This document is based on FRAV-34-04 pursuant to the outcomes of discussions held during the 33rd FRAV session. Text subject to outstanding comments is contained in [brackets].

Recommendations concerning Safety Requirements for the Assessment of Automated Driving Systems and ADS Vehicles

1. Introduction

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

1.2. 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.

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

1.4. Driving

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

1.4.2. Driving involves three behavioural levels: strategic, tactical, and operational.[1]

1.4.3. 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.

1.4.4. 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.

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

1.4.6. 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.

1.4.7. 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] Michon, J.A., 1985. "A Critical View of Driver Behavior Models: What Do We Know, What Should We Do?" In L. Evans & R. C. Schwing (Eds.). Human behavior and traffic safety (pp. 485-520). New York: Plenum Press, 1985.

1.4.8. 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, however, can be made during a trip. For example, when deciding to leave the motorway for lesser roads.

1.4.9. 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.

1.4.10. 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.

1.4.11. 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.

1.4.12. 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.

1.5. Automated driving

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

[1.5.2. 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.]

1.5.3. 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.

1.5.4. 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.

[1.5.5. 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.]

[1.5.6. The requirements recommended in this document address misuse prevention and the safety of user interactions such as transitions of vehicle control; however, the fallback-user role also suggests traffic laws to codify obligations of fallback users to maintain their readiness to drive the vehicle during a trip.]

[1.5.7. The conditions under which an ADS is designed to operate are known as the Operational Design Domain (ODD), including 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.]

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

1.5.9. 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.

[1.5.10. Driver performance of the DDT is based on human physical, sensory, and cognitive capabilities. ADS performance of the DDT is based on hardware and software. Therefore, the definition of DDT as applied to an ADS must be understood in these terms.]

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

[1.5.11.1 Sensing and perception

ADS sensing and perception includes monitoring the driving environment via 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.]

1.5.11.2. Planning and decision

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

[1.5.11.3. Control

Control refers to object and event response execution via lateral and/or longitudinal motion control and enhancing vehicle conspicuity via lighting and signalling.]

1.6. Automated Driving Systems

[1.6.1. Based on the above, ADS need to be understood 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).]

[1.6.2. 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.]

[1.6.3. Driving automation systems that require human support to fulfil aspects of the DDT fall below the level of an ADS.]

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

[1.7. ADS functions]

[1.7.1. ADS integrate subsets of hardware and software (i.e., functions) designed to perform aspects of the DDT.]

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

[1.7.3. A function enables the ADS to perform one or more elements of the DDT.]

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

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

1.7.6. 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.

[1.7.7. However, functions that enable performance of the DDT and functions that ensure safe use, including the safety of user interactions, involve distinctly different objectives and requirements.]

1.7.8. Safe ADS performance of the DDT

[1.7.8.1. 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 of the vehicle shall not cause crashes or disrupt traffic and ADS shall avoid crashes where preventable.]

[1.7.8.2. 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 its ODD. 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.]

[1.7.8.3. These recommendations intentionally omit specifications for individual DDT functions. As noted above, performance of the DDT is dependent on traffic conditions where such functions cannot be limited to representative specifications. For example, a representative crash test at 56 kph ensures safety at lower speeds. This approach cannot be applied to driving where safety involves real time tactical and operational adaptation to dynamic road conditions. Tactical and operational functions are interdependent where the complexity of their interactions needs to be assessed under diverse traffic conditions.]

[1.7.8.4. By ensuring that an ADS will be subjected to traffic scenarios covering 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.]

[1.7.9. Safe use of ADS and ADS vehicles]

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

[1.7.9.2. 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.[2] ADS should be designed to foster a level of trust that is aligned with their capabilities and limitations to ensure proper use.]

[1.7.9.3. 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,

[2] Raja Parasumaran and Victor Riley. Humans and Automation: Use, Misuse, Disuse, Abuse. Human Factors, 1997, 39(2), 230-253.

requests, and feedback, and both misuse prevention as well as safeguards in the event of misuse.]

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

1.7.9.5. 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.

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

[1.7.9.7. 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.]

1.7.9.8. 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.

1.8. ADS features

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

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

[1.8.3. 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.]

1.8.4. 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.

[1.8.5. 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 ADS hardware and software designed specifically for use within an 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 in on-road traffic. (See Section I.A. for general background and especially Section I.B., paragraphs 25-29, for application to ADS.)]

3.8. *"(ADS) fallback response"* means an ADS-initiated transition of control or an ADS-controlled procedure to place the vehicle in a minimal risk condition.

[3.9. *"Fallback user"* means a user designated to assume the role of driver upon completion of a transition of control.]

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.

3.12. *"Operational functions"* refer to basic capabilities such as to control lateral and longitudinal motion of the vehicle.

[3.13. "Other *road user (ORU)"* means any entity using a roadway and capable of safety-relevant interaction with an ADS vehicle.]

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

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

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

3.17. *"Tactical functions*" refer to the real-time planning, decision, and execution of manoeuvres.

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

[3.18.1. *"Critical scenario"* means a traffic scenario representing unusual and/or unexpected object behaviours and/or road conditions.]

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

[3.18.3. *"Nominal scenario"* means a traffic scenario representing usual and/or expected object behaviours and/or road conditions.]

[3.19. *"Transition of control (TOC)"* means a procedure by which the ADS hands over dynamic control of the vehicle to the fallback user such that the fallback user is given the role of driver upon completion.]

3.20. *"(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.

3.21. *"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.

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 transfer of control procedures, including ADS notifications and fallback user responses.

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

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

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

5. ADS Safety Requirements

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

5.1. 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.

5.2. 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.

5.3. 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.

5.4. 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).[3]

5.5. 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.

5.6. 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.

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

5.8. ADS Performance of the DDT under Nominal Traffic Scenarios

5.8.1. 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.

5.8.2. 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.

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

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

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

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

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

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

5.8.5. The ADS shall recognize the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 4.9.

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

5.8.6.1. The ADS shall detect and respond when one or more ODD conditions are not fulfilled by preventing possible activation.

5.8.6.2. The ADS shall detect and respond when one or more ODD conditions are no longer fulfilled by executing a transition of control or by placing the vehicle in an MRC.

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

5.8.8. The ADS shall detect and respond to objects and events relevant to its performance of the DDT. See Appendix B.

[3] ECE/TRANS/WP.29/2019/34/Rev.2 as amended

5.8.9. The ADS shall recognize markings and signals used to indicate priority vehicles within the ODD of its feature(s).

5.8.10. The ADS shall classify priority vehicles within the ODD of its feature(s) in accordance with the relevant traffic law(s).

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

[5.8.12. The driving behaviour of the ADS shall not disrupt the flow of traffic.]

[5.8.13. The driving behaviour of the ADS shall not require other road users to take evasive action to avoid a collision with the ADS vehicle.]

[5.8.14. The driving behaviour of the ADS shall not cause a collision.]

5.8.15. The ADS shall comply with traffic rules and regulations relevant to its performance of the DDT. See Annex A for a method for converting traffic rules and regulations into elements applicable to scenario generation and the establishment of behavioural competencies.

[5.8.16. ADS shall comply with the traffic laws in nominal conditions, except when in specific circumstances or when necessary to enhance the safety of the vehicle's occupants and/or other road users.]

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

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

5.8.19. The ADS shall signal intended changes of direction.

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

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

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

5.9. ADS Performance of the DDT under Critical Traffic Scenarios

5.9.1. 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.

5.9.2. 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.

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

5.9.4. 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.

5.9.4.1. In the absence of a fallback-ready user, the ADS should fall back directly to a Minimal Risk Condition (MRC).

5.9.4.2. If the ADS is designed to request and enable intervention by a human driver, the ADS should execute an MRM in the event of a failure in the transition of control to the user.

5.9.4.2.1. Upon completion of an MRM, a user may be permitted to assume control of the vehicle.

5.9.4.2.2. The user should be permitted to override the ADS to assume full control over the vehicle.

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

5.9.5.1. The ADS should signal its intention to place the vehicle in an MRC to the ADS user or vehicle occupants as well as other road users (e.g., by hazard lights).

[5.9.6. In the event of a collision, the ADS shall stop the vehicle and deactivate.]

[5.9.6.1. ADS reactivation should not be possible until the safe operational state of the ADS has been verified.]

[5.9.7. The ADS shall avoid disruption to flow of traffic where possible.]

[5.9.8. The ADS shall avoid non-compliance with the traffic laws, rules and regulations where possible.]

[5.9.9. The ADS shall attempt to minimize collision severity.]

5.10. ADS Performance of the DDT under System Failure Scenarios

5.10.1 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.

[5.10.2. 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.]

[5.10.2.1. The ADS should perform self-diagnosis of faults in accordance with the OEMs prescribed list.]

[5.10.2.2. The ADS should detect system malfunctions/abnormalities and evaluate system's ability to fulfil the entire DDT.]

5.10.3. The ADS shall be designed to protect against unauthorized access. The measures ensuring protection from unauthorized access should be provided in alignment with engineering best practices.]

[5.10.4. The ADS shall signal [faults/failures] compromising its capability to perform the entire DDT relevant to the ODD of its feature(s).]

[5.10.5. The ADS shall be designed to protect against unauthorized modifications to safety-critical hardware and software.]

[5.10.6. The ADS may continue to operate in the presence of [faults/failures] that do not prevent that ADS from fulfilling the safety requirements applicable to the ADS.]

[5.10.6.1. The limited operation of the ADS should comply to the normally applicable safety requirements.]

[5.10.6.2. For situations where the ADS is not able to perform the DDT safely, the ADS should have the function to prevent activation. If the ADS has OTA functionality, this function may be activated remotely if the authorities or the vehicle manufacturer determine that the ADS is unsafe.]

[5.10.7. The ADS shall signal [faults/failures] compromising its ability to execute the DDT.]

[5.10.7.1. The ADS should signal [faults/failures] affecting the ability to execute the DDT.]

[5.10.8. In the event the ADS is unable to continue to operate, it shall either attempt to transition control to the fallback user or achieve a minimal risk condition. If the fallback user does not respond, it shall achieve a minimal risk condition.]

Note: Section 5.11. has been subject to comments in its entirety, including a request to review applicability of the proposed requirements to ADS. Therefore, the section should be considered as "bracketed" until FRAV conducts its review.

[5.11. Interactions between Users of ADS Vehicles and the ADS

5.11.1. Until now it has always been clear who's driving, who is responsible for performing the driving task, not only for controlling the vehicle but also for perceiving and interpreting the environment and for choosing a cause of action. That clarity is fading with the introduction of automation in the vehicle and will become even less clear with the introduction of automated driving systems (ADSs) where it concerns vehicles equipped with ADS that can also be driven by a human being inside the vehicle.

[5.11.2. In vehicles that can still be driven by a human every part of the driving task that is not automated needs to be performed by a human and every part of the driving task that is not 'perfectly' automated needs to be compensated for by a human. It therefore has to be clear who performs which part of the driving task during a trip. It has to be clear what a human can and cannot do while the ADS performs (a part of) the driving task. It has to be clear when the ADS can no longer perform the driving task and the human has to take over. It has to be clear if the ADS is activated or can be activated. This kind of clarity is essential for safety, essential for a safe use of the ADS. And this clarity is provided through the interaction between the human and the ADS. The interaction is more than the interface and includes for example how an ADS 'behaves' in the perception of its user (e.g., if braking then standby mode; not only how much it decelerates).]

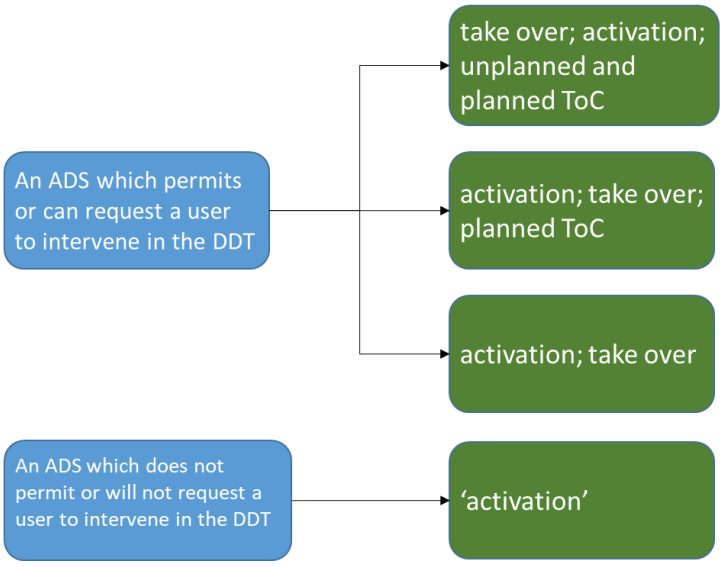
5.11.3. The following recommendations mainly focus on vehicles that can also be driven by a human. The recommendations applying to vehicles that cannot be driven by a human being will be indicated in ????

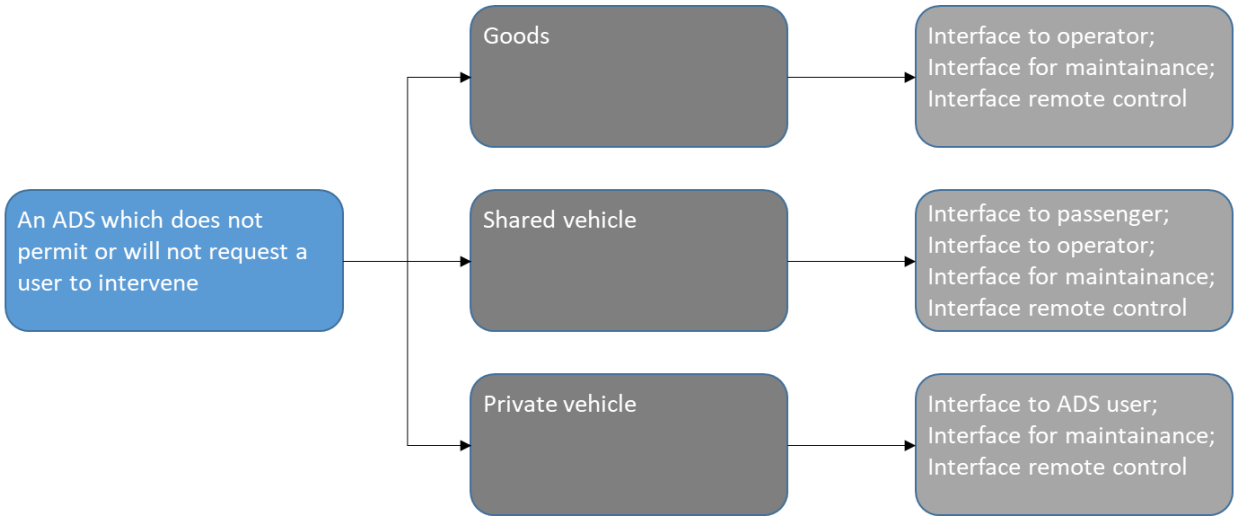
Considerations

Vehicle that can (still) be driven by a user

Vehicle that can be driven by maintenance personnel (not 'ordinary' user) or steward

Vehicle that can be driven by remote operator





5.11.3.1. The ADS and its features shall have a high-level commonality of design of the user interaction, and the interface.

5.11.3.1.1. The ADS should be designed to foster a level of trust that is aligned with its capabilities and limitations to ensure proper use of the system

5.11.3.1.2. The operation of the interaction shall at least have in common:

(a) The sequence of actions and states in the activation of the ADS

(b) The sequence of actions and states in the transition of control process from the ADS to the user

(c) The sequence of actions and states in the de-activation of the ADS

(d) The role of the user after a transition of control from the ADS to the user or after the deactivation of the ADS. This role shall normally be a fully engaged driver without any control assistance (temporarily intervening safety systems such as ESC will remain activated)

5.11.3.1.3 The interaction should be simplified:

(a) .....

(b) [Limit the number of potential transitions]

(c) [Limit the number of settings]

(d) [Limit the number of different interaction modes]

5.11.4. A high-level commonality in the interaction processes between the vehicle and a user for all brands and models helps drivers to develop and apply a single mental model of how their responsibilities relate to the level of automation and of how to interact with the systems. It also helps to reduce the risk of user confusion (e.g., mode confusion) when changing vehicle.

5.11.4.1. The ADS HMI shall provide clear, conspicuous and unambiguous information to support comprehension by the user.

5.11.4.1.1. The vehicle shall indicate its ADS capabilities in terms of their automated [features] and their ODD.

5.11.4.1.2. The ADS shall inform the user on the current conditions:

(a) ADS status information

(b) The availability of automated features

(c) Responsibility

(d) Permitted NDRA or not-permitted NDRA

(e) Potential roles to activate

(f) “Standard” information

(i) [.....]

(g) ADS failure information

5.11.4.1.3. The ADS shall inform the user in time on the upcoming conditions:

(a) ODD boundaries

(b) Upcoming actions or change in roles

(c) Oncoming decisions/manoeuvers

(d) Estimated time until take over in normal conditions

(e) Transition-related communication.

5.11.4.1.4. The ADS shall ensure that safety related information is prioritised and presented in a clear and unambiguous manner.

5.11.5. To ensure that there is no mode confusion or a lack of clarity about responsibilities of the ADS and the user or a lack of clarity about the capabilities of the ADS it is essential that specific kind of information needs be presented such that the information is well received and well understood.

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

5.11.5.1.1. The controls dedicated to the ADS shall be clearly distinguishable from other controls

5.11.5.1.2. The ADS shall be designed to prevent inadvertent activation or deactivation

5.11.5.1.3. The ADS shall provide feedback when the user attempts to enable unavailable functions

5.11.6. For a safe use of the ADS mode confusion needs to be avoided. Therefore, it is essential that an ADS cannot be activated by mistake within the ODD nor that it can de-activated. Misuse of the ADS can for example be that a fall-back user is sleeping while the ADS performs the driving task.

5.11.6.1. The ADS shall ensure safe ADS feature activation.

5.11.6.1.1 The ADS shall inform the user that preconditions for activation are met

5.11.6.1.2. The activation shall follow a common sequence of actions and states

5.11.6.1.3. The ADS shall provide confirmation that the system is activated

5.11.7 Paragraphs 5.11.6.1, 5.11.8, and 5.11.9. strongly rely on the commonality concept. That’s why some of the detailed provisions are also presented under paragraph 5.11.3.1. To avoid mode confusion after a transition of control the transition should be to a fully engaged driver without any assistance. If assistance would still be possible this could, for example, be indicated and the user could activate that specific kind of ADAS.

5.11.8. An ADS which permits a transition of control shall be designed to ensure safe transitions of control.

5.11.8.1. The Transition of control process shall follow a common sequence of actions and states

5.11.8.2. Transition of control shall return to a common default user role

(a) The role of the user after a transition of control from the ADS to the user or after the deactivation of the ADS. This role shall normally be a

fully engaged driver without any control assistance (temporarily intervening safety systems such as ESC will remain activated)

5.11.8.3. The ADS shall continuously verify whether the user is available for the Transition of Control and

(a) adapt the Transition of Control process, including the time budget where feasible, to the state of the user and/or to the ADS.

(b) warn the user if not available when required

(c) register user response indicating readiness for transfer of control

5.11.8.4. The ADS shall verify that the user is in stable control of the vehicle to complete the Transition of Control process

5.11.8.5. During transition, the ADS shall remain active until the Transition of control has been completed or the ADS reaches a minimal risk condition

5.11.9. An ADS which permits user-initiated takeovers of control shall be designed to ensure a safe user-initiated takeover process.

5.11.9.1. Such ADS shall allow the user to to initiate a take-over process.

5.11.9.2. The deactivation shall follow a common sequence of actions and states in the transition of control (change of user roles)

5.11.9.3. The ADS shall momentarily delay deactivation of driving control when immediate human resumption of control could compromise safety.

5.11.9.4. The ADS shall provide clear, specific feedback of the completion of a user initiated take over.

5.11.9.5. The user initiated take over shall return to a common default user role being the driver.

(a) The role of the user after a transition of control from the ADS to the user or after the deactivation of the ADS. This role shall normally be a fully engaged driver without any control assistance (temporarily intervening safety systems such as ESC will remain activated)

5.11.10. The ADS shall be supported by documentation and tools to facilitate user understanding of the functionality and operation of the system.

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

5.11.10.1.1. The details of their user-centred design process

5.11.10.1.2. Its intended educational approach:

(a) Theoretical and practical training

(b) How its HMI design aligns with common HMI and interaction

5.11.10.1.3. Owner's manual describing at least:

(a) An operational description of ADS' (features) capabilities and limitations (the information should also refer to specific scenarios)

(b) A description of the roles and responsibility of driver/user and ADS when an ADS (feature) is on/off

(c) A description on the permitted transitions of roles and the procedure for those transitions

(d) A general overview of NDRA allowed when an ADS feature is active

5.11.10.2. The ADS manufacturer / vehicle manufacturer (as appropriate) shall create the following in-vehicle tools such that

5.11.10.2.1. the ADS supports the user in correct operation (coaching)

5.11.10.2.2. the ADS gives prompt feedback on erroneous operation

5.11.11. The documentation and tools that are provided by the ADS manufacturer / vehicle manufacturer on the ADS will ensure that the user of an ADS can develop a general mental model of how the system functions, its capabilities, the user responsibilities and a more specific mental model of how to interact with the systems. A correct mental model is necessary for correct usage and expectations of the ADS.

5.11.11.1. The HMI of an ADS which permits a transition of control shall be integrated with the entire vehicle HMI

5.11.11.1.1. The vehicle and ADS HMI need to take into account potential impairments of users (such as colour blindness, impaired hearing) which do not require specific hardware adaptations of the vehicle.

5.11.12. To avoid mode confusion it has to be clear to the user the differences between the different levels of automation that can be available in a vehicle so that an ADAS mode can never be confused with an ADS mode.

5.11.12.1. A dedicated ADS vehicle shall provide vehicle occupants with means to request a minimal risk manoeuvre to stop the fully automated vehicle.

5.11.12.2. A dedicated ADS shall ensure that it operates within operational relevant legal boundaries.]

5.12. Safety throughout the Useful Life of the ADS Vehicle

5.12.1. This section addresses the safe use of an ADS during the useful life of the ADS vehicle.

[5.12.1.1. The ADS should signal required system maintenance to the user.]

[5.12.1.2. The ADS shall detect malfunctions and abnormalities that compromise its capability to perform the entire DDT as provided by the manufacturer under Section 4.]

[5.12.1.3. The ADS shall perform self-diagnosis of system integrity in accordance with the manufacturer documentation provided under Section 4.]

[5.12.1.4. The ADS shall be accessible for the purposes of maintenance and repair to authorized persons.]

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

[5.12.1.6. 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.]

[5.12.1.7. In response to a fault, the ADS may limit the ODD to enable 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 within the limited ODD.]

[5.12.1.8. Remote termination of the availability of the ADS or its feature(s) to the user by an authorized entity shall be possible in ADS vehicles equipped with wireless connectivity enabling access to the ADS (e.g., over-the-air software update capability).]

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

[5.12.1.10. Pursuant to vehicle damage, ADS reactivation shall not be possible until the safe operational state of the ADS has been verified.

6. Appendices

A. ODD Descriptions for ADS Features

[This appendix provides mandatory guidelines for the documentation of ODD conditions under which an ADS is designed to operate. These guidelines promote consistency across manufacturer descriptions of each ODD to facilitate use of this information in ADS assessments.]

ODD Documentation

1. To the extent provided, the documentation shall use the terms and measurement units provided in the Compendium of ODD Conditions.

2. The manufacturer may describe additional conditions where not provided for in the Compendium of ODD Conditions.

3. Each ODD condition and/or boundary shall be defined in measurable and/or verifiable terms.

Note: The inclusion of a compendium has been questioned in its entirety. Therefore, this section should be considered in brackets.

[Compendium of ODD Conditions

1. Precipitation (rain, snow)

2. Time of day (light intensity, including the case of the use of lighting devices)

3. Visibility

4. Road and lane markings

B. Object and Events

This appendix provides a listing of objects and events that may be relevant to ADS performance of the DDT within the ODD of a feature.

1. Motor vehicle

2. Motorcycle

3. Cyclist

4. Pedestrian

5. Stationary obstacle

6. Road accident scene

7. Road safety agent

8. Law enforcement agent

9. Emergency vehicle

C. Material to be Included in the Owner's Manual

[This appendix provides a list of information that shall be provided at a minimum in the vehicle owner's manual.]

1. An operational description of ADS' (features) capabilities and limitations (the information should also refer to specific scenarios).

[2. A description of the roles and responsibility of driver/user and ADS when an ADS (feature) is on/off.]

3. A description on the permitted transitions of roles and the procedure for those transitions.

[4. A general overview of NDRA allowed when an ADS feature is active.]

7. Annexes

A. Approach to Derive Verifiable Performance