Transmitted by GRVA

Informal document **WP.29-186-08**
186th WP.29, 8-11 March 2022,
Agenda item 2.3

# Proposal for Guidelines and Recommendations concerning Safety Requirements for Automated Driving Systems

For information toWP.29 at its March 2022 session, based on GRVA-12-23

## 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 does not constitute a formal or informal proposal. FRAV will issue such proposals in one or more separate documents as determined and approved by the group.

## 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 application of ADS hardware and software 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 qualified human being engaged in dynamic control of the vehicle.

2.6. “Dynamic control” means the real-time execution of operational and tactical functions required to operate a vehicle based on perception, information processing, and decision making.

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

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

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

2.7.2.1. Sensing and perception, including:

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

2.7.2.1.2. Perceiving other vehicles and road users, the roadway and its fixtures, objects in the vehicle’s path, and relevant environmental conditions.

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

2.7.2.1.4. Positional awareness.

2.7.2.2. Planning and decision, including

2.7.2.2.1. Prediction of actions of other road users.

2.7.2.2.2. Response preparation.

2.7.2.2.3. Maneuver planning.

2.7.2.3. Control, including

2.7.2.3.1. Object and event response execution.

2.7.2.3.2. Lateral vehicle motion control.

2.7.2.3.3. Longitudinal vehicle motion control.

2.7.2.3.4. Enhancing conspicuity via lighting, signaling and/or gesturing, etc.

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

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

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

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

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

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

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

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

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

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

2.18. "Transition of control (TOC)" means a procedure by which the ADS engages the fallback user in dynamic control of the vehicle such that the fallback user assumes the role of driver upon completion.

2.19. "(ADS) User" means a human being engaged in the use of an ADS vehicle 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 covered 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 a fallback user.

3.4.3.1. The manufacturer shall provide written information on the roles and responsibilities of the fallback user, 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 fallback 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).

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.

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

4.1.4. The ADS shall comply with safety-relevant traffic laws according to the ODD of the feature in use.

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

4.2. ADS interactions with ADS vehicle users

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 be designed to 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.

4.2.7. 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.

4.3. ADS management of safety-critical situations

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.

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

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 to system malfunctions and abnormalities relevant to its performance of the DDT.

4.4.2. The ADS shall be designed to protect against unauthorized access.

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).

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

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 recommendations applicable to the ADS.

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

4.5. ADS maintenance of a safe operational state.

4.5.1. The ADS should signal required system maintenance to the user.

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

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

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

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.

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 for application of the safety requirements to the NATM methods and tools."