

### Workshop on ADS Safety Elements

This document includes an editorial review of the ADS Safety Elements proposed in FRAV-12-08, undertaken based on discussions held on a 2-days workshop (Tuesday 1<sup>st</sup> June and Thursday 3<sup>rd</sup> June 2021).

During the first session it was agreed that, before proceeding with more detailed discussions on verifiable requirements and safety approaches, a review of the ADS Safety Elements was appropriate to remove repetitions, group items with similar content under the same section and finally to reach a consensus on the fundamentals under which a whole set of detailed requirements will be developed.

To pursue this goal, all the comments received in the documents FRAV-08-09, FRAV-09-08, FRAV-10-11 and FRAV-12-08 were divided into 2 categories:

- Editorial amendments to the ADS Safety Elements, considered to support the review of the list as per Part 1 of this document.
- Detailed Requirements and Safety Approaches, noted down for further discussions and moved to the detailed requirements section of the Table in Part 2 (see FRAV-15-09)

Important to note that during the process only one safety item was completely removed from the list - "*The ADS should be permanently disabled in the event of obsolescence*" -, as deemed not appropriate for the discussions.

### **FIRST PART: ADS Safety Topics**

#### The ADS should drive safely

1. The ADS should be capable of performing the entire Dynamic Driving Task (DDT)
2. The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s)
3. The ADS should detect and respond to objects and events relevant for the DDT
4. The ADS should comply with traffic rules
5. The ADS should interact safely with other road users
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
10. ~~The ADS (when the ADS is activated) should be informed the user about the ADS status (when the ADS is activated) with regards to ODD~~
11. The ~~ADS user~~ should be permitted ~~the User~~ to take over control from the ADS, if the ADS is designed to request and enable intervention by a human driver
12. The ADS should safely manage transitions of control to the user
13. The ADS should safely respond to user input errors

**Commented [A1]:** Subject should be "the ADS" because these are requirement for ADS.

14. The ADS should provide feedback to the user on its operational status
15. The ADS should warn the user of failures to fulfill user roles and responsibilities
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 driving 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
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
21. Pursuant to a traffic accident, the ADS should stop the vehicle

The ADS should safely manage failure modes

22. The ADS should detect **and respond** system malfunctions and abnormalities
23. The ADS should be protected from unauthorized access
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
25. The ADS should signal major **[faults/failures]** and resulting operational status.

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-during lifetime of the system~~~~the event of discontinued-~~  
~~production/support/maintenance.~~
- ~~29.~~ ~~When ADS safety is not ensured, the ADS should not be activated.~~
- ~~28-30.~~ The status of ADS should be readable for the User and authorized persons.

**Formatted:** Font: 10.5 pt, Bold, Font color: Blue

**Formatted:** Font: Not Italic

**Formatted:** Font: Not Italic

**Formatted:** Font: Not Italic

**Formatted:** Font: 10.5 pt, Bold, Font color: Blue

**SECOND PART: Detailed Requirements**

|  | <b>Performance Topic</b>  | <b>Detailed Requirements</b> | <b>Measurable / Verifiable Criteria</b> |
|--|---|------------------------------|---|
| The ADS should drive safely                  |   |                              |   |
| 1  | The ADS should be capable of performing the entire Dynamic Driving Task (DDT)                     |                              |   |
| 2  | The ADS should recognize the ODD conditions and boundaries of the ODD of its feature(s)           |                              |   |
| 3  | The ADS should detect and respond to objects and events relevant for the DDT                      |                              |   |
| 4  | The ADS should comply with traffic rules  |                              |   |
| 5  | The ADS should interact safely with other road users  |                              |   |
| 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 |                              |   |
| 10   | The user should be informed about the ADS status (when the ADS is activated) with regards to ODD  |                              |   |

Submitted by the experts from Japan

FRAV-16-06  
16<sup>th</sup> FRAV Session  
6 July 2021

|  |   |  |  |
|--|---|--|--|
| 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   |  |  |
| 12   | The ADS should safely manage transitions of control to the user   |  |  |
| 13   | The ADS should safely respond to user input errors  |  |  |
| 14   | The ADS should provide feedback to the user on its operational status   |  |  |
| 15   | The ADS should warn the user of failures to fulfill user roles and responsibilities   |  |  |
| 16   | ADS vehicles that may operate without a <b>[user-in-charge/in-vehicle driver]</b> should provide means for occupant communication with <b>[a remote operator/user-in-charge/human driver/remote assistance personnel]</b> |  |  |
| 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  |  |  |
| 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   |  |  |

Formatted: Font: Times New Roman, 10 pt

|  |   |  |   |
|--|---|--|---|
| 20   | The ADS should signal its intention to place the vehicle in an MRC  |  |   |
| 21   | Pursuant to a traffic accident, the ADS should stop the vehicle   |  |   |
| The ADS should safely manage failure modes       |   |  |   |
| 22   | The ADS should detect <b>and respond</b> system malfunctions and abnormalities  |  |   |
| 23   | The ADS should be protected from unauthorized access  |  |   |
| 24   | Provided a failure does not <b>significantly</b> compromise ADS performance, the ADS should respond safely to the presence of a <b>[faults/failure]</b> in the system |  |   |
| 25   | The ADS should signal major <b>[faults/failures]</b> and resulting operational status   |  |   |
| The ADS should maintain a safe operational state |   |  |   |
| 26   | <b>[The ADS should signal required system maintenance to the user.]</b>   |  |   |
| 27   | <b>[The ADS should be accessible for the purposes of maintenance and repair to authorized persons.]</b>   |  |   |
| 28   | ADS safety should be ensured <u>during lifetime of the system in the event of discontinued production/support/maintenance.</u>  | <ul style="list-style-type: none"> <li><u>The manufacturer should have ADS safety management system for ensuring over lifetime of the system.</u></li> </ul> | <ul style="list-style-type: none"> <li><u>The manufacturer has ADS safety management system or not</u></li> </ul> |

- Formatted: Font: Times New Roman, 10 pt
- Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.29"
- Formatted: List Paragraph, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.29"
- Formatted: Font: Times New Roman, 10 pt
- Formatted: List Paragraph, Indent: Left: 0.29"
- Formatted: Font: Times New Roman, 10 pt

|           |  |   |  |
|-----------|--|---|--|
| <u>29</u> | <u>[When ADS safety is not ensured, the ADS should not be activated.]</u>          | <ul style="list-style-type: none"><li>• <u>[The ADS should have a function which makes the system inactivate remotely, if the system has OTA functionality, in case ADS safety is not ensured.]</u></li></ul> | <ul style="list-style-type: none"><li>• <u>[The ADS has the remote disabling function or not.]</u></li></ul>                                     |
| <u>30</u> | <u>[The status of ADS should be readable for the User and authorized persons.]</u> | <ul style="list-style-type: none"><li>• <u>[The ADS should have functionality to display ADS level of the vehicle and executable DDT function information.]</u></li></ul>                                     | <ul style="list-style-type: none"><li>• <u>[ADS level (current and potential)]</u></li><li>• <u>[Executable DDT function(current)]</u></li></ul> |

- Formatted:** Font: Times New Roman, 10 pt
- Formatted:** List Paragraph, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.29"
- Formatted:** Font: Times New Roman, 10 pt
- Formatted:** Font: Times New Roman, 10 pt
- Formatted:** List Paragraph, Bulleted + Level: 1 + Aligned at: 0" + Indent at: 0.29"
- Commented [A2]:** ADS should display "what this ADS can do" in order to provide information to users or other stakeholders (This function is especially important if the vehicle is updated).
- Formatted:** Font: Times New Roman, 10 pt
- Formatted:** Font: Times New Roman, 10 pt