

FR INPUTS

As a follow-up to the 9th FRAV informal group meeting, FRAV stakeholders are kindly requested to comment on the discussion topics derived from the five starting points. During the session, FRAV agreed and the secretary was directed to prepare a single document to gather comments for further FRAV consideration.

The aim of the following table is to gather stakeholder views on the meaning or underlying safety goals related to and/or derived from the performance topics. Based on those views, the table further requests stakeholder views on criteria, metrics, and performance indicators that might be used to define safety requirements that can be measured and/or verified.

The following example for filling in the table illustrates the desired level of detail (it does not propose comments for stakeholder response). The “Interpretation/Goals” column should be used to comment on the performance topic and views on its significance to the development of safety requirements. The “Measurable/Verifiable Criteria” column should be used to suggest indicators or performance metrics for safety goals proposed under the “goals” column. The intention is not to request technical proposals for requirements, limits, or values. The aim is to identify factors that might be useful in defining measurable/verifiable requirements to ensure desirable safety outcomes.

The first column should be

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
The ADS should control the longitudinal and lateral motion of the vehicle.	<ul style="list-style-type: none"> • The ADS should smoothly execute maneuvers. • The ADS driving behavior should meet public expectations. • The vehicle movements should be safe. • The ADS driving behavior should not cause collisions or disrupt traffic. • This topic should not be considered. • This topic should focus on safety. • This topic should include the impact on other road users and traffic flows. • 	<ul style="list-style-type: none"> • Relative speed and distance from a preceding vehicle should be sufficient to avoid a collision. • Relative speed and distance from a preceding vehicle should be consistent with safe human driving performance data. • Lane positioning should ensure a safe lateral distance from an adjacent vehicle (consistent with safe human driving performance data). • Lane changes should be smooth with lateral acceleration compatible with/comparable to safe human driving. •

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from ADS should drive safely)		
The ADS should perform the entire Dynamic Driving Task.	<ul style="list-style-type: none"> • What is our interpretation of this function? • DDT = OEDR + Control longitudinal & Lateral • This performance topic is the header of the all the following 	<ul style="list-style-type: none"> • What criterion to validate?
1- The ADS should control the longitudinal and lateral motion of the vehicle.	<p>This item should concentrate on maneuver execution by the ADS.</p> <ul style="list-style-type: none"> • In an understandable way for other road user • Smooth • Safely <p>(Some standard maneuvers are defined in NHTSA Testable Framework)</p>	<p>Objective criteria to be defined per maneuver</p> <ul style="list-style-type: none"> - Interdistance time - Maneuver duration - Maximum acceleration - ...
2- The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).	<ul style="list-style-type: none"> • All boundaries of the ODD should be described, even attribute not in the ODD (in order to detect and respond in a sufficient timeframe before ODD exit) • The ODD, shall be described and provided to audit of homologation process. • The ADS shall detect all ODD attributes. 	<ul style="list-style-type: none"> • The applicant should demonstrate how these requirements are taken into account for the design of the ADS, translated in technical requirements and verified in the process. • In a second time, standardize the rules and the verification process, and associated criteria.
3- The ADS should detect, recognize, classify, and prepare to respond to objects and events in the traffic environment.	<ul style="list-style-type: none"> • All Objects and Events should be described, and associated response should also be described. (For us, NHTSA document describing OEDR process (Testable Framework..., sept.2019), is the standard to use to answer this topic) • Should include self check (incl. DSSAD) or auto diagnosis 	<ul style="list-style-type: none"> • The applicant should demonstrate how these requirements are taken into account for the design of the ADS, translated in technical requirements and verified in the process. In a second time, standardize the rules and the verification process, and associated criteria.
The ADS should respect traffic rules.	An item should concentrate on:	<ul style="list-style-type: none"> • The applicant should demonstrate how these requirements are taken into account for the design

	<ul style="list-style-type: none"> • A list of traffic rules to respect in the ODD should be defined (<i>should be done by each country</i>) • Identify common traffic rules, and differences, and propose common requirements. • Some will be objective, but other will be subjective 	<p>of the ADS, translated in technical requirements and verified in the process.</p> <ul style="list-style-type: none"> • In a second time, standardize the rules and the verification process, and associated criteria.
The ADS should interact safely with other road users.	<ul style="list-style-type: none"> • Already taken into account above requirements. 	<ul style="list-style-type: none"> •
The ADS should adapt its behavior in line with safety risks.	<ul style="list-style-type: none"> • This compliance should be verified in a Risk Analysis 	<ul style="list-style-type: none"> • For Audit, Applicant should provide the Risk Analysis and associated Safety Concept.
The ADS should adapt its behavior to the surrounding traffic conditions.	<p>The vehicle shall manage risks according to the following rules:</p> <ul style="list-style-type: none"> • Vehicle shall not create accident by its own • Vehicle shall be robust, as far as reasonably possible, to risks caused by others • Vehicle shall comply with applicable driving rules (including those applicable to human drivers) unless it is the only way to avoid an accident 	<ul style="list-style-type: none"> •
The ADS driving behavior should not disrupt the flow of traffic.	<ul style="list-style-type: none"> • Vehicle shall not create accident by its own • Vehicle shall be robust, as far as reasonably possible, to risks caused by others • Vehicle shall comply with applicable driving rules (including those applicable to human drivers) unless it is the only way to avoid an accident 	<ul style="list-style-type: none"> •
The ADS behavior should not be the critical factor in causation of a collision.	<p>This rule shall be fulfilled:</p> <ul style="list-style-type: none"> • wherever the vehicle is driving (e.g. country, road, ...) <p>whenever the vehicle is driving (e.g. despite dynamic lane assignment; time dependent rule, introduction of a new type of traffic sign; rule change ...)</p>	<ul style="list-style-type: none"> •

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from the ADS should interact safely with the user)		
Activation of an ADS feature should only be possible when the conditions of its ODD have been met.	<ul style="list-style-type: none"> • The vehicle shall not be in AD mode out of its ODD • Manufacturers and other entities should develop tests and standards to established a safe ODD 	<ul style="list-style-type: none"> • ODD description shall be available • Audit of the document explaining the process to established a safe ODD • Tests should be described and conducted to verify no activation of the ADS outside the ODD.
The ADS should signal when conditions indicate a probable ODD exit.	<ul style="list-style-type: none"> • An HMI should be triggered to alert the driver, with a sufficient timeframe <p>The driver shall be clearly informed of:</p> <ul style="list-style-type: none"> • the vehicle behavior in AD mode and the limits of this behavior <p>His own responsibilities, the procedures to comply with (e.g. takeover procedure) and possible consequences if he does not comply.</p>	<ul style="list-style-type: none"> • Tests should be described and conducted to verify probable ODD exit
The user should be permitted to override the ADS to assume full control over the vehicle.	<ul style="list-style-type: none"> • Whatever the situation, nominal driving, MRM, of EM, the user should be able to override the the ADS. 	<ul style="list-style-type: none"> • Criteria should be defined to detect an intentional override (e.g. steering torque > threshold). • Tests should be described and conducted to verify this requirement.
The ADS should safely manage transitions of control to the user.	<ul style="list-style-type: none"> • The AD mode deactivation (end of vehicle longitudinal and lateral control) shall only be performed when system has verified that the driver has taken over vehicle control. This verification shall at least include a criterion on vehicle lateral control (except if the vehicle is already stopped). • When the driver takes over vehicle control on her/his own (without prior system request), the vehicle shall not disturb the driver takeover by 	<ul style="list-style-type: none"> • The goals of the column 2 for us are considered as requirements to be tested in the validation phase. • Tests should be described and conducted to verify this requirement.
Prior to a transition of control to the user, the ADS should verify the availability of the user to assume control.		
Pursuant to a transition, the ADS should verify full control of the vehicle by the user prior to deactivation.		

	<p>an inappropriate action (e.g. by switching headlamps off, at night).</p> <ul style="list-style-type: none"> • When the driver takes over after a system request, the system shall give back the control to the driver with a vehicle configuration maximizing driver controllability (e.g. wipers ON in case of rain, headlamps ON by night). • ECE R 157 : 5.1.3. The activated system shall exercise control over systems required to support the driver in resuming manual control at any time (e.g. demist, windscreen wipers and lights). 	
The ADS should tolerate user input errors.	•	•
The ADS should provide feedback to the user on its operational status.	<ul style="list-style-type: none"> • The driver shall be clearly informed that the vehicle is in AD mode or not 	<ul style="list-style-type: none"> • Make sure the information is available and understandable for the user. • Can be verify during Audit and/or Open Road Tests
The ADS should warn the user of failures to fulfill user roles and responsibilities.	<p>The driver shall be clearly informed of:</p> <ul style="list-style-type: none"> • the vehicle behavior in AD mode and the limits of this behavior (and particularly in case of failure) • his own responsibilities, the procedures to comply with (e.g. takeover procedure) and possible consequences if he does not comply. 	• Can be verify during Audit and/or Tests Tracks
The user should be provided with information regarding user roles and responsibilities for the safe use of the ADS.		•
ADS vehicles that may operate without a user-in-charge should provide means for occupant communication with a remote operator.	<ul style="list-style-type: none"> • The global system should be described including the different components and their interactions. (e.g. Vehicle, Infrastructure, Supervision, ...) 	•
Upon completion of an MRM, a user may be permitted to assume control of the vehicle.	<ul style="list-style-type: none"> • Included in : The user should be permitted to override the ADS to assume full control over the vehicle. 	•

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from the ADS should manage safety-critical situations)		
The ADS should recognize and respond to road-safety agents.	•	• Tests should be defined and conducted, normally covered by ODD and OEDR.
The ADS should mitigate the effects of road hazards.	• Already included in Safety Analysis.	•
The ADS should execute a safe fallback response as conditions warrant.	• Already included in ODD and OEDR response	•
In the absence of a fallback-ready user, the ADS should automatically achieve a Minimal Risk Condition (MRC).*	• MRC shall be defined and described • MRM to reach MRC shall be defined and describe	• Test to check if MRC is triggered in case of absence of fallback-ready use
The ADS should place the vehicle in an MRC in the event of a failed transition of full control to the user.*	• The procedure shall be described, and a test shall verify the conformity.	• Test to check if MRC is triggered in case of absence of failed transition
The ADS should achieve a Minimal Risk Condition (MRC) prior to deactivation.*	• MRC shall be specified, with criteria regarding its termination	• Test to check if MRC is triggered and achieved before any deactivation of the ADS
The ADS should signal its intention to place the vehicle in an MRC.*	• MRC shall be specified, with criteria regarding its intention	• While the MRC is triggered, test to check if intention is signaled
The ADS should safely manage short-duration ODD exits.	In AD mode, if situation would be difficult to control by the driver (taking into account vehicle technical status and urgency level) the vehicle: • shall manage the situation at best effort without requesting the driver to takeover, • shall inform the driver.	•

* These topics were modified from the original proposals in response to the 7th session discussion on minimal risk maneuvers.

<p>Pursuant to a collision, the ADS should stop the vehicle and deactivate.</p>	<p>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:</p> <ul style="list-style-type: none">• inhibit AD mode reactivation until proper operation has been verified,• perform predefined MRM in the best possible way, according to vehicle operational status and current situation• Vehicle could also, simultaneously, request the driver to takeover vehicle control if vehicle and current situation are sufficiently controllable by the driver.	<ul style="list-style-type: none">•
---	--	---

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
Derived from the ADS should safely manage failure modes (ISO 26262) and safety hazards (ISO 21448) => should address both functional (ISO 26262) and operational safety(ISO 21448)		
The ADS should detect system malfunctions and abnormalities.	<ul style="list-style-type: none"> • Safety concepts have to be defined regarding malfunctions and abnormalities (to address ISO 26262 and 21448). 	<ul style="list-style-type: none"> • Audits + tests
The ADS should execute a safe fallback response upon detection of a failure that compromises performance of the DDT.	<ul style="list-style-type: none"> • Failure that compromise performance of the DDT shall be defined • Fallback responses shall be specified 	<ul style="list-style-type: none"> • Requirement based tests & verification
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.	<ul style="list-style-type: none"> • Trigger a safe state until the driver takeover or the MRM is achieved 	<ul style="list-style-type: none"> • Requirement based tests & verification
The ADS should signal faults and resulting operational status.	<ul style="list-style-type: none"> • Shall be specified by OEM 	<ul style="list-style-type: none"> • Requirement based tests & verification
(Derived from the ADS should maintain a safe operational state)		
The ADS should be permanently disabled in the event of obsolescence.	<ul style="list-style-type: none"> • Shall be specified by OEM 	<ul style="list-style-type: none"> • Requirement based tests & verification
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.	<ul style="list-style-type: none"> • In case of failure impacting safety in AD mode, an appropriate degradation concept shall be to inhibit AD mode until next vehicle switch off and vehicle proper operation has been verified either by self-diagnostic or by maintenance. 	<ul style="list-style-type: none"> • Requirement based tests & verification
The ADS should signal required system maintenance to the user.	<ul style="list-style-type: none"> • Shall be specified by OEM 	<ul style="list-style-type: none"> • Requirement based tests & verification
The ADS should be accessible for the purposes of maintenance and repair to authorized persons.	<ul style="list-style-type: none"> • Is the idea to protect the ADS from an unauthorized access ? 	<ul style="list-style-type: none"> •
ADS safety should be ensured in the event of discontinued production/support/maintenance.	<ul style="list-style-type: none"> • A procedure should be produced. 	<ul style="list-style-type: none"> •