**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 1st June and Thursday 3rd 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

1. Activation of an ADS feature should only be possible when the conditions of its ODD have been met
2. The user should be informed about the ADS status (when the ADS is activated) with regards to ODD
3. 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
4. The ADS should safely manage transitions of control to the user
5. The ADS should safely respond to user input errors
6. The ADS should provide feedback to the user on its operational status
7. The ADS should warn the user of failures to fulfill user roles and responsibilities
8. 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

1. The ADS should execute a safe fallback response in the event of a failure of the ADS and/or othervehicle system that prevents the ADS from performing the DDT
2. 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
3. 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
4. The ADS should signal its intention to place the vehicle in an MRC
5. Pursuant to a traffic accident, the ADS should stop the vehicle

The ADS should safely manage failure modes

1. The ADS should detect **and respond** system malfunctions and abnormalities
2. The ADS should be protected from unauthorized access
3. Provided a failure does not **significantly** compromise ADS performance, the ADS should respond safely to the presence of a **[faults/failure]** in the system
4. The ADS should signal major **[faults/failures]** and resulting operational status.

The ADS should maintain a safe operational state

1. **[The ADS should signal required system maintenance to the user.]**
2. **[The ADS should be accessible for the purposes of maintenance and repair to authorized persons.]**
3. ADS safety should be ensured in the event of discontinued production/support/maintenance

|  |  |  |  |
| --- | --- | --- | --- |
| **SECOND PART: 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 |  |  |
| 10 | The user should be informed about the ADS status (when the ADS is activated) with regards to ODD |  |  |
| 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 **[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 othervehicle 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 the event of discontinued production/support/maintenance |  |  |