Transmitted by the experts from OICA/CLEPA

Document FRAV-05-06
5th FRAV session
15 October 2020

Safety Requirements for Automated Driving Systems
Draft Industry Position

After FRAV 01 (Berlin) 09-10 October 2019, the group was set homework in preparation for FRAV 02 (Tokyo) 14-15 January 2020. Two of these were to:

- Draft descriptions for FRAV common functional performance requirements (FPR)
- Expand and detail FPR OICA document "Safety Element List (FRAV-01-13rev.1).

With this is mind Industry drafted and submitted (FRAV-02-13) a list of functional requirements taking into account the following documents published by various stakeholders:

- WP.29 framework document, 2019
- WP.1 resolution on the deployment of highly automated vehicles, 2017
- EC : guidance for application of article 20 of vehicle safety Directive, 2019
- Intel, Aptiv et al : safety first for autonomous driving, 2019
- Uber Advanced Technology Group: A Principled Approach to Safety, 2018
- US-DOT : autonomous driving vision for safety & framework for ADS testable cases and scenarios, 2018
- US DOT safety vision 2.0, 2016
- Transport Canada : safety assessment for ADS in Canada, 2018
- OICA : future certification of ADS, 2018
- France Eco System (VMAD 04-07), 2019

Industry did not draft any new requirements itself; this was mainly an administrative exercise that reviewed all suggested requirements from various documents / guidelines and consolidated/removed any requirements that were repeated, and slightly adjusted/merged the safety elements to give the document better structure.

Following the request from the Secretary prior to FRAV-05, Industry has restructured the document to align with the key safety elements proposed by FRAV leadership.

Safety Requirements

1. <u>ADS should drive safely. (ADS driving behavior, compliance with traffic laws….)</u>
    - 1.1. The ADS should not cause any traffic accidents that are reasonably foreseeable and preventable.
    - 1.2. The ADS should have predictable behaviour.
    - 1.3. The ADS should react to unforeseen situations in a way that minimizes risk.
    - 1.4. 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.
    - 1.5. The ADS should drive in accordance with the traffic rules.
    - 1.6. The ADS should prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects.
    - 1.7. The ADS should implement safe and appropriate responses when subjected to reasonably foreseeable scenarios within the ODD.

2. ADS should interact safely with the user. (Usability, user communications, misuse prevention, transfers of control….)

   2.1. When needed, communication with other road users should provide sufficient information about the vehicle's status and intention.
   2.2. The activation of the ADS should only be possible when the conditions of the ODD are met.
   2.3. 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.
   2.4. The ADS deactivation should only be performed when it has been verified that the user has taken over control.
   2.5. When necessary the ADS should protect the vehicle control against inadvertent or undeliberate user intervention.
   2.6. The mode concept should be designed in a way that minimizes mode confusion at the user and system level.
   2.7. The ADS should clearly inform user about the operational status (operational, failure, etc.) in an unambiguous manner.
   2.8. When the ADS is active it should be capable of determining the user's status.
   2.9. If applicable other activities 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.
   2.10. 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 take-over request.
   2.11. The system should be capable of transferring control back to the user in a safe manner.
   2.12. The system shall be able to determine whether or not the user has taken over.
   2.13. 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).
   2.14. 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.

3. ADS should manage safety-critical situations. (Response to other road-user actions, emergency situations, post-crash, occupant protection….)

   3.1. The ADS shall communicate critical messages to vehicle's users and other road users when needed.
   3.2. 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.
   3.3. The ADS should 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.
   3.4. After detection of a first significant shock while driving (e.g. frontal collision with airbags triggering or lateral collision during an insertion), the vehicle should:
      a) inhibit AD mode reactivation until proper operation has been verified,
      b) immediately attempt to achieve a safe state in the best possible way, according to vehicle operational status and current situation
   3.5. The ADS may also, simultaneously, request the user to takeover vehicle control if vehicle and current situation are sufficiently controllable.

4. ADS should safely manage failure modes. (DDT-related functions and response to loss of function)

4.1. 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.

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

4.3. The Minimal Risk Manoeuvre (MRM) should be capable of achieving a 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.

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

5. ADS should ensure a safe operational state. (Maintenance, updates, obsolescence….)

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