Submitted by GRVA

Informal Document **WP.29-191-07**
191st WP.29, 14-16 November 2023
Provisional agenda item 2.3.

# Guidelines for Regulatory Requirements and Verifiable Criteria for ADS Safety Validation

This document was endorsed by the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) at its 17th session and was prepared by the Informal Working Group on Functional Requirements for Automated Vehicles (FRAV). The document provides guidelines to support the development of regulatory requirements and verifiable criteria for the assessment of Automated Driving Systems and vehicles equipped with such systems in accordance with the FRAV terms of reference and the WP.29 Framework document on automated/autonomous vehicles.[1] It is submitted to WP.29 as an update to WP.29-191-xx endorsed by WP.29 in June and corresponds to the FRAV deliverable requested by the Framework Document for mid 2023.

1. Introduction

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

1.2. The development of these recommendations involved extensive consideration of what an ADS is and how ADS relate to human roles in driving. Accordingly, the definition of ADS is central to these recommendations. Two leading international standards bodies, SAE and ISO, define ADS as: "The hardware and software that are collectively capable of performing the entire DDT (Dynamic Driving Task) on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD)."[2]

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

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

1.5. Driving.

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

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

[1] ECE/TRANS/WP.29/1147/Annex V and ECE/TRANS/WP.29/2019/34/Rev.2, respectively.

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

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

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

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

1.5.6. For example, a decision to drive from home to a workplace involves a strategic assessment of the current conditions, the risks involved in driving under those conditions, and the probability for arriving at work on time. While driving, the driver makes tactical decisions based on conditions encountered along the way such as to change lanes or turn onto another street. In changing lanes, the driver makes a tactical assessment that the lane change is feasible, actuates the direction indicators and steers the vehicle while maintaining an appropriate speed, often with continuous adjustments on the operational level.

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

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

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

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

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

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

1.6. Automated driving.

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

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

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

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

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

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

1.6.7. The conditions under which an ADS is designed to operate are known as the Operational Design Domain (ODD), which include but are not limited to aspects such as roadway speed limits, road designs (surface, geometry, infrastructure, etc.), weather conditions, and traffic densities.

The ODD may include constraints or limitations on ADS use such as maximum vehicle speed, maximum rate of rainfall, or road type.

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

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

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

1.6.10.1. Sensing and Perception

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

1.6.10.2. Planning and Decision

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

1.6.10.3. Control

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

1.7. Automated Driving Systems

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

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

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

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

1.8. ADS functions: DDT Performance Capabilities

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

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

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

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

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

1.8.6. Safe ADS performance of the DDT

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

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

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

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

1.8.7. Additional ADS Capabilities: Safe use of ADS and ADS vehicles

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

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

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

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

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

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

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

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

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

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

1.9. ADS features

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

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

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

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

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

2. Purpose.

2.1. This document provides recommendations for safety requirements for ADS. This output is intended to support future initiatives under the 1958, 1997, and/or 1998 Agreements.

2.2. Usage of the verbal forms “shall” (indicating an obligatory provision) and “may” (indicating a permissive provision) should be understood within the context of providing recommendations per the preceding paragraph.

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. *“Automated Driving System (ADS)”* means the hardware and software that are collectively capable of performing the entire DDT on a sustained basis regardless of whether it is limited to a specific operational design domain (ODD).

3.2. *“(ADS) feature”* means an application of an ADS designed specifically for use within an Operation Design Domain (ODD).

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

3.4. *“ADS vehicle”* means a vehicle equipped with an ADS.

3.5. *“Behavioural competency”* means an expected and verifiable capability of an ADS feature to operate a vehicle within the ODD of the feature.

3.6. *“Driver”* means a human being who performs in real time part or all of the DDT.

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

3.7.1. When the ADS is in operation, the DDT is always performed in its entirety by the ADS ("the entire DDT" as stated in the definition of an "Automated Driving System" under para. 3.1.) 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.

3.7.1.1. 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.

3.7.1.2. Planning and decision include:

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

3.7.1.3. Control includes:

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

3.7.1.4. The DDT excludes strategic functions.

3.7.2. *"Strategic function"* means a capability to issue commands, instructions, or guidance for execution by an ADS.[3]

3.7.3. *"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.[4]

3.7.4. *"Operational function"* means a capability to control the real-time motion of the vehicle.[5]

---

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

[4] 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.

[5] 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.

3.8. *"(ADS) fallback response"* means a system-initiated deactivation to manual driving or an ADS-controlled procedure to place the vehicle in a minimal risk condition.

3.9. *"Fallback user"* means a user designated to perform the DDT pursuant to an ADS fallback response.

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

3.11. *"Operational Design Domain (ODD)"* means the operating conditions under which an ADS feature is specifically designed to function.[6]

3.12. *"Other road user (ORU)*" means an entity in the ADS vehicle environment capable of motion and coordinated interaction with the ADS vehicle.

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

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

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

3.16. *"Traffic scenario"* means a description of one or more real-world driving situations that may occur during a given trip.

3.16.1. *"Nominal scenario"* means a traffic scenario representing usual and/or expected objects, object behaviours and/or road conditions.

3.16.2. *"Critical scenario"* means a traffic scenario representing unusual and/or unexpected objects, object behaviours, and/or road conditions.

3.16.3. *"Failure scenario"* means a traffic scenario representing a system failure that compromises the capability of the ADS to perform the entire DDT.

3.17. *"Transition of control (TOC)"* means a procedure by which the ADS transfers performance of the DDT to an ADS vehicle user.

3.18. *"(ADS) User"* means a human being using an ADS where dynamic control of the vehicle is entirely maintained on a sustained basis by the ADS performance of the DDT.

3.19. *"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.

---

[6] 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.

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).

4.2. 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).

4.3. The manufacturer shall establish terms for the correct use of the ADS and its feature(s).

4.4. 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.

4.5. The manufacturer shall provide written instructions for the activation and deactivation of the ADS.

4.6. The manufacturer shall provide written information on ADS responses to ADS vehicle user interventions in the dynamic control of the vehicle.

4.7. The manufacturer shall provide written descriptions of the transition of control procedures, including ADS notifications and fallback user responses.

4.8. The manufacturer shall list the potential faults identifiable by the diagnostic system(s) of the ADS.

4.9. The manufacturer shall establish the ODD conditions and boundaries of each ADS feature in measurable and/or verifiable terms.

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.

5. ADS Safety Requirements

5.1. The following subsections recommend criteria for validating the safety of ADS and/or ADS vehicles.

5.2. 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.

5.3. Subsections 5.8, 5.9, and 5.10 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.

5.4. 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.

5.5. Annex A 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.

5.6. 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).

5.7. The behavioural competencies define ADS responses that comply with the following global requirements (Subsections 5.8, 5.9, and 5.10) within the bounds of a relevant safety model quantifying dimensions for assessment of ADS performance (as described in Annex A). 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.

5.8. Compliance with the recommended requirements under Subsections 5.8., 5.9., and 5.10. is determined by verifying that the ADS demonstrates the behavioural competencies associated with the scenarios relevant to the ODD of its features.

5.9. These requirements shall be applied in the definition of behavioural competencies to be demonstrated under traffic scenarios.

5.10. ADS Performance of the DDT under Nominal Traffic Scenarios

5.10.1. 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.

5.10.2. 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.

5.10.3. This section recommends requirements for assessing ADS performance of the DDT under normal operational and driving conditions.

5.10.4. The ADS shall be capable of performing the entire Dynamic Driving Task (DDT) within the ODD of its feature(s).

5.10.4.1. The ADS shall operate the vehicle at safe speeds.

5.10.4.2. The ADS shall maintain appropriate distances from other road users by controlling the longitudinal and lateral motion of the vehicle.

5.10.4.3. The ADS shall adapt its driving behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic).

5.10.4.4. The ADS shall adapt its driving behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).

5.10.5. 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.

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

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

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

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

5.10.8. The ADS shall detect and respond to objects and events relevant to its performance of the DDT.

5.10.9. The ADS shall detect and respond to priority vehicles in service in accordance with the relevant traffic law(s).

5.10.10. 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.

5.10.11. Under nominal traffic scenarios, the driving behaviour of the ADS shall not cause a collision.

5.10.12. The ADS shall comply with traffic rules in accordance with application of relevant law within the area of operation.

5.10.13. The ADS shall interact safely with other road users.

5.10.14. The ADS shall avoid collisions with safety-relevant objects where possible.

5.10.15. The ADS shall signal intended changes of direction.

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

5.10.17. The ADS shall signal its operational status in accordance with national rules.

5.10.18. Pursuant to a passenger request under para. 5.13.4.3., the ADS shall bring the vehicle to a safe stop.

5.11. ADS Performance of the DDT under Critical Traffic Scenarios

5.11.1. 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.

5.11.2. 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.

5.11.3. This section recommends requirements for assessing the ADS performance of the DDT under critical driving conditions.

5.11.3.1. The requirements of section 5.10. shall continue to apply during critical scenarios as far as is reasonably practicable under the specific circumstances with the aim of minimising overall risk.

5.11.4. In the event of a collision, the ADS shall stop the vehicle in an MRC and/or in accordance with applicable traffic laws.[7]

5.11.4.1. The ADS shall not resume travel until the safe operational state of the ADS vehicle has been verified.

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

5.11.4.2. The ADS may resume the trip where permissible under the applicable traffic rule(s) and other safety considerations.

5.12. ADS Performance of the DDT under System Failure Scenarios

5.12.1. 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.

5.12.1.1. 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.

5.12.2. 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.

5.12.2.1. 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.

5.12.2.2. 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.

5.12.2.3 The ADS shall adapt its performance of the DDT in accordance with the severity of the fault to ensure road safety

5.12.2.3.1. 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.

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

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

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

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

5.12.4. 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.

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

5.12.4.2. 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.

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

5.13. Recommendations for safe interactions between Users and ADS.

5.13.1. Scope and purpose.

5.13.1.1. This section provides recommendations on the design of the ADS user interactions between users and ADS vehicles to obtain safe operation of ADS vehicles.

5.13.1.2. These recommendations do not apply to ADS vehicles and ADS features designed without accommodations for a user.

5.13.1.3. The types of ADS users considered in this document are driver, fallback user, passenger.

5.13.2. General recommendations

5.13.2.1. The ADS shall signal the presence of any failure that limits the operation of an available feature.

5.13.2.2. The ADS shall signal its intention to place the vehicle in an MRC to the ADS user(s).

5.13.2.3. An ADS that controls the operation of doors shall provide an emergency override to the user.

5.13.2.4. 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.

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

5.13.3.1. General recommendations.

5.13.3.1.1. 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.

5.13.3.2. The ADS shall be designed to prevent misuse and errors in operation by the user.

5.13.3.2.1. The vehicle controls dedicated to the ADS shall be clearly identified and distinguishable to accommodate only the appropriate interactions.[8]

[8] 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.

5.13.3.2.2. 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.

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

5.13.3.3. Recommendations on the ADS feature activation.

5.13.3.3.1. 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.

5.13.3.4. Recommendations on ADS feature deactivation to manual driving.

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

5.13.3.4.2. At the completion of the deactivation process, lateral and longitudinal control shall be returned to the driver without any continuous control assistance active.[9]

5.13.3.5. ADS features that allow a user-initiated system deactivation to manual driving.[10]

5.13.3.5.1. 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).

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

[10] 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.

(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.

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

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

5.13.3.6.1. 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.

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

5.13.4.1. The ADS shall provide the passenger(s) with means to request to stop the vehicle.

5.13.4.2. The ADS vehicle shall provide safety-related information to the passengers.

5.13.4.3. The ADS shall not initiate motion unless the safety risks to the passenger(s) have been mitigated.

5.13.4.4. The ADS may provide the user(s) with information related to ongoing operations (e.g., destination, upcoming stops, route progress).

5.13.4.5. 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.

5.14. Safety throughout the Useful Life of the ADS and its Features

5.14.1. This section addresses the safe use of an ADS and its feature(s) during the useful life of the ADS vehicle.

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

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

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

5.14.4. ADS safety shall be ensured in the event of discontinued production, support, and/or maintenance.

# Annex A.

## Approach to Derive Verifiable Performance

1. Purpose of this document

This document provides an overview on an approach that may be used to derive verifiable performance criteria for the certification or, as relevant, for self-certification of ADS, based on the manufacturer/ ADS developer's description of the Operational Design Domain (ODD) of the ADS. Such criteria would be developed by identifying behavioural competencies that embody and correspond to specific FRAV ADS Safety Requirements, as introduced in Section 5, and relevant scenarios that may be used to validate the ADS's competencies.

The suggested approach includes a description of how such competencies can be classified into nominal, critical and failure categories and mapped to the relevant scenarios, selected either from the VMAD existing database, or identified through the application of knowledge and data-based approaches. Such methodology provides meaningful content to ensure integration with the work of VMAD and assessment according to the relevant VMAD test methods.

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

2. Introduction and approach

2.1. Operational Design Domain

Operational design domain (ODD) refers to:

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

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

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

The conditions constituting the ODD in which the ADS was designed to operate will help determine which ADS competencies are required. For example, if an ADS has an ODD which comprises of roads with non-signalised junctions, one of the required behaviour competencies for the ADS in that ODD could potentially be "unprotected left or right

turn". However, the same behaviour competency may not be required if the ODD of an ADS is limited to motorways or highways with signalised junctions.

2.2. Behavioural competencies

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

The Automated Vehicle Safety Consortium ("AVSC")) has provided these definitions[11]:

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

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

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

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

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

Failure situations involve those in which the ADS or another vehicle system experiences a fault or failure that removes or reduces the ADS's

[11] AVSC Best Practice for Evaluating Behavioral Competencies for Automated Driving System Dedicated Vehicles (ADS-DVs).

ability to perform the DDT, such as sensor or computer failure or a failed propulsion system.

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

For this, the following is needed:

- An overview of reasonable expectations (which might occur in different ODDs),
- An overview of reference behaviours / safety models that define the boundary between avoidable accidents and mitigation (note that these reference behaviours will not be used for anything else than providing this boundary as a performance criterion).
- A matrix combining suggested reference behaviours / safety models with driving situations.

3. Behavioural Competencies Identification

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

- ODD Analysis
- Driving Situation Analysis
- OEDR Analysis.

3.1. ODD analysis

This analysis represents the first step with the aim to identify the characteristics of the ODD. An ODD may consist of stationary physical elements (e.g., physical infrastructure), environmental conditions, dynamic elements (e.g., reasonably expected traffic level and composition, vulnerable road users) and operational constraints to the specific ADS application. Various sources provide useful guidance

for precisely determining the elements of a particular ODD and their format definition.[12,13, 14, 15]

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

3.2. Driving situation analysis

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

An example of this analysis is given in Table 1, where static and dynamic behaviours of other objects (including other road users) that the ADS is reasonably expected to encounter within the ODD are described. In the case of vehicles, this includes behaviours such as "acceleration", "deceleration", "cut-in"; for pedestrians, examples of dynamic behaviours include "crossing road", "walking on sidewalk", etc. Some of these behaviours may involve nominal situations (e.g., lead vehicle deceleration at a rate reasonably expected in light of traffic and other circumstances within the bounds of physical limitations[16]) while others may involve critical situations (e.g., sudden cut-ins or unpredictable pedestrian or cyclist behaviour, including behaviours that may violate local traffic laws such as crossing a road outside a designated cross walk).

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

Table 1: Static / Dynamic elements and their properties

| Objects | Events/Interactions |
|---|---|

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

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

[14] ASAM OpenODD

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

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

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

| | |
|---|---|
| | Crosswalk,<br>Railroad crossing<br>School zone,<br>… |
| Vehicle signals | Turn signals |

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

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

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

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

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

| | |
|---|---|
| Cyclist crossing road | Yield, decelerate, stop |

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

3.4. Nominal Situation Competencies

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

Therefore, an approach to codify rules of the road to provide additional specificity was developed in Paragraph **[6]**. Additionally, application of models involving safe driving behaviour may be needed in addition to reference to codified rules of the road in developing behavioural competencies for nominal driving situations.

3.5. Critical Situation Competencies

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

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

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

Development of behavioural competencies for critical driving situations faces several challenges. No general consensus exists on the

appropriate models for the behaviour of ORUs or appropriate responses by the ADS to unreasonable ORU behaviours that make a crash imminent.

3.6. Failure Situation Competencies

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

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

4. Scenario Identification

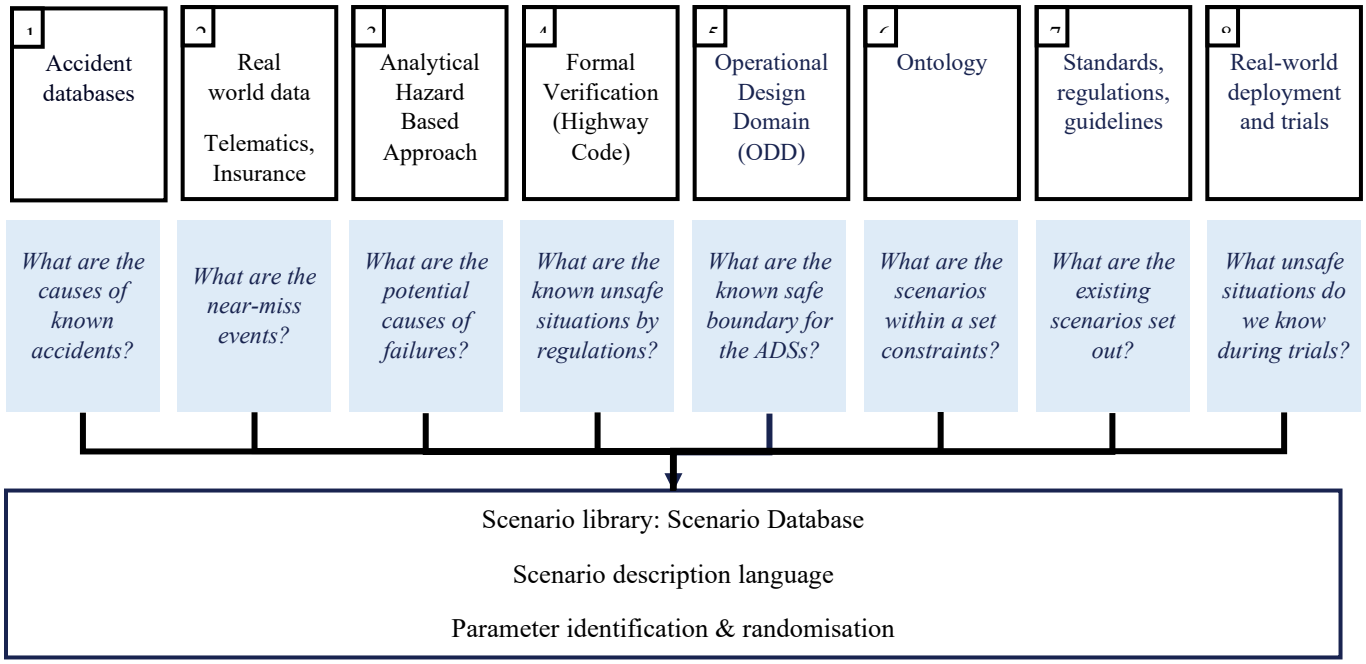
To ensure that the behavioural competences identified in the previous paragraphs are ready to be assessed through the application of simulations or physical testing, ODD-relevant scenarios must be developed. Scenario creation involves use of assumptions concerning the actions of road users that incorporate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

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

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

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

Figure 1




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

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

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

Furthermore, the existing scenarios already defined in the standards, regulations or guidelines (Option 6 - KB) can also be utilized for the testing of ADSs, for example the scenarios set out in ISO22737 and NCAP. ISO22737 has been developed for low-speed automated driving systems (LSAD) and the NCAP provides a set of testing scenarios for the safety assurance of vehicles. Option 7 (DB) includes the scenarios

that occur during real world trials and deployments. Such scenarios might have not been considered pre-deployment but are key learnings.

4.1. Assumptions: Logical to concrete scenarios

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

5. Application of Rules of Road as Pass criteria and requirements

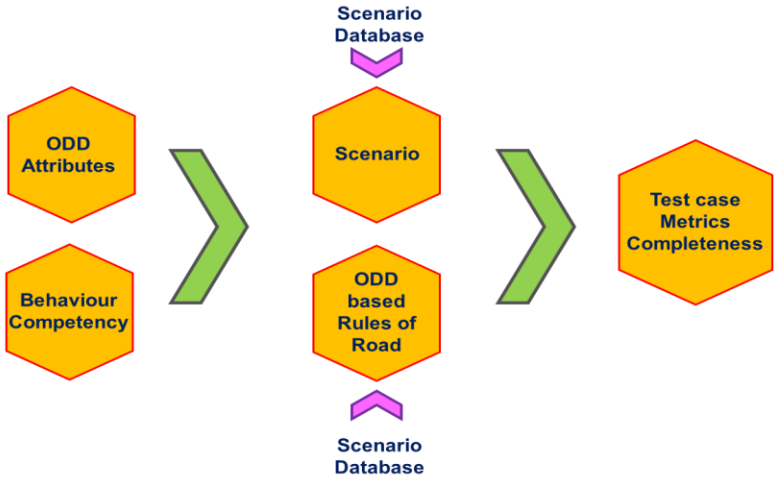
An approach to define an acceptance criterion related to nominal driving situations is to evaluate the ADS performance against the rules of the road. Furthermore, ADS safety requirements state that *"The ADS shall comply with traffic laws"* (para. 5.10.14.). It is challenging to test against this requirement in the absence of codified rules of the road.

Section 8 below demonstrates a framework for codifying the rules of the road to govern the behaviour of ADSs. The approach may be used to define "good behaviour" to inform validation and verification processes (including for scenario-based testing) for nominal scenarios.

5.1. Using rules of the road as pass criteria

Figure 2 illustrates the use of codified rules of the road as a pass criterion for scenario-based testing activities. Every test scenario definition will have ODD and behaviour competency attributes defined. Every rule of the road will also have ODD and behaviour competency attributes as part of its definition. Therefore, it is possible to map every scenario to a corresponding rule(s) of the road using ODD and behaviour tags or labels in a scenario catalogue.

Figure 2: Rules of the road as pass/fail criteria




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

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

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

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

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

The purpose of this document (which could be annexed to FRAV's final result, or could possibly be integrated into another annex to that final result document) is to define a process as to how concrete performance criteria for future ADS regulations could be developed.

The set of safety models described in this document should be regarded as a set of tools, whereas selecting the right tool (the right safety model)

depends on the boundary conditions and should be the task of groups dedicated to writing concrete regulations. Hence in this document, there exists no preference for any of the safety models being depictured.

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

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

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

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

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

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

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

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

- the balance between risk to the ADS itself vs. risk towards the accident partner (e.g. for pedestrians, it would very likely be acceptable to have a slightly increased risk for the typically belted ADS occupants when the risk for the pedestrian would be significantly reduced, e.g. by earlier or stronger brake intervention; for unmanned ADS similar risk balance considerations have to be done),
- the assumed anticipation level (e.g. is it feasible to anticipate actions of other traffic parameters and start countermeasures earlier, or will it be a simple reaction to faults),
- the environmental condition parameters. (e.g. what level of friction is typically available where the ADS are travelling),
- the balance between efficiency and acceptable remaining risk (e.g. passing a pedestrian with no acceptable risk would be possible only

with very low speeds, which would render the current sidewalk close to streets infrastructure useless for automation).

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

Example Regulation XXX =

{Situation / parameter range 1, avoidance = fsafetymodel,1(parameters a,b,c);

# address pedestrian accidents in urban areas

Situation / parameter range 2, avoidance = fsafetymodel,2(parameters d,e,f);

# address car-car accidents with cut-in on motorways…}.

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

Table 3: Overview of Safety Models that have been previously presented in the DDT workstream

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

| | |
|---|---|
| | anticipation of other vehicle behaviour into account |

The full description of all proposed safety models as well as the driving dynamics background will be included in the final guidelines document, perhaps as a separate annex. For several of the models, this information is already available in FRAV-38-07, it is expected that improved versions of the document will be made available in later FRAV meetings.

7. Performance Evaluation and Targets

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

On the other hand, failure situations are performed to assess the ADS ability to recognise faults / failures in the system, and respond in compliance with the principles highlighted by FRAV.

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

Annex 1—Appendix 1

8. Codification methodology for rules of the road

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

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

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

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

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

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

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

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

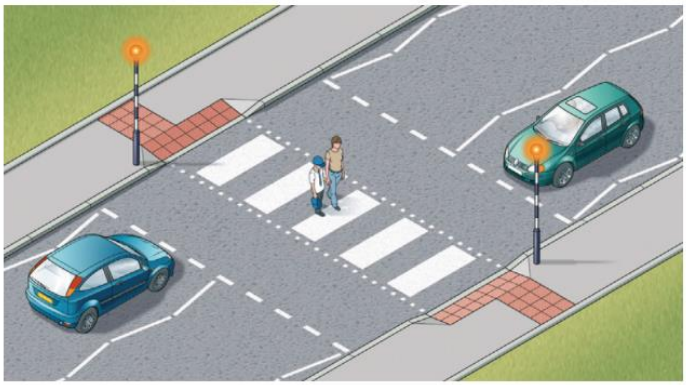
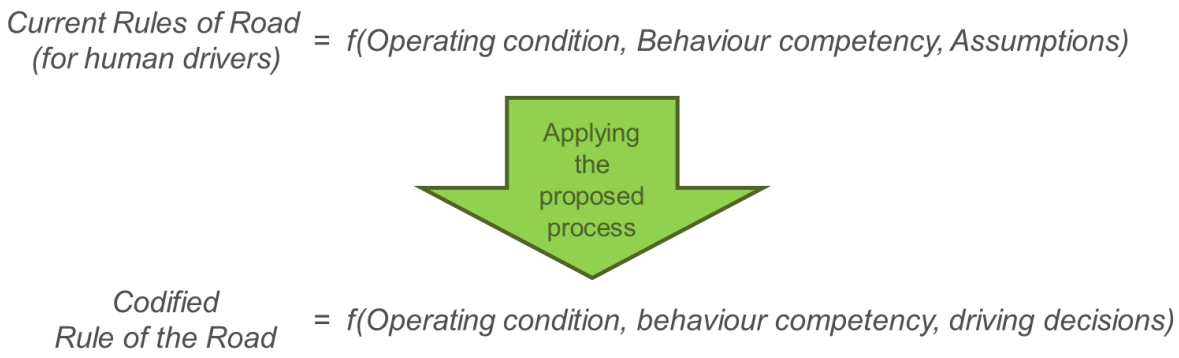


*Figure 3: Example of zebra crossing from UK's Highway Code:*
*Source: https://www.gov.uk/guidance/the-highway-code/rules-for-pedestrians-1-to-35#rule19*

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

Figure 4 illustrates this process. After following the codification process of defining the "rules of the road", there will be no underlying "assumptions" (see section 8.1). Furthermore, for all areas or jurisdiction or country, there will be a minimum set of behaviour code rules which will have consistent "driving characteristics" – the base or common set of rules of the road (for ADS).

Figure 3. Converting current rules of the road (for human drivers) to codified rules for ADS.




8.1. Codification methodology

The codification methodology is a four-step process:

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

8.1.1. Vienna Convention codification example

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

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

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

Step 1: Identify Terms and Construct a Vocabulary

The rule is re-stated below highlighting important terms:

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

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

Step 2: Identify Unspecified Terms

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

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

Step 3: Identify Predicates and Functions

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

**Shall not <u>overtake</u> <u>another vehicle</u>**

- **approaching pedestrian crossing on carriageway or signposted,**
- **or stopped immediately before crossing,**

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

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

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

Step 4: Express Rule in First Order Logic

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

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

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

The rules are as follows:

| | | |
|---|---|---|
| Rule | isEgo(x) ∧ isOtherRoadUser(y) | x is the ego and y is the |

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

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