Informal Working Group on Functional Requirements for Automated Vehicles (FRAV) Progress Report to GRVA

1. Preface

This document provides a review of FRAV's work to date on safety requirements for Automated Driving Systems (ADS). The development of these requirements presents challenges because an ADS is tasked with the act of driving a vehicle. Driving involves not only the performance of the driver in controlling the vehicle motion but also in responding to the behaviors of other road users and conditions that may arise in the road environment. In the case of an ADS, an additional layer of complexity involves interactions between the ADS and the user(s) of the ADS vehicle as well as attention to system safety and safety throughout the life of the vehicle. While this paper describes FRAV's work, FRAV notes that its discussions have raised diverse points requiring additional attention towards defining clear and precise definitions and requirements. This document summarizes FRAV views and intentions while recognizing that aspects may be subject to change as the work progresses.

2. Definition of an ADS

2.1. Driving. Driving is a complex activity with traffic laws and codes of behavior based upon human cognitive strengths and weaknesses. Driving involves three behavioral levels: strategic (general trip planning: determination of trip goals, route, and modal choice, evaluation of costs and risks), tactical (maneuvering to negotiate the directly prevailing circumstances within the constraints of the general strategic goals), and operational (basic vehicle-control skills).[1] The levels relate to perception, information processing, and decision making under uncertainty.[2] The real-time operational and tactical functions required to operate a vehicle in on-road traffic are collectively known as the Dynamic Driving Task (DDT).[3] 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. Tactical functions include but are not limited to maneuver planning (motion control), enhancing conspicuity (lighting, signaling, gesturing, etc.), and interactions with other road users. Operational and tactical functions also include monitoring the driving environment (object and event detection, recognition, classification, and response preparation) and object and event response execution.

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

---

[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.

[2] Michon, J.A., 1979 (update 2008). "Dealing with Danger", Summary Report of the Workshop on Physiological and Psychological Factors in Performance under Hazardous Conditions with Special Reference to Road Traffic Accidents, Gieten, Netherlands, May 23-25, 1978.

[3] FRAV is discussing strategic, operational, and tactical functions in relation to ADS roles in performance of the DDT. Some elements that might be considered strategic could fall within a role of an ADS (for example, decisions that may be taken on the route(s) to follow in reaching a destination).

FRAV has tentatively agreed that the ODD refers to external conditions, including aspects such as speed ranges, road designs, uses, and conditions, weather conditions, and traffic densities.[4]

ADS may be designed to operate with or without a qualified driver in the vehicle. The roles and responsibilities of an ADS user differ depending upon its configuration, intended uses, and limitations on its use. FRAV has noted that user roles and responsibilities (and possibly other aspects) may also impose constraints on the use of an ADS.[5]

The diverse configurations covering driving automation systems and user roles and responsibilities have been categorized under six levels of automation in the SAE Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016). The level of automation and the ODD of an ADS describe a usage specification.

2.3. Automated Driving Systems. An ADS consists of hardware and software that are collectively capable of performing the entire DDT on a sustained basis. Driving automation systems that require human driver support to fulfill aspects of the DDT fall below the level of an ADS.

2.4. Automated Driving System functions. ADS integrate subsets of hardware and software designed to perform aspects of the DDT. ADS functions, in general, correspond to system-level capabilities integrated into the ADS design. A function enables the ADS to perform one or more elements of the DDT. A 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. Functions may ensure the correct use of the ADS and safe transfers of control to a user. Functions represent the first level of safety that an ADS must fulfill. These functions correspond to essential capabilities without which an ADS cannot be deemed safe in the operation of a vehicle.

2.5. Automated Driving System features. Although an ADS performs the entire DDT on a sustained basis, an ADS may be designed to operate within one or more ODD. Each set of ODD-specific capabilities has a unique set of constraints defining the conditions under which the ADS may be used. 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. ADS features may use some or all of the ADS functions.

3. Structure for ADS safety requirements

3.1. Scope. Because ADS will have diverse configurations, intended uses, and limitations, FRAV concluded that performance requirements should not be exclusively focused on particular ADS applications or usage specifications. Usage-specific requirements would result in unmanageable constellations of provisions while leaving open the risk of ADS applications falling outside the established requirements. Conversely, such requirements would risk safety requirements that would interfere with innovation and the evolution of ADS by artificially forcing ADS into particular use cases or ODD boundaries. Therefore, FRAV determined that ADS safety demanded a holistic approach covering all ADS configurations while enabling the application of requirements to individual ADS applications.

The requirements will address Category 1 and 2 vehicles as defined by Special Resolution 1; however, FRAV has noted that certain ADS vehicle configurations may fall outside the current vehicle definitions (including those in the Consolidated Resolution on the Construction of Vehicles—RE3—of the 1958 Agreement).

---

[4] FRAV is discussing constraints on the use of ADS. The constraints relate to the design and intended uses of the ADS and may include aspects such as a maximum speed boundary or constraints on permissible user activities while the ADS is in operation.

[5] FRAV has considered a proposal to define "Operational Domain Conditions" (ODC) but has not reached consensus decision pending the elaboration of safety requirements.

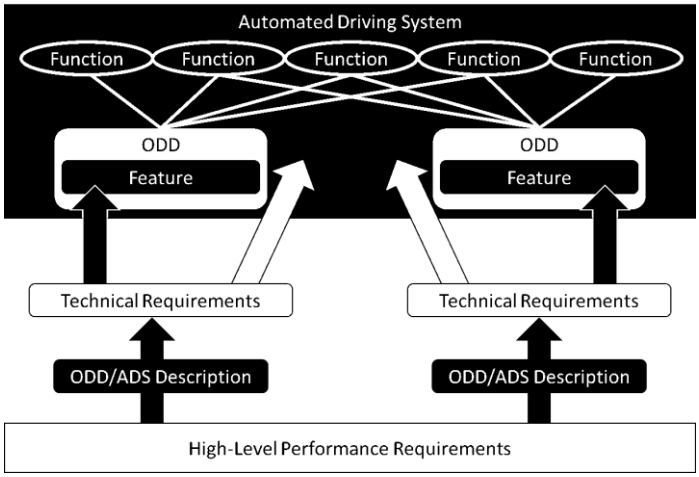
FRAV's intention is to cover all on-road ADS vehicles with three or more wheels, excluding motorcycle derivations.

3.2. ADS descriptions. Although the safety requirements cover all ADS applications, each individual ADS should be assessed based on its configuration, intended uses and limitations on its use. FRAV concluded that the ODD and other safety-related use constraints of each ADS should be described in verifiable terms. Manufacturers should be free to determine ADS configurations, uses, and limitations; however, manufacturers should be obliged to describe the ADS in a reasonably uniform and verifiable manner. These descriptions would enable objective determinations on the application of safety requirements to the ADS under assessment. In this way, safety requirements can be defined for all ADS while enabling the assessment of each individual ADS configuration.

3.3. ADS safety requirements. Requirements for the safety assessment of an individual ADS depend upon its intended uses and limitations on its use (i.e., its features). For example, all ADS would be expected to detect and respond to road conditions that may be encountered during operation. However, correct responses of individual ADS to these conditions may differ. An ADS designed to operate under adverse road conditions would be expected to adapt its driving behavior accordingly. A different ADS encountering those same conditions may be designed to transfer control of the vehicle to the human user. The safety requirements, therefore, will cover ADS functions (such as detection of ODD conditions) and minimum performance specifications relevant to safety.

Intended uses and limitations on the use of an ADS also relate to user roles and responsibilities. Commonality of user controls across vehicle makes and models has been a long-established safety principle in order to avoid excessive learning curves when moving from one vehicle to another and to reduce the risks of user confusion. ADS safety includes attention to the diverse configurations, variations in the roles and responsibilities of users, and misuse prevention.

3.4. Overall approach. The ADS description requirements enable FRAV to define performance requirements where specific parameters for each individual ADS can be objectively determined based upon its intended uses and limitations. For example, distinctions can be made regarding constraints on speed or levels of precipitation.



This approach provides flexibility at the technical level without compromising safety or the assessment methods. The diversity of ADS configurations can be captured by the requirements without prescribing boundaries or applications of the technologies. FRAV has described the requirements as being "high-level" in the sense of being applicable across all ADS; however, the requirements will be defined at a level of detail to enable their application at a technical level based on each individual ADS configuration, its intended use(s), and limitations on the use of its feature(s) as defined in the ADS description.

4. Elaboration of ADS safety requirements

4.1. Guiding principle. FRAV has held extensive discussions regarding expectations for ADS performance, criteria to guide the development of requirements, and methods for determining performance specifications.

In the immediate future, ADS will be deployed into human-dominated traffic. The vehicles must integrate safely into current traffic patterns, including attention to traffic flows. ADS driving behaviors will need to

conform with human expectations in order to ensure reasonable predictability and public acceptance. Obviously, ADS are designed for human use and will similarly need to meet user expectations, including attention to the mental models upon which humans will base their understanding of ADS use. Research on crash causation shows that human decision, recognition, performance, and non-performance errors are the critical factors in more than 90% of crashes. ADS can significantly contribute to road safety by addressing crash causation factors.

Various methods have been proposed to ensure that ADS satisfy these imperatives. FRAV has considered a "Careful and Competent Human Driver" (CCD) approach rooted in analysis of human driver behaviors to define quantitative parameters for ADS driving performance. FRAV has also considered analysis of ADS technological capabilities under a "State-of-the-Art" approach. Several stakeholders have developed mathematical models to establish performance parameters. Other interested parties have proposed that ADS should generate a "statistical positive risk balance" such that vehicles operating in automated mode demonstrate superior performance when compared statistically against human driving performance data. FRAV has concluded that these various approaches have merits that may be useful in determining optimal performance specifications, including nominal driving performance and in setting boundaries between crash avoidance and crash mitigation. In some cases, combinations of these approaches offer paths towards defining optimal specifications.

FRAV has also agreed that the safety requirements should meet a set of criteria to ensure desirable outcomes. The safety requirements should result in ADS performance that significantly improves road transport (including safety and efficiency) and meets public expectations (social acceptance). The requirements should adhere to well-established best practices to result in performance-based, technology-neutral, and objectively verifiable specifications. The requirements should also be feasible given current technological capabilities and costs.

Based on these deliberations, FRAV is currently considering an overall vision to guide discussions on performance specifications:

> ADS performance should be consistent with safe human driving behaviors while avoiding recognition, decision, and performance errors and the introduction of unreasonable ADS-specific risks.

This vision aims to capture FRAV expectations for performance, the scope of the safety requirements, and the approaches to determining specifications. ADS performance should be compatible with current traffic patterns and safe human driving behaviors to ensure reasonable predictability and public acceptance. Research indicates that nearly all current crashes involve human errors or negligence as the critical factor. ADS are not human; however, ADS will interact with humans, including vehicles driven by humans. Understanding the critical factors in crash causation supports deliberations on behaviors ADS may encounter and informs discussions on ways that ADS may improve road safety. Lastly, the vision recognizes that ADS are new technologies, requiring attention to their use by humans, interactions with other road users, and their functional safety. FRAV has identified safety aspects for further elaboration, such as commonality across user interfaces (HMI), management of failure modes, and operational safety throughout the life of the vehicle.

4.2. "Top-down" approach. FRAV determined that a "top-down" approach would ensure coverage of all aspects of ADS safety. Under this approach, FRAV gathered extensive input across its more than 100

stakeholders, including the review of national and regional guidelines regarding automated vehicles. From this input, FRAV identified five main aspects of ADS performance:

1. ADS should drive safely. (Ensure safe behavior of the ADS as "the driver")
2. ADS should interact safely with the user. (Ensure safe use of ADS and safe interactions with the user such as transfers of control, user override, etc.)
3. ADS should manage safety-critical situations. (Differentiate between normal driving and emergency situations to ensure safe responses to the latter)
4. ADS should safely manage failure modes. (Ensure safe responses to system malfunction, physical damage, etc.)
5. ADS should maintain a safe operational state. (Ensure safety throughout the useful life of the ADS, such as safety-critical updates, responses to obsolescence, end of production, etc.)

From these categories, FRAV has derived 40 inter-related safety topics:[6]

1. The ADS should perform the entire Dynamic Driving Task.
2. The ADS should control the longitudinal and lateral motion of the vehicle.
3. The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).
4. The ADS should detect, recognize, classify, and prepare to respond to objects and events in the traffic environment.
5. The ADS should respect traffic rules.
6. The ADS should interact safely with other road users.
7. The ADS should adapt its behavior in line with safety risks.
8. The ADS should adapt its behavior to the surrounding traffic conditions.
9. The ADS driving behavior should not disrupt the flow of traffic.
10. The ADS behavior should not be the critical factor in causation of a collision.
11. Activation of an ADS feature should only be possible when the conditions of its ODD have been met.
12. The ADS should signal when conditions indicate a probable ODD exit.
13. The user should be permitted to override the ADS to assume full control over the vehicle.
14. The ADS should safely manage transitions of control to the user.
15. Prior to a transition of control to the user, the ADS should verify the availability of the user to assume control.
16. Pursuant to a transition, the ADS should verify full control of the vehicle by the user prior to deactivation.
17. The ADS should tolerate user input errors.
18. The ADS should provide feedback to the user on its operational status.
19. The ADS should warn the user of failures to fulfill user roles and responsibilities.
20. The user should be provided with information regarding user roles and responsibilities for the safe use of the ADS.
21. ADS vehicles that may operate without a user-in-charge should provide means for occupant communication with a remote operator.
22. Upon completion of an MRM, a user may be permitted to assume control of the vehicle.
23. The ADS should recognize and respond to road-safety agents.
24. The ADS should mitigate the effects of road hazards.
25. The ADS should execute a safe fallback response as conditions warrant.
26. In the absence of a fallback-ready user, the ADS should automatically achieve a Minimal Risk Condition (MRC).
27. The ADS should place the vehicle in an MRC in the event of a failed transition of full control to the user.

[6] This list concerns discussion topics. These topics are generating further discussions as intended and should be understood as interim points to be superseded as FRAV continues it work.

28. The ADS should achieve an MRC prior to deactivation.
29. The ADS should signal its intention to place the vehicle in an MRC.
30. The ADS should safely manage short-duration ODD exits.
31. Pursuant to a collision, the ADS should stop the vehicle and deactivate.
32. The ADS should detect system malfunctions and abnormalities.
33. The ADS should execute a safe fallback response upon detection of a failure that compromises performance of the DDT.
34. Provided a failure does not compromise ADS performance of the entire DDT, the ADS should respond safely to the presence of a fault in the system.
35. The ADS should signal faults and resulting operational status.
36. The ADS should be permanently disabled in the event of obsolescence.
37. Pursuant to a collision and/or a failure detected in DDT-related functions, ADS activation should not be possible until the safe operational state of the ADS has been verified.
38. The ADS should signal required system maintenance to the user.
39. The ADS should be accessible for the purposes of maintenance and repair to authorized persons.
40. ADS safety should be ensured in the event of discontinued production/support/maintenance.

5. Status of FRAV activities

5.1. Data collection. In order to ensure that ADS performance requirements result in behaviors compatible with human-dominated traffic and real-world driving, FRAV requires data on human driving, current traffic patterns, and crash causation. FRAV has already received significant input concerning human driving behaviors, driver models, and traffic patterns and flows. FRAV has discussed methods for quantifying and otherwise analyzing human and ADS performance parameters. These discussions have also considered driving behaviors under nominal conditions and methodologies for determining feasible boundaries between collision avoidance and crash mitigation. FRAV has requested stakeholders to provide further input towards building out its understanding.

5.2. Elaboration of safety requirements. FRAV is working through the 40 safety topics to identify measurable/verifiable criteria for assessing performance in achieving the desired safety outcomes. The safety topics involve subsidiary issues that FRAV needs to isolate to ensure clear descriptions of desired performance. In addition, FRAV expects further consideration of the methodologies for determining and justifying specific minimum performance limits, ranges, or other objective verifications.

5.3. Elaboration of ADS description requirements. FRAV expects its deliberations on the safety topics and eventual requirements to raise awareness of ODD conditions and other elements that may impact ADS performance. These variables and conditions will be integrated into the requirements for ADS descriptions.

6. Coordination with VMAD

6.1. FRAV-VMAD coordination meetings. The leaderships of FRAV and VMAD hold regular meetings to review the status of their activities, expectations for progress, and anticipated needs. FRAV strives to align its activities with those of VMAD. Participation in FRAV and VMAD substantially overlaps. The FRAV leadership has requested its stakeholders to remain aware of the need to integrate the FRAV outcomes with those of VMAD and to raise awareness within FRAV of any perceived areas of complementarity or possible divergence.

6.2. Scenarios. FRAV distinguishes between the nominal driving behavior of ADS (e.g., ADS behavior should not cause crashes) and ADS behavior in response to safety-critical events (e.g., ADS response to error or negligence on the part of another road user). Nominal driving involves an understanding of typical and safe driving maneuvers and interactions with other road users. Safety-critical responses involve an understanding of crash causation and sudden conditions that may arise in the roadway. FRAV will also define ODD elements for

use in ADS descriptions. FRAV deliberations on ODD, crash causation, and driving behaviors and responses may be useful to VMAD in the development of scenarios.

6.3. Audit. FRAV has defined an ADS in terms of functions and features. FRAV is pursuing safety requirements to address failure management and operational safety. FRAV deliberations on safety requirements related to functions and system safety may contribute to the objective assessment of ADS functional safety.

6.4. Virtual testing. FRAV recognizes the complexity of traffic and a need to ensure ADS behaviors consistent with human-dominated traffic and human road-user expectations. In particular, FRAV has devoted attention to the impact of ADS performance specifications on traffic flows and human driver behaviors. Given the importance of virtual testing to the assessment of ADS performance across ranges of conditions, FRAV deliberations on performance specifications conducive to the smooth integration of ADS into human-dominated traffic may provide context useful in assessing the fidelity of virtual testing tool chains.

6.5. Physical testing. FRAV will develop performance specifications that in many cases will be suitable for assessment under physical tests, such as responses to safety-critical conditions, ODD exits, or damage to a function. These deliberations should contribute to the development of track, real-world, or other physical test methods.

6.6. In-service performance. FRAV has define a safety category concerning the safe operational state of the ADS throughout the lifetime of the vehicle. These deliberations may contribute to VMAD considerations regarding in-service monitoring and reporting on ADS performance.

6.7. Integration under the New Assessment/Test Method (NATM). The FRAV approach to ADS safety requirements includes a manufacturer description of the ADS to be assessed. The NATM will need a procedure for the review and verification of these ADS descriptions. FRAV will provide requirements for the preparation and contents of an ADS description. Under the NATM, the description should be verified for fulfillment of these requirements (e.g., coverage of the ODD elements, stipulation of ODD conditions in accordance with the verifiable criteria specified by the description requirements).

In addition, the application of the safety requirements depends upon the ODD of the ADS feature under assessment. For example, FRAV expects to define performance requirements related to ODD exits. The manufacturer specifies the ODD boundaries in the description of the ADS. Therefore, assessment of fulfillment of the requirements for ODD exits will depend upon the boundaries stipulated by the manufacturer. The NATM should have a procedure to apply the ODD boundaries to the method(s) used to assess performance of the ADS related to an ODD exit (e.g., use of the ADS is limited to speeds below 90 kph such that the ODD-exit requirements and assessment method(s) would be applied based on this technical specification). The ADS descriptions and safety requirements should also play a role in determining the relevance of scenarios developed by VMAD to a given ADS configuration and their application to the test and assessment methods.

7. Outlook for 2021

FRAV aims to provide its recommendations for ADS safety requirements for GRVA consideration in February 2022. As explained, these safety requirements aim to cover all ADS configurations, intended uses, and limitations on use.

Under its top-down approach, the work on safety requirements has and will continue to move through phases, each producing a higher level of detail. FRAV held a general phase where the group reviewed regional and national guidelines and solicited a wide range of stakeholder input on potential safety requirements. FRAV reached agreement on a structure to enable the assessment of an individual ADS within a framework of requirements covering all aspects of ADS safety. To facilitate further deliberations, FRAV reached agreement on a core set of draft terms and definitions, resolving a number of initial questions regarding aspects of the safety requirements. FRAV developed a structure for the elaboration of the requirements based on five initial statements covering the principal aspects of ADS safety raised by its general discussions. FRAV used this

framework to prepare the current list of 40 topics. As intended, the 40 topics are generating further stakeholder input towards reaching agreement on specific elements and criteria for ADS safety to be addressed under the ADS descriptions and in the ADS performance requirements.

FRAV aims to reach agreement on ADS description elements, safety aspects to be verified, and their verification criteria by May 2021. FRAV aims to define specifications for these requirements by September 2021. Given the complexity of the task and the likelihood of open issues requiring additional effort, FRAV reserves the post-September period for finalization of its recommendations for the February 2022 GRVA session.

FRAV recognizes priorities identified by stakeholders, including Contracting Parties to the WP.29 Agreements, as well as by the Informal Working Group on Validation Methods for Automated Driving (VMAD). ADS technologies are in the early stages of deployment, including the evolution of current ADAS (i.e., SAE Level 2 driving automation systems) into ADS (i.e., SAE Level 3+ Automated Driving Systems). In particular, FRAV recognizes the interest in demonstrating the NATM via its application to ADS configurations designed for use on divided highways. While FRAV cannot afford to ignore the variety of current and anticipated ADS deployments, the group recognizes the extensive discussions in GRVA regarding applications for use on divided highways and interest in FRAV outcomes that may offer solutions for the assessment of these applications. Nonetheless, FRAV's priority concerns recommendations on safety requirements applicable across all ADS configurations and uses. FRAV's intended outcome would be applicable—but not limited—to individual ADS configurations such as for motorway use. Should an aspect of its work involve prioritization of work elements, FRAV would seek to align the work with VMAD where mutually beneficial.