

Submitted by Japan

FRAV-18-10.rev1
18th FRAV Session
09 September 2021

Workshop on ADS Safety Elements

This document includes an editorial review of the ADS Safety Elements proposed in FRAV-12-08 based on comments received in the documents:

- FRAV-08-09
- FRAV-09-08
- FRAV-10-11
- FRAV-12-08
- Dynamic Driving Task workstream
- Other Road Users workstream
- Human Factors workstream

This document needs to be reviewed in conjunction with **FRAV-18-09** (excel), providing the rationale behind the consolidation exercise proposed in the table below.

Modifications to the existing text of FRAV-18-06, in **red bold** for new or ~~strikethrough~~ for deleted characters.

Safety Topics and Detailed Requirements

	Performance Topic	Detailed Requirements	Measurable / Verifiable Criteria
The ADS should drive safely			
1	The ADS should be capable of performing the entire Dynamic Driving Task (DDT)	<ul style="list-style-type: none"> • The capability of the ADS to perform the entire DDT should be determined in the context of the ODD of the ADS • As part of the DDT, the ADS shall be able to: <ul style="list-style-type: none"> ○ Operate at safe speeds; ○ Maintain appropriate distances from [other road users] by controlling the longitudinal and lateral motion of the vehicle; ○ Adapt its behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic) ○ Adapt its behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority) 	
2	The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s)	<ul style="list-style-type: none"> • The ADS should be able to determine when the conditions are met for activation. • The ADS should detect and respond when one or more ODD conditions are not or no longer fulfilled. • The ADS should be able to anticipate planned exits of the ODD • The ODD conditions and boundaries (measurable limits) should be established by the manufacturer. • The ODD conditions to be recognized by the ADS should include: <ul style="list-style-type: none"> ○ Precipitation (rain, snow) ○ Time of day (light intensity, including the case of the use of lighting devices) ○ Visibility ○ Road and lane markings 	
3	The ADS should detect and respond to objects and events relevant for the DDT	<ul style="list-style-type: none"> • [Objects and events might include, but are not limited, to: 	

		<ul style="list-style-type: none"> ○ Vehicles, motorcycles, bicycles, pedestrians, obstacles ○ Road accidents ○ Road safety agents / enforcement agents ○ Emergency vehicles] 	
4	The ADS should comply with traffic rules [in the country of operation / within the ODD]	<ul style="list-style-type: none"> ● [ADS should comply with the traffic laws in nominal conditions, except when in specific circumstances or when necessary to enhance the safety of the vehicle's occupants and/or other road users] 	
5	The ADS should interact safely with other road users	<p>The ADS should interact safely with other road users, such as via:</p> <ul style="list-style-type: none"> ● [Signaling maneuver intentions] ● [Signaling ADS status (active/inactive)] ● [The ADS should inform its status and next intended actions for other road users surrounding the ADS by visible way, (e.g. driving mode indication)] 	
6	The ADS should adapt its behavior in line with safety risks		
7	The ADS should adapt its behavior to the surrounding traffic conditions		
8	The ADS driving behavior should not disrupt the flow of traffic		
The ADS should interact safely with the user			
9	<p>Activation of an ADS feature should only be possible when the conditions of its ODD have been met</p> <p>User interaction with and the interface of ADS (features) should have high-level commonality</p>	<ol style="list-style-type: none"> 1) The ADS (features) should use interfaces with high-level of commonality 2) The operation of the interaction should have in common: <ol style="list-style-type: none"> a) [use of common sequence of states in the transition/activation/overriding/...] 3) The interaction should be simplified: <ol style="list-style-type: none"> a) [Limit the number of roles] 	

Commented [1]: This is a sensitive issue and should not be explicitly stated as being allowed to violate the traffic laws.

Commented [2]: Base document : FRAV 11-09 ((AVSR chair) GRE Task Force on Automated Vehicle Signalling Requirements-WP.1-2020-Informal 13)

	<p>of design so as to support users' mental model of system operation</p>	<p>b) [Limit the number of potential transitions] c) [Limit the number of settings] d) [Limit the number of different interaction modes]</p>	
<p>10</p>	<p>The user should be informed about the ADS status (when the ADS is activated) with regards to ODD</p> <p>The ADS should provide clear and unambiguous information to the user</p>	<p>1) The ADS should inform the user on the current conditions: a) ADS status information b) User Role c) Potential roles to activate d) Responsibility e) Permitted NDRA f) "Standard" information i) Vehicle speed, range and Time to Fuel g) ADS failure information h) Availability of automated features</p> <p>2) The ADS should inform the user on the upcoming conditions: a) ODD boundaries b) Upcoming actions or change in roles c) Oncoming decisions/manoeuvres d) Estimated time to overtake in normal conditions e) Warning for upcoming transition request f) Confirmation request for upcoming transition</p> <p>3) The ADS should present the information so as to assure a safe interaction: a) Timing requirements b) Priority requirements c) Saliency requirements</p> <p>4) The ADS should have functionality to display whether ADS is active or not.</p> <p>5) The ADS should have functionality to display information about executable DDT function and ODD.</p>	<ul style="list-style-type: none"> · ADS level (current and potential) · Executable DDT function(current)

11	<p>The user should be permitted to take over control from the ADS, if the ADS is designed to request and enable intervention by a human driver</p> <p>The ADS should prevent misuse and errors in operation</p>	<ol style="list-style-type: none"> 1) The ADS should be designed to prevent inadvertent activation or deactivation 2) The controls dedicated to the ADS should be clearly distinguishable from other controls 3) The ADS should be designed to avoid activation of an ADS outside its ODD 4) The ADS should be designed to avoid illegal settings <p>The ADS should provide feedback when the user attempts to enable not allowed functions</p>	
12	<p>The ADS should safely manage transitions of control to the user</p> <p>The ADS should assure a safe ADS feature activation</p>	<ol style="list-style-type: none"> 1) The ADS should inform the user that preconditions for activation are met 2) The activation should follow a common sequence <ol style="list-style-type: none"> a) Common sequence to be a pass/fail criterion 3) The ADS should provide confirmation that the system is activated 	
13	<p>The ADS should safely respond to user input errors</p> <p>The ADS should assure a safe Transition Of Control</p>	<ol style="list-style-type: none"> 1) The interaction should follow a common sequence in the transition of control (change of user roles) <ol style="list-style-type: none"> a) Common sequence to be a pass/fail criterion <div data-bbox="604 889 1087 1144" data-label="Diagram"> </div> <p>Figure 2 — System-initiated transition from automated to manual driving (concepts are further specified in S.3.2 and S.3.3)</p>	<ol style="list-style-type: none"> 2) Transition of control should return to a common default user role (to prevent mode confusion and other risks)

¹ Reference: ISOxxx

		<ul style="list-style-type: none"> a) This should normally be fully engaged driving (conventional driver) b) Common default user to be a pass/fail criterion 3) The ADS should continuously verify whether the user is available for the transition of control and warn the user if not available when required (MRM to be specified elsewhere) 4) The ADS should verify that the driver is in stable control of the vehicle to complete the Transfer of Control to the user 5) During transition, the ADS should remain active until the transfer of control has been completed or the ADS reaches a minimal risk condition 	
14	<p>The ADS should provide feedback to the user on its operational status</p> <p>The ADS should assure a safe user initiated take over</p>	<ul style="list-style-type: none"> 1) Under safe conditions the user is allowed to initiate a take-over of the ADS 2) The deactivation should follow a common sequence <ul style="list-style-type: none"> a) Common sequence to be a pass/fail criterion 3) The ADS should prevent and warn a user for a user initiated take over that would likely lead to an unsafe situation 4) The ADS should provide a clear feedback of the successful user initiated take over <ul style="list-style-type: none"> a) The clear feedback should be a pass/fail criterion 5) The user initiated take over should return to a common default user role (to prevent mode confusion and other risks) <ul style="list-style-type: none"> a) This should normally be fully engaged driving (conventional driver) <p>Common default user role to be a pass/fail criterion</p>	
15	<p>The ADS should warn the user of failures to fulfill user roles and responsibilities</p> <p>The ADS manufacturer should provide tools for the authorized user to learn about system functionality and operation.</p>	<p><i>On the general <u>mental model</u> (common understanding):</i></p> <ul style="list-style-type: none"> 1) ADS manufacturer should describe the possible educational approach: <ul style="list-style-type: none"> a) Theoretical and practical training b) How it aligns with common HMI and interaction 2) ADS manufacturer should provide documented information on ADS (features) capabilities and limitations (the information should also refer to specific scenarios) 	

Commented [3]: Should be defined in the text.

		<p>3) ADS manufacturer should provide documented information on roles and responsibility of Driver/user and ADS when ADS (feature) is on/off</p> <p>4) ADS manufacturer should provide documented information on allowed transition of roles and procedure for the transition (activation/deactivation, ToC, Override)</p> <p>5) ADS manufacturer should provide a list of NDRA allowed when an ADS feature is active</p> <p><i>On the applied mental model (understanding the ADS-specifics)</i></p> <p>6) The ADS supports the user in correct operation (coaching)</p> <p>7) The ADS gives prompt feedback on erroneous operation</p>	
16	ADS vehicles that may operate without a [user-in-charge/in-vehicle driver] should provide means for occupant communication with [a remote operator/user-in-charge/human driver/remote assistance personnel]		
The ADS should manage safety-critical situations			
17	The ADS should execute a safe fallback response in the event of a failure of the ADS and/or other vehicle system that prevents the ADS from performing the DDT	<ul style="list-style-type: none"> • In the absence of a fallback-ready user, the ADS should fall back directly to a Minimal Risk Condition (MRC) • If the ADS is designed to request and enable intervention by a human driver, the ADS should execute an MRM in the event of a failure in the transition of control to the user <ul style="list-style-type: none"> ○ [Upon completion of an MRM, a user may be permitted to assume control of the vehicle] ○ [The user should be permitted to override the ADS to assume full control over the vehicle] 	
18	In the absence of a fallback ready user, the ADS should fall back directly to a Minimal Risk Condition if a failure of the ADS and/or other vehicle system prevents the ADS from performing the DDT		

19	If the ADS is designed to request and enable intervention by a human driver, the ADS should execute an MRM in the event of a failure in the transition of control to the user		
20	The ADS should signal its intention to place the vehicle in an MRC	<ul style="list-style-type: none"> The ADS should signal its intention to place the vehicle in an MRC to: <ul style="list-style-type: none"> ADS user or vehicle occupants Other road users (e.g., by hazard lights) 	
21	Pursuant to a traffic accident, the ADS should stop the vehicle	<ul style="list-style-type: none"> ADS reactivation should not be possible until the safe operational state of the ADS has been verified 	
The ADS should safely manage failure modes			
22	The ADS should detect and respond system malfunctions and abnormalities	<ul style="list-style-type: none"> The ADS should perform self-diagnosis of faults in accordance with the OEMs prescribed list The ADS should detect system malfunctions/abnormalities and evaluate system's ability to fulfill the entire DDT The ADS should have a function which makes the system inactivate remotely, if the system has OTA functionality, in case ADS safety is not ensured. 	The ADS has the remote disabling function or not.
23	The ADS should be protected from unauthorized access	<ul style="list-style-type: none"> The measures ensuring protection from an authorized access should be provided in alignment with engineering best practices 	
24	Provided a failure does not significantly compromise ADS performance, the ADS should respond safely to the presence of a [faults/failure] in the system	<ul style="list-style-type: none"> The limited operation of the ADS should comply to the normally applicable safety requirements 	
25	The ADS should signal major [faults/failures] and resulting operational status	<ul style="list-style-type: none"> The ADS should signal [faults/failures] affecting the ability to execute the DDT 	

The ADS should maintain a safe operational state		
26	[The ADS should signal required system maintenance to the user.]	
27	[The ADS should be accessible for the purposes of maintenance and repair to authorized persons.]	
28	ADS safety should be ensured in the event of discontinued production/support/maintenance during lifetime of the system.	<ul style="list-style-type: none"> The manufacturer should have ADS safety management system for ensuring over lifetime of the system. The manufacturer has ADS safety management system or not