Submitted by the experts from OICA and CLEPA

Document FRAV-02-13
2nd FRAV session, 14-15 January 2020
Agenda item 6.5.

Functional Requirements for Automated/Autonomous Vehicles

Draft Industry Position

Detailed wording has not yet been fully agreed

1 System Behaviour

1.1 Dynamic behaviour in road traffic

1.1.1 The Automated Driving System (ADS) shall:

a) not cause any traffic accidents that are reasonably foreseeable and preventable.
b) have predictable behaviour.
c) react to unforeseen situations in a way that minimizes risk.

1.1.2 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.

1.2 Adherence to rules of the road (Federal and local laws)

1.2.1 The ADS shall:

a) drive in accordance with the traffic rules.
b) prioritize actions that will maintain the safe flow of traffic and prevent collisions with other road users and objects.

1.3 [Interaction with other road users.

1.3.1 When needed, communication with other road users shall provide sufficient information about the vehicle's status and intention.]

2 Operational Design Domain (ODD)

2.1 The manufacturer shall declare the scope of the ADS (so called operational design domain(s) (ODD)) e.g. where and when the ADS is designed to operate. This shall include at a minimum:

a) Road conditions (motorways/expressways, general roads, number of lanes, existence of lane marks, roads dedicated to automated driving vehicles, etc.)
b) Geographical area (urban and mountainous areas, geofence setting, etc.)
c) Environmental conditions (weather, night-time limitations, etc.)
d) Speed range
e) Other conditions that must be fulfilled for the safe operation of the ADS.

2.2 It is necessary to clearly define the split in responsibilities between the driver and the ADS.
2.3 The ADS must be capable of identifying when conditions defining the ODD are met and predicting when they will no longer be met.

3 Object and Event Detection and Response (OEDR)

3.1 Object and Event Detection and Response (OEDR) refers to 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.
3.2 The ADS shall have OEDR capabilities that support safe and appropriate actions when subjected to reasonably foreseeable scenarios within the ODD.

4 Human Machine Interface (HMI)

4.1 Activation / deactivation

4.1.1 The activation of the ADS shall only be possible when the conditions of the ODD are met.
4.1.2 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.
4.1.3 The ADS deactivation shall only be performed when it has been verified that the user has taken over control.
4.1.4 When necessary the ADS shall protect the vehicle control against inadvertent or undeliberate user intervention.
4.1.5 The mode concept shall be designed in a way that minimizes mode confusion at the user and system level.

4.2 System Status

4.2.1 The ADS shall clearly inform user about the operational status (operational, failure, etc.) in an unambiguous manner.

4.3 Occupant Monitoring

4.3.1 When the ADS is active it shall be capable of determining the user's status.
4.3.2 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.

4.4 Take-Over request

4.4.1 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.

4.4.2 The system shall be capable of transferring control back to the user in a safe manner.

4.5 Communication of Critical Messages

4.5.1 The ADS shall communicate critical messages to vehicle's users and other road users when needed.

4.5.2 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.

5 Failsafe Response

5.1 Understanding the system limits and boundaries

5.1.1 The ADS shall 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.

5.1.2 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.

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

5.2 Take over of DDT (if required, based on level of automation)

5.2.1 The system shall be able to determine whether or not the user has taken over.

5.2.2 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).

5.2.3 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.

5.3 Minimal Risk Manoeuvre

5.3.1 The Minimal Risk Manoeuvre (MRM) shall 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.

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

6 Safety of In-use Vehicles

6.1 Inspections/Repair/Modifications processes

Not within the scope of UNECE's Informal Working Group – Functional Requirements for Automated vehicles (FRAV).

6.2 Maintenance of existing level of crashworthiness (for vehicles carrying occupants)

Requirements covered by UNECE's Working Party on Passive Safety (GRSP)

6.3 Vehicle state monitoring

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

6.4 Post-crash behaviors (Collision Notification to Occupants and Emergency services; Return to a safe-state)

6.4.1 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:

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

6.4.2 The ADS may also, simultaneously, request the user to takeover vehicle control if vehicle and current situation are sufficiently controllable.