Submitted by the expert from SAE

Document FRAV-09-06
9th FRAV session
12 January 2021

This is a revision of Document 5 building from FRAV-03-05-Rev.1. Previously considered text is shaded in green, meaning that FRAV has reviewed and accepted the text under its working consensus. This status does not mean the text has been formally approved by FRAV for submission to GRVA and/or WP.29. Document 5 only reflects FRAV discussions to date pending further work.

New paragraphs and changes to the previous version of Document 5 are shaded in blue. Outstanding paragraphs under consideration from the previous version are shaded in yellow. In the case of changes to pre-existing text (whether considered by FRAV or not), the proposal for revised text is in the second column for comparison against the earlier text in the first column.

Unshaded text is carried over from FRAV-03-05-Rev.1 and has not yet been discussed/accepted as working text by FRAV.

Current Text and Proposals (green = accepted, blue = new text for consideration, yellow = previous text still under consideration, unshaded = not yet discussed)	Alternative text to previous text	*Explanatory remarks*
1. Purpose of this document		
1.1. FRAV has established this document to facilitate and document its work. Known as "Document 5", this text is updated periodically to reflect the current working consensus of the group. 1.2. This document provides a basis for periodically reporting FRAV progress to GRVA and WP.29. The document also aims to inform other WP.29 informal working groups, and especially the GRVA Informal Working Group on Validation Methods for Automated Driving (VMAD), on FRAV activities and progress. 1.3. This document does not constitute a formal or informal text for submission to GRVA or WP.29. FRAV will issue such proposals in separate documents as determined and approved by the group.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*

2. Abbreviations, Acronyms, and Definitions 2.1. The introduction of automated driving systems and related technologies has resulted in a proliferation of new terms and concepts. This chapter defines abbreviations, acronyms, and terms as used in this document. 2.2. Acronyms and Abbreviations 2.2.1. ADS: Automated Driving System		*Introduced in FRAV-03-05-Rev.1*
2.2.2. DDT: Dynamic Driving Task		*Added per FRAV-06-05 as reviewed during the 7th FRAV session.*
2.2.3. ODD: Operational Design Domain		
2.3. Definitions		
2.3.1. *"Automated Driving System (ADS)"* means the hardware and software that are collectively capable of performing the entire DDT on a sustained basis.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
2.3.2. *"(ADS) feature"* means an application of ADS hardware and software designed specifically for use within an ODD.	2.3.2. *"(ADS) feature"* means an application of an ADS designed specifically for use within an ODD.	*Proposal to revise pursuant to the 7th FRAV session discussion.*
2.3.3. *"(ADS) function"* means an application of ADS hardware and software designed to perform a specific portion of the DDT.	2.3.3. *"(ADS) function"* means an application of an ADS designed to perform a specific portion of the DDT.	*Proposal to align the function definition with the phrasing of the feature definition per the 7th FRAV session discussion.*
2.3.4. *"ADS vehicle"* means a vehicle equipped with an ADS.		

3.2.2. *"Dynamic driving task (DDT)"* 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).	2.3.5. *"Dynamic driving task (DDT)"* means all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic. 2.3.5.1. Driving involves three behavioral levels: strategic (trip planning), tactical (maneuvering), and operational (basic skills).[1] The levels relate to perception, information processing, and decision making under uncertainty.[2] According to SAE J3016, operational effort involves split-second reactions, such as making micro-corrections while driving. 2.3.5.2. Operational functions include, but are not limited to: • Lateral vehicle motion control via steering, • Longitudinal vehicle motion control via acceleration and deceleration. 2.3.5.3. Tactical functions include, but are not limited to: • Maneuver planning via motion control, • Enhancing conspicuity via lighting, signaling, gesturing, etc. 2.3.5.4. Operational and tactical functions include, but are not limited to: • Monitoring the ~~vehicle~~ driving environment via object and event detection, recognition, classification, and response preparation, • Object and event response execution	*Proposal pursuant to the 7th FRAV session discussion.*

[1] Michon, J.A., 1985. A CRITICAL VIEW OF DRIVER BEHAVIOR MODELS: WHAT DO WE KNOW, WHAT SHOULD WE DO? In L. Evans & R. C. Schwing (Eds.). Human behavior and traffic safety (pp. 485-520). New York: Plenum Press, 1985.

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

	5.3.5.5 The DDT excludes strategic functions.	
2.3.6. *"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 due to a DDT performance-relevant system failure in the ADS and/or other vehicle system or upon exit from the ODD.	Note: without the suggested limiting language, there is a serious risk of misunderstanding the MRC concept by applying it to situations not involving ADS or vehicle failure or ODD exit.	*Proposal to introduce definitions of MRC and MRM given the discussion on elaboration of the starting point "The ADS should manage safety-critical situations".*
2.3.7. *"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~~ avoids unreasonable risks in traffic.	"Minimize" implies achieving the smallest possible risk, which suggests the need to determine a single safe state in innumerable traffic situations. The suggestion allows for a broader range of reasonably safe options.	
2.3.8. "Operational Design Domain (ODD)" means the operating conditions under which an ADS feature is specifically designed to function.		*Introduced in FRAV-03-05-Rev.1*
2.3.9. *"User"* means a human being who plays any of the following roles with respect to an ADS vehicle: in-vehicle (conventional) driver, remote driver, passenger, or DDT fallback-ready user.~~responsible for the ADS vehicle who is qualified, fit, and capable of performing the DDT.~~ Insert where appropriate; "*In-vehicle* (or *conventional) driver*" means a driver who manually exercises in-vehicle braking, accelerating, steering, and transmission gear selection input devices in order to operate a vehicle. "*Remote driver"* means a driver who is not seated in a position to manually exercise in-vehicle braking, accelerating, steering, and transmission gear	Note: the suggested definitions come from SAE J3016. We highly recommend use of these definitions to ensure consistency with SAE and ISO definitions that clearly distinguish the human roles in driving. Not suggested here is the additional user category called "driverless dispatch operator" (a user who dispatches an ADS-equipped vehicle in driverless operation).	*Initial definitions to be accepted with the understanding that revisions and additional definitions may be needed. Stakeholders supposed that:* • *a user in the vehicle may need to be differentiated from a user with a line of sight to the vehicle,* • *definition for an occupant without a capability to intervene in the DDT (passenger) may be needed.* *Since these definitions are specific to terms used in Document 5, FRAV would be expected to add or refine user-related*

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: Italic

Formatted: Font: (Default) Times New Roman, 10 pt

Formatted: Font: (Default) Times New Roman, 10 pt

selection input devices (if any) but is able to operate the vehicle. "*Passenger"* means a user in a vehicle who has no role in the operation of that vehicle.		*definitions as needed in defining safety requirements.* *"Fallback-ready user" is suggested because this term may be useful in discussing transitions of DDT control, etc. J3016 definition provided for comparison with proposed definition based on FRAV work and availability of other definitions for future consideration and discussion.*
3.29.3 [DDT] FALLBACK-READY USER The user of a vehicle equipped with an engaged level 3 ADS feature who is able to operate the vehicle and is receptive to ADS-issued requests to intervene and to evident DDT performance-relevant system failures in the vehicle compelling him or her to perform the DDT fallback.	2.3.9.1 *~~"Fallback-ready user"~~* ~~means a user determined by the ADS to be receptive to a transition of control.~~ "Determined by the ADS to be receptive" should not be part of the definition of the user. The user may be fallback-ready regardless of the ADS's determination. The need for the ADS to make that determination is a possible requirement.	
2.3.9.2. *~~"User-in-charge"~~* ~~means a user in or with a line of sight to the vehicle.~~	See "remote driver" definition above, which encompasses those outside the vehicle whether or not within line of sight.	
2.3.9.3. *~~"Remote operator"~~* ~~means a user other than a user-in-charge.~~	See "remote driver" definition above. Referring to this person as an 'operator" will cause confusion.	
	2.3.10. *"Safe fallback response"* means a successful transition of control to an ADS user or automatic execution of an ADS maneuver that places the ADS vehicle in a Minimal Risk Condition.	

Formatted: Font: (Default) Times New Roman, 10 pt

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.	2.3.10. "~~Transition~~ Transfer of control" means a transfer of full ~~control over~~ responsibility for performance of the DDT from the ADS to a user. "Transition" seems to mean moving between modes of operation in either direction. The intent here seems to be to define an actual transfer from the ADS. Because the DDT includes control (and other) functions, "control over" seems confusing. This clarification may help. Also, because the original definition was about a "demand" perhaps it would be useful to incorporate the J3016 definition of "request to intervene": Notification by an ADS to a fallback-ready user indicating that s/he should promptly perform the DDT fallback, which may entail resuming manual operation of the vehicle (i.e., becoming a driver again), or achieving a minimal risk condition if the vehicle is not drivable	*As noted during the 7th FRAV session discussion, a transfer of control to a user may involve diverse safety factors and conditions. The original term and definition in FRAV-05-03-Rev.1 was taken from the draft ALKS regulation prepared by the ACSF informal group. The term and definition proposed here addresses aspects raised in FRAV discussions.* • *The safety concern is "control" over the DDT, more than the "demand" itself.* • *Under some conditions, the ADS and user would share control until the ADS can verify that the user is in full control.* • *An ADS may need to interrupt a transition and fall back on an MRM.* • *FRAV has terms to simplify and clarify the definition (ADS, DDT, user).* *The secretary notes that "logical and intuitive" is subjective. FRAV can be expected to define requirements governing transitions of control, user interfaces and feedback, etc. under the starting points.*
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).		*Not addressed in this document.*

Formatted: Font: (Default) Times New Roman, 10 pt

3.2.6. *"Operating environment"* means the reasonably foreseeable conditions which a vehicle can be expected to encounter when in automated mode.		*Not addressed in this document.*

3. ADS Safety Requirements		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session. Section number changed pursuant to separate of FRAV-06-05 into "Document 4" and "Document 5".*
3.1. Driving a motor vehicle in traffic is a complex task requiring continuous awareness of roadway conditions, control of the vehicle motion, interactions with other road users, and adaptation of the vehicle motion to changes in roadway conditions.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.2. ~~The automation of driving obligates manufacturers, safety authorities, and other stakeholders in road transportation to ensure that Automated Driving Systems perform safely in traffic.~~	3.2. ADS performance should be consistent with safe human driving behaviors while avoiding human recognition, decision, and performance errors and the introduction of unreasonable ADS-specific risks.	*Proposal pursuant to the 8th FRAV session discussion. The proposal is to describe the overall level of safety agreed by FRAV in this paragraph. The word "safe" has been added based on input from the UK and USA. OICA suggested adding "unreasonable" to qualify "new risks".*

3.3. The assurance of ADS safety involves attention to specific performance and behavioral competencies required to operate a vehicle in traffic and the application of methods and practices to verify that ADS perform as intended.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.4. This document addresses minimum requirements necessary to ensure that an ADS is safe for use on public roads.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*

3.5. Unlike human drivers broadly licensed to operate a vehicle on all roadways, ADS may be designed to operate under specific conditions.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.6. In order to ensure public safety while benefiting from the potential of ADS to reduce crashes, injuries, and deaths (especially related to human driving errors), manufacturers and safety authorities anticipate a prudent and gradual introduction of these technologies.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.7. ~~As a result, stakeholders anticipate a wide variety of ADS applications carefully designed to operate within their performance limits.~~	3.7. As a result, stakeholders anticipate a wide variety of ADS applications carefully designed to operate within their performance capabilities.	*"Limits" replaced with "capabilities" per the 7th FRAV session discussion to avoid confusion with limit requirements.*
3.8. This document describes requirements designed to ensure that ADS perform safely on public roadways.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.9. The safety requirements address ADS in two ways. The document first defines conditions that may describe or limit the use of an ADS based on the manufacturer's assessment of its capabilities. The document then describes minimum performance requirements to ensure safe use of ADS.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.10. The performance requirements apply to ADS regardless of their individual configurations. The definition of conditions that may impact performance requires manufacturers to fully describe the intended uses and limitations of an individual ADS.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*

3.11. In combination, the ADS descriptions and the ADS performance requirements ensure that each ADS can be assessed for safe operation.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.12. These safety requirements for ADS descriptions and performance are designed to enable the validation of ADS safety prior to their introduction on the market.		*Accepted per FRAV-06-05 as reviewed during the 7th FRAV session.*
3.13. The safety of an ADS may be considered from five fundamental perspectives: • ADS should drive safely. • ADS should interact safely with the user. • ADS should manage safety-critical situations. • ADS should safely manage failure modes. • ADS should maintain a safe operational state.		*The initial points were accepted per FRAV-06-05 as reviewed during the 7th FRAV session. The proposal is to expand the text to provide additional context for understanding the scope and purpose of requirements to be elaborated under each item.*

3.13.1. The ADS should drive safely.	4.13.1. *The ADS should drive safely.* In performing the entire DDT, the ADS assumes the role of the vehicle driver. Under this perspective, the ADS should fulfill the same maxims taught to human drivers such as to respect traffic rules, to share the road, to signal intentions, and to expect even unusual driving situations ~~the unexpected~~. The performance requirements should ensure ADS driving behaviors consistent with good driving practices, including aspects that may be specific to the ADS as the driver of the vehicle.	
3.13.2. The ADS should interact safely with the user.	4.13.2. *The ADS should interact safely with the user.* ADS are intended for human use. ADS safety requirements should ensure accurate user understanding of the ADS (capabilities and limitations), user appreciation of her or his roles and responsibilities, and the safety of transitions of control between the ADS and the user.	*This text is based on the proposal of the Netherlands (with input from Leeds University and Canada) in FRAV-08-10. The proposed text has been modified for clarity and textual consistency.*
	4.13.2.1. ADS users do not correspond to a uniform profile but exhibit diverse characteristics across a spectrum of behaviors (abilities, limitations, understanding, experience, alertness, etc.). To understand the ADS, each user forms a mental model of its operation and use. One of the challenges is to safely accommodate the full spectrum of ADS users in order to ensure predictable interactions and a more error-tolerant system.	
	4.13.2.2. Commonality across user interfaces and system responses, including in ~~transitions~~ transfers of control, enables users to form reliable mental models applicable to any ADS. This commonality curtails learning curves and	*"Commonality" taken from the Leeds University chat response to OICA: "The GEAR 2030 Final Report used the term "commonality" of HMI, in order not to suggest any complete harmonisation. So yes,*

	promotes correct ADS use (while also facilitating user education). As with today's vehicle controls, the users' mental models based on such commonality enable correct understanding of any ADS without a need to learn a new model for each ADS configuration.	*there needs to be some flexibility to allow for OEM differentiation and to permit innovations, but the basic operation of the HMI does need to be harmonised for the reasons suggested. The analogy is with the controls and dashboard ot today's vehicles.*
	4.13.2.3. ADS use involves interactions including, but not necessarily limited to communication of information and transitions of vehicle control. In order to fulfill his/her roles, the user should have information about the ADS status, its operation, its intentions and the expected user responsibilities. Transitions of control may occur under diverse conditions involving different degrees of cooperation and possible fallback options to ensure safety. The user interface needs to ensure proper user inputs and feedback to facilitate correct use of the ADS and safeguard against misuse or user error.	
3.13.3. The ADS should manage safety-critical situations.	4.13.3. *The ADS should manage safety-critical situations.* Driving involves the assessment of risks and responses to those risks, often involving degrees of uncertainty. A driver cannot control the actions of other road users or the conditions of the road environment. Situations may arise that require a driver to take evasive action. An unexpected condition may require a period of ADS and user cooperation or mutual support to complete a transition of control. A fallback-ready user may be unavailable. The ADS vehicle may be subject to a collision caused by another road user. While performing the DDT (or even part of the DDT during a transition of control), the ADS should	

Commented [DS1]: I think this starts to blur the line between situations involving crash avoidance maneuvers, which the ADS must be able to handle by itself as part of performing the ENTIRE DDT, and situations requiring fallback due to an ADS or vehicle system failure or ODD exit (discussed below). In no situation should an ADS and human driver share control and especially in the midst of a safety-critical situation-- that's below Level 3.

	manage responses to such safety-critical conditions to avoid and/or mitigate risks.	
3.13.4. The ADS should safely manage failure modes.	4.13.4. *The ADS should safely manage failure modes.* A condition, such as an internal malfunction or damage to a component or the failure of a vehicle system on which ADS performance relies, may render an ADS operationally unsafe. The ADS should detect and respond to such conditions. ADS may also have diverse strategies and capabilities to safely permit continued operation in the presence of a failure. This perspective aims to ensure that failures specific to the functioning of ADS hardware and software do not result in unreasonable risks to safety.	

3.13.5 The ADS should maintain a safe operational state.	4.13.5 *The ADS should maintain a safe operational state.* As a software-driven system, an ADS may be impacted for better or for worse by the evolution of technologies. Motor vehicles may remain in use for two decades or more which requires attention to ensure that the ADS remains operationally safe throughout the useful life of the vehicle. This perspective aims to address ADS responses to external factors that may arise during the useful life of the ADS vehicle, including verification of its operational state pursuant to a collision, vulnerabilities that may arise with technological changes, and obsolescence.	

4. Operational Design Domain (ODD)		
4.1. This chapter concerns the description of an Operational Design Domain (ODD).		
4.2. For the assessment of vehicle safety, the vehicle manufacturer should describe the ODD of each ADS feature available on the vehicle in accordance with the provisions of this chapter.		
4.3. The purpose of an ODD description is to inform determinations on the requirements and scenarios applicable to an ADS feature.		

5.4. The ODD description shall include (at a minimum):		*FRAV has agreed to consider requirements for the content of an ODD description during the course of drafting proposals for functional requirements. As noted above, the ODD description should be aligned with the requirements in a manner that facilitates decisions on which requirements are applicable to a given ADS.*
5.4.1. Roadway types and characteristics [Road conditions (motorways/expressways, general roads, number of lanes, existence of lane marks, roads dedicated to automated driving vehicles, etc.)]		*Not addressed in this document.*
5.4.2. Geographic area [Geographical area (urban and mountainous areas, geofence setting, etc.)]		*Not addressed in this document.*
5.4.3. Speed range		*Not addressed in this document.*
5.4.4. Environmental conditions [Environmental conditions (weather, night-time limitations, etc.)]		*Not addressed in this document.*
5.4.5. V2X dependencies (e.g., dependence on connectivity and availability of vehicle, infrastructure or other external sources of data)		*Not addressed in this document.*

5.4.6. Other constraints [Other conditions that must be fulfilled for the safe operation of the ADS.]		*Not addressed in this document. FRAV notes the proposal from China to define "ODC" as a broader level of design constraints than covered by ODD. FRAV has agreed in principle that ODD refers to ambient conditions (i.e., conditions surrounding the vehicle). FRAV has agreed that other design constraints (such as reliance on the user to fulfill safety-critical roles outside the ADS capabilities) may be relevant to manufacturer descriptions of an ADS. FRAV has agreed to further consider the structure and content of this chapter once the group has a better understanding and consensus on the items that should be covered by the ADS descriptions.*

5. ADS Performance Requirements		*Currently 40 subtopics under the five starting points.*
5.1. The ADS should drive safely.		
5.1.1. The ADS should be capable of performing the entire Dynamic Driving Task.		
5.1.1.1. The ADS should control the longitudinal and lateral motion of the vehicle.		
5.1.1.2. The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).		
5.1.1.3. The ADS should detect, recognize, classify, and prepare to respond to objects and events in the traffic environment.		

5.1.2. The ADS should respect traffic rules.		
5.1.3. The ADS should interact safely with other road users.		
5.1.4. The ADS should adapt its behavior in line with safety risks.		
5.1.5. The ADS should adapt its behavior to the surrounding traffic conditions.		
5.1.5.1. The ADS driving behavior should not disrupt the flow of traffic.		*Proposed by JRC related to the discussions on "string stability".*
5.1.6. The ADS behavior should not be the critical factor in the causation of a collision.		
5.2. ADS should interact safely with the user consistent with the intended role of the user~~.~~		*Harmonized*
5.2.1. Activation of an ADS feature should only be possible when the conditions of its ODD have been met.		
5.2.2. The ADS should signal when conditions indicate a probable ODD exit.		
5.2.3. The user should be permitted to override the ADS to assume full control over the vehicle if the ADS is designed to request and enable intervention by a human driver.	It's important to distinguish between an ADS designed to request human intervention and one that is not.	
5.2.4. The ADS should safely manage ~~transitions~~ transfers of full control to the user if the ADS is		

designed to request and enable intervention by a human driver.		
5.2.4.1. Prior to a ~~transition~~ transfer of control to the user, the ADS should verify the availability of the user to assume control.		
5.2.4.2. Pursuant to a ~~transition~~transfer of control, the ADS should verify full control of the vehicle by the user prior to deactivation.		
5.2.5. The ADS should ~~tolerate~~ safely respond to user input errors.		
5.2.6. The ADS should provide feedback to the user on its operational status.		
5.2.7. The ADS should warn the user of failures to fulfill user roles and responsibilities.		
5.2.8. The user should be provided with information regarding user roles and responsibilities for the safe use of the ADS.		
5.3. ADS should manage safety-critical driving situations.		
5.3.1. The ADS should recognize and respond to road safety agents.		
5.3.2. The ADS should mitigate the effects of road hazards.		
5.3.3. The ADS should execute a safe fallback response ~~as conditions warrant~~ in the event of a failure of		

the ADS and/or other vehicle system that prevents the ADS from performing the DDT.		
5.3.3.1. In the absence of a fallback-ready user, the ADS should fall back directly to ~~an MRM~~ Minimal Risk Condition if a failure of the ADS and/or other vehicle system prevents the ADS from performing the DDT.		
5.3.3.2. If the ADS is designed to request and enable intervention by a human driver, ~~T~~the ADS should execute an MRM in the event of a failure in the transition of full control to the user.		
5.3.3.3. Pursuant to an MRM, the ADS should place the vehicle in a Minimal Risk Condition prior to deactivation.		
5.3.3.4. The ADS should signal an MRM.		
5.3.5. ADS vehicles that may operate without ~~a user in charge~~ an in-vehicle driver should provide means for occupant communication with ~~a remote operator~~ remote assistance personnel.		
5.3.6. The ADS should safely manage short-duration transitions between ODD.		
5.3.7. Upon completion of an MRM, the user may be permitted to assume control of the vehicle if the ADS is designed to request and enable intervention by a human driver.		

Commented [DS2]: Signal to whom? How? If to other road users, use of directional signals and flashers may be contemplated. If to users, an indicator may be contemplated.

5.3.8. Pursuant to a collision, the ADS should stop the vehicle and ~~deactivate~~ inhibit ADS reactivation until its capability to proceed has been verified.		
5.4. ADS should safely manage failure modes.		
5.4.1. The ADS should detect system malfunctions and abnormalities.		
5.4.2. The ADS should execute a safe fallback response upon detection of a failure that compromises performance of the DDT.		
5.4.3. Provided a failure does not compromise ADS performance of the entire DDT, the ADS should respond safely to the presence of a fault in the system.		
5.4.4. The ADS should signal faults and resulting operational status.		
5.5. ADS should ensure a safe operational state.		
5.5.1. The ADS should be permanently disabled in the event of obsolescence.		
5.5.2. Pursuant to a collision and/or a failure detected in DDT-related functions, ADS activation should not be possible until the safe operational state of the ADS has been verified.		
5.5.3. The ADS should signal required system maintenance to the user.		

5.5.4. The ADS should be accessible for the purposes of maintenance and repair to authorized persons responsible for maintenance and repair of the ADS.		
5.5.5. ADS safety should be ensured in the event of discontinued production/support/maintenance.		*JRC*

—NO CHANGES HAVE BEEN MADE FROM THE PREVIOUS VERSION AFTER THIS POINT—

FRAV has begun a review of proposals for safety requirements collected from across its stakeholder group (shown below). These proposals have been consolidated and tentatively categorized in document FRAV-07-10. FRAV has begun a process to describe the intent of these proposals in accordance with the safety perspectives described under paragraph 4.13. above. The outcomes of this process will be reflected in an updated version of document FRAV-06-04. Following FRAV consideration of this revised document, the outcomes will be transposed into Document 5, especially under section 5 concerning ADS performance requirements. FRAV will pursue an iterative process to derive safety requirements from this elaboration of the initial perspectives (aka, starting points) to reach optimal levels of detail to enable the assessment of an ADS. Simultaneously, FRAV will identify ODD conditions relevant to the performance requirements for inclusion under section 4 concerning ODD. These conditions will be elaborated to provide measurable/verifiable descriptions and structured to facilitate public understanding of ADS uses and limitations and to provide a basis for assessment of an individual ADS with regard to the safety requirements.

4.1.	It is necessary to clearly define the split in responsibilities between the driver and the ADS.		*Not addressed in this document.*
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.		*Not addressed in this document.*
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.		*Not addressed in this document.*
4.4.	Requirements under consideration include:		*Not addressed in this document.*

4.4.1.	The Automated Driving System (ADS) shall react to unforeseen situations in a way that minimizes risk.		*Not addressed in this document.*
4.4.2.	The vehicle shall demonstrate adequate mitigation of risks (e.g. approaching ODD boundaries), safe driving behavior and good Human Machine Interface.		*Not addressed in this document.*
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)		*Not addressed in this document.*
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.		*Not addressed in this document.*
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.		*Not addressed in this document.*
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.]		*Not addressed in this document.*
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.		*Not addressed in this document.*
4.4.8.	If an update renders the system obsolete or otherwise no longer supported, it shall not permit activation		*Not addressed in this document.*

4.4.9. Dynamic behavior in road traffic		*Not addressed in this document.*
4.4.9.1. When in automated driving mode,		*Not addressed in this document.*
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.]		*Not addressed in this document.*
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.]		*Not addressed in this document.*

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.		*Not addressed in this document.*
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.		*Not addressed in this document.*

6.	Execution of Dynamic Driving Tasks		*Not addressed in this document.*
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).		*Not addressed in this document.*
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.		*Not addressed in this document.*
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).		*Not addressed in this document.*

6.4. Object and Event Detection and Response (OEDR)		*Not addressed in this document.*
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.		*Not addressed in this document.*
6.4.2. The ADS shall have OEDR capabilities that support safe and appropriate actions when subjected to reasonably foreseeable scenarios within the ODD.		*Not addressed in this document.*
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 …)]		*Not addressed in this document.*
6.4.4. Objects and events include, but are not limited to, the following:		*Not addressed in this document.*
6.4.4.1. The system shall be able to detect the roadway		*Not addressed in this document.*
6.4.4.2. The system shall be able to identify lane location (w/, w/o markings)		*Not addressed in this document.*
6.4.4.3. The system shall be able to detect and identify lane markings		*Not addressed in this document.*
6.4.4.4. The system shall be able to detect objects in its defined field of view		*Not addressed in this document.*
6.4.4.5. The system shall be able to estimate the speed and heading of objects		*Not addressed in this document.*
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		*Not addressed in this document.*

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)		*Not addressed in this document.*
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		*Not addressed in this document.*
6.4.4.9. The system shall treat objects which cannot be classified with increased uncertainty		*Not addressed in this document.*
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)		*Not addressed in this document.*
6.4.4.11. The system shall take into consideration that other road users may not respect traffic laws		*Not addressed in this document.*
6.4.4.12. The system shall detect and respond appropriately to emergency service vehicles (e.g., yielding the right of way at intersections)		*Not addressed in this document.*
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		*Not addressed in this document.*
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		*Not addressed in this document.*

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]		*Not addressed in this document.*
6.5. Longitudinal and lateral motion control		*Not addressed in this document.*
6.5.1. Normal Driving		*Not addressed in this document.*
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.		*Not addressed in this document.*
6.5.1.2. The automated driving system shall execute such maneuvers without causing outcomes resulting in injury or death.		*Not addressed in this document.*
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		*Not addressed in this document.*

	communication with other road users when needed).]		
6.5.2.	Other Driving		*Not addressed in this document.*
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.		*Not addressed in this document.*
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.		*Not addressed in this document.*
7.	Human-Machine Interface/Operator Information		*Not addressed in this document.*
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 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.).		*Not addressed in this document.*

7.2. Requirements under consideration include:		*Not addressed in this document.*
7.2.1. Activation and deactivation		*Not addressed in this document.*
7.2.1.1. The activation of the ADS shall only be possible when the conditions of the ODD are met.		*Not addressed in this document.*
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.		*Not addressed in this document.*
7.2.1.3. Human override of system control		*Not addressed in this document.*
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).		*Not addressed in this document.*
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.		*Not addressed in this document.*
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.		*Not addressed in this document.*
7.2.1.3.4. When necessary the ADS shall protect the vehicle control against inadvertent or undeliberate [unintentional] user intervention.		*Not addressed in this document.*
7.2.1.4. The ADS deactivation shall only be performed when it has been verified that the user has taken over control.		*Not addressed in this document.*

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.]		*Not addressed in this document.*
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.]		*Not addressed in this document.*

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.		*Not addressed in this document.*
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.		*Not addressed in this document.*
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.]		*Not addressed in this document.*
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.]		*Not addressed in this document.*
7.2.6.1.1. System availability		*Not addressed in this document.*
7.2.6.1.2. System mode active		*Not addressed in this document.*
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.]		*Not addressed in this document.*
7.2.6.3. Critical messages [Communication of critical messages to the driver]		*Not addressed in this document.*
7.2.6.4. Transition demand [Communication of Take-over request to the driver.] [The system shall clearly		*Not addressed in this document.*

	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]		*Not addressed in this document.*
7.2.6.6.	Status of driver availability [Driver availability and override possibility (if required, based on level of automation)]		*Not addressed in this document.*
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		*Not addressed in this document.*
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.		*Not addressed in this document.*
7.2.7.	The vehicle shall signal to other road users [Demonstration of signaling features. Interaction with other road users.]:		*Not addressed in this document.*
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.]		*Not addressed in this document.*
7.2.7.2.	Initiation of a minimal risk maneuver		*Not addressed in this document.*
7.2.7.3.	Other safety-critical information.		*Not addressed in this document.*
7.2.8.	Activities other than driving		*Not addressed in this document.*
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.		*Not addressed in this document.*