Guidelines and Recommendations
concerning
Safety Requirements for Automated Driving Systems

1. Purpose of this document

1.1. FRAV has established this document to facilitate and record its work in progress. Contents of this document may change in accordance with FRAV decisions.

1.2. This document may inform interested parties on the status of work within FRAV.

1.3. This document is for informational purposes and should be read as a work-in-progress, not as a formal or informal proposal to establish requirements under WP.29 procedures pursuant to the 1958, 1997, and/or 1998 Agreements.

1.4. This document provides recommendations for ADS safety requirements intended to inform WP.29 discussions on future initiatives respectively under the 1958, 1997, and/or 1998 Agreements.

1.5. Where applicable, the text uses the verbal forms "shall" and "may"; however, these paragraphs should be understood within the context of providing recommendations (paras. 1.3. and 1.4. above).

2. Definitions

2.1. *"Automated Driving System (ADS)"* means the hardware and software that are collectively capable of performing the entire DDT on a sustained basis.

2.2. *"(ADS) feature"* means an application of ADS hardware and software designed specifically for use within an ODD.

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

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

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

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

2.6.1. The DDT excludes strategic functions such as trip scheduling and selection of destinations and waypoints.

2.6.2. The operational and tactical functions of the DDT can be logically grouped under three general categories:

2.6.2.1. Sensing and perception, including:

2.6.2.1.1. Monitoring the driving environment via object and event detection, recognition, and classification.

2.6.2.1.2. Perceiving other vehicles and road users, the roadway and its fixtures, objects in the vehicle's driving environment and relevant environmental conditions.

2.6.2.1.3. Sensing the ODD boundaries, if any, of the ADS feature.

2.6.2.1.4. Positional awareness.

2.6.2.2. Planning and decision, including

2.6.2.2.1. Prediction of actions of other road users.

2.6.2.2.2. Response preparation.

2.6.2.2.3. Maneuver planning.

2.6.2.3. Control, including

2.6.2.3.1. Object and event response execution.

2.6.2.3.2. Lateral vehicle motion control.

2.6.2.3.3. Longitudinal vehicle motion control.

2.6.2.3.4. Enhancing conspicuity via lighting and signaling.

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

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

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

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

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

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

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

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

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

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

2.17. *"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.

2.18. *"(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. Guidelines for ADS descriptions

3.1. General considerations

3.1.1. ADS may be designed for specific purposes and to operate under prescribed conditions.

3.1.2. The conditions under which an ADS is designed to operate are known collectively as the Operational Design Domain (ODD).

3.1.2.1. The ODD conditions 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.

3.1.3. ADS may or may not be designed to transfer control to a qualified driver in the vehicle. The roles and responsibilities of an ADS user differ depending upon the ADS configuration, intended uses, and limitations on its use.

3.1.4. ADS safety requirements need to address the diversity of configurations, intended uses, and limitations on use while addressing usage specifications of individual ADS.

3.1.5. Therefore, FRAV intends to provide guidelines for the manufacturer's description of an ADS, including measurable/verifiable ODD specifications, to enable the application of safety requirements to the ADS under assessment.

3.2. The manufacturer shall describe the ADS configuration and the intended uses and limitations on the use of its feature(s).

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

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

3.3.1. The ODD conditions addressed by the manufacturer shall, at a minimum, include:

3.3.1.1. Precipitation (rain, snow).

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

3.3.1.3. Visibility.

3.3.1.4. Road and lane markings.

3.3.1.5. Road surface adhesion

3.3.1.6. Country of operation.

3.3.1.7. V2x dependencies, if any.

3.4. The manufacturer shall establish terms for the correct use of the ADS.

3.4.1. The manufacturer shall provide written information on the intended uses and limitations on the use of the ADS feature(s).

3.4.2. The manufacturer shall describe means made available to the public to promote a correct understanding of the intended uses and limitations on the use of the ADS.

3.4.3. The manufacturer shall provide the following information for ADS designed to interact with an ADS vehicle user.

3.4.3.1. The manufacturer shall provide written information on the roles and responsibilities of the ADS vehicle user(s), including activities other than driving.

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

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

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

3.4.3.5. The manufacturer shall provide information detailing the human-machine interactions, including HMI tell-tales, indicators, and displays.

4. ADS safety recommendations

4.1. ADS performance of the DDT

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

[Each ADS feature shall be subjected to traffic scenarios relevant to its ODD as declared by the manufacturer in accordance with the guidelines provided under paragraph 3.3. above. The ODD-based scenario-generation framework provides a worldwide process for applying ODD elements to derive nominal scenarios (see flowchart). ADS capability to perform the DDT shall be demonstrated via the feature's response to each scenario. The

Commented [CJ1]: Should define different user's responsibilities. Passengers on a shuttle will have different responsibilities such as requesting the vehicle to make a stop compared to a fallback user who may have to take control of the DDT.

Commented [PA2R1]: Perhaps it would be good for FRAV to add some illustrative example here adding...."such as, but not limited to, requesting the vehicle to make a stop; requesting the vehicle to make an emergency stop; requesting safety/security assistance from a remote monitor etc."..

Commented [CJ3]: Who is the recipient of these instructions? General public, regulators, first responders etc. might need this information. Think about vehicle use case as well. For example, shuttle users may need instructions on how to request a stop or initiate an emergency brake.

AVSC document *Best Practice for First Responder Interactions with Fleet-Managed Automated Driving System-Dedicated Vehicles* indicates that Developers and manufacturers should provide instructions in the interaction plans for safely disengaging the drive system, ensuring the ADS-DV will not self-drive, and ensuring safe operations around the vehicle.

Instructions could also be communicated via diagrams, graphics, videos.

ADS shall demonstrate behavioural competencies relevant to the scenarios (described in an anncx). The cumulative outcome of the ADS feature responses across the relevant scenarios shall demonstrate fulfillment of paragraph 4.1.1.]

- **Definition of DDT**
- **Guidelines for ODD descriptions**
- **ODD-based scenario-generation method, covering behavioural competencies and nominal scenarios**

4.1.2. The ADS shall recognize the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 3.3.

[Each ADS feature shall be subjected to traffic scenarios relevant to its ODD as declared by the manufacturer in accordance with the guidelines provided under paragraph 3.3. above. The ODD-based scenario-generation framework provides a worldwide process for applying ODD elements to derive nominal scenarios (see flowchart). ADS recognition of ODD conditions and boundaries shall be demonstrated via the feature's response to the ODD conditions across the scenarios. The cumulative outcome of the ADS feature responses across the relevant scenarios shall demonstrate fulfilment of paragraph 4.1.2.]

- **Proposal for requirement to address exceeding ODD boundaries (responses to ODD conditions per ADS design)**
- **Guidelines for ADS feature ODD descriptions**
- **ODD-based scenario generation method**

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

[Each ADS feature shall be subjected to traffic scenarios relevant to its ODD as declared by the manufacturer in accordance with the guidelines provided under paragraph 3.3. above. ADS detection and response to objects and events shall be demonstrated via the feature's response to the conditions contained in each scenario. The properties and behaviours of scenario objects shall be consistent with an OEDR framework designed to enable the integration of assumptions regarding the physical, functional, and behavioural properties of these scenario objects as relevant to ensuring road safety. The responses shall fulfil the global safety requirements. The cumulative outcome of the ADS feature responses across the relevant scenarios shall demonstrate fulfilment of paragraph 4.1.3.]

4.1.4. The ADS shall comply with ~~safety-relevant~~ all applicable traffic **rules and regulations in the jurisdiction where it is operating (including those) relevant to its performance of the DDT and** the ODD of the feature in use.

[Document 5 shall provide a methodology for converting traffic laws into ODD and performance components. Each ADS feature shall be subjected to traffic scenarios relevant to its ODD as declared by the manufacturer in accordance with the guidelines provided under paragraph 3.3. above. The scenarios shall integrate the ODD components extracted from the relevant traffic laws per the conversion methodology. ADS compliance with the prevailing traffic laws of each scenario shall be demonstrated via the feature's response under each scenario per the DDT performance elements extracted via the conversion methodology. The cumulative outcome of the ADS feature responses across the relevant scenarios shall demonstrate fulfillment of paragraph 4.1.4.]

4.1.4.1. See Appendix [x] for recommendations on the conversion of traffic laws into verifiable criteria for ADS assessment.

4.1.5. The ADS shall interact safely (and something akin to comfort, not upsetting—natural, reasonable, expected, predictable…see detailed provisions in Table 1) with other road users.

[Each ADS feature shall be subjected to traffic scenarios relevant to its ODD as declared by the manufacturer in accordance with the guidelines provided under paragraph 3.3. above. Per paragraph 4.1.3., these scenarios shall include other road users foreseeable [ensure interpretation that covers unusual or illegal users which are nonetheless foreseeable] **within the ODD of the ADS feature. The ADS shall respond to the presence of other road users within each scenario in accordance the traffic laws prevailing under the scenario per paragraph 4.1.4. and within the DDT performance expectations as defined by one or more safety models provided in Document 5. The cumulative outcome of the ADS feature responses across the relevant scenarios shall demonstrate fulfilment of paragraph 4.1.5.]**

[Would this requirement address "traffic disruption"? Does this ensure ADS behaviors that would not cause a collision?]

4.2. ADS interactions with ADS vehicle users **[Should this section be moved to follow after the current sections 4.3. and 4.4. given the intention to address ADS responses to safety-critical situations and failure modes at least in part via the ODD-based approach to scenario generation and assessment against safety models?]**

[The Users workstream initially provided input focused on identifying possible user roles. Interactions are dependent upon

Commented [CJ4]: Do we need to specify relevance to ODD and DDT? Can we say "all applicable traffic rules and regulations in the respective jurisdiction where it is operating."

Commented [CJ5]: Canada recommends the following text: "The ADS shall interact in a safe and predictable manner with other road users.

Including predictable is important for ORUs to understand the system's movements so they can respond accordingly. Vehicle should act in consistent manner. Behaviour should be predictable.

Commented [CJ6]: It could be problematic if safety recommendations are tested unidimensionally. Canada recommends adding the following text at the end of section 4.1. "The ADS must perform the whole DDT with interactions between a complex combination of objects, events and ODD factors. When assessing the ADS it is important to consider testing against multiple safety requirements rather than testing against requirements individually."

these roles. For example, a fallback user would not be involved in activating an ADS feature; the feature has to be in use in order for a user to be in the role of fallback to the ADS. Input has been provided suggesting that ADS configurations/use cases can be differentiated based on whether the vehicle is designed to transport human beings and whether such human beings would have any roles in vehicle operation or be limited to passengers. In-vehicle occupant roles have been identified as "driver", "fallback user", or "passenger", aligning with a detailed provision in Table 1 that interactions should be simplified, including by limiting the number of roles. Additional input has suggested possible external roles such as dispatcher or remote operator.

Therefore, should the user interaction requirements be structured to enable objective decisions on which requirements apply to which ADS use cases based on the possible roles of human users of the ADS vehicle. If so, should FRAV define user roles, create subsections of requirements based on these roles, and add provisions requiring the manufacturer the declare the permissible roles of users of the ADS vehicle?

How can the requirements below and the detailed provisions in Table 1 be transformed into objective and verifiable requirements for ADS interactions with users performing these various roles?]

Vehicle/ADS configuration versus user roles. Regulation should define user roles. Repetition issue—would we repeat same functional requirements under each role. [15 user roles?]

User workstream will provide a proposal in September for a path to feasible verifiable requirements/recommendations, including proposal on whether requirements should have a logical structure and if so, what structure (e.g., how to break down into subsets of requirements that can be objectively applied to various ADS configurations/use cases). Review Table 1 detailed requirements to bring into main body of D5.

4.2.1. User interaction with and the interface of ADS (features) shall have a high-level commonality of design.

4.2.2. The ADS HMI shall provide clear and unambiguous information to the user.

4.2.3. The ADS shall be designed to prevent misuse and errors in operation.

4.2.4. The ADS shall ensure safe ADS feature activation.

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

4.2.6. An ADS which permits user takeovers of control shall be designed to ensure safe user-initiated takeovers.

Commented [CJ7]: Should we also include remote monitor. Someone who would not take control of the DDT or dispatch but only monitor the vehicle.

Commented [CJ8]: Yes this would be a good idea and important for future deployment to ensure consumer awareness.

Commented [CJ9]: Are we talking about all users? We should clarify this. We are supportive of this being all ADS users.

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

4.3. ADS management of safety-critical situations

[It seems that this section can be further elaborated per the work of the DDT workstream. Conceptually, each ADS feature would be subjected to critical scenarios relevant to its ODD as declared by the manufacturer per the guidelines under paragraph 3.3. Safety models would address the feasibility of collision avoidance given the dynamic behaviors of objects in the scenarios, providing boundaries between collision avoidance and crash mitigation. The ADS would be expected to avoid collisions where feasible and execute a collision mitigation response where contact is unavoidable. It seems appropriate for Document 5 to have provisions addressing collision avoidance and traffic disruption per the AV Framework Document.]

[There seem to be at least two subcategories for safety-critical situations: ADS response critical scenarios and ADS post-crash behaviour.]

- **Requirement to address (unforeseen) ODD exit (e.g., encountering icy roadway)—possible degraded performance/fallback)**
- **Short-duration, temporary excursion from ODD versus full exit. Would transient exits be part of nominal DDT capabilities (i.e., managed by ADS design)?**
- **Is sudden ODD exit a critical situation or under nominal? Is the critical section limited to ORU behaviours?**
- **Where are requirements for successfully navigating critical scenarios (collision avoidance as opposed to executing fallbacks)? Unforeseen situations due to unforeseen ORU actions?**

4.3.1. 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 (failure part should be in failure section, not critical situations section) or in the event of an exit from the ODD. **[Should this be moved under "ADS management of system failures"?]**

Commented [CJ10]: Yes we agree to move this to management of system failures.

4.3.2. The ADS shall **[externally?]** signal its intention to place the vehicle in an MRC. ADS shall signal internally and externally. This paragraph covers external signal—agree that internal signal should be covered by user-interactions requirements. Requirement involves sequence so more than signalling intention—includes procedure (which could involve driver recovery). Be careful not to confuse external signalling for hazard situation with "external signalling" as being discussed in

relation to GRE AVSR cooperation. Don't contradict what expected from human driver.

4.3.3. Pursuant to a traffic accident, the ADS shall stop the vehicle.

4.4. ADS management of system failures

4.4.1. The ADS shall detect and respond appropriately to system malfunctions and abnormalities relevant to its performance of the DDT. Take diversity of scenarios/context into account. Allowing system to be hacked is a failure of the system. System response while driving—need to integrate ADS response into requirement.

[Paragraph 3.2.1. states that the manufacturer shall declare faults detectable by the ADS. Presumably, there could be test procedures to induce system faults. The VMAD virtual testing pillar has some references to applying this method to assess ADS responses to malfunctions and abnormalities.]

4.4.2. The ADS shall be designed to protect against unauthorized access to the ADS functions. **[Does this relate to user interactions and system maintenance?]** Refers to external threats like cyber security. What is relationship with UN R155? Generally referring to cyber security. ADS would be subject to UN R155/Guidelines under 1998 Agreement.

4.4.3. The ADS shall signal [faults/failures] compromising its capability to perform the entire DDT relevant to the ODD of its feature(s). **[Signal to whom? It would seem that signaling to a user would be covered under section 4.2. Does this relate to 4.5.1. on signaling required maintenance? It would seem that 4.3.1. relates to signaling a fallback to an MRC. Presumably, a fallback to a user could be a permissible response.]**

4.4.4. The ADS shall be designed to protect against unauthorized modifications to safety-critical hardware and software. **[Should this be moved to the maintenance section? This does not concern ADS management of a failure.]** **Failure to prevent tampering is a system failure. Detection and coping.**

4.4.5. 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.

[This seems to be within the scope of the DDT workstream concept where the ADS feature would be subjected to "failure scenarios".]

4.5. ADS maintenance of a safe operational state.

Issue of vehicle communications and whether working. If change sign, vehicle can see; if change traffic rule, how would ADS capture? Means to note rule changes and ensure ADS updates?

UN R155/R156 address software so maintenance here mainly hardware?

4.5.1. The ADS should signal required system maintenance to the user [not really ADS user—concept in UK of vehicle keeper].

[Does this relate to user interactions? Does this relate to the manufacturer documentation (i.e., periodic maintenance)?

4.5.2. The ADS should be accessible for the purposes of maintenance and repair to authorized persons.

[How does one determine who is an "authorized person"? How does this relate to 4.4.4. on protecting the ADS against "unauthorized modifications"?]

Relates to principles of training and education.

4.5.3. ADS safety should be ensured in the event of discontinued production/support/maintenance.

[Do we have ideas for what response might be permissible? What would happen if an ADS could not be updated to handle new scenarios? Would it be permissible for an ADS to continue to operate in the knowledge that it would fail to respond appropriately to an identified scenario added after its initial certification?] How was this handled under cyber security/OTA updates? If required updates cannot be effected, ADS has to go away (cannot be used anymore)? FRAV should provide guidance to CPs? UNECE mechanism exists in UN R130 requesting CPs to provide info (e.g., lane widths in countries). Driver's license analogy: keep license even though traffic laws evolve. ADS frozen if cannot be updated, but still can be used at state of latest update? EN50126-1:2017 standard. Japan (FRAV-21) proposal to require functionality to enable remotely preventing activation/disabling ADS. Must have responsible entity for ADS—can't have vehicles not backed by responsible entity. UN R157 prohibits continued operation of system that can no longer meet requirements. Manufacturer required to have process for managing continued compliance with requirements over vehicle lifetime. Management-based requirement (ref. CSMS, SUMS)? Should be first step in addressing this issue?

4.6. The following table provides additional information on the elaboration of ADS safety requirements for use under the New Assessment/Test Method (NATM).

Commented [CJ11]: An entity should always be required to remain responsible for an ADS and would be responsible for updates, receiving notifications that the system needs maintenance, etc. This could be the manufacturer or a third party who would be qualified to undertake this work. Some entity should always remain responsible for an ADS otherwise the system should be decommissioned.

Commented [CJ12]: User may only be a passenger in a shuttle for example so not all users would be required to be aware that the system requires maintenance. We should specify to whom the ADS will signal maintenance issues. If the vehicle is a shuttle the system might signal to a remote supervisor.

Commented [CJ13]: Recommend adding the following: An entity should always remain responsible for the ADS. An entity must always remain liable for the ADS to ensure that it remains compliant and to address any potential liability issues. In the event that an entity fails to remain responsible, the ADS should be decommissioned.

[The table was introduced as a means to move from high-level requirements to a more detailed level and then to verifiable requirements. The WP.29 secretariat has informed FRAV that this kind of table with bullet lists is not acceptable for legal texts (e.g., GTR, UN Regulations). Should the workstreams be tasked with reaching agreement on provisions that can be moved into the ADS safety requirements (section 4.)?]

4.6.1. The table is structured in accordance with five core safety aspects:

4.6.1.1. The ADS should drive safely.

4.6.1.2. The ADS should interact safely with the ADS vehicle user(s).

4.6.1.3. The ADS should manage safety-critical traffic situations.

4.6.1.4. The ADS should safely manage failure modes.

4.6.1.5. The ADS should maintain a safe operational state.

4.6.2. The left column ("safety requirements") reproduces ADS safety recommendations presented above (paras. 4.1-4.5. inclusive).

4.6.2.1. These recommendations have been generally accepted by FRAV as a basis for further elaboration of safety requirements.

4.6.3. The right column ("detailed provisions") provides additional information concerning the elaboration of the safety recommendations in the left column.

4.6.3.1. ADS safety requirements shall be verifiable and/or measurable under the NATM tools and methods.

4.6.3.2. The right column highlights aspects that may be suitable for the development of such measurable/verifiable criteria for assessing ADS fulfilment of the safety requirements. These items are all under discussion and not yet agreed by FRAV.

4.6.3.3. The elaboration of these safety requirements involves collaboration with the Validation Methods for Automated Driving informal working group, including consideration of the following aspects.

4.6.3.3.1. Consideration of traffic scenarios that define conditions the ADS may encounter, including nominal performance of the DDT, ADS responses to safety-critical traffic situations, and ADS responses to system failures.

4.6.3.3.2. Consideration of the assessment methods to be used in evaluating ADS performance against the safety requirements such as virtual testing, track tests, and under real-world driving on public roads.

4.6.3.3.3. Consideration of the procedures for determining ADS configurations, intended uses, and limitations on use to ensure assessments appropriate across the diversity of ADS.

4.6.3.3.4. Consideration of procedures for monitoring the performance of ADS in the field, including attention to data collection and analysis to provide appropriate reporting on performance metrics.

4.6.3.4. Based on the above, FRAV anticipates the development of measurable/verifiable criteria to enable application of the NATM methods and tools in assessing compliance with the recommended requirements provided in Table 1.

Table 1. ADS Safety Recommendations and Development of Detailed Provisions

	Safety Recommendations	Detailed Provisions (under discussion)
The ADS should drive safely.		
1.	The ADS shall be capable of performing the entire Dynamic Driving Task (DDT) within the ODD of its feature(s).	• The capability of the ADS to perform the entire DDT should be determined in the context of the ODD of the ADS • As part of the DDT, the ADS should be able to: o Operate at safe speeds. o Maintain appropriate distances from [other road users] by controlling the longitudinal and lateral motion of the vehicle. o Adapt its behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic). o Adapt its behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority).
2.	The ADS shall recognize the conditions and boundaries of the ODD of its feature(s) pursuant to the manufacturer's declaration under paragraph 3.3.	• The ADS should be able to determine when the conditions are met for activation. • The ADS should detect and respond when one or more ODD conditions are not or no longer fulfilled. • The ADS should be able to anticipate planned exits of the ODD • The ODD conditions and boundaries (measurable limits) should be established by the manufacturer. • The ODD conditions to be recognized by the ADS should include: o Precipitation (rain, snow) o Time of day (light intensity, including the case of the use of lighting devices) o Visibility o Road and lane markings

3.	The ADS shall detect and respond to objects and events relevant to its performance of the DDT.	• Objects and events might include, but are not limited, to:
		  ○ Vehicles, motorcycles, bicycles, pedestrians, obstacles
		  ○ Road accidents
		  ○ Road safety agents / enforcement agents
		  ○ Emergency vehicles
		• The ADS shall detect objects in and around its path of travel that exceed a minimum size.
		• The ADS shall recognize objects as static or mobile.
		• The ADS shall recognize markings and signals used to indicate priority vehicles within the ODD of its feature(s).
		• The ADS shall classify priority vehicles within the ODD of its feature(s) in accordance with the relevant traffic law(s).
		• The ADS shall yield the right of way to priority vehicles in service in accordance with the relevant traffic law(s).

4.	The ADS shall comply with safety-relevant traffic laws according to the ODD of the feature in use.	• ADS should 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.	The ADS shall interact safely with other road users.	• The ADS shall avoid collisions with safety-relevant objects where possible. • The ADS shall signal intended changes of direction. • The ADS shall signal its operational status (active/inactive) as needed.

Commented [CJ14]: It may be out of scope for FRAV to suggest circumventing traffic laws. Some traffic laws may provide flexibility to address situations such as initiating otherwise illegal maneuvers to avoid a collision while other jurisdictions may not allow this. FRAV may want to consider rewording this detailed provision. We would suggest the following text: "ADS should comply with the traffic laws in nominal conditions. If it becomes necessary to circumvent traffic laws in specific circumstances or when necessary to enhance the safety of the vehicle's occupants and/or other road users the ADS should take into consideration how to do so within the respective traffic laws of the jurisdiction."

The ADS should interact safely with the ADS vehicle user(s).		

6.	User interaction with and the interface of ADS (features) shall have a high-level commonality of design.	• 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.[1]
		• The operation of the interaction shall have in common:
		  o use of common sequence of states in the transition/activation/overriding/…
		• The interaction should be simplified:
		  o Limit the number of roles
		  o Limit the number of potential transitions
		  o Limit the number of settings
		  o Limit the number of different interaction modes

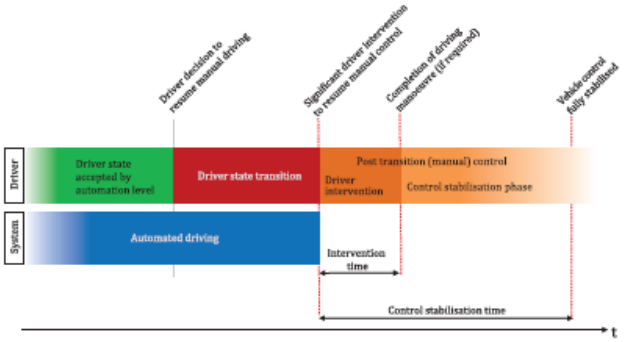
7.	The ADS HMI shall provide clear and unambiguous information to the user.	• The vehicle shall indicate its ADS capabilities in terms of their automated features and their ODD.
		• The ADS shall inform the user on the current conditions:
		  o ADS status information
		  o The availability of ADS features
		  o User Role
		  o Responsibility
		  o Permitted NDRA
		  o Potential roles to activate
		  o "Standard" information:
		  ▪ Vehicle speed, range, and Time to Fuel
		  o ADS failure information
		• The ADS shall inform the user on the upcoming conditions:
		  o ODD boundaries
		  o Upcoming actions or change in roles
		  o Oncoming decisions/manoeuvers
		  o Estimated time until take over in normal conditions
		  o Transition related communication.
		• The ADS shall ensure that safety related information is prioritized and presented in a clear and unambiguous manner.

8.	The ADS shall be designed to prevent misuse and errors in operation.	• The ADS shall be designed to prevent inadvertent activation or deactivation. • The controls dedicated to the ADS shall be clearly distinguishable from other controls. • The ADS shall provide feedback when the user attempts to enable unavailable functions.

[1] Calibrated Trust: A state where the automation user's trust in the automation, as well as their use of the automation, is appropriately adjusted to the actual performance of the automation (McGuirl & Sarter, 2006). See P. 89 Human Factors Design Guidance for Level 2 and Level 3 Automated Driving Concepts (nhtsa.gov)

9.	The ADS shall be designed to ensure safe ADS feature activation.	• The ADS shall inform the user that preconditions for activation are met. • The activation should follow a common sequence of actions and states: o Common sequence to be a pass/fail criterion. • The ADS shall provide confirmation that the system is activated.

10.	An ADS which permits a transition of control shall be designed to ensure safe transitions of control.	• The interaction shall follow a common sequence of actions and states in the Transition of control (change of user roles):
		  o Common sequence to be a pass/fail criterion.
		• Transition of control shall return to a common default user role (to prevent mode confusion and other risks):
		  o This shall normally be fully engaged driving (conventional driver; safety systems such as ESC will remain activated).
		  o Common default user to be a pass/fail criterion.
		• The ADS shall continuously verify whether the user is available for the transition of control and
		  o adapt the Transition of Control process, including the time budget where feasible, to the state of the user and/or to the ADS.
		  o warn the user if not available when required
		  o register user response indicating readiness for transfer of control.
		• The ADS shall verify that the driver is in stable control of the vehicle to complete the transfer of control to the user.
		• During transition, the ADS shall remain active until the transition of control has been completed or the ADS reaches a minimal risk condition.

11.	An ADS which permits user takeovers of control shall be designed to ensure safe user-initiated takeovers.	• The user is allowed to initiate a takeover of the ADS.
		• The deactivation shall follow a common sequence (change of user role).
		  ○ Common sequence to be a pass/fail criterion.
		 
		
		(ISO/TR 21959-1:2020(E))
		• The ADS may momentarily delay deactivation of driving control when immediate human resumption of control could compromise safety.
		• The ADS shall provide clear, specific feedback of the completion of a user initiated take over.
		  ○ The clear and specific feedback shall be a pass/fail criterion
		• The user initiated take over shall return to a common default user role being the driver.
		  ○ This shall normally be a fully engaged driver without any control assistance systems with the exception of mandated systems (conventional driver)
		  ○ Common default user role to be a pass/fail criterion

12.	The use of the ADS shall be supported by documentation and tools to facilitate the user in understanding the functionality and operation of the system.	Documentation:
		The ADS manufacturer / vehicle manufacturer (as appropriate) should create documentation available for audit on:
		• Its intended educational approach:
		  o Theoretical and practical training
		  o How its HMI design aligns with common HMI and interaction
		• Owner's manual describing at least:
		  o An operational description of ADS' (features) capabilities and limitations (the information should also refer to specific scenarios)
		  o A description of the roles and responsibility of driver/user and ADS when an ADS (feature) is on/off
		  o A description on the permitted transitions of roles and the procedure for those transitions
		  o A general overview of NDRA allowed when an ADS feature is active
		Tools (in-vehicle):
		• The ADS supports the user in correct operation (coaching)
		• The ADS gives prompt feedback on erroneous operation

13.	The integration of an ADS which permits a transition of control with the entire vehicle HMI shall be assured	• The entire HMI design should be defined and the integration with ADS HMI assured by analysis and/or test. • The vehicle and ADS HMI needs to take into account potential impairments of users (such as colour blindness, impaired hearing) which do not require specific hardware adaptations of the vehicle.
	ADS manufacturers shall follow a human centred design process of the vehicle. (footnote)	• Analyses of user needs and risk, setting safety and usability objectives, as well as specifying user requirements and ensuring user understanding and context • Producing design solutions to meet these requirements • Conducting evaluations, particularly real world testing on real users (i.e., not the engineers developing the products) • Human factors design and testing activities should be assigned to qualified personnel, with clearly defined roles and responsibilities, including process oversight and sign-off. • Device performance should be monitored in the field and this information should be used to set future design targets and evaluate designs against these requirements.[2]

[2] Evaluation should include an analysis of the user's correct interpretation of the actual driving mode and its affiliated responsibilities and (driving) tasks:
- In the moment of a mode transition.
- While driving with the same automation mode for a certain period of time

14.	Passenger-carrying ADS vehicles that may operate without a fallback user shall provide means for ensuring passenger safety.	• For the safety of the occupants, the ADS vehicle should:
		  ○ Stop in accordance with the designated route;
		  ○ Open the service doors when at a stop and close them before starting moving again;
		  ○ Achieve a minimum-risk condition (MRC) by demand of the vehicle occupants upon application of the designated control (button);
		  ○ Provide sound notification to the occupants in the case of emergency braking.
		• For the occupant information, the ADS vehicle should provide audio messages to the occupants about approaching a stop and starting the motion after a stop.
		• The ADS vehicle should provide voice communication between the occupant compartment and a remote operation dispatcher/assistance personnel.

The ADS should manage safety-critical situations.		
13.	The ADS shall execute a fallback response in the event of a failure in the ADS and/or other vehicle system that prevents the ADS from performing the DDT.	• In the absence of a fallback-ready user, the ADS should fall back directly to a Minimal Risk Condition (MRC) • 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 o Upon completion of an MRM, a user may be permitted to assume control of the vehicle o The user should be permitted to override the ADS to assume full control over the vehicle
14.	The ADS shall signal its intention to place the vehicle in an MRC.	• The ADS should signal its intention to place the vehicle in an MRC to: o ADS user or vehicle occupants o Other road users (e.g., by hazard lights)
15.	Pursuant to a traffic accident, the ADS shall stop the vehicle.	• ADS reactivation should not be possible until the safe operational state of the ADS has been verified.
The ADS should safely manage failure modes.		
16.	The ADS shall detect and respond to system malfunctions and abnormalities relevant to its performance of the DDT.	• The ADS should perform self-diagnosis of faults in accordance with the OEMs prescribed list • The ADS should detect system malfunctions/abnormalities and evaluate system's ability to fulfill the entire DDT
17.	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.
18.	The ADS shall signal [faults/failures] compromising its capability to perform the entire DDT relevant to the ODD of its feature(s).	
19.	The ADS shall be designed to protect against unauthorized modifications to safety-critical hardware and software.	
20.	The ADS may continue to operate in the presence of [faults/failures] that do not prevent that ADS from fulfilling the safety recommendations applicable to the ADS.	• The limited operation of the ADS should comply to the normally applicable safety requirements. • 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.

21.	The ADS shall signal [faults/failures] compromising its ability to execute the DDT.	• The ADS should signal [faults/failures] affecting the ability to execute the DDT.
The ADS should maintain a safe operational state.		
22.	The ADS should signal required system maintenance to the user.	
23.	The ADS should be accessible for the purposes of maintenance and repair to authorized persons.	
24.	ADS safety should be ensured in the event of discontinued production/support/maintenance.	

Appendix [x]

Conversion of Traffic Laws into Verifiable Criteria for ADS Assessment

[This appendix will provide recommendations on procedures for transforming traffic laws into verifiable criteria for determining ADS compliance with the laws.]

[Additional appendices]

[FRAV anticipates the development of safety models to enable scenario-specific and ODD-specific determinations on ADS compliance with certain DDT-performance provisions. This ODD-based approach to the development of safety models permits the application of local variables and assumptions in determining ADS compliance with relevant requirements.]