This document integrates items raised in the discussions of FRAV-02-05 during the 2nd FRAV informal group session. This document is an interim draft for further discussion.

The document proposes draft text. In cases where stakeholders have proposed similar or related text, the alternative or complementary text is provided in brackets to facilitate comparison and synthesis.

The sidebars provide supplemental context or highlight issues for consideration. For example, some text is taken from approved WP.29 documents such that changes to the text could impact the source document(s) or necessitate approval from GRVA or WP.29 to use the alternative text. Specific questions or proposals raised are highlighted in red.

Draft Report 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. Background

The background section documents the basis and development of the paper (as is done in GTR technical reports).

1.1. 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 the Working Party on Automated/Autonomous and Connected Vehicles (GRVA) to develop functional (performance) requirements for automated[/autonomous] vehicles, in particular, the combination of the different functions for driving:

First two paragraphs taken from the Framework Document and ToR.

Should we delete the term “autonomous” per SAE J3016 recommended practice as proposed by Russia? If so, should FRAV recommend this to GRVA?

- longitudinal control (acceleration, braking and road speed)
- lateral control (lane discipline)
- environment monitoring (headway, side, rear)
- minimal risk maneuver
- transition demand

- HMI (internal and external)
- driver monitoring.

1.2. This work should also cover the requirements for Functional Safety. FRAV has been further mandated 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, hereafter, the Framework Document):

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

1.3. The Framework Document established one deliverable specific to functional performance requirements for automated vehicles. GRVA was requested to submit a document on "common functional requirements [based] on existing national/regional guidelines and other relevant reference documents (1958 and 1998 Agreements)" for consideration during the 180th (March 2020) session of WP.29.

1.4. Although not specified in the FRAV Terms of Reference, the Framework Document implies and GRVA has requested that FRAV provide the basis for this submission to WP.29. Therefore, FRAV considered a "Comparison table of ADS Guidelines in USA, Canada, Japan, EU, Australia and China" (VMAD-01-04) prepared by OICA. At its first session (FRAV-01, 9-10 October 2019, Berlin), FRAV further considered a table of "common AV safety elements" (FRAV-01-13) whereby OICA distilled its comparison table into a single set of elements. Pursuant to an FRAV request, OICA aligned its table with the Framework Document in a revised document (FRAV-01-13/Rev.1).

1.5. The basis for this present document was an effort to transpose the FRAV-01-13/Rev.1 table into a format suitable for long-term development of more detailed provisions as well as for use in FRAV meeting sessions (e.g., projection on a screen). Originally presented as FRAV-02-05, FRAV has decided to reserve the number "05" for future versions. For example, FRAV will use FRAV-03-05 for this document as considered during its 3rd session (FRAV-03, 14-15 April 2020, Paris), FRAV-04-05 during its 4th session (FRAV-04, 8-9 September 2020, Santa Clara), and so on.

2. Purpose

2.1. FRAV has prepared this document to provide a structure for fulfillment of the objectives defined in its Terms of Reference. This structure aims to promote coordination between the work of FRAV and that of other WP.29 informal working groups addressing areas related to automated driving. In particular, the document aims

to facilitate alignment between FRAV and the work of the GRVA 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.

2.2. FRAV proposes to progressively refine this document as an instrument towards the delivery of proposals for functional performance requirements. Final decisions on the proposals rest 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.

3. Definitions

3.1. 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, voluntary standards, and guidelines available across the Contracting Parties in developing its proposals.

This is not a legal document; the document provides definitions to support mutual understanding of terms used in the document, not to propose regulatory definitions.

3.2. Examples of terms discussed within FRAV include the following:

3.2.1. *"Automated Driving System (ADS)"* means the hardware and software that are collectively capable of performing the entire dynamic driving task (DDT) on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD); this term is used specifically to describe a level 3, 4, or 5 driving automation system.

3.2.2. *"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). [1]

[1] Definition derived from SAE J3016:2018

3.2.3. *"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.[2]

3.2.4. *"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.[3]

3.2.5. *"New Assessment/Test Method (NATM)"* means the tools and methodologies for the assessment of automated vehicle safety performance under development by the GRVA Informal Working Group on Validation Methods for Automated Driving (VMAD).

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

3.2.7. *"Operational design domain (ODD)"* 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.[4]

FRAV recommends consistent use of "operational design domain" (ODD) and avoidance of the term "operational domain" (OD). OD does not have a uniform definition and introduces unnecessary risks of confusion with the term ODD.

3.2.8. *"Transition demand"* is a logical and intuitive procedure to transfer the dynamic driving task from automated control by the system to human driver control.[5]

4. System Safety [System Behavior]

4.1. It is necessary to clearly define the split in responsibilities between the driver and the ADS.

[2] Definition derived from SAE J3016:2018

[3] 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.

[4] Definition from SAE J3016:2018

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

4.2. 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 risk [introduce unreasonable risks], meaning that automated/autonomous vehicle systems, while in automated mode, shall not cause any traffic accidents [incidents/events] resulting in [destruction of property,] injury or death that were reasonably foreseeable and preventable.

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

4.4. Requirements under consideration include:

4.4.1. The Automated Driving System (ADS) shall react to unforeseen situations in a way that minimizes risk.

4.4.2. The vehicle shall demonstrate adequate mitigation of risks (e.g. approaching ODD boundaries), safe driving behavior and good Human Machine Interface

4.4.3. 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)

4.4.4. When in the automated driving mode, the vehicle shall not cause any traffic collision that are rationally [reasonably] foreseeable and preventable. Any avoidable accident shall be avoided.

4.4.5. When in automated driving mode, 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 ODD.

4.4.6. [The nominal operation of the ADS shall result in equal or safer performance than a human driver. i.e. achieve a neutral or positive risk balance.] [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.]

4.4.7. 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.

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

This paragraph is taken from the Framework Document. The suggestion is to replace "cause any non-tolerable risk" with "introduce unreasonable risks" to align with the body of consumer law related to the term "unreasonable risk" (e.g., 15 U.S.C. 2064(b)(3)). The suggestion is to replace "accidents" with another term of art per Fenton v. Thorley: "The word accident is not a technical legal term with a clearly defined meaning."

Canada has proposed addition of "destruction of property".

4.4.9. Dynamic behavior in road traffic

4.4.9.1. When in automated driving mode,

4.4.9.1.1. The vehicle shall respond to reasonably foreseeable conditions within its operating environment without causing an event resulting in [destruction of property,] injury or death; [The system shall adapt to the driving conditions (reduce speed on wet/snowy/icy/gravel roads or due to visibility factors, road geometry)] [The system shall anticipate possible collisions and act in a manner to reduce their possibility of occurrence] [The Automated Driving System (ADS) shall not cause any traffic accidents that are reasonably foreseeable and preventable.]

4.4.9.1.2. The vehicle shall not disrupt the normal flow of traffic [The Automated Driving System (ADS) shall have predictable behavior] [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)] [That Automated Driving System (ADS) shall have predictable behaviour.]

4.4.9.1.3. The vehicle shall comply with all applicable road traffic laws except in cases where compliance would conflict with the above subparagraphs. [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)] [The ADS shall drive in accordance with the traffic rules.

4.4.9.1.4. The ADS shall prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects.

5. Operational Design Domain (ODD)

5.1. 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.

This paragraph comes from the Framework Document. The Framework Document specifically places responsibility for ODD definition on the manufacturer. FRAV agrees that ODD definition is a manufacturer responsibility but notes that this view does not prejudice the powers of safety authorities to define minimum performance requirements for automated vehicles that may impact ODD definitions (i.e., result in de facto or de jure minimum ODD requirements).

5.2. 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.

5.3. The manufacturer shall declare the scope of the ADS (so called operational design domain(s) (ODD)) e.g. where and when the ADS is designed to operate.

5.4. The ODD description shall include (at a minimum):

The cited items are taken from the Framework Document. SAE J3016 refers to "environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics" (see ODD definition in "Definitions" chapter).

5.4.1. Roadway types [Road conditions (motorways/expressways, general roads, number of lanes, existence of lane marks, roads dedicated to automated driving vehicles, etc.)]

5.4.2. Geographic area [Geographical area (urban and mountainous areas, geofence setting, etc.)]

5.4.3. Speed range

5.4.4. Environmental conditions [Environmental conditions (weather, night-time limitations, etc.)]

5.4.5. V2X dependencies (e.g., dependence on connectivity and availability of vehicle, infrastructure or other external sources of data)

5.4.6. Other constraints [Other conditions that must be fulfilled for the safe operation of the ADS.]

6. Execution of Dynamic Driving Tasks

6.1. 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).

6.2. 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.

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

6.4. Object and Event Detection and Response (OEDR)

6.4.1. *"Object and Event Detection and Response (OEDR)"* means the detection by an ADS of circumstances that are relevant to the immediate driving task, as well as the implementation of the appropriate response to such circumstances.

6.4.2. The ADS shall have OEDR capabilities that support safe and appropriate actions when subjected to reasonably foreseeable scenarios within the ODD.

6.4.3. The automated driving system shall detect and classify objects and events that may be reasonably expected within its operational domain. [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 …)]

6.4.4. Objects and events include, but are not limited to, the following:

6.4.4.1. The system shall be able to detect the roadway

This chapter structure tries to reconcile disparities between the Framework Document, the ToR, and SAE J3016. The ToR specifies longitudinal/lateral motion control and OEDR. The Framework Document only identifies OEDR specifically (motion control is captured or implied elsewhere in the text). J3016 defines DDT as motion control plus OEDR. Therefore, this document uses DDT as the chapter heading with subchapters for OEDR and motion control to adhere to the FRAV ToR.

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

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

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

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

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

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

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

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

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

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

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

6.4.4.13. 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

6.4.4.14. 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 maneuver without requiring hard braking of an oncoming vehicle

6.4.4.15. The automated driving system shall detect conditions within its operating environment that fall outside the boundaries of its operational design domain. [The ADS must be capable of identifying when conditions defining the ODD are met and predicting when they will no longer be met.] [The automated driving system shall detect and respond to conditions within its operating environment that

indicate the approach of boundaries of its operational design domain as defined in paragraph 3.2.[explanation: for safe driving it is needed that detection and reaction are before the actual exceedance of the ODD]

6.4.4.16.

6.5. Longitudinal and lateral motion control

6.5.1. Normal Driving

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

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

6.5.1.3. The automated driving system shall execute such maneuvers without disrupting the normal flow of the surrounding traffic. [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.] [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).]

6.5.2. Other Driving

6.5.2.1. The automated driving system shall execute a failsafe [safe fallback] response when the conditions defined for its operational design domain are not present.

6.5.2.2. The automated driving system shall execute an emergency response when conditions for the execution of a failsafe [safe fallback] response are not present.

7. Human-Machine Interface/Operator Information

7.1. 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

This section draws from FRAV-01 and especially China's well-received paper concerning structuring of FRAV to cover nominal driving conditions and conditions outside the generally accepted notions for normal driving (e.g., crash event scenarios, edge/corner cases).

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.).

7.2. Requirements under consideration include:

7.2.1. Activation and deactivation

7.2.1.1. The activation of the ADS shall only be possible when the conditions of the ODD are met.

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

7.2.1.3. Human override of system control

7.2.1.3.1. 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).

7.2.1.3.2. 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.

7.2.1.3.3. Means shall be provided to the user to deactivate or override the ADS in an easy manner. The ADS may however momentarily delay deactivation if safety is compromised by the immediate input of the user.

7.2.1.3.4. When necessary the ADS shall protect the vehicle control against inadvertent or undeliberate [unintentional] user intervention.

7.2.1.4. The ADS deactivation shall only be performed when it has been verified that the user has taken over control.

7.2.2. 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. [Demonstration of driver availability (awareness, readiness and engagement) and override feature] [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.] [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.] [When the ADS is active it shall be capable of determining the user's status.] [If the system is designed to request and enable the user to take over control under some circumstances, the ADS shall ensure through appropriate design and warnings that the user remains available to respond to the takeover request.]

7.2.3. The system shall have intuitive user controls and communications systems. [If the vehicle has multiple systems with varying degrees of driver interaction, distinct symbols and activation methods shall be used to avoid mode confusion] [The mode concept shall be designed in a way that minimizes mode confusion at the user and system level.]

7.2.4. 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.

7.2.5. Information shall be available to the vehicle's user that clearly defines their responsibilities, the procedures to comply with a takeover requests, and possible consequences if they do not comply.

7.2.6. The vehicle shall clearly communicate to the user: [The ADS shall communicate critical messages to vehicle's users and other road users when needed.]

7.2.6.1. Status of the automated driving system [Communication of the system status to the driver] [The system HMI will clearly indicate if the system is active, available or disabled] [The ADS shall clearly inform user about the operational status (operational, failure, etc.) in an unambiguous manner.]

China introduced the concept of "Operational Domain Conditions" (FRAV-02-09 and FRAV-02-15) which connects ODD with concepts of system dependency on driver fulfillment of safety-critical responsibilities. The number of comments related to this driver-system interaction suggests an important subset for FRAV consideration.

7.2.6.1.1. System availability

7.2.6.1.2. System mode active

7.2.6.2. System malfunction [Communication of malfunctions to the driver] [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.] [The system shall be equipped with a monitoring system that can detect: faults, malfunctions or other abnormalities of system components and monitor system performance.]

7.2.6.3. Critical messages [Communication of critical messages to the driver]

7.2.6.4. Transition demand [Communication of Take-over request to the driver.] [The system shall clearly communicate the need, and provide the driver sufficient time for take-over requests]

7.2.6.5. Initiation of minimal risk maneuver [Recognition of MRM in operation by the driver]

7.2.6.6. Status of driver availability [Driver availability and override possibility (if required, based on level of automation)]

7.2.6.7. 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

7.2.6.8. 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.

7.2.7. The vehicle shall signal to other road users [Demonstration of signaling features. Interaction with other road users.]:

7.2.7.1. Intentions to undertake dynamic driving tasks [The system shall clearly communicate its intentions to pedestrians, cyclists and other road users (e.g., turn signals, speed change, high beam flash, other external communication)] [When needed, communication with other road users shall provide sufficient information about the vehicle's status and intention.]

7.2.7.2. Initiation of a minimal risk maneuver

7.2.7.3. Other safety-critical information.

7.2.8. Activities other than driving

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

7.2.8.2. 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).

7.2.8.3. If applicable, activities other than driving that are provided by the ADS to the user once the ADS is activated shall be automatically suspended as soon as the ADS issues a transition demand or is deactivated.

7.2.9. Vehicles without driver controls

7.2.9.1. 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.

7.2.9.2. For ADS designed to operate with no driver present in the vehicle e.g. driverless shuttles, an audio and visual communication channel shall be provided to exchange emergency notifications.

8. Failsafe [Safe Fallback] Response

8.1. 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”.

8.2. The ADS shall be equipped with appropriate technical measures that continuously monitor system performance, perform fault detection and hazard analysis, signal any

detected malfunctions that affect the system performance, and ultimately take corrective actions or revert to a minimal risk condition when needed.

8.3. The ADS should therefore be designed, to the extent practicable, to function predictably, controllably, and safely in the presence of faults and failures affecting the system performance.

8.4. In case of failure impacting the safety of the ADS, an appropriate control strategy shall be in place as long as the failure exists.

8.5. When in automated driving mode,

8.5.1. 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].

8.5.2. Failsafe responses shall only be initiated when conditions permit their completion.

8.5.3. 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

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

8.5.5. 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

8.5.6. 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.)

8.6. Failsafe responses include:

8.6.1. Transition demand [Takeover of DDT (if required, based on level of automation)]

8.6.1.1. The system shall be capable of transferring control back to the user in a safe manner.

8.6.1.2. The system shall be able to determine whether or not the user has taken over.

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

8.6.1.3.1. the driver overrides the system or

8.6.1.3.2. 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.

8.6.1.4. The system shall give sufficient lead time 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. [The ADS shall remain active as long as the vehicle's user has not taken over, or the ADS has reached a Minimal Risk Condition (MRC).]

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

8.6.1.6. 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.

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

8.7. Minimal risk maneuver

8.7.1. 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.

8.7.2. The Minimal Risk Manoeuvre (MRM) shall be capable of achieving an MRC when a given trip cannot or should not be completed for example in case of a failure in the ADS or other vehicle systems.

8.7.3. Fallback strategies shall take into account that users may be inattentive, drowsy, or otherwise impaired, and shall therefore be implemented in a manner that will facilitate safe operation and minimize erratic driving behaviour.

8.7.4. 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.

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

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

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

8.7.8. 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.

8.7.9. 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.

8.8. Emergency maneuver

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

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

8.9. [Crashworthiness/compatibility]

8.10. Post-crash behavior [Post-crash behaviors (Collision Notification to Occupants and Emergency services; Return to a safe state)]

8.10.1. 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

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

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

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

8.10.5. After detection of a first significant shock while driving (e.g. frontal collision with airbags triggering or lateral collision during an insertion), the vehicle shall:

8.10.5.1. inhibit AD mode reactivation until proper operation has been verified,

8.10.5.2. immediately attempt to achieve a safe state in the best possible way, according to vehicle operational status and current situation

8.10.6. The ADS may also, simultaneously, request the user to takeover vehicle control if vehicle and current situation are sufficiently controllable.

9. [In-use Performance] [Safety of In-use Vehicles

9.1. Inspections/Repair/Modifications processes

9.1.1. Not within the scope of UNECE's Informal Working Group – Functional Requirements for Automated vehicles (FRAV).

9.2. Maintenance of existing level of crashworthiness (for vehicles carrying occupants)

9.2.1. Requirements covered by UNECE's Working Party on Passive Safety (GRSP)

9.3. Vehicle state monitoring

9.3.1. Any safety related failures regarding the roadworthiness of the ADS shall be systematically reported to the vehicle user.

10. Consumer education and training

11. Other items for consideration (not clear where to position in document)

11.1. Demonstration of activation/deactivation of AV mode.

11.2. The system Software and Hardware versions shall be accessible

11.3. Dealing with fault conditions separately from operational requirements (UK)