Submitted by the experts from Germany

FRAV-19-06
19th FRAV Session
16 September 2021

Workshop on ADS Safety Elements

This document includes an editorial review of the ADS Safety Elements proposed in FRAV-12-08 based on comments received in the documents:

- FRAV-08-09
- FRAV-09-08
- FRAV-10-11
- FRAV-12-08
- Dynamic Driving Task workstream
- Other Road Users workstream
- Human Factors workstream

This document needs to be reviewed in conjunction with **FRAV-18-09** (excel), providing the rational behind the consolidation exercise proposed in the table below.

Submitted by the experts from Germany

FRAV-19-06
19th FRAV Session
16 September 2021

Safety Topics and Detailed Requirements

	Performance Topic	**Detailed Requirements**	**Measurable / Verifiable Criteria**
The ADS should drive safely			
1	The ADS should be capable of performing the entire Dynamic Driving Task (DDT)	• The capability of the ADS to perform the entire DDT should be determined in the context of the ODD of the ADS • As part of the DDT, the ADS shall be able to: ○ Operate at safe speeds; ○ Maintain appropriate distances from **[other road users]** by controlling the longitudinal and lateral motion of the vehicle; ○ Adapt its behaviour to the surrounding traffic conditions (e.g., by avoiding disruption to the flow of traffic) ○ Adapt its behaviour in line with safety risks (e.g., by giving all road users and passengers the highest priority)	
2	The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s)	• The ADS should be able to determine when the conditions are met for activation. • The ADS should detect and respond when one or more ODD conditions are not or no longer fulfilled. • The ADS should be able to anticipate planned exits of the ODD • The ODD conditions and boundaries (measurable limits) should be established by the manufacturer. • The ODD conditions to be recognized by the ADS should include: ○ Precipitation (rain, snow) ○ Time of day (light intensity, including the case of the use of lighting devices) ○ Visibility ○ Road and lane markings	
3	The ADS should detect and respond to objects and events relevant for the DDT	• **[Objects and events might include, but are not limited, to:**	

		○ **Vehicles, motorcycles, bicycles, pedestrians, obstacles** ○ **Road accidents** ○ **Road safety agents / enforcement agents** ○ **Emergency vehicles]**	
4	The ADS should comply with traffic rules **[in the country of operation / within the ODD]**	• ADS should comply with the traffic laws in nominal conditions, except when in specific circumstances or when necessary to enhance the safety of the vehicle's occupants and/or other road users	
5	The ADS should interact safely with other road users	The ADS should interact safely with other road users, such as via: • **[Signaling maneuver intentions]** • **[Signaling ADS status (active/inactive)]**	
6	~~The ADS should adapt its behavior in line with safety risks~~		
7	~~The ADS should adapt its behavior to the surrounding traffic conditions~~		
8	~~The ADS driving behavior should not disrupt the flow of traffic~~		
The ADS should interact safely with the user			
9	~~Activation of an ADS feature should only be possible when the conditions of its ODD have been met~~ ~~User I~~**interaction with the ADS and the interface of ADS (features) should have high-level commonality of design** ~~**so as to support users' mental model of system operation**~~	1) The ADS (features) should use interfaces with high-level of commonality 2) The **operation** of the interaction should **have** in common: a) [use of common sequence of states in the transition/activation/overriding/…] 3) The interaction should be simplified: a) [Limit the number of roles] b) [Limit the number of potential transitions] **c) [Limit the number of settings]** **d) [Limit the number of different interaction modes]**	

Commented [WA1]: It should be described in the detailed requirements column what a high-level commonality really is. At the moment, to my understanding, this is not sufficiently related.

Commented [WA3]: Can the roles really be limited by Human Factors Design or isn´t this at the end linked to the Use Case?

Commented [WA2]: I don´t see an added value in introducing this research term ("mental model") here. Even within Human Factos research this term is defined very differently. Do the detailed requirements change, if we leave this term out of the topic?

Commented [WA4]: What is the difference of interaction modes and transitions? To my understanding, if one is limited, the other one will be limited automatically as well (fewer modes, fewer potential transitions).

10	~~The user should be informed about the ADS status (when the ADS is activated) with regards to ODD~~ **The ADS should provide clear and unambiguous information to the user**	1) The ADS should **inform** the user on the current conditions: a) **ADS** status information b) User Role **c) Potential roles to activate** d) Responsibility e) Permitted NDRA f) “Standard” information i) Vehicle speed, range and Time to Fuel g) ADS failure information h) Availability of automated features 2) The ADS should **inform** the user on the upcoming conditions: a) ODD boundaries **b) Upcoming actions or change in roles** c) Oncoming decisions/manoeuvers d) Estimated time to overtake in normal conditions e) Warning for upcoming transition request f) Confirmation request for upcoming transition 3) The ADS should present the information so as to assure a safe interaction: a) Timing requirements b) Priority requirements c) Saliency requirements	
11	~~The user should be permitted to take over control from the ADS, if the ADS is designed to request and enable intervention by a human driver~~ **The ADS should prevent misuse and errors in operation**	1) The ADS should be designed to prevent inadvertent activation or deactivation 2) The controls **dedicated to** the ADS should be clearly distinguishable from other controls 3) The ADS should be designed to avoid activation of an ADS outside its ODD 4) The ADS should be designed to avoid illegal settings The ADS should provide feedback when the user attempts to enable not allowed functions	

Commented [WA6]: Is there a difference between User Role and Responsibility? To my understanding, this is strongly linked to each other and should be put together

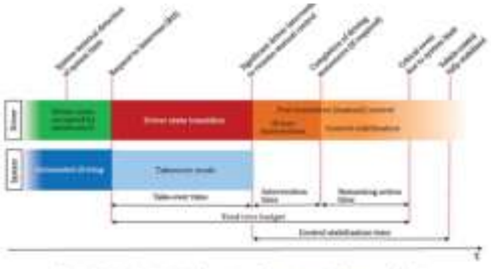
Commented [WA5]: “Clear and unambiguous” describe the way of presenting an information. However, the concrete (minimum) content of information should be defined first. Again, for my understanding, the detailed requirements are not sufficiently related to the performance topic. Does it make sense to split this into two aspects?

Commented [WA7]: Isn´t this at the end an open list with too many aspects? Maybe the ADS should inform the user what is not permitted or simply more generally what role and responsibility is required

Commented [WA8]: Can a safe interaction really be assured? I would propose to promote safe interaction in this case by means of good design.

Commented [WA9]: “Prevent” is a very hard term here. ADS design can promote proper system use; however, misuse and errors will still be in place. Full prevention seems rather unrealistic.

Commented [WA10]: What are “not allowed functions”?

12	~~The ADS should safely manage transitions of control to the user~~ **The ADS should assure a safe ADS feature activation**	1) The ADS should inform the user that preconditions for activation are met 2) The activation should follow a common sequence a) Common sequence to be a pass/fail criterion 3) The ADS should provide confirmation that the system is activated	
13	~~The ADS should safely respond to user input errors~~ **The ADS should assure a safe Transition Of Control**	1) The interaction should follow a common sequence in the transition of control (change of user roles) a) Common sequence to be a pass/fail criterion  Driver System Driver state transition Automated driving Takeover mode Take-over time Intervention time Remaining action time Control stabilization time t Figure 2 — System-initiated transition from automated to manual driving (concepts are further specified in 5.3.2 and 5.3.3) [1] 2) Transition of control should return to a common default user role (to prevent mode confusion **and other risks**) a) This should normally be fully engaged driving (conventional driver) b) Common default user to be a pass/fail criterion 3) The ADS should **continuously** verify **whether** the user is available for the transition of control **and warn the user if not available when required** (MRM to be specified elsewhere) 4) The ADS should verify that the driver is in stable control of the vehicle to complete the Transfer of Control to the user	

Commented [WA11]: Can an ADS really "assure" this? To my understanding, the design can only promote proper system use, but not assure it. At the end it is still the driver which plays an important role

Commented [WA12]: Is this status information or and additional message? In case of the former one, it is already required in topic 10.

Commented [WA13]: How will stable control be defined? How long does it take to verify, that a driver is in stable control?

Commented [WA14]: What about assistance during the transfer process? For example, wouldn´t it make sense to require an earlier intervention by a lane keeping system in case the driver has problems in lateral control of the vehicle?

[1] Reference: ISOxxx

		5) During transition, the ADS should remain active until the transfer of control has been completed or the ADS reaches a minimal risk condition	
14	~~The ADS should provide feedback to the user on its operational status~~ **The ADS should assure a safe user initiated take over**	**1) Under safe conditions the user is allowed to initiate a take-over of the ADS** 2) The deactivation should follow a common sequence a) Common sequence to be a pass/fail criterion 3) The ADS should **prevent and** warn a user for a user initiated take over that **would likely** lead to an unsafe situation 4) The ADS should provide a clear feedback of the successful user initiated take over a) The clear feedback should be a pass/fail criterion 5) The user initiated take over should return to a common default user role (to prevent mode confusion **and other risks**) a) This should normally be fully engaged driving (conventional driver) Common default user role to be a pass/fail criterion	
15	~~The ADS should warn the user of failures to fulfill user roles and responsibilities~~ **The ADS manufacturer should provide tools for the authorized user to learn about system functionality and operation.**	*On the general mental model (common understanding):* 1) **ADS manufacturer** should describe the possible educational approach: a) Theoretical and practical training b) How it aligns with common HMI and interaction 2) **ADS manufacturer** should provide documented information on ADS (features) capabilities and limitations (the information should also refer to specific scenarios) 3) **ADS manufacturer** should provide documented information on roles and responsibility of Driver/user and ADS when ADS (feature) is on/off 4) **ADS manufacturer** should provide documented information on allowed transition of roles and procedure for the transition (activation/deactivation, ToC, Override) 5) **ADS manufacturer** should provide a list of NDRA allowed when an ADS feature is active	

Commented [WA15]: Will oversteering of the system then still be possible?

Commented [WA16]: How will unsafe be defined and differentiated from a safe situation?

Commented [WA17]: Again, is this just status information or is some additional information required?

Commented [WA18]: What if users do not want to use this information? Will this be mandatory prior to usage or provided optionally by User Manuals / Quick Start Guides as already done now for assisted driving functions?

Commented [WA19]: Will this be a full list or just examples?

		On the applied mental model (understanding the ADS-specifics) 6) The ADS supports the user in correct operation (coaching) 7) The ADS gives prompt feedback on erroneous operation	
16	ADS vehicles that may operate without a **[user-in-charge/in-vehicle driver]** should provide means for occupant communication with **[a remote operator/user-in-charge/human driver/remote assistance personnel]**		
The ADS should manage safety-critical situations			
17	The ADS should execute a safe fallback response in the event of a failure of the ADS and/or other vehicle system that prevents the ADS from performing the DDT	• In the absence of a fallback-ready user, the ADS should fall back directly to a Minimal Risk Condition (MRC) • If the ADS is designed to request and enable intervention by a human driver, the ADS should execute an MRM in the event of a failure in the transition of control to the user ○ **[Upon completion of an MRM, a user may be permitted to assume control of the vehicle]** ○ **[The user should be permitted to override the ADS to assume full control over the vehicle]**	
18	~~In the absence of a fallback-ready user, the ADS should fall back directly to a Minimal Risk Condition if a failure of the ADS and/or other vehicle system prevents the ADS from performing the DDT~~		
19	~~If the ADS is designed to request and enable intervention by a human driver, the ADS should execute an MRM in the event of a failure in the transition of control to the user~~		
20	The ADS should signal its intention to place the vehicle in an MRC	• The ADS should signal its intention to place the vehicle in an MRC to: ○ ADS user or vehicle occupants	

Commented [WA20]: Is this intended by normal system design or by a special kind of coaching program?

		○ Other road users (e.g., by hazard lights)	
21	Pursuant to a traffic accident, the ADS should stop the vehicle	• ADS reactivation should not be possible until the safe operational state of the ADS has been verified	
The ADS should safely manage failure modes			
22	The ADS should detect **and respond** system malfunctions and abnormalities	• The ADS should perform self-diagnosis of faults in accordance with the OEMs prescribed list • The ADS should detect system malfunctions/abnormalities and evaluate system's ability to fulfill the entire DDT	
23	The ADS should be protected from unauthorized access	• The measures ensuring protection from an authorized access should be provided in alignment with engineering best practices	
24	Provided a failure does not **significantly** compromise ADS performance, the ADS should respond safely to the presence of a **[faults/failure]** in the system	• The limited operation of the ADS should comply to the normally applicable safety requirements	
25	The ADS should signal major **[faults/failures]** and resulting operational status	• The ADS should signal **[faults/failures]** affecting the ability to execute the DDT	
The ADS should maintain a safe operational state			
26	**[The ADS should signal required system maintenance to the user.]**		
27	**[The ADS should be accessible for the purposes of maintenance and repair to authorized persons.]**		
28	ADS safety should be ensured in the event of discontinued production/support/maintenance		