Submitted by the experts from Germany

FRAV-10-07
10th FRAV session
27 January 2021

As a follow-up to the 9th FRAV informal group meeting, FRAV stakeholders are kindly requested to comment on the discussion topics derived from the five starting points. During the session, FRAV agreed and the secretary was directed to prepare a single document to gather comments for further FRAV consideration.

The aim of the following table is to gather stakeholder views on the meaning or underlying safety goals related to and/or derived from the performance topics. Based on those views, the table further requests stakeholder views on criteria, metrics, and performance indicators that might be used to define safety requirements that can be measured and/or verified.

The following example for filling in the table illustrates the desired level of detail (it does not propose comments for stakeholder response). The "Interpretation/Goals" column should be used to comment on the performance topic and views on its significance to the development of safety requirements. The "Measurable/Verifiable Criteria" column should be used to suggest indicators or performance metrics for safety goals proposed under the "goals" column. The intention is not to request technical proposals for requirements, limits, or values. The aim is to identify factors that might be useful in defining measurable/verifiable requirements to ensure desirable safety outcomes.

The "Guardrails"-Approach for ADS safety regarding the dynamic driving task

Problem

When specifying criteria for Automated Driving Systems, it is most important to leave the behavior itself to the manufacturer and NOT specify exact driving maneuvers that are considered safe in the first place, but make it impossible to achieve the most safest behavior.

Examples

An ADS drives on a highway in the center lane, overtaking occasionally vehicles on the slower lane. The faster lane is empty. It could be considered safe if the ADS is centered in its own lane, associated criteria being a tolerance of X cm with respect to the center. This also fixes the lateral safety distance to the vehicles being overtaken. It could also be considered safe if the speed of the ADS is maintained at the allowed speed limit and is not changing.

An advanced ADS may be in a position to determine that some vehicles are more likely to cut into the ego lane and thus might want to increase the safety distance by positioning itself more on the far side of its own lane. It could also come to the conclusion that the speed difference to the possible threats should be lower to decrease the risk when approaching, it could on the other hand increase the speed just after the critical point (e.g. passing the front edge of the possible threat) to decrease the risk until the other vehicle is overtaken.

It should NOT be required by the regulator that the ADS user's acceleration level is comfortable – this is a criterion for user acceptance of the ADS and will be the aim of the vehicle manufacturer to be better than the competition.

There will be an infinite number of situations where the most obvious safe behavior is probably not the safest when rethinking, such as discussed in this example. A safe behavior requires a large amount of data to learn from, which certainly cannot be achieved by the regulator.

Solution

The regulator cannot specify what is a safe behavior due to lack of data and disambiguity of situations (more than one behavior is safe). Since this is not possible, the regulator should rather specify "guardrails" for safe behavior, not the behavior itself. The guardrails promoted by Germany are the following, and specifically in this order:

- **Follow traffic regulations**
- **Do not cause accidents**
- **Iron out mistakes of others as good as (physically/technically/logically in the sense of anticipation/whichever is safer) possible**
  - **Define "as good as physically/technically/logically possible" by determining which collisions caused by mistakes of others have to be avoided and which just mitigated. This should be done by using physical parameters like TTC, distance, speed, etc.**

The regulator should stop after this.

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
The ADS should control the longitudinal and lateral motion of the vehicle.	• The ADS should smoothly execute maneuvers. • The ADS driving behavior should meet public expectations. • The vehicle movements should be safe. • The ADS driving behavior should not cause collisions or disrupt traffic. • This topic should not be considered. • This topic should focus on safety. • This topic should include the impact on other road users and traffic flows. • ….	• Relative speed and distance from a preceding vehicle should be sufficient to avoid a collision. • Relative speed and distance from a preceding vehicle should be consistent with safe human driving performance data. • Lane positioning should ensure a safe lateral distance from an adjacent vehicle (consistent with safe human driving performance data). • Lane changes should be smooth with lateral acceleration compatible with/comparable to safe human driving. • ….

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from ADS should drive safely)		
The ADS should perform the entire Dynamic Driving Task.	• **See below**	• **Not verifiable, top-level requirement**
The ADS should control the longitudinal and lateral motion of the vehicle.	• **This includes the "entire DDT" topic from above. It is NOT necessary to define criteria for how exactly the vehicle should drive, because this would limit the manufacturers in inventing the best possible strategies. It should rather define "guardrails" (see introduction), between which the vehicle performance may be set, by defining WHAT kind of accidents should NOT happen.**	• **Not verifiable, top-level requirement**
The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s).	• **Recognizing alone is no statement at all. I can recognize that I leave the ODD and still do it**	• **Verifiable, relevant for the start of a transition**
The ADS should detect, recognize, classify, and prepare to respond to objects and events in the traffic environment.	• **This is not compatible with the "guardrails"-approach since no quality of the response is required.** • **The response is important, not the preparations and calculations the vehicle performs without responding.**	• **Verifiable, yet not relevant to the "guardrails" approach, especially not relevant to the safety goals (do not cause accidents).**
The ADS should respect traffic rules.	• **Very relevant criterion**	• **This is already a verifiable requirement, given that for any given situation, it should be possible to find a Boolean result to whether the vehicle respects traffic rules. Further work is just defining assessment methods → could be done within VMAD**
The ADS should interact safely with other road users.	• **According to the "guardrails", "safely" should be interpreted as "irons out mistakes of others to the largest possible extend" and "does not CAUSE accidents". There should**	• **Not verifiable.**

	not be specific artificial requirements for the behavior itself.	
The ADS should adapt its behavior in line with safety risks.	• **No, because this is not verifiable, and to our understanding it will not be possible to define the one safe set of requirements for this. There is a plethora of methods the ADS could use to increase the level of safety that we cannot foresee at this stage.** • **An example: we could come to the conclusion that staying in the center of the lane would be considered safe. But when overtaking other vehicles in adjacent lanes, drifting to the own lane's edge will increase the lateral safety distance and thus increase safety.**	• **Not verifiable**
The ADS should adapt its behavior to the surrounding traffic conditions.	• **Not compatible the guardrails**	• **Needs further specification to become verifiable. And these specifications should not aim to specify a certain behavior of the vehicle.**
The ADS driving behavior should not disrupt the flow of traffic.	• **At least in Germany, this aspect is already included in "follow traffic rules" – there is a set of rules which states you should not drive too slow unnecessarily, and you should maintain the distance.** • **We need to avoid redundant requirements.**	•
The ADS behavior should not be the critical factor in causation of a collision.	• **This is too unspecific. It should not cause collisions.**	• **"It should not cause collisions" is already verifiable, considering that for any given accident, it is possible to determine who was at fault. And the answer should be that it was NOT the ADS.**
The ADS should not cause accidents	• **Specific**	• **Needs a definition of scenarios and a check whether the ADS does cause accidents or not. → VMAD**

The ADS should iron out mistakes of others the the largest extend possible	• **The largest extend being what is physically/technically according to the state of the art/logically possible**	• **Requires the identification of relevant accident scenarios, definition of performance requirements for pass/fail-tests for these scenarios** • **Proposed task for FRAV: draft sub-top-level requirements**

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from the ADS should interact safely with the user)		
Activation of an ADS feature should only be possible when the conditions of its ODD have been met.	• **Specific**	• **Verifiable.**
The ADS should signal when conditions indicate a probable ODD exit.	• **Possibly specific. Needs to become clearer:**	• **The ADS should signal to the driver with sufficient lead time (e.g. 10 seconds) in advance when an ODD exit is probable .**
The user should be permitted to override the ADS to assume full control over the vehicle.	• **Specific**	• **Any overruling should lead to ADS deactivation with the relevant safety measures (e.g. control handover after a specific time, or when the handover is considered safe). It should not be possible to cancel the deactivation.** • **Possibly define the lead time and require the vehicle to be able to fully perform the DDT in that time.**
The ADS should safely manage transitions of control to the user.	• **Unspecific – further specifications needed (e.g. transition time, traffic related situation for the transition).**	•
Prior to a transition of control to the user, the ADS should verify the availability of the user to assume control.	• **Availability of the user should be verified continuously during ADS operation**	•
Pursuant to a transition, the ADS should verify full control of the vehicle by the user prior to deactivation.	• **Full control by the user should be specified with regard to Situation Awareness**	•
The ADS should tolerate user input errors.	• **Should not only tolerate but implement an adequate coping strategy for input errors**	•
The ADS should provide feedback to the user on its operational status.	• **Feedback should be provided continuously** • **Feedback should make changes in the situation clear to the driver**	•

The ADS should warn the user of failures to fulfill user roles and responsibilities.	• ADS should warn the user in case he/she is detected unavailable to take over control	•
The user should be provided with information regarding user roles and responsibilities for the safe use of the ADS.	• Term ‘information’ should be specified (e.g. what kind of information? User Manual, Display Information, Warnings, etc.?) • depending on the piece of information that is to be provided, the way of “providing” those information needs to be adapted, e.g. general information on user roles should be provided prior to the ride, whereas hints/alerts addressing specific undesired behavior should be given upon occurrence	•
ADS vehicles that may operate without a user-in-charge should provide means for occupant communication with a remote operator.	• Ok.	•
Upon completion of an MRM, a user may be permitted to assume control of the vehicle.	• Ok.	•

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from the ADS should manage safety-critical situations)		
The ADS should recognize and respond to road-safety agents.	• **Unspecific. Recognizing itself should not be a relevant criterion for performance since it is ALWAYS redundant to the action/intervention and thus provides no safety benefit.**	•
The ADS should mitigate the effects of road hazards.	• **Road hazards being mistakes of other vehicles: OK, needs further specs.** • **Road hazards such as weather, potholes: No, it should not mitigate these, it should avoid accidents due to these.**	•
The ADS should execute a safe fallback response as conditions warrant.	• **Ok, but unspecific.**	•
In the absence of a fallback-ready user, the ADS should automatically achieve a Minimal Risk Condition (MRC).[*]	• **Ok.**	• **Specific, verifiable**
The ADS should place the vehicle in an MRC in the event of a failed transition of full control to the user. [*]	• **Ok.**	• **Specific, verifiable**
The ADS should achieve a Minimal Risk Condition (MRC) prior to deactivation. [*]	• **Ok.**	• **Specific, verifiable**
The ADS should signal its intention to place the vehicle in an MRC. [*]	• **Ok.**	• **Specific, verifiable**
The ADS should safely manage short-duration ODD exits.	• **Is this a) a quick reaction to an ODD exit? Then OK, ODD exit procedures apply** • **Is this b) a off-on-situation for the ODD (e.g. shortly driving through a non-ODD condition being still active? Then not OK. Any ODD exit shall lead to deactivation with the**	•

[*] These topics were modified from the original proposals in response to the 7th session discussion on minimal risk maneuvers.

	relevant procedures.	
Pursuant to a collision, the ADS should stop the vehicle and deactivate.	• **OK.**	• **Specific and verifiable.**

Submitted by the experts from Germany

FRAV-10-07
10th FRAV session
27 January 2021

Performance Topic	Interpretation/Goals	Measurable/Verifiable Criteria
(Derived from the ADS should safely manage failure modes)		
The ADS should detect system malfunctions and abnormalities.	•	•
The ADS should execute a safe fallback response upon detection of a failure that compromises performance of the DDT.	•	•
Provided a failure does not compromise ADS performance of the entire DDT, the ADS should respond safely to the presence of a fault in the system.	•	•
The ADS should signal faults and resulting operational status.	•	•
(Derived from the ADS should maintain a safe operational state)		
The ADS should be permanently disabled in the event of obsolescence.	•	•
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.	•	•
The ADS should signal required system maintenance to the user.	•	•
The ADS should be accessible for the purposes of maintenance and repair to authorized persons.	•	•
ADS safety should be ensured in the event of discontinued production/support/maintenance.	•	•