Transmitted by the experts from Japan
(comments on FRAV-06-11 transmitted by Germany)

Document FRAV-07-08~~XX~~
7th FRAV session
17 November 2020

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.
~~1.3.~~1.4. The nominal operation of the ADS shall result in equal or safer performance than a competent and careful human driver.
~~1.4. The nominal operation of the ADS shall result in equal or safer performance than a~~ competent and careful ~~human driver. i.e. achieve a neutral or positive risk balance.~~
1.5. The ADS shall not cause a collision due to its own driving behavior.
~~1.5.~~1.6. The ADS should drive in accordance with the traffic rules.
~~1.6.~~1.7. The ADS should ~~prioritize actions that will maintain the safe flow of traffic and~~ prevent collisions with other road users and objects.
~~1.7.~~1.8. The ADS should implement safe and appropriate responses ~~when subjected to reasonably foreseeable~~relevant ~~scenarios~~ within the ODD.

2. ADS should interact safely with the driver and other road users.

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. 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.
~~2.7.~~2.8. When the ADS is active, it should be capable of determining the user's status.
~~2.8. When the ADS is active it should be capable of determining the user's status.~~

Commented [MLIT1]: <overall comment> Is there any intention for differentiating "should" and "shall" in this document?

Commented [A2]: This term needs to be defined: foreseeable by whom? ADS with sensors, expert driver, neural network, programmer of ADS?

Commented [MLIT3]: What kind of behaviour is considered to be not predictable? Need further explanation.

Commented [MLIT4]: Need definition of "positive risk balance". Is it acceptable for society if there is an accident that can be avoidable by human driver?

Commented [A5]: Requirement has to be stricter: ADS shall not cause a collision due to its own driving behavior at all!
Justification: ADS does not get tired and does not have lapses and is thus deemed to be significantly better than the human.
And:
ADS shall react on other vehicles wrong behavior with the best collision avoidance/mitigation strategy possible using state of the art technology.
Justification: ADS will not be able to iron out all mistakes of others but with state of the art tech reaction times can be significantly better than the human.

Commented [MLIT6]: This sentence should remain, since proposal from Germany does not fully cover this original sentence.

Commented [A7]: …and since I like clear statements, I would not like this "prioritize"-construction.

Commented [A8]: I would even go further to remove this statement. It is safe if there are no collisions, and the safe flow of traffic will need further definitions anyway.

Commented [A9]: Traffic flow and safety should not be mentioned in a single bulletpoint. It must be made clear that safety has priority over traffic flow.

Commented [MLIT10]: We believe scenarios are the way of validation, not requirement

Commented [MLIT11]: Japan considers interaction with other road users is also important issue.

Commented [A12]: What is the added value in this sentence that is not very precisely and more to the point expressed under No. 2.5? (i.e. are we sure that systems are sufficiently mature to override ("delay") driver input in general?)

Commented [A13]: This requirement is redundant to No 2.10.

Commented [MLIT14]: Not redundant because 2.10 may be accomplished without 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 (level 3 and 4 systems), 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.

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 safety-critical situations ~~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.~~3.2. 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.~~3.3. 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.~~3.4. inhibit AD mode reactivation until proper operation has been verified,
~~3.6.~~3.5. immediately attempt to achieve a safe state in the best possible way, according to vehicle operational status and current situation
3.6. The ADS may also, simultaneously, request the user to takeover vehicle control if vehicle and current situation are sufficiently controllable.
~~The ADS shall react on other vehicles wrong behavior with the best collision avoidance/mitigation strategy possible using state of the art technology.~~

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 Minimum Risk Condition (-MRC)~~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.

Commented [MLIT15]: It seems that responsibility can be different depends on traffic rules and other aspects. Other wording should be considered.

Commented [A16]: The headline suggests how the dynamic driving task should be handled, but then it is about HMI (1, 2, 4, 5, 7), Failure (3)..

My suggestion would be to not have this section and move the individual topics to where they better fit.

Commented [MLIT17]: This part is applicable to only level 4 driverless vehicles. We prefer to discussing this kind of issues in the later stage.

Commented [A18]: Should this probably go to section 4?

Commented [A19]: We should separate between "no crash has happened yet" and "in crash" and "post crash"

Commented [MLIT20]: The meaning of "state of the art" is still not clear to us. Does it mean "the latest technology" or something else? If it means the latest technology, only one technology among several technologies shall be accepted, and this concept is against "technology neutral". If it does not mean the latest technology, the wording is not appropriate.
Since there are ambiguity, this paragraph should be deleted.

Commented [MLIT21]: This word is unclear. We need to find criteria.

Commented [MLIT22]: In the case of level 3 system, transition demand should be initiated before starting MRM, shouldn't it?

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.