point 177]*.
- 27.
28. 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 *[GRVA-16-39e point 178]*.
- 29.
30. 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 *[GRVA-16-39e point 179]*.
- 31.
32. 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 *[GRVA-16-39e point 180]*.

Exchange of Information

- 33.
34. 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 *[GRVA-16-39e point 181]*.
- 35.
36. Safety Authorities should participate regularly in the exchange and analysis of information contained in the Common Central Repository *[GRVA-16-39e point 182]*.
- 37.
38. 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 *[GRVA-16-39e point 183]*.
- 39.
40. The exchange of relevant information among involved Contracting Parties / Authorities should be required in case of accidents/incidents investigations *[GRVA-16-39e point 184]*.
- 41.
42. 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 *[GRVA-16-39e point 185]*.

Protection of information

- 43.
44. 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 *[GRVA-16-39e point 186]*.
- 45.
46. 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. *[GRVA-16-39e point 187]*
- 47.
48. 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

Submitted by the expert from SAE

FRAV-VMAD-01-09
1st FRAV/VMAD session
29-30 November 2023

attention only because they have been reported under the ISMR occurrence-reporting scheme, except in cases of gross negligence[*GRVA-16-39e point 188*].

49.

50. 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[*GRVA-16-39e point 189*].

51.

Annex 2 – ISMR Matrix

The matrix indicates which requirements are suitable for ISMR activities [New]

The matrix is aimed at providing guidelines for manufacturer and authorities in regard to the monitoring of ADS operations [New].

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.

| Requirement | | Pillar | | |
|---|---|------------|--|---|
| Section | Text | Monitoring | Comments | General note |
| ADS Performance of the DDT under Nominal Traffic Scenarios | | | | |
| 6.3.1.1 | 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 | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 6.3.1.2 | 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) | |
| 6.3.1.3 | 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) | |
| 6.3.1.4 | 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) | |

| Requirement | | Pillar | | |
|-------------|--|------------|---|---|
| Section | Text | Monitoring | Comments | General note |
| 6.3.2 | 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) | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 6.3.3 | 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 | |
| 6.3.4 | 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 | |
| 6.3.5 | 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. | |
| 6.3.6 | 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. | |
| 6.3.7 | The ADS shall interact safely with other road users. | | it can be monitored via dedicated SPIs | |
| 6.3.8 | The ADS shall avoid collisions with safety-relevant objects where possible. | | it can be monitored via dedicated SPIs | |

| Requirement | | Pillar | | |
|--|--|------------|--|---|
| Section | Text | Monitoring | Comments | General note |
| 6.3.9 | The ADS shall signal intended changes of direction. | | It could be monitored, but It is a signaling requirement, mainly related to the Design. | |
| 6.3.10 | 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. | |
| 6.3.11 | Pursuant to a passenger request under para. 7.4.1, the ADS shall bring the vehicle to a safe stop. | | It can be monitored | |
| ADS Performance of the DDT under Critical Traffic Scenarios | | | | |
| 6.4.1 | The requirements of section 6.3. shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk. | | Same consideration of 6.3 applies | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirement |
| 6.4.2 | 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 | |
| 6.4.3 | 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 | |
| 6.4.4 | 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 | | | | |
| 6.5.1 | The requirements of section 5.8 shall continue to apply during failure scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk. | | Same consideration of 5.10 applies | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 6.5.2 | 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 4. | | 1) To be monitored 2) ADS faults to be reported through periodic reporting. | |

| Requirement | | Pillar | | |
|-------------|--|------------|---|---|
| Section | Text | Monitoring | Comments | General note |
| 6.5.2.1 | 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 | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 6.5.2.2 | 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 | |
| 6.5.2.3 | 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 | |
| 6.5.2.4 | 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. | |
| 6.5.2.4.1 | 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 | |
| 6.5.3 | Remote termination of individual or multiple ADS or feature(s) by the manufacturer and/or service operator shall be possible when requested by Authorities. | | 1) it could be monitored but it is mainly a design requirement. 2) The remote termination could be a potential occurrence to be reported. | |
| 6.5.3.1 | 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. | |
| 6.5.3.2 | Remote termination of an ADS or ADS feature(s) shall render them unable to be activated by user. | | 1) it could be monitored but it is mainly a design requirement. 2) The remote termination could be a potential occurrence to be reported. | |

| Requirement | | Pillar | | |
|---|---|------------|--|---|
| Section | Text | Monitoring | Comments | General note |
| ADS Performance of the DDT at ODD Boundaries | | | | |
| 6.6.1 | The ADS shall recognise the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 4.9. | | 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 | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 6.6.2 | The ADS shall be able to determine when the conditions are met for activation of each feature. | | It can be monitored | |
| 6.6.2.1 | 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 | |
| 6.6.2.2 | 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 it can be monitored, Notes: it could be a triggering condition for DSSAD. | |
| 6.6.3 | The ADS shall be able to anticipate foreseeable exits from the ODD of each feature. | | | |
| Minimum Risk Condition Requirements | | | | |
| 6.7.1 | The ADS shall signal its intention to place the vehicle in an MRC. | | It can be monitored. It is a Safety Critical information | critical occurrences to be reported as short-term report can be the result of not |
| 6.7.2 | 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 | |

| Requirement | | Pillar | | |
|---|---|------------|--|---|
| Section | Text | Monitoring | Comments | General note |
| 6.7.2.1 | 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 | compliance with ADS safety requirements |
| 6.7.2.2 | 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 | |
| 6.7.2.2.1 | 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 is 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. | | | | |
| 7.2.1 | 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 | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 7.2.2 | 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 | |
| 7.2.3 | An ADS that controls the operation of doors shall provide an emergency override to the user. | | 1) Design requirement | |
| 7.2.4 | 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. | | | | |
| 7.3.1.1 | 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 | critical occurrences to be reported as short-term report can be the result of not compliance |

| Requirement | | Pillar | | |
|---|---|------------|-----------------------|---|
| Section | Text | Monitoring | Comments | General note |
| 7.3.1.2 | The ADS shall be designed to prevent misuse and errors in operation by the user. | | 1) Design requirement | with ADS safety requirements |
| 7.3.1.2.1 | The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions.[1] | | | |
| 7.3.1.2.2 | 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. (c) Any failure of the ADS that limits the operation of an available feature. | | 1) Design requirement | |
| 7.3.1.2.3 | The ADS shall indicate the availability of a feature for activation. | | 1) Design requirement | |
| Recommendations on the ADS feature activation. | | | | |
| 7.3.2.1 | 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. | | 1) Design requirement | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| Recommendations on ADS feature deactivation to manual driving. | | | | |
| 7.3.3.1.1. | The ADS shall have a monitoring system to support safe and appropriate engagement of the user as necessary. | | 1) Design requirement | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 7.3.3.1.1. | 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 | |

| Requirement | | Pillar | | |
|--|---|------------|---|--|
| Section | Text | Monitoring | Comments | General note |
| ADS features that allow a user-initiated system deactivation to manual driving. | | | | |
| 7.3.4.1 | <p>The ADS shall be designed to ensure a safe user-initiated system deactivation process.</p> <p>(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.</p> <p>(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).</p> <p>(c) The user-initiated system deactivation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.</p> <p>(d) The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process.</p> <p>(e) The ADS shall provide a specific indication of the completion of the deactivation of the ADS.</p> <p>(f) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.</p> <p>(g) If applicable, ADS features operating control of closures shall no longer influence closures or the controls associated with closures.</p> | | <p>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.</p> <p>2)Prevention of takeover under unsafe conditions to be reported according to NATM occurrence list</p> <p>3) Driver unavailability (where applicable) and other user related occurrences to be reported according to section 8 occurrence list</p> | <p>critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements</p> |
| ADS features that have a system-initiated deactivation to manual driving. | | | | |

| Requirement | | Pillar | | |
|-------------|---|------------|---|--|
| Section | Text | Monitoring | Comments | General note |
| 7.3.5.1. | <p>The ADS shall ensure a safe system-initiated deactivation to a fallback user.</p> <p>(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.</p> <p>(b) The system-initiated deactivation to manual driving process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards.</p> <p>(c) The ADS shall:</p> <p>(i) Continuously assess whether the fallback user is available for a system-initiated deactivation.</p> <p>(ii) Provide effective procedures for re-engaging the fallback user who has been detected not to be available.</p> <p>(iii) Trigger an MRM where it has not been possible, feasible and/or safe to re-engage the fallback user.</p> <p>(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).</p> <p>(d) The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process.</p> <p>(e) The ADS shall remain active until the system initiated deactivation process has been completed or the ADS vehicle reaches a minimal risk condition.</p> <p>(f) The ADS shall provide a specific indication of the completion of the deactivation of the ADS.</p> <p>(g) If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving.</p> <p>(h) If applicable, ADS features operating control of closures shall no</p> | | <p>1) It could be monitored to some extent. However, most of the points are not suitable for ISMR. The point c) can be monitored.</p> <p>2) Occurrences related to Transfer of Control failure and Driver unavailability already included in the occurrence list of section 8</p> | <p>critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements</p> |

| Requirement | | Pillar | | |
|---|--|------------|-----------------------|---|
| Section | Text | Monitoring | Comments | General note |
| | longer influence closures or the controls associated with closures. | | | |
| ADS features that do not allow a user to take manual control of the DDT. | | | | |
| 7.4.1. | The ADS shall provide the passenger(s) with means to request to stop the vehicle. | | 1)Design requirement, | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| 7.4.2. | The ADS vehicle shall provide safety-related information to the passengers. | | 1)Design requirement, | |
| 7.4.3. | The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated. | | It can be monitored | |
| 7.4.4. | The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress). | | 1)Design requirement, | |
| 7.4.3. | 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 | | 1)Design requirement, | |

| Requirement | | Pillar | | |
|--|--|------------|--|---|
| Section | Text | Monitoring | Comments | General note |
| | shall be put in place to prevent access to controls. | | | |
| Safety throughout the Useful Life of the ADS and its Features | | | | |
| x | The ADS shall provide an interface for the purposes of maintenance and repair by authorized persons. | | 1)Design requirement, | critical occurrences to be reported as short-term report can be the result of not compliance with ADS safety requirements |
| x | 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 | |
| x | The measures ensuring protection from unauthorized access should be provided in alignment with engineering best practices. | | 1) Design requirement, | |
| x | ADS safety shall be ensured in the event of discontinued production, support, and/or maintenance. | | 1)Design requirement, | |

Annex 3 – 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 templates³² and in the NHTSA ADS standing order³³.

| 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] |

³² <https://www.allianz.co.uk/content/dam/onemarketing/azuk/allianzcouk/broker/docs/support/european-accident-statement-form.pdf>

³³ https://static.nhtsa.gov/odi/ffdd/sgo-2021-01/SGO-2021-01_Data_Element_Definitions.pdf

| | | |
|--|--|---------------------------------|
| 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 | | Text(50) |
| City | | Text(50) |
| ZIP code | | Number(10) |
| Street | | Text(50) |
| GNSS coordinates | | [longitude, latitude] |

| | | |
|-------------------------|--|--------------------|
| 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 should be 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;
- (c) minor: the vehicle can be rendered operational by simple repairs/replacement;
- (d) none: the vehicle sustained no damage;
- (e) 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 CAdAS³⁴ 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;
- (c) 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;
- (e) 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 Scheme³⁵ (AIS) injury classification is recommended, either on single injuries or at the person level, reporting MAIS.

| 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.

³⁴ https://road-safety.transport.ec.europa.eu/system/files/2021-07/cadas_glossary_v_3_8.pdf

³⁵ <https://www.aaam.org/abbreviated-injury-scale-ais/>

| VEHICLE | | |
|-------------------------------|--|-----------|
| Vehicle Identification Number | | Text(17) |
| Serial number | | Text(50) |
| License plate | | Text(10) |
| State 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 applicable³⁶. 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 |
|-----------------|
|-----------------|

³⁶ https://www.nhtsa.gov/sites/nhtsa.gov/files/pre-crash_scenario_topology-final_pdf_version_5-2-07.pdf

| | |
|--------------------------------|--|
| 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);
- (c) 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;
- (e) 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 | | Number(10) |
| Cumulative time travelled by ADS | | 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) |
| <ul style="list-style-type: none"> Safety critical occurrences known to the ADS manufacturer or OEM | | Number(10) |
| <ul style="list-style-type: none"> Occurrences related to ADS operation outside its ODD | | Number(10) |
| <ul style="list-style-type: none"> ADS failure to achieve a minimal risk condition when necessary | | Number(10) |
| <ul style="list-style-type: none"> Modifications made by the ADS manufacturer or OEM to address an | | Number(10) |

| | | |
|---|--|------------|
| identified and significant ADS safety issue | | |
| Occurrences covered under the periodic reporting provisions | | Number(10) |
| <ul style="list-style-type: none"> • Communication-related occurrences | | Number(10) |
| <ul style="list-style-type: none"> • Cybersecurity-related occurrences | | Number(10) |
| <ul style="list-style-type: none"> • Interaction with remote operator if applicable | | Number(10) |
| <ul style="list-style-type: none"> • Driver unavailability (where applicable) and other user-related occurrences | | Number(10) |
| <ul style="list-style-type: none"> • Occurrences related to Transfer of Control failure | | Number(10) |
| <ul style="list-style-type: none"> • Prevention of takeover under unsafe conditions | | Number(10) |
| <ul style="list-style-type: none"> • Occurrences related ADS failure | | Number(10) |
| <ul style="list-style-type: none"> • Maintenance and repair problems | | Number(10) |
| <ul style="list-style-type: none"> • Occurrences related to unauthorized modifications | | Number(10) |
| <ul style="list-style-type: none"> • 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) |
| <ul style="list-style-type: none"> • ADS vehicle occupants | | Number(10) |
| <ul style="list-style-type: none"> • Other road users | | Number(10) |
| Serious injures | | Number(10) |
| <ul style="list-style-type: none"> • ADS vehicle occupants | | Number(10) |

Submitted by the expert from SAE

FRAV-VMAD-01-09
 1st FRAV/VMAD session
 29-30 November 2023

| | | |
|---|--|------------|
| <ul style="list-style-type: none"> Other road users | | Number(10) |
| Minor injures | | Number(10) |
| <ul style="list-style-type: none"> ADS vehicle occupants | | Number(10) |
| <ul style="list-style-type: none"> Other road users | | Number(10) |
| Unknown injures | | Number(10) |
| <ul style="list-style-type: none"> ADS vehicle occupants | | Number(10) |
| <ul style="list-style-type: none"> Other road users | | Number(10) |
| Accident and serious incidents | | Number(10) |
| Minor incidents | | Number(10) |

| OCCURRENCES AGGREGATE DESCRIPTION | | |
|--|--|------------|
| Collision with: | | - |
| <ul style="list-style-type: none"> Passenger car | | Number(10) |
| <ul style="list-style-type: none"> VAN | | Number(10) |
| <ul style="list-style-type: none"> Truck | | Number(10) |
| <ul style="list-style-type: none"> Bus | | Number(10) |
| <ul style="list-style-type: none"> Other: Vehicle | | Number(10) |
| <ul style="list-style-type: none"> Motorcycle | | Number(10) |
| <ul style="list-style-type: none"> Cyclist | | Number(10) |
| <ul style="list-style-type: none"> Pedestrian | | Number(10) |
| <ul style="list-style-type: none"> Other: VRU | | Number(10) |
| <ul style="list-style-type: none"> 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 4 - Matrix of DDT and User requirements with applicable test pillars

1.1 Annex X contains the matrix which provides guidelines linking the DDT and user requirements to the applicable pre-deployment validation pillars.

- 1.2 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.
- 1.3 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.
- 1.4 The matrix uses a green, orange, red, white colour scheme to indicate the relative applicability of the pillars.
 - 1.4.1 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.
 - 1.4.2 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.
 - 1.4.3 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.
 - 1.4.4 White represents a requirement related to the design of the system, which should be assessed via the Audit pillar.
- 1.5 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.
- 1.6 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 | | |
|---|---|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| ADS Performance of the DDT under Nominal Traffic Scenarios | | | | |
| 6.3.1.1 | The ADS shall operate the vehicle at safe speeds. | | | |
| 6.3.1.2 | The ADS shall maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle. | | | |
| 6.3.1.3 | The ADS shall adapt its driving behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic). | | | |
| 6.3.1.4 | The ADS shall adapt its driving behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority). | | | |
| 6.3.2 | The ADS shall detect and respond to objects and events relevant to its performance of the DDT. | | | |
| 6.3.3 | The ADS shall detect and respond to priority vehicles in service in accordance with the relevant traffic law(s). | | | |

| Requirement | | Test Pillars | | |
|--|--|--------------|--------|------------|
| Section | Text | Virtual | Track | Real-world |
| 6.3.4 | 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. | Green | Orange | Green |
| 6.3.5 | Under nominal traffic scenarios, the driving behaviour of the ADS shall not cause a collision. | Green | Green | Green |
| 6.3.6 | The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation. | Green | Green | Green |
| 6.3.7 | The ADS shall interact safely with other road users. | Green | Green | Green |
| 6.3.8 | The ADS shall avoid collisions with safety-relevant objects where possible. | Green | Green | Green |
| 6.3.9 | The ADS shall signal intended changes of direction. | Green | Green | Green |
| 6.3.10 | The ADS shall signal its operational status in accordance with national rules. | Green | Green | Green |
| 6.3.11 | Pursuant to a passenger request under para. 7.4.1., the ADS shall bring the vehicle to a safe stop. | Green | Green | Green |
| ADS Performance of the DDT under Critical Traffic Scenarios | | Grey | Grey | Grey |
| 6.4.1 | The requirements of section 6.3. shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk. | Green | Green | Red |
| 6.4.2 | In the event of a collision, the ADS shall stop the vehicle in an MRC and/or in accordance with applicable traffic laws. | Green | Green | Red |
| 6.4.2.1 | The ADS shall not resume travel until the safe operational state of the ADS vehicle has been verified. | Green | Green | Red |
| 6.4.2.2 | The ADS may resume the trip where permissible under the applicable traffic rule(s) and other safety considerations. | Green | Green | Red |

| Requirement | | Test Pillars | | |
|---|--|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| ADS Performance of the DDT under Failure Scenarios | | | | |
| 6.5.1 | The requirements of section 6.3 shall continue to apply during failure scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk. | | | |
| 6.5.2 | 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 . | | | |
| 6.5.2.1 | 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. | | | |
| 6.5.2.2 | 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. | | | |
| 6.5.2.3 | The ADS shall adapt its performance of the DDT in accordance with the severity of the fault to ensure road safety. | | | |
| 6.5.2.4 | 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. | | | |
| 6.5.2.4.1 | The limited operation of the ADS should comply to the normally applicable safety requirements. | | | |
| 6.5.3 | Remote termination of individual or multiple ADS or feature(s) by the manufacturer and/or service operator shall be possible when requested by Authorities. | | | |

| Requirement | | Test Pillars | | |
|---|--|--------------|--------|------------|
| Section | Text | Virtual | Track | Real-world |
| 6.5.3.1 | Remote termination for an ADS performing the DDT shall be capable of triggering an ADS fallback response. | Green | Green | Orange |
| 6.6.3.2 | Remote termination of an ADS or ADS feature(s) shall render them unable to be activated by user. | Green | Green | Green |
| ADS Performance of the DDT at ODD Boundaries | | Grey | Grey | Grey |
| 6.6.1 | The ADS shall recognise the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 5.2 . | Green | Orange | Green |
| 6.6.2 | The ADS shall be able to determine when the conditions are met for activation of each feature. | Green | Orange | Green |
| 6.6.2.1 | The ADS shall prevent activation of a feature unless the ODD conditions of the feature are met. | Green | Orange | Green |
| 6.6.2.2 | The ADS shall execute a fallback response when one or more ODD conditions of the feature in use are no longer met. | Green | Orange | Green |
| 6.6.3 | The ADS shall be able to anticipate foreseeable exits from the ODD of each feature. | Green | Orange | Green |
| Minimum Risk Condition Requirements | | Grey | Grey | Grey |
| 6.7.1 | The ADS shall signal its intention to place the vehicle in an MRC. | Green | Green | Orange |
| 6.7.2 | 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. | Green | Green | Orange |
| 6.7.2.1 | In the absence of a fallback-ready user, the ADS shall fall back directly to an MRC. | Green | Green | Orange |
| 6.7.2.2 | 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. | Green | Green | Orange |

| Requirement | | Test Pillars | | |
|-------------|--|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| 6.7.2.2.1 | Upon completion of a fallback to an MRC, a user may be permitted to assume control of the vehicle. | | | |

| Requirement | | Test Pillars | | |
|---|---|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| Recommendations for safe interactions between Users and ADS. | | | | |
| 7.2.1 | The ADS shall signal the presence of any failure that limits the operation of an available feature. | | | |
| 7.2.2 | The ADS shall signal its intention to place the vehicle in an MRC to the ADS user(s). | | | |
| 7.2.3 | An ADS that controls the operation of doors shall provide an emergency override to the user. | | | |
| 7.2.4 | 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. | | | | |
| 7.3.1.1 | 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. | | | |

| Requirement | | Test Pillars | | |
|---|---|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| 7.3.1.2 | The ADS shall be designed to prevent misuse and errors in operation by the user. | Audit | | |
| 7.3.1.2.1 | The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions. | Audit | | |
| 7.3.1.2.2 | 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. | | | |
| (c) | Any failure of the ADS that limits the operation of an available feature. | | | |
| 7.3.1.2.3 | The ADS shall indicate the availability of a feature for activation. | | | |
| Recommendations on the ADS feature activation. | | | | |
| 7.3.2.1 | 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. | Audit | | |
| (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. | | | | |
| 7.3.3.1.1 | The ADS shall have a monitoring system to support safe and appropriate engagement of the user as necessary. | Audit | | |

| Requirement | | Test Pillars | | |
|--|---|--------------|--------|------------|
| Section | Text | Virtual | Track | Real-world |
| 7.3.3.1.2 | At the completion of the deactivation process, lateral and longitudinal control shall be returned to the driver without any continuous control assistance active. | Green | Green | Green |
| ADS features that allow a user-initiated system deactivation to manual driving. | | Grey | Grey | Grey |
| 7.3.4.1 | The ADS shall be designed to ensure a safe user-initiated system deactivation process. | Grey | Grey | Grey |
| (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. | Green | Green | Orange |
| (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). | Green | Orange | Red |
| (c) | The user-initiated system deactivation process (e.g., sequence of actions and states) shall take into account relevant recommendations or standards. | Audit | | |
| (d) | The ADS shall assess the user is suitably engaged to resume the DDT before completion of the deactivation process. | Orange | Green | Green |
| (e) | The ADS shall provide a specific indication of the completion of the deactivation of the ADS. | Green | Green | Green |
| (f) | If applicable upon ADS deactivation, the vehicle controls, indicators, warnings, and tell-tales shall be set to an appropriate state for manual driving. | Green | Green | Green |

| Requirement | | Test Pillars | | |
|--|---|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| (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. | | | | |
| 7.3.5.1 | 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. | Audit | | |
| (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 an MRM 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). | | | |

| Requirement | | Test Pillars | | |
|--|--|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| (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. | | | | |
| 7.4.1 | The ADS shall provide the passenger(s) with means to request to stop the vehicle. | Audit | | |
| 7.4.2 | The ADS vehicle shall provide safety-related information to the passengers. | | | |
| 7.4.3 | The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated. | | | |
| 7.4.4 | The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress). | | | |

Submitted by the expert from SAE

FRAV-VMAD-01-09
1st FRAV/VMAD session
29-30 November 2023

| Requirement | | Test Pillars | | |
|-------------|---|--------------|-------|------------|
| Section | Text | Virtual | Track | Real-world |
| 7.4.5 | 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 |