Safety Requirements for Automated Driving Systems

The text reproduced below was prepared by the FRAV secretary to enumerate proposals for ADS safety objectives. This text is based upon the FRAV co-chair proposals for "starting points" (FRAV-05-03) and the "administrative exercise" of OICA/CLEPA consolidating items taken from the WP.29 AV Framework Document (WP.29/2019/34/Rev.1), national and regional guidelines, and other sources considered by FRAV.

For the 6th session, FRAV has requested stakeholders to provide input towards reaching consensus on no more than ±10 safety objectives under each item.

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 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 driver.

This starting point aims to focus attention on the interaction performance of an ADS with regard to the ADS user. The intention is to enumerate performance elements to ensure correct understanding of the limitations and possibilities of the ADS and safe transitions of control between the ADS and the user.
The ADS-user doesn't have an average user-profile, but covers a wide spectrum of different dimensions (abilities, limitations, understanding, experience, alertness,….). To understand the ADS, the user forms a mental model[1] of it. One of the challenges is to safely accommodate the wide spectrum of the different ADS-users in order to have more predictable Human Machine interaction and error tolerant system.
Human Machine Interaction (included transition of control) and relevant interfaces need to be developed in an harmonized way in order to promote an accurate and reliable mental model of all ADS and support learning and the effectiveness of common driver training [proposal to WP1] for the all users

1. When needed, communication with other road users should provide sufficient information about the vehicle's status and intention.(this is communication to external)

[1] A driver's mental model is comprised of their understanding, belief and expectations of the system that they are interacting with. Some of this information is based on what they know and have learned about the system(the general metal model). However, since driving is a dynamic task, a driver's mental model is a dynamic thing(applied mental model). A safe and useful system is one that supports a driver in this changing environment through safe and effective interactions between the vehicle and driver. With ADAS & ADS the vehicle itself has capability and it and the driver each need to have an understanding of the other's role and functions as driving conditions change. (See General Mental Model & Applied Mental model components from Seppelt & Victor, 2020).

2. The ADS provides a harmonized transition of control with harmonized defined states and interaction
3. The interaction between the ADS and the user needs to be developed according to harmonized HMI design principles in order to promote an accurate mental model the ADS and to prevent mode confusion between different car makers and models
4. The HMI should always clearly inform the user about the current operational status (operational, failure, etc.) in an unambiguous, salient and harmonized manner

On harmonized interaction and transition of control

a. The human machine interaction and transition of control follow a safe, logical, understandable and consistent/ predictable pattern.

b. The mode concept should be designed in a way that minimizes mode confusion at the user and system level.

~~b.~~c. 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.[This second sentence needs rephrasing to better reflect the intentions]

~~c.~~d. The ADS deactivation should only be performed when it has been verified that the user has taken over control.

e. The system should be capable of transferring control back to the user in a safe manner. [comparable to a]

~~d.~~a. ~~When necessary the ADS should protect the vehicle control against inadvertent or undeliberate user intervention.~~

~~e.~~a. ~~The mode concept should be designed in a way that minimizes mode confusion at the user and system level.~~

f. When the ADS is active it should be capable of determining the user's status and availability. (only when it is active?)

~~g. The system should be capable of transferring control back to the user in a safe manner.~~

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

~~i.~~h. 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).

i. 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.

j. 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.

k. When necessary the ADS should protect the vehicle control against inadvertent or undeliberate user intervention.

On harmonized Human Machine Interface

a. The ADS should clearly and unambiguously indicate availability to be switched on.

b. The ADS should always clearly inform user about the current operational status (operational, available, failure, etc.) in an unambiguous, salient and harmonized manner.

c. The ADS continuously informs the user of its capability to perform the driving task.

~~d.~~a. ~~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.~~

~~e.~~a. ~~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.~~

~~f.~~d. 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.

[Earlier text from FRAV-06-04, used in this proposal when marked green]

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

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 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:
3.5. inhibit AD mode reactivation until proper operation has been verified,
3.6. immediately attempt to achieve a safe state in the best possible way, according to vehicle operational status and current situation
3.7. 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.

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 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.

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