Submitted by the IWG on
Functional Requirements for Automated Vehicles
(FRAV)

Informal Document **WP.29-180-10**
180th WP.29 session, 9-13 March 2020
Agenda item 2.3.

Common Functional Performance Requirements for Automated Driving Systems and ADS-Equipped Vehicles

1. Purpose

In accordance with the WP.29 Framework Document on Automated/Autonomous Vehicles (WP.29/2019/34/Rev.2, hereafter, the Framework Document), this document provides common functional performance requirements based on national/regional guidelines and other relevant reference documents consistent with the 1958 and 1998 Agreements. The document is based primarily upon discussions held among the experts of the Informal Working Group on Functional Requirements for Automated Vehicles (FRAV) under the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) and informal documents GRVA-05-40 and GRVA-05-41 as presented during the 5th GRVA session (10-14 February 2020). This document highlights common concepts identified through the first two FRAV sessions. These concepts are not exhaustive and many, if not all, will undergo changes as the FRAV and GRVA work progresses. This document does not constitute a proposal, formal or otherwise, for automated vehicle legal requirements but may serve to support discussions across WP.29 and its subsidiary bodies.

2. Background

Pursuant to the Framework Document and the Terms of Reference (WP.29/1147/Annex V) agreed by WP.29, FRAV drew from previous work of the Informal Working Group on Validation Methods for Automated Driving (VMAD) to consider a "Comparison table of ADS Guidelines in USA, Canada, Japan, EU, Australia and China" (VMAD-01-04) prepared by OICA. OICA further assisted the FRAV deliberations by preparing a table of "common AV safety elements" (FRAV-01-13) that distilled the comparison table into a single set of common elements. Following discussions during the first FRAV session (9-10 October 2019, Berlin), OICA revised this table to improve its alignment with the Framework Document (FRAV-01-13/Rev.1). The FRAV co-chairs (China, Germany, and the United States of America) requested stakeholders to draft proposals for functional performance requirements based upon this table of common elements.

During this first session, FRAV agreed to pursue a top-down or "stepwise" approach in the development of functional performance requirements. In order to cope with the complexity of traffic conditions, FRAV agreed to proceed from high-level requirements towards more detailed requirements as may be warranted to address particular safety needs.

In preparation for its second session (14-15 January 2020, Tokyo), the FRAV co-chairs directed the FRAV secretary to prepare a document transposing FRAV-01-13/Rev.1 into a format suitable for long-term development. The purpose of this new document (FRAV-02-05) was to facilitate the systematic discussion of each of the safety elements with the aim to gather additional input from all the FRAV stakeholders.

During FRAV-02, document FRAV-02-05 was expanded to include input from the stakeholders, including documents:

- Comments on FRAV-01-13/Rev.1
    - FRAV-02-06 (EC)
    - FRAV-02-08 (Canada)
    - FRAV-02-11 (Switzerland)
- Comments on FRAV-02-05
    - FRAV-02-07 (Netherlands)
    - FRAV-02-10 (OICA/CLEPA)
    - FRAV-02-12 (Canada)
- Proposal for high-level functional requirements
    - FRAV-02-13 (OICA/CLEPA)
- Proposal to define “Operational Design Conditions (ODC)”, including driver status requirements
    - FRAV-02-09 (China/CATARC)

The discussions and input resulted in document FRAV-02-05/Rev.1 which was considered during the second day of the session. FRAV-02 approved the document as the basis for further developing proposals for functional performance requirements.

Given the intention to continue using the document as a tool for capturing and considering all stakeholder input, FRAV decided to reserve the document number “05” for all future iterations. Hence, FRAV refers to this documentation tool as “Document 5”.

At the conclusion of the FRAV-02 session, the FRAV co-chairs directed the FRAV secretary to prepare a consolidated and updated revision of Document 5 (FRAV-02-05/Rev.2) as a means to gather further input in preparation for the third FRAV session (FRAV-03, 14-15 April 2020, Paris).

In preparation for the 5th GRVA session, the FRAV co-chairs directed the FRAV secretary to prepare a status report (GRVA-05-40) detailing the broad areas of agreement within the group and a summary presentation (GRVA-05-41) highlighting topics that GRVA might wish to bring to the attention of WP.29. The US co-chair of FRAV presented these documents and received comments during the session.

3. Introductory comments

Throughout its deliberations, FRAV has repeatedly referred to the 1958 and 1998 Agreements and to the WP.29 AV Framework Document for guidance. During the course of these discussions, FRAV has identified elements that WP.29 may wish to consider towards refining its efforts to address vehicle automation.

3.1 Vehicle definitions and classifications

Following discussions on the scope of work during its first session, FRAV tasked the experts from the United Kingdom to conduct a review of Special Resolution No. 1 (SR1) with regard to automated vehicle configurations. As a result, FRAV has identified possible issues with current definitions of vehicle classifications:

- SR1 definitions refer to drivers and driver seating positions. As a result, automated vehicles without driver controls would appear to fall outside the current classifications.

- Definitions limited to the number of seating positions would appear to leave unclassified a vehicle designed to carry small numbers of standing passengers.

WP.29 may wish to refer these observations to GRSG (as the custodian of the resolutions on vehicle classifications) for further consideration.

3.2 Framework Document

In accordance with its agreed methodology to proceed from high-level requirements, FRAV has frequently referred to the Framework Document, including its “Safety Vision” statement and in particular paragraph 7: “The level of safety to be ensured by automated/autonomous vehicles implies that ‘an automated/autonomous vehicle shall not cause any non-tolerable risk’, meaning that automated/autonomous vehicle systems, under their automated mode ([ODD/OD]), shall not cause any traffic accidents resulting in injury or death that are reasonably foreseeable and preventable”.

Given the importance of this statement in establishing high-level performance requirements, WP.29 may wish to consider improvements to the text in response to the following issues raised in GRVA by FRAV.

3.2.1 Operational Domain

FRAV has noted the use of “OD” and “ODD”, often interchangeably, in the Framework Document and other WP.29 documents. During GRVA (and other WP.29) discussions, some stakeholders have raised concerns over use of the word “design” in “operational design domain”, noting that vehicle regulations strive to avoid “design-restrictive” requirements. Moreover, as stated in the Framework Document, the definition of the ODD of a vehicle, ADS, or ADS feature is a manufacturer responsibility, raising concerns over use of this term in the establishment of requirements by safety authorities. The term OD was proposed to differentiate between the ODD defined by the manufacturer and minimum operational conditions that might be established by the safety authority.

However, FRAV notes that the term ODD has been defined under the SAE Surface Vehicle Recommended Practice J3016:2018 “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles” (hereafter, SAE J3016) and is used across the Contracting Party guidelines. Perhaps more importantly, this term (as defined under SAE J3016) is currently used across a large array of activities devoted to advancing driving automation worldwide.

After extensive consideration, FRAV has determined that the term ODD is sufficient to enable the development of functional performance requirements and does not prejudice the ability of safety authorities to establish minimum requirements related to ODD definitions. Whether directly or indirectly, functional performance requirements define minimum acceptable performance parameters for automated vehicles. These requirements influence manufacturer ODD definitions without necessarily restricting design decisions or the development of technological solutions.

Therefore, FRAV has determined that use of alternative terms, including “operational domain” or OD, is unnecessary and arguably counterproductive. Given the widespread acceptance of ODD and its use in research and the development of standards worldwide, deviation from this term appears antithetical to the goals of harmonization. WP.29 may wish to consider removing the references to “OD” from the Framework Document.

3.2.2 Autonomy

FRAV also considered use of the term “autonomous” by the Framework Document in particular and WP.29 in general. SAE J3016 includes “autonomous” in its list of deprecated terms and cautions against its usage.[1] The term is functionally imprecise, encourages ADS misuse (e.g., user overreliance), and has given rise to widespread improper use as synonymous with “automated”.

In legal terms, “autonomous” refers to the capacity for self-governance, including responsibility for one’s own actions. The J3016 Recommended Practice notes that even the most advanced ADS do not meet this level of independent control or behavior. SAE J3016 states, “This usage obscures the question of

[1] SAE J3016:2018, Section 7. Deprecated Terms. This section lists terms that are functionally imprecise (and therefore misleading) and/or that are frequently misused by application to lower levels of driving automation (i.e., levels 1 and 2) in which the driving automation system does not perform the entire DDT.

whether a so-called “autonomous vehicle” depends on communication and/or cooperation with outside entities for important functionality”.

Although such autonomy may be theoretically possible given future advances in robotics and artificial intelligence, FRAV sees nothing in the foreseeable future to suggest the development of ADS along these lines. ADS remain dependent upon external inputs and/or cooperation (e.g., system design, software algorithms and updates, system maintenance, user commands and interactions).

Moreover, WP.29 specifically establishes requirements that allocate responsibilities between manufacturers and authorities or their agents for the assurance of vehicle safety. The notion that WP.29 stakeholders would sanction the deployment of vehicles capable of behaving independently of manufacturer and/or user control (i.e., autonomously) seems improbable.

Therefore, FRAV has submitted to GRVA that vehicles equipped with ADS are “automated” but not “autonomous”. WP.29 may wish to consider removing references to “autonomous” from the Framework Document and discouraging its use in other instances.

3.2.3 Accidents

The use of “accidents” has raised some comments within FRAV. This term does not have a clear legal definition and implies an absence of responsibility. Given that FRAV has been mandated to develop requirements that recognize safety authority and manufacturer responsibilities towards ensuring safety, the term “accidents” should be replaced by a more neutral term such as “events” or a more specific term such as “collisions”. WP.29 may wish to consider alternative language in the Framework Document.

3.2.4 Free of unreasonable safety risks

FRAV discussions have repeatedly included the phrase “free of unreasonable safety risks” (as used under the “System Safety” and “Validation of System Safety” elements of the Framework Document) as a high-level performance standard. Moreover, ISO 26262 ‘Road Vehicles—Functional Safety” defines functional safety as the “absence of unreasonable risk”.[2] This standardized terminology appears to more clearly capture the intent of the reference to “non-tolerable risks”. WP.29 may wish to consider revising the “Safety Vision” accordingly.

[2] ISO 26262 defines functional safety as the absence of unreasonable risk due to any potential source of harm caused by malfunctioning behavior of electrical and or electronic systems. A malfunctioning behavior is not limited to failures but also includes unintended behavior (with respect to design intent).

3.2.5 Disruption of the flow of normal traffic

FRAV discussions have repeatedly noted that vehicles operating in automated mode should not unnecessarily disrupt the normal flow of traffic, relating to the notion that vehicles in automated mode should behave in ways that other road users can anticipate.

In paragraph 6 of the Safety Vision, the Framework Document extends this concept to include behavior consistent with user expectations: “If automated/autonomous vehicles confuse users, disrupt road traffic, or otherwise perform poorly then they will fail”. However, this cautionary statement is not reflected elsewhere in guiding the work on performance requirements.

Driving entails the prioritization of competing demands (e.g., compliance with traffic laws versus risk to human life). While safeguarding human life sits at the apex of priorities, ensuring the smooth flow of traffic plays an important role given its relationship to crash causation and to the negative health, safety, and economic impacts of traffic congestion. The Framework Document specifies prevention of death or injury and compliance with traffic rules; however, the FRAV stakeholder input (and paragraph 6 of the Framework Document) suggests a third priority in between these two levels: the vehicles in automated mode should behave in ways consonant with the surrounding traffic, the expectations of other road users, and the expectations of the vehicle users.

In this regard, prioritizing functional performance requirements conducive to the assurance of safe traffic flows seems consistent with the intent of the Framework Document. WP.29 may wish to consider this aspect of automated vehicle interaction with surrounding traffic in its high-level guidance.

3.2.6 Destruction of property

Canada has proposed that the performance criteria should also aim to avoid the destruction of property in addition to outcomes resulting in injury or death given the economic consequences of vehicle crashes. Although “destruction of property” would likely require definition (e.g., prioritizing avoidance of injury or death over property damage), this addition appears consistent with the intent to avoid collisions where possible. WP.29 may wish to consider including destruction of property within the hierarchy of the Framework Safety Vision.

3.2.7 Drivers and users

The Framework Document describes system safety as “When in the automated mode, the automated/autonomous vehicle should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations.” FRAV has noted that vehicles equipped with automated driving systems do not necessarily have a human driver as implied by this description and may be operated or supervised remotely. WP.29 may wish to consider replacing the term “driver” with the broader term “vehicle user(s)”.

3.2.8 Compliance with road-traffic regulations

FRAV stakeholders have noted that strict observance of traffic regulations is not always consistent with safety. Traffic authorities, whether explicitly or implicitly, categorically accept temporary suspension of compliance with traffic regulations in the interests of ensuring a safe response to objects or events in the roadway. In this regard, the reference to ensuring compliance with road-traffic regulations in the description of System Safety appears superfluous. A vehicle free of unreasonable safety risks would by definition observe traffic safety laws except in cases where strict compliance would result in unreasonable risks to safety.

3.2.9 Object and Event Detection and Response

The Framework Document identifies OEDR as a distinct topic, stating "The automated/autonomous vehicles shall be able to detect and respond to object/events that may be reasonably expected in the [ODD/OD]".

Contracting Party guidelines and FRAV stakeholders consider OEDR to be an element of System Safety. OEDR includes both the environmental monitoring and response-preparation functions and the response execution (vehicle motion, signaling, etc.) function. As such, OEDR functionalities are central to system design and performance and should be addressed under System Safety requirements.

Nonetheless, FRAV agreed during its first session that detailed technical requirements and test procedures may be needed in some cases. As FRAV develops the higher-level requirements needed to capture the diversity of traffic conditions under System Safety, the group expects to identify areas where such technical requirements would be beneficial. These requirements would offer a common baseline for assessment of vehicle performance (e.g., motion and other physical behaviors) under defined conditions. The selected criteria would facilitate objective, quantitative, and comparable assessments of vehicle performance that can be consistently reproduced.

WP.29 may wish to consider placing OEDR under subparagraph 9(a) on System Safety while refining the scope of subparagraph 9(b) to focus on the OEDR response execution aspect (e.g., physical performance such as longitudinal/lateral motion control and signaling).

3.2.10 Human-Machine Interface and Operator Information

The Framework Document states, "Automated/autonomous vehicle should include driver engagement monitoring in cases where drivers could be involved (e.g. take over requests) in the driving task to assess driver awareness and readiness to perform the full driving task. The vehicle should request the driver to hand over the driving tasks in case that the driver needs to regain a proper control of the vehicle. In addition, automated vehicle *[sic]* should allow interaction with other road users (e.g. by means of external HMI on operational status of the vehicle, etc.)".

The Framework Document text presents significant problems, including its emphasis on "driver" involvement given the development of automated vehicles without driver controls. FRAV has noted possible differences in requirements between vehicles with and without controls, including vehicles designed for remote operation. For example, a vehicle without driver controls might still benefit from a means for vehicle occupants or remote operators to intervene.

The objective(s) of the sentence "The vehicle should request the driver to hand over the driving tasks in case that the driver needs to regain a proper control of the vehicle" is not clear and appears inherently contradictory. It would seem that the intention is for the driver to take over control of the vehicle from the automated driving system.

Automated vehicles will interact with other road users. This interaction is not "allowed" by the vehicle; road users interact as a matter of co-existing on the roadway. The object of the last sentence in the above citation would appear more accurately described in terms of the vehicle communicating information to other road users as needed to promote safe interactions and in compliance with traffic regulations.

FRAV has discussed the complexity of driver monitoring both conceptually and in terms of functional performance requirements. SAE J3016 offers distinctions among "monitoring", "awareness", and "receptivity", noting as an example that a person may become aware of a fire alarm without "monitoring" the fire alarm. Monitoring can also to be a two-way street: the system may monitor the user, but the user may also need to monitor the system. As noted above, concerns have been raised over interdependency between the system and user; the driver state could relate to the "intended use of the ADS" (e.g., its ODD). A system that requires a driver's hands on the wheel or a requisite level of driver alertness should not be used if those conditions are not fulfilled.

The intent of the HMI description appears to be that an automated driving system dependent upon the user for safety-critical functionalities should monitor user fulfillment of such roles as may be necessary to ensure correct use of the system. The automated system should transfer control to the driver upon request. In addition, the automated vehicle should communicate safety-critical information as needed to surrounding road users.

WP.29 may wish to consider revision of this paragraph.

3.2.11 Failsafe response

The Framework Document describes "Failsafe response" as "The automated/autonomous vehicles should be able to detect its *[sic]* failures or when the conditions for the [ODD/OD] are not met anymore. In such a case the vehicle should be able to transition automatically (minimum risk manoeuvre) to a minimal risk condition".

The Framework Document associates the "failsafe response" with system failures, exits from the ODD, and minimal risk maneuvers (MRM). FRAV notes that responses to the absence of conditions prescribed by an ODD can fall within the normal and expected behavior of an ADS. FRAV stakeholders have noted that “failsafe” is generally understood as a mechanism or system that returns the vehicle to a safe state specifically in the event of a system failure or malfunction. Therefore, “failsafe response” does not seem to correspond to the intent of the Framework Document. FRAV stakeholders have proposed the term “safe fallback response” to capture not only responses to failure modes but also nominal performance, including normal responses to planned and unplanned ODD exits.

In addition, the fallback response to a system failure or an ODD exit would not necessarily be limited to an MRM. For example, in vehicles equipped with driver controls, the fallback could be a safe transition of control to the driver.

Categorically, a safe fallback is a response either by the user or by the system to a system failure or an ODD exit. A fallback strategy can be a transition demand or an MRM and can involve a sequence of fallback responses.

3.2.12 “Minimal” and “minimum”

FRAV has also noted the frequent use of “minimum” and “minimal” interchangeably (as is the case in the above paragraph from the Framework Document). The accurate term is “minimal”. This term is consistent with SAE J3016 and recognizes that the ADS has no control over the vehicle environment. The “minimal risk maneuver” places the vehicle in a “minimal risk condition” within the limits of the options available (e.g., availability or absence of an unobstructed hard shoulder by the roadside). Given the diversity of road conditions, an absolute “minimum” cannot be established outside of a highly defined scenario or set of circumstances.

WP.29 may wish to reconsider subparagraph 9(b) for improvement based upon the above perspectives.

3.2.13 Rational versus reasonable

FRAV has noted the use of “rationally” in place of “reasonably” in WP.29 documents. As noted above, the ISO definition of functional safety refers to “unreasonable risk”.[3] Logically, the inverse of this concept would refer to “reasonable risk”, not “irrational risk”. Moreover, a “reasonableness” standard is well-established under English-language regulatory and administrative law. This standard is used both in connection with the “foreseeability” principle and in the exercise of due care in product design. In definitional terms, “rational” and “irrational” refer to mental competency whereas “reasonable” and “unreasonable” refer to decision-making based upon consideration of available information and the weighing of probabilities. For accuracy and consistency, WP.29 may wish to encourage the use of

[3] ISO 26262 "Road vehicles – Functional safety" defines functional safety as “Absence of unreasonable risk due to hazards caused by malfunctioning behavior of Electrical/Electronic systems”, supporting use of “unreasonable risk” as the preferred terminology.

“reasonable” and “unreasonable” when referring to safety while discouraging the use of “rational” in such contexts.

3.2.14 Other elements in the Framework Document

FRAV discussions have raised items outside the scope of the topics specified under its Terms of Reference. These items include “in-use performance” and “post-crash safety”.

FRAV suggests that GRVA and WP.29 may wish to consider the unallocated topics of the Framework Document (“vehicle maintenance and inspection”, “consumer education and training”, “crashworthiness and compatibility”, and “post-crash AV behavior”) for improvement and/or attribution.

FRAV has discussed possible needs related to the “in-use performance” of ADS. The Framework Document refers to “vehicle maintenance and inspection”; however, manufacturers have a limited capacity to address what are often vehicle-owner responsibilities related to maintenance. FRAV anticipates consideration of requirements to ensure that an ADS cannot be used while in an unsafe state and notes the work of the EDR/DSSAD informal working group related to user responsibilities.

FRAV has agreed that in the event of a collision, an automated vehicle should be placed in a state that minimizes safety risks to vehicle occupants, bystanders, and first-responders as well as to ensure that safety-critical damage to the ADS would preclude use of the automated driving mode(s) post-crash pending repair of the damage.

“Consumer education and training” has not produced a consensus opinion; however, FRAV has discussed the risks of ADS misuse as pertinent to functional performance requirements. In general, “consumer education and training” would seem to extend well beyond the scope of motor-vehicle safety regulation, including areas addressed by road traffic rules and WP.1.

“Crashworthiness and compatibility” falls under the scope of the Working Party on Passive Safety (GRSP). Nonetheless, FRAV would like guidance regarding whether its work should include provisions that might support GRSP considerations.

4. Common Functional Performance Requirements

4.1 Operational Design Domain

4.1.1 Explanatory Note

Safety authorities will require ODD definitions to establish the basis for the assessment of an ADS or feature thereof. For example, an ODD limiting the intended use of the ADS to speeds below 60 kph would determine the applicable functional performance requirements. The assessment might verify that the ADS recognizes and responds correctly (e.g., executes a fallback response) to this boundary condition while evaluating vehicle performance of the ADS in operation at speeds below the 60 kph boundary condition. If the ODD boundary were set at 120 kph, the test and assessment methods would be different.

Given the importance of ODD definition to the assessment of automated vehicles, systems, and features, manufacturers and safety authorities will need a shared methodology to describe a minimum array of ODD elements and its documentation by the manufacturer applicable to the ADS or ADS feature.[4]

As indicated above, the ODD is not necessarily defined at the vehicle level. NHTSA has noted in its research report "A Framework for Automated Driving System Testable Cases and Scenarios" that ODD definitions will likely vary for each ADS feature.[5] Some features may be limited by ODD conditions that are not applicable or relevant to other features of the system.

4.1.2 Principles for ODD definition

1) The Operational Design Domain (ODD) describes the operating conditions under which an ADS or feature thereof is specifically designed to function.[6]

2) The vehicle manufacturer defines and documents the ODD.[7]

3) The safety authority defines methods for describing ODD elements and the manufacturer documentation necessary to enable assessment of the vehicle, system, or feature.

4) The vehicle manufacturer transmits the required ODD documentation to the safety authority and/or its designated agent.

5) The safety authority and/or its designated agent verifies whether the manufacturer's submission, including ODD definition(s), complies with the documentation requirements.

4.2 System Safety

4.2.1 Explanatory Note

Under the Framework Document, the demonstration of system safety is a manufacturer responsibility. Manufacturers are obliged to generate evidence demonstrating "a robust design and validation process based on a systems-engineering approach with the goal of designing ADS free of unreasonable safety

[4] In line with its terms of reference, FRAV notes work on an industry standard (ISO/WD 34503: "Road vehicles — Taxonomy for operational design domain for automated driving systems") under ISO Technical Committee 22/Subcommittee 33. The Working Draft (WD) of the proposed standard has been approved for registration as a Committee Draft (CD).

[5] See, for example, FRAV-01-14: "A Framework for Automated Driving System Testable Cases and Scenarios", Chapter 3.

[6] SAE J3016:2018, section 3.22.

[7] WP.29/2019/34/Rev.2, paragraph 9, subparagraph (e): "Vehicle manufacturers should document the ODD available on their vehicles and the functionality of the vehicle within the prescribed ODD."

risks".[8] The role of safety authorities and/or their authorized agents is to verify that manufacturers have complied with minimum requirements and have furnished the requisite documentation regarding the development and validation of the ADS.

Functional performance requirements for system safety, therefore, will have to describe capabilities that should be integrated into the ADS design and the performance levels that should be demonstrated by a vehicle manufacturer through its validation processes.

The following capabilities and performance levels are intended to be consistent with FRAV's interpretation of the Framework Document's "System Safety" topic: When in automated driving mode, a vehicle should be free of unreasonable safety risks to the vehicle user(s) and to other road users and ensure compliance with road-traffic regulations consistent with the assurance of road safety.

4.2.2 System Design Capabilities

6) The safety authority should define the manufacturer documentation required to enable the assessment of the ADS design capabilities.

7) The manufacturer should furnish documentation compliant with the safety authority requirements.

8) An ADS should be capable of object and event detection and response (OEDR).[9]

9) The OEDR function should be designed to monitor the driving environment as needed to operate the vehicle.[10]

10) The OEDR monitoring function should be capable of detecting, recognizing, classifying, and preparing a response to objects and events in the driving environment.[11]

11) The OEDR function should be capable of controlling the longitudinal and/or lateral motion of the vehicle in response to conditions in the driving environment.[12]

12) The ADS should be capable of detecting when the conditions of its ODD are not present.

[8] WP.29/2019/34/Rev.2, paragraph 9, subparagraph (f).
[9] WP.29/2019/34/Rev.2, paragraph 9, subparagraph (d).
[10] SAE J3016:2018, section 3.19.2.
[11] SAE J3016:2018, section 3.20.
[12] SAE J3016:2018, section 3.20 and section 3.13, Note 1 regarding the DDT defines OEDR as "monitoring the driving environment" and "object and event response execution" where both elements include operational and tactical effort. In terms of automated driving, tactical effort involves maneuvering the vehicle in traffic. Operational effort involves split-second reactions, such as making micro-corrections to steering, braking and accelerating to maintain lane position in traffic or to avoid a sudden obstacle or hazardous event in the vehicle's pathway (Section 8.11). Section 3.13 defines the DDT as including longitudinal and lateral motion control and OEDR functions of monitoring and response execution. Therefore, it seems useful to distinguish between the data collection and analysis (monitoring) and vehicle motion control (response execution) functions of the OEDR.

13) The ADS should be capable of monitoring and detecting safety-critical deficiencies in its functional status, including system failures and performance errors.[13]

14) In cases where the ADS is dependent upon a human operator to fulfill all or part of a functional performance requirement, the system should be capable of monitoring the human operator's readiness to fulfill such requirements as needed to ensure safe use.

4.2.3 System-safety functional performance

15) The safety authority should define the methodologies (e.g., on-road testing, closed track testing, simulation testing) a manufacturer may use to demonstrate the functional performance of the vehicle, system, or feature with regard to system safety.

16) The manufacturer should furnish documentation on the performance of the vehicle, system, or feature during its testing of functional performance in accordance with the requirements of the safety authority.

17) Activation of the ADS or a feature thereof should only be possible when the conditions of the system's or feature's ODD are present.

18) During ADS operation, the system should execute a safe fallback response when the conditions of its ODD are no longer present or safety-critical conditions outside the ODD are detected. If the ODD conditions only pertain to a feature of the ADS, the feature may be temporarily disabled if doing so does not create an unreasonable safety risk.

19) Activation of the ADS should only be possible when the system is in a functional state that is free of unreasonable safety risks. In the event of a safety-critical deficiency detected during ADS operation, the system should execute a safe fallback response.

20) The ADS in operation should detect, recognize, classify, and respond to traffic signals, including prioritization in the event of multiple signals (e.g., traffic lights, road signs, temporary signals, signals from authorized personnel).

21) The ADS in operation should detect the approach of a priority vehicle (e.g., detect its special luminous and audible warnings) and respond by adapting the automated vehicle's motion to ensure room for the priority vehicle to pass or, if necessary, by stopping the automated vehicle. Similarly, the ADS in operation should detect, recognize, classify, and respond to signals and/or gestures of authorized personnel in the roadway.

[13] Under SAE J3016:2018, OEDR also includes driving events associated with system actions or outcomes, such as undiagnosed driving automation system errors or state changes. The latter responds to FRAV stakeholder input regarding system "risk mitigation" and "reaction to unforeseen situations".

22) If safe use of the ADS is dependent upon human support and the ADS detects a safety-critical deficiency in the human operator’s status, the system should prompt a return of the human operator to the required state of readiness and/or to execute a safe fallback response.

23) Under reasonably foreseeable conditions and where preventable, the vehicle in automated driving mode should not disrupt the normal flow of traffic unless necessary to mitigate risks of collision, injury, or death.

24) Under reasonably foreseeable conditions and where preventable, the vehicle in automated driving mode should not cause collisions or other events resulting in destruction of property, injury, or death.

25) The vehicle in automated driving mode should comply with traffic laws and regulations except in cases where such compliance would unnecessarily disrupt the flow of traffic and/or introduce unreasonable risks to the safety of its occupants and/or other road users. In such cases, the ADS should execute a response consistent with the flow of traffic and risk mitigation.

4.3 Object and Event Response Execution

4.3.1 Explanatory Note

Although conventional third-party testing cannot capture the diversity of conditions that vehicles may encounter during use over long periods of time, such testing can assess essential capabilities and provide important data for use in determining compliance with performance requirements.

FRAV has gathered an extensive list of proposals for performance thresholds; however, the proposals require further consideration. Categorically, FRAV is considering performance requirements related to normal driving and response(s) to other driving objects and events (i.e., critical situations).

It should be noted that functional performance requirements related to response execution are dependent upon the ODD of the vehicle, system, or ADS feature. At this point in its efforts, FRAV can only stipulate to broad principles.

4.3.2 Response Execution under Normal Driving Conditions

Analogous to testing of human drivers, automated vehicles will likely be tested by third parties to evaluate performance in executing common driving tasks such as turns, stops, lane discipline, and so on. Therefore, FRAV anticipates defining functional performance requirements corresponding to specific tasks relevant to the ODD of its ADS or ADS features.

26) The vehicle should be tested to assess its longitudinal and lateral motion responses to objects and events (e.g., signals, markings, other road users) within the ODD of its ADS or feature thereof.

27) The vehicle should be tested to assess its responses to the absence of conditions prescribed by the ODD of its ADS or feature thereof.

4.3.3 Response Execution to Safety-Critical Objects or Events

Automated vehicles will have to contend with the behavior and actions of other road users. FRAV anticipates that vehicles will be tested by third parties to assess performance under defined conditions representative of safety-critical situations that arise in real-world traffic. FRAV expects to work closely with VMAD to define functional performance requirements suitable to assessing vehicle-motion responses to such representative scenarios.

28) The vehicle should be tested to assess its longitudinal and/or lateral motion responses to the behavior of other road users.

4.4 Human Machine Interface and Operator Information

4.4.1 Explanatory Note

FRAV has gathered extensive stakeholder input on potential HMI requirements for further consideration. As the Framework Document and the FRAV Terms of Reference stipulate, HMI addresses both internal (i.e., vehicle occupant) and external (i.e., interactions with other road users) aspects.

The stakeholder input regarding internal HMI might further be categorized under misuse, abuse, and disuse headings. HMI functional performance requirements will need to balance these three considerations.

Given the expected diversity across ADS systems and automated vehicles, functional performance requirements related to HMI should mitigate the risks of misuse by providing clear indications of the system status and clear information regarding system use.

At the same time, the HMI should mitigate against user abuse, or intentional misuse, of the ADS capabilities. As noted in China’s proposal for the definition of “operational design conditions”, manufacturers should exercise due care in designing systems to mitigate foreseeable risks of intentional misuse such as a willful disregard of driver information. For example, if a system depends upon a driver in the driver’s seat for safety-related functionalities, reasonable solutions should be integrated into the vehicle design to ensure driver fulfillment of this safety prerequisite.

Lastly, widespread use of automated driving technologies are expected to contribute substantially to the prevention of crashes, injury, and death in traffic. As noted in the Framework Document, if ADS confuse, disconcert, or annoy users, the systems will not win public confidence. In this regard, the systems should behave in ways consonant with user expectations and allow users to assume control of the vehicle as may be desired in a safe manner.

4.4.2 Principles for HMI-related functional performance requirements

29) The ADS should provide the user with information necessary to enable correct use of the system or feature thereof.

30) In vehicles intended for driver use, the ADS should allow the user to assume control of the vehicle whenever conditions permit a safe transfer of control.

31) In cases of vehicles not intended for driver use, the ADS should allow for the occupant(s) to safely interrupt a trip.

32) The vehicle should signal its intentions for longitudinal and/or lateral motion to surrounding road users as needed to ensure road safety and comply with traffic regulations.

33) The vehicle should signal its initiation of a minimal risk maneuver to surrounding road users.

4.5 Safe Fallback Response

4.5.1 Explanatory Note

Depending upon the capabilities of an ADS, a safe fallback response may be carried out by the driver or the system. A safe fallback response may be triggered by a planned or unplanned ODD exit or by a system failure. The ADS safe fallback response may be a corrective action, transfer of control to the driver, or the execution of a minimal risk maneuver (MRM) by the driver or the system. The MRM places the vehicle in a minimal risk condition (MRC). Per SAE J3016, an MRC is a condition to which a user or an ADS may bring a vehicle after performing the DDT fallback (i.e., executing the safe fallback response) in order to reduce the risk of a crash when a given trip cannot or should not be completed.

Consequently, the safe fallback response as currently under consideration by FRAV stakeholders is somewhat broader in scope than the SAE J3016 definition of the DDT Fallback. Under SAE J3016, the DDT Fallback is defined as “the response by the user to either perform the DDT or achieve a minimal risk condition after occurrence of a DDT performance-relevant system failure(s) or upon operational design domain (ODD) exit, or the response by an ADS to achieve [a] minimal risk condition, given the same circumstances”. This definition limits the ADS fallback responses to a transfer of control to the driver or an automated MRM that interrupts the trip (i.e., brings the vehicle to a stop). However, some FRAV stakeholder input suggests the potential for a corrective response by the system. Hypothetically, a system could detect a failure in a direction indicator and respond by adapting its behavior or limiting available features. In addition, an MRM could be triggered by the user or by detection of an unsafe driver state (e.g., a medical emergency).[14] As noted by China in its “ODC” proposal, SAE J3016 does not appear to address such driver state issues.

Until such time as FRAV has clarified its scope, a safe fallback response should be understood as a response by the ADS that maintains vehicle occupant and other road-user safety in the event of an ODD exit or system failure.

4.5.2 Principles for safe fallback responses

34) A safe fallback response is an ADS response or sequence of responses to an exit from the ODD, a system failure, or a failure or incapacity of the driver to fulfill safety-critical roles.

35) The safe fallback response of the ADS may transfer vehicle control to the driver when the system has determined that the driver is capable of assuming control over the vehicle behavior.

36) During a safe fallback response transferring control to the driver, ADS should maintain vehicle control until the system has determined that the driver has assumed full control over the vehicle behavior.

37) The safe fallback response of the ADS should consist of an MRM when the system has determined that the driver is incapable of assuming control over the vehicle.

38) In cases where the system determines a failure of the user to fulfill a safety-critical role, the ADS should prompt a return of the user to the required state.

39) In cases where the system determines an incapacity of the user to fulfill a safety-critical role, the ADS should execute an MRM.

40) The ADS should execute an MRM in response to a user request.

41) The MRM should place the vehicle in an MRC in a manner consistent with traffic safety.

[14] See GRVA-05-63 for an example of this application.