Prepared by the FRAV co-chairs

Document FRAV-02-05/Rev.1
2nd FRAV session, 14-15 January 2020
Agenda items 6.5. and 7.

Submitted by the Informal Working Group on
Functional Requirements for Automated
and Autonomous Vehicles (FRAV)

Informal Document GRVA-05-xx
5th GRVA Session, 10-14 February 2020
Agenda Item xx

This document integrates items raised in the discussions of FRAV-02-05 during the first day (14 January 2020) session of the 2nd FRAV informal group meeting. This document is an interim draft for further discussion.

This document is a conceptual draft intended for review and discussion purposes only. Nothing in this document should be construed as a position, implied or explicit, of the FRAV informal group or any of its participants or stakeholders.

Statement on
Common Functional Performance Requirements
for Automated and Autonomous Vehicles

This document has been prepared by the Informal Working Group on Functional Requirements for Automated and Autonomous Vehicles (FRAV) to describe functional performance requirements that may be applicable to automated and/or autonomous vehicles. It is based upon ECE/TRANS/WP29/2019/34/Rev.1, WP.29-179-23, and ACSF-24-05.

1. Purpose of the Statement

Under its Terms of Reference (WP.29/1147/Annex V), the Informal Working Group on Functional Requirements for Automated/Autonomous Vehicles (FRAV) has been established by WP.29 under GRVA to develop functional (performance) requirements for automated/autonomous vehicles, in particular, the combination of the different functions for driving:

- longitudinal control (acceleration, braking and road speed)
- lateral control (lane discipline)
- environment monitoring (headway, side, rear)
- minimum risk manoeuvre
- transition demand
- HMI (internal and external)
- driver monitoring.

This work should also cover the requirements for Functional Safety. FRAV has been further instructed to pursue this work in line with the following principles/elements described in the WP.29 Framework Document on Automated/Autonomous Vehicles (WP.29/2019/34/Rev.2):

- System safety
- Failsafe Response
- HMI/Operator information
- OEDR (Functional Requirements).

FRAV has prepared this document to provide a structure for fulfillment of this work. This structure aims to promote alignment between the work of FRAV and the work of the Informal Working Group on Validation Methods for Automated Driving (VMAD). VMAD has been tasked to develop a New Assessment/Test Method to include assessment of compliance with the common functional performance requirements to be developed by FRAV.

FRAV proposes to progressively refine this document as an instrument towards the delivery of proposals for functional performance requirements. Final decisions on the proposals rests with WP.29 and the Contracting Parties. As such, this document does not propose a legal text. The document aims to inform WP.29 and the Contracting Parties and support such decisions as WP.29 and the Contracting Parties may wish to take.

At the present time, FRAV has been tasked to deliver common functional requirements [based] on existing national/regional guidelines and other relevant reference documents (1958 and 1998 Agreements) for submission to WP.29 for its 180th session in March 2020. Therefore, FRAV provides the following synthesis of the guidelines and other reference documents to describe the proposed scope, structure, and direction of its work for consideration by WP.29 and the Contracting Parties.

2. Definitions

The introduction of automated driving systems and related technologies has resulted in a proliferation of new terms and concepts. Therefore, FRAV proposes to provide definitions of the terms used in the provisions for functional performance requirements developed by the group. In line with its Terms of Reference, FRAV will consider existing research and voluntary standards available across the Contracting Parties in developing its proposals. Examples of terms discussed within FRAV include the following:

2.1. “Dynamic driving task” means all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including without limitation: Lateral vehicle motion control via steering (operational); Longitudinal vehicle motion control via acceleration and deceleration (operational); Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical); Object and event response execution (operational and tactical); Maneuver planning (tactical); and Enhancing conspicuity via lighting, signaling and gesturing, etc. (tactical).

2.2. *"Minimal risk condition"* means a condition to which a user or an automated driving system may bring a vehicle in order to reduce the risk of a crash when a given trip cannot or should not be completed.[1]

2.3. *"Minimal risk maneuver"* means a procedure automatically performed by the automated driving system to place the vehicle in a minimal risk condition in a manner that minimizes risks in traffic.[2]

2.4. *"Operating environment"* means the operating conditions which a vehicle can reasonably be expected to encounter when in automated mode.

2.5. *"Operational design domain"* refers to the operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.[3] The operational design domain is a subset of the operating environment.

2.6. *"Transition demand"* is a logical and intuitive procedure to transfer the dynamic driving task from automated control by the system to human driver control.[4]

2.7. *"VMAD"* refers to the GRVA informal working group on Validation Methods for Automated Driving.

2.8. *"VMAD scenario"* refers a configuration of traffic variables as defined within the VMAD traffic scenario database.

2.9. *"VMAD traffic scenario database"* is the proposed database or catalog of traffic conditions that are reasonably foreseeable under which a vehicle can reasonably be expected to avoid causing an event resulting in injury or death.

3. System Safety

When in 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. This level of safety implies that an automated/autonomous vehicle shall not cause any non-tolerable [unacceptable level of] risk, meaning that automated/autonomous vehicle systems, while in automated mode, shall not cause any traffic accidents

[1] Definition derived from SAE J3016:2018

[2] Definition derived from ACSF-24-05 (clean); however, the term "minimal" has been substituted for "minimum" and the definition refers to the minimal risk condition for consistency with SAE J3016:2018. The definition omits the ACSF reference to "after a transition demand" under the assumption that such maneuvers could be executed by Level 4/5 vehicles without driver controls or the demand could be skipped if the driver monitoring system detects that a transition to the driver is not appropriate.

[3] Definition from SAE J3016:2018

[4] Definition from ACSF-24-05 (clean)

[incidents/events] resulting in injury or death that were reasonably foreseeable and preventable.

In terms of its alignment with the VMAD NATM structure, System Safety is closely associated with the Audit phase(s) where manufacturer documentation provides the basis for an assessment of vehicle system design safety and safe performance across the scenarios applicable to the vehicle.

3.1. Activation and use of the vehicle in automated mode shall only be possible within the boundaries of the automated driving system's operational design domain.

3.2. When in automated driving mode,

3.2.1. The vehicle shall respond to reasonably foreseeable conditions within its operational domain without causing an event [crash] resulting in injury or death [or property damage];

3.2.1.1. Adapt to conditions (road geometry, weather)

3.2.1.2. VRU risks

3.2.1.3. Does not disrupt traffic

3.2.2. The vehicle shall comply with all applicable road traffic laws except in cases where such compliance would conflict with paragraph 2.2.1.

3.3. [Functional requirements related to overall system design safety (e.g., CEL)?]

3.3.1. Dealing with fault conditions separately from above operational (UK)

3.4. The System must comply with the traffic rules but may temporarily bend these rules (during an emergency, uncommon or edge case situation), if such actions reduce safety risks or are required for the safe flow of traffic (e.g., crossing a double centre line to go around an obstacle)

3.5. The System shall behave in a way that maintains the safe flow of traffic and is predictable to other road users and "comfortable" to occupants (following distance, lane centering, gradual acceleration/braking/steering, proper signaling)

3.6. The system shall adapt to the driving conditions (reduce speed on wet/snowy/icy/gravel roads or due to visibility factors, road geometry)

3.7. The system shall anticipate possible collisions and act in a manner to reduce their possibility of occurrence

3.8. The system shall minimize the risks to vulnerable road users (VRU) in the case of an imminent collision (e.g., hit vehicle instead of VRU)

3.9. If an update renders the system obsolete or otherwise no longer supported, it shall not permit activation

3.10. When in the automated driving mode ("Operational Domain"-OD), the automated vehicle drives and shall replace the driver for all the driving tasks for all the situations which can be reasonably expected in the OD.

3.11. When in the automated driving mode, the vehicle shall not cause any traffic collision that are rationally foreseeable and preventable. Any avoidable accident shall be avoided, The overall safety target shall be at least as good as manual driving, i.e. P (accident with fatalities)< 10-8 /h and P(accident with light or severe injuries) <10-7/h.

3.12. The vehicle shall also be designed to minimize potential effects of errors from the vehicles' users, inside and outside of the vehicle, and of other road users.

3.13. The vehicle shall be able to keep a safe distance with other vehicles in front, exhibit caution in occluded areas, leave time and space for others in lateral maneuvers, be cautious with right-of-ways and if a traffic collision can be safely avoided without causing another it shall be avoided.

3.14. When in the automated driving mode, the vehicle shall, as far as possible, have a predictable and careful behaviour and shall allow an appropriate interaction with other road users (e.g. obey to orders by authorities or communication with other road users when needed).

4. Operational Design Domain (ODD)

This chapter concerns the description of a vehicle’s Operational Design Domain (ODD). The ODD describes the specific conditions under which the automated vehicle is intended to operate in automated mode. For the assessment of vehicle safety, the vehicle manufacturer should document the ODD of the vehicle and the functionality of the vehicle within the prescribed ODD. Within the context of an efficient method to validate compliance with functional performance requirements, safety authorities and vehicle manufacturers will need a shared methodology to describe this functionality and its documentation. Given the anticipated need to understand the ODD in relation to the proposed VMAD scenario database, the ODD and scenario database methodologies will also need to be compatible.

4.1. In line with the Framework Document, the ODD description shall include (at a minimum):[5]

4.1.1. Roadway types

4.1.2. Geographic area

4.1.3. Speed range

4.1.4. Environmental conditions

4.1.5. Other constraints

[5] FRAV will consider ISO/WD 34503: Road vehicles — Taxonomy for operational design domain for automated driving systems

4.1.6. The system shall have a clearly defined ODD for each function with at minimum consideration for variables such as weather, road type, speed

4.1.7. The system shall be able to detect its OD

4.1.8. The system shall not allow activation of a function if the OD is outside the function's ODD

5. Execution of Dynamic Driving Tasks

This chapter refers to physical demonstration that a vehicle can safely respond to reasonably foreseeable conditions applicable to its vehicle automation system. Vehicle automation systems will execute dynamic driving tasks (DDT). The DDT encompasses all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic including without limitation:

- Lateral vehicle motion control via steering (operational)
- Longitudinal vehicle motion control via acceleration and deceleration (operational)
- Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical)
- Object and event response execution (operational and tactical)
- Maneuver planning (tactical)
- Enhancing conspicuity via lighting, signaling and gesturing, etc. (tactical).

For simplification purposes, SAE J3016 refers to the third and fourth items collectively as Object and Event Detection and Response (OEDR). In line with its Terms of Reference and the Framework Document, FRAV accepts this shorthand, describing the DDT as the complete OEDR and longitudinal/lateral motion control.

This chapter is closely associated with the physical testing phase(s) of the VMAD NATM (e.g., manufacturer on-road and track testing, third-party track and real-world testing).

5.1. Object and Event Detection and Response (OEDR)

5.1.1. The automated driving system shall detect and classify objects and events that may be reasonably expected within its operational domain.

5.1.1.1. The system shall be able to detect the roadway

5.1.1.2. The system shall be able to identify lane location (w/, w/o markings)

5.1.1.3. The system shall be able to detect and identify lane markings

5.1.1.4. The system shall be able to detect objects in its defined field of view

5.1.1.5. The system shall be able to estimate the speed and heading of objects

5.1.1.6. The system shall be able to classify static and dynamic objects in its defined field of view which are foreseeable in the OD (at minimum, it must classify: light vehicles, heavy vehicles, pedestrians, cyclists, motorcyclist, emergency vehicles, animals, traffic control devices, traffic signs …)

5.1.1.7. The system shall be able to recognize and respond to traffic control devices, traffic signs and infrastructure including the state of traffic control devices

5.1.1.8. The system shall be able to detect indications of object intent (e.g., turn signal, acceleration, location in lane, body position, eye glaze)

5.1.1.9. The system shall be able to predict the behaviour of detected objects and take appropriate action to reduce the risk of collisions

5.1.1.10. The system shall treat objects which cannot be classified with increased uncertainty

5.1.1.11. The system shall be able to recognize and react to service providers with responsibilities to direct traffic (e.g., police, construction worker)

5.1.1.12. The system shall take into consideration that other road users may not respect traffic laws

5.1.1.13. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections)

5.1.1.14. The system sensors shall be capable of detecting objects within the lane in front of the vehicle up to at least the minimal braking distance required for the vehicle to come to a full stop

5.1.1.15. The system shall not allow a lane change unless the rear sensors are capable of detecting objects to the immediate sides and in both rear adjacent lanes at a distance that would allow the manoeuvre without requiring hard braking of an oncoming vehicle

5.1.2. The automated driving system shall detect conditions within its operational domain that fall outside the boundaries of its operational design domain as defined in paragraph 3.2.

5.2. Normal Driving

5.2.1. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain.

5.2.1.1. The automated driving system shall execute such maneuvers without causing outcomes resulting in injury or death.

5.2.1.2. The automated driving system shall execute such maneuvers without disrupting the normal flow of the surrounding traffic.

5.3. Other Driving

5.3.1. The automated driving system shall execute a failsafe response when the conditions defined for its operational design domain are not satisfied for a duration exceeding [time limit].

5.3.2. The automated driving system shall execute an emergency response when conditions for the execution of a failsafe response are not present.

6. Human-Machine Interface/Operator Information

This chapter refers to internal and external human interactions with the automated vehicle and automation system. As with conventional vehicles, human ability to safely use the vehicle cannot involve significant learning curves. Therefore, automated vehicles will require a level of uniformity in their interactions with human users. To the extent that an automated system relies upon human involvement for safe operation, the automated vehicle will require measures to minimize risks of misuse and abuse and to respond safely in cases where the human driver fails to fulfill minimum requirements for safe use. Automated/autonomous vehicles that may require the driver to assume control of the driving task will require the means to assess driver awareness and readiness to perform the full driving task. In addition, automated vehicles will need means to interact safely with other road users (e.g. by means of external HMI on operational status of the vehicle, etc.).

6.1. The vehicle manufacturer shall define the operational design condition under which the automated driving system is designed to be activated, operated and deactivated.

6.2. Vehicles equipped with automated driving systems that may require driver intervention (e.g., transition demand) shall detect if the driver is available to take over the driving task by continuously monitoring the driver.[6]

6.3. The vehicle shall clearly communicate to the user:

6.3.1. Status of the automated driving system

6.3.1.1. System availability

6.3.1.2. System mode active

6.3.1.3. System malfunction

6.3.2. Critical messages

6.3.3. Transition demand

6.3.4. Initiation of minimal risk maneuver

6.3.5. Status of driver availability

6.4. The vehicle shall signal to other road users:

6.4.1. Intentions to undertake dynamic driving tasks

6.4.2. Initiation of a minimal risk maneuver

6.4.3. Other safety-critical information.

6.4.4. Communication of Take-over request to the driver.

6.4.5. Communication of the system status to the driver.

6.4.6. Communication of malfunctions to the driver.

6.4.7. Communication of critical messages to the driver.

[6] Derived from ACSF-24-05 (clean), para. 2.6.2.

6.4.8. Recognition of MRM in operation by the driver.

6.4.9. Demonstration of activation/deactivation of AV mode.

6.4.10. Demonstration of driver availability (awareness, readiness and engagement) and override feature.

6.4.11. Demonstration of signaling features. Interaction with other road users.   The system shall have intuitive user controls and communications systems

6.4.12. The system HMI will clearly indicate if the system is active, available or disabled

6.4.13. If the vehicle has multiple systems with varying degrees of driver interaction, distinct symbols and activation methods shall be used to avoid mode confusion

6.4.14. The system Software and Hardware versions shall be accessible

6.4.15. The system shall clearly communicate: degraded operation, malfunctions, failures, required system maintenance, emergency conditions, ongoing minimal risk manoeuvres or take-over requests to the driver/occupants.

6.4.16. The system shall clearly communicate the need, and provide the driver sufficient time for take-over requests

6.4.17. The system shall be able to, at minimum, bring the vehicle to a gradual stop if the driver has not taken over the driving task after the provided take-over time

6.4.18. The system shall be able to execute emergency manoeuvres in an attempt to avoid imminent hazards

6.4.19. If the system shall monitor the take-over-ready driver, in the case of a level 3 system, the driver must remain available for system operation. In the case of a level 4+ system, a take-over request shall not be issued to a driver who is unavailable.

6.4.20. The system shall clearly communicate its intention to pedestrians, cyclists and other road users (e.g., turn signals, speed change, high beam flash, other external communication)

6.4.21. Driver availability and override possibility (if required, based on level of automation)

6.4.22. (AV 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)

6.4.23. The driver shall be made aware of the use and the limits of the automated driving mode, as well as which tasks other than driving may be enabled by the system for the driver (This is only about the technical capability of the system and without prejudice to national traffic rules).

6.4.24. If the system is designed to request the driver to take over under some circumstances, the system shall monitor whether the driver is ready to take over driving from the system. It shall ensure through appropriate design (e.g. driver monitoring system) and warnings that the driver remains available to respond to take over request and prevent any foreseeable and preventable misuse by the driver in the OD.

6.4.24.1. Means shall be provided to humans (driver or if no driver, passenger or operation control center) to deactivate or override immediately the automated mode in an easy manner (deliberate action).The system may however momentarily delay deactivation (and may include a driver take over request if there is a driver) when an immediate human deactivation could compromise safety.

6.4.24.2. During the whole MRM, the driver can take over in usual way.

6.4.25. For vehicles designed to operate only with no driver (e.g. driverless shuttles), a communication function shall be provided to send an emergency notification to an operation control centre. A camera and voice communication device shall be provided in the vehicle so that an operation control centre can monitor the situation inside the vehicle.

7. Failsafe Response

Each automated/autonomous vehicle must be able to detect system failures and when the conditions of its ODD are no longer present (ODD exit). In such cases, the vehicle must have appropriate fallback strategies to ensure safety, including transition of control to the driver and minimal risk maneuver(s) in the event that a transition to the driver cannot be safely executed. This chapter describes such “failsafe responses”. Items under discussions within FRAV include:

7.1. When in automated driving mode,

7.1.1. The vehicle shall automatically initiate a failsafe response or sequence of failsafe responses in response to detection of conditions outside its operational design domain for a duration not to exceed [time limit].

7.1.2. Failsafe responses shall only be initiated when conditions permit their completion in compliance with paragraph 2.2.

7.2. Failsafe responses include:

7.2.1. Transition demand

7.2.1.1. The system may request the driver to take over with a sufficient lead time in particular when

7.2.1.1.1. -the driver overrides the system or

7.2.1.1.2. -when the system determines that it is difficult to continue automated driving mode, such as when the situation becomes outside the OD, or when a problem has occurred to the automated vehicle. "

7.2.1.2. The system shall give sufficient leadtime to the driver to take over and shall remain in the automated driving mode as long as the driver has not taken over, and/or will otherwise transfer to a minimum risk manoeuvre.

7.2.1.3. The system shall be designed to enable the driver to clearly recognize the take over request from the system.

7.2.1.4. The system shall be able to determine whether or not the driver has taken over. This verification shall at least include a criterion on vehicle lateral control by the driver unless the vehicle is already stopped.

7.2.1.4.1. When the driver takes over control on his own (manual deactivation/override), the system shall not disturb the driver take over by inappropriate action(e.g. by switching off light by night).

7.2.1.4.2. When the driver takes over after a system request, the system shall give back control to the driver with a vehicle confirguration maximizing driver controlability (e.g. wipers ON in case of rain, headlamps ON by night).

7.2.1.4.3. Non-driving activities allowed in the AD mode shall be consistent with the available delay for the driver to takeover after a system request.

7.2.1.5. For vehicles designed to operate only with no driver (e.g. driverless shuttles), a communication function shall be provided to send an emergency notification to an operation control centre. A camera and voice communication device shall be provided in the vehicle so that an operation control centre can monitor the situation inside the vehicle.

7.2.2. Minimal risk maneuver

7.2.2.1. When the system detects that it is difficult to continue in the automated driving mode, it shall be able to transfer to a minimal risk condition (with or without take over request) through a minimal risk manoeuvre.

7.2.2.2. A minimum risk manoeuvre shall be perfomed in case of shock in the best possible way, according to vehicle operational status and current situation.

7.2.2.3. The minimum risk manoeuvre shall lead to a vehicle stop.

7.2.2.4. The Minimum Risk Manoeuvre (MRM) shall comply with traffic rules. MRM settings for automated vehicles may include measures to stay in or change the lane while warning to the surrounding and automatically stop the vehicle in a safe manner on the side of the road.

7.2.2.5. The driver may be asked to take over at the end of the minimum risk manoeuvre (e.g. to park on the side of the road in case of level 3 lane keeping system). If the driver does not respond to the take over request, the vehicle shall be stopped in parking mode and the AD mode shall be desactivated.

7.2.3. Emergency maneuver

7.3. The system shall anticipate a function crossing the ODD boundaries and seek to remain within the function's ODD limits

7.4. Upon crossing the function ODD limits, the system shall take action to minimize risks (e.g., re-enter function ODD limits, revert to minimal risk condition, transition to driver, emergency manoeuvre) and notify the occupants the ODD boundary has been crossed

7.5. The system shall not cross and re-enter function ODD limits cyclically and shall seek other actions to minimize risks if this occurs

7.6. The system shall have appropriate redundancies that allow it to, at minimum, execute an emergency stop in the case of any system failure or emergency

7.7. The system shall be equipped with a monitoring system that can detect: faults, malfunctions or other abnormalities of system components and monitor system performance

7.8. The system shall take appropriate measures when a system abnormality/fault is detected in order to reduce risk (degraded mode, limp mode, revert to minimal risk condition etc.)

7.9. The system shall communicate with occupants, authorities, owners, operators or first responders after an abnormality/fault is detected, after a collision or after otherwise manoeuvred to a minimal risk condition

8. Post-crash behavior

8.1. Following a collision, the vehicle shall be brought to a complete stop to the best capabilities of the system and shall be brought to a minimal-risk state

8.2. The system shall inform the occupants and contact emergency service providers, owners and/or operators

8.3. Prior to re-activation, the system shall conduct self-diagnostics to ensure it is capable of operation

8.4. Upon direction by emergency personnel or authorised user, the system, if able, shall move off the roadway