Document FRAV-08-09
8th FRAV session
8 December 2020

Co-Chairs' Proposal to Guide Further Work on Safety Requirements for Automated Driving Systems

This document proposes a list of topics for discussion at future FRAV session. The list is based on 142 candidate safety requirements gathered from FRAV stakeholders (FRAV-03-07), the MLIT categorization of the candidates under the agreed starting points (FRAV-06-07), the OICA/CLEPA administrative review of national/regional ADS guidelines and related resources (FRAV-06-04), and the OICA/CLEPA classification of candidates based on the administrative review (FRAV-07-09). For transparency and to support further efforts, a concordance of the stakeholder input with these discussion topics has also been provided (FRAV-08-09-App.1).

1. ADS should drive safely.

This starting point aims to focus attention on the performance of an ADS as the driver of the vehicle. The intention is to enumerate performance elements nominally within the control of the driver.

1.1. The ADS should perform the entire Dynamic Driving Task safely.

1.1.1. The ADS should control the longitudinal and lateral motion of the vehicle safely.

~~1.1.2. The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).~~

~~1.1.3.~~1.1.2. The ADS should ~~detect, recognize, classify, and prepare to~~ respond to objects and events in the traffic environment safely.

1.2. The ADS should ~~respect~~ comply with traffic rules.

1.3. The ADS should interact safely with other road users.

1.4. The ADS should adapt its behavior in line with safety risks.

1.5. The ADS should adapt its behavior to the surrounding traffic conditions.

1.6. The ADS behavior should not be the critical factor in the causation of a collision.

1.7. The ADS should adapt to ODD boundary safely.

1.7.1. Activation of an ADS feature should only be possible when the conditions of its ODD have been met.

1.7.2. The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).

1.7.3. The ADS should safely manage short-duration transitions between ODD.

Commented [MLIT1]: Needless to say, "safely" is added to this and next sentence.

Commented [MLIT2]: Too detail and the word "respond" contains these meanings.

Commented [MLIT3]: The word "respect" is weak, and suggest to replace to "comply with".

Commented [MLIT4]: Question. What is the difference from 1.4. and 1.5.? If 1.4. covers 1.5., 1.5. should be deleted.

Commented [MLIT5]: We suggest to add an ODD paragraph in order to easily deal with the related requirements. The subparagraphs are copies from other part of this document.

Formatted

2. ADS should interact safely with the user.

This starting point aims to focus attention on the performance of an ADS with regard to the ADS user. The intention is to enumerate performance elements to ensure correct use of the ADS and safe transitions of control from the ADS to the user.

~~2.1. Activation of an ADS feature should only be possible when the conditions of its ODD have been met.~~

~~2.2.~~2.1. The ADS should signal timely when conditions indicate a probable ODD exit.

~~2.3.~~2.2. The user should be permitted to override the ADS to assume full control over the vehicle.

~~2.4.~~2.3. The ADS should safely manage transitions of full control to the user.

~~2.4.1.~~2.3.1. Prior to a transition of control to the user, the ADS should verify the availability of the user all the time to assume control and support the driver in resuming manual control at any time.

~~2.4.2.~~2.3.2. Pursuant to a transition, the ADS should verify full control of the vehicle by the user prior to deactivation.

~~2.5.~~2.4. The ADS should tolerate user input errors.

~~2.6.~~2.5. The ADS should provide feedback to the user on its operational status.

~~2.7.~~2.6. The ADS should warn the user of failures to fulfill user roles and responsibilities.

~~2.8.~~2.7. The user should be provided with information regarding user roles and responsibilities for the safe use of the ADS.

Commented [MLIT6]: In order to verify the safe transition, the user should be monitored all the time by driver monitoring system.

Commented [MLIT7]: Functions such as demist, windscreen wipers and lights should be managed properly in order for safe transition.

Document FRAV-08-09
8th FRAV session
8 December 2020

3. ADS should manage safety-critical situations.

This starting point aims to focus attention on the performance of an ADS in response to conditions that warrant exceptional reactions. The intention is to enumerate performance elements to ensure safe ADS responses to abrupt actions of other road users, incapacitation of the user, and unanticipated conditions (i.e., "emergency situations").

~~3.1. The ADS should recognize and respond to road safety agents.~~

~~3.2.~~3.1. The ADS should mitigate the effects of road hazards and collisions.

~~3.3.~~3.2. The ADS should execute a Minimal Risk Maneuver (MRM) as conditions warrant.

~~3.3.1.~~3.2.1. In the absence of a fallback-ready user, the ADS should fall back directly to an MRM.

~~3.3.2.~~3.2.2. The ADS should execute an MRM in the event of a failure in the transition of full control to the user.

~~3.3.3.~~3.2.3. Pursuant to an MRM, the ADS should place the vehicle in a Minimal Risk Condition prior to deactivation.

~~3.4.~~3.3. The ADS should signal an MRM.

~~3.5.~~3.4. ADS vehicles that may operate without a user-in-charge should provide means for occupant communication with a remote operator.

~~3.6. The ADS should safely manage short-duration transitions between ODD.~~

~~3.7.~~3.5. Upon completion of an MRM, the user may be permitted to assume control of the vehicle.

~~3.8.~~3.6. Pursuant to a collision, the ADS should stop the vehicle and deactivate.

Commented [MLIT8]: This requirement is already included in the traffic rule requirement(1.3.)

Commented [MLIT9]: Collision seems to be different from road hazards. This includes emergency manoeuvre for mitigating collisions.

4. ADS should safely manage failure modes.

This starting point aims to focus on the performance of an ADS in response to system failure modes. The intention is to enumerate performance elements related to failures that render the ADS incapable of performing the entire Dynamic Driving Task.

4.1. The ADS should detect system malfunctions and abnormalities.

4.2. The ADS should execute a safe fallback response upon detection of a failure that compromises performance of the DDT.

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~~ failure in the system.

4.4. The ADS should signal ~~faults~~ failures and resulting operational status.

4.4.

Commented [MLIT10]: Words should be aligned to failures if there are no difference in meaning.

Commented [MLIT11]: Question. What is the difference from 4.2. and 4.3.? If 4.2. covers 4.3., 4.3. should be deleted.

5. ADS should ensure a safe operational state.

This starting points aims to focus attention on the assurance of ADS operational safety throughout the useful life of the vehicle. The intention is to enumerate performance elements to ensure the maintenance of the ADS in a safe state, including decommissioning in the event of obsolescence.

5.1. The ADS should be permanently disabled in the event of obsolescence.

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.

~~5.3. The ADS should signal required system maintenance to the user.~~

~~5.4.~~5.3. The ADS should be accessible for the purposes of maintenance and repair to authorized persons.

Commented [MLIT12]: Requirements related to maintenance is not specific to ADS and should notp be described here.