Submitted by the experts from the Netherlands

Document FRAV-02-07
2nd FRAV session, 14-15 January 2020
Agenda items 6.5. and 7.

Submitted by the Informal Working Group on Functional Requirements for Automated and Autonomous Vehicles (FRAV)

Informal Document GRVA-05-xx
5th GRVA Session, 10-14 February 2020
Agenda Item xx

Common Functional Performance Requirements for Automated and Autonomous Vehicles

This document has been prepared by the Informal Working Group on Functional Requirements for Automated and Autonomous Vehicles (FRAV) to describe functional performance requirements that may be applicable to automated and/or autonomous vehicles. It is based upon ECE/TRANS/WP29/2019/34/Rev.1, WP.29-179-23, and ACSF-24-05.

1. Definitions

1.1. *"Minimal risk condition"* means a condition to which a user or an automated driving system may bring a vehicle in order to reduce the risk of a crash when a given trip cannot or should not be completed.[1]

1.2. *"Minimal risk maneuver"* means a procedure automatically performed by the automated driving system to place the vehicle in a minimal risk condition in a manner that minimizes risks in traffic.[2]

1.3. *"Operational domain"* means the operating conditions which a vehicle can reasonably be expected to encounter when in automated mode. These conditions will be established by the VMAD scenario database.This is a tricky sentence, the amount of reasonably expected conditions is much broader than what VMAD will consider for the scenario database. The proposal is to skip the second sentence and also the word reasonably in the first sentence. The operational domain is whatever and wherever is possible in practice for a vehicle in automated mode. Depending on the level of automation, the vehicle has to deal with the situation and/or involve the driver in an acceptable manner

[1] Definition derived from SAE J3016:2016

[2] Definition derived from ACSF-24-05 (clean); however, the term "minimal" has been substituted for "minimum" and the definition refers to the minimal risk condition for consistency with SAE J3016:2016. The definition omits the ACSF reference to "after a transition demand" under the assumption that such maneuvers could be executed by Level 4/5 vehicles without driver controls or the demand could be skipped if the driver monitoring system detects that a transition to the driver is not appropriate.

1.4. *"Operational design domain"* refers to the operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.[3] The operational design domain is a subset of the operational domain.

1.5. *"Transition demand"* is a logical and intuitive procedure to transfer the dynamic driving task from automated control by the system to human driver control.[4]

1.6. *"VMAD"* refers to the GRVA informal working group on Validation Methods for Automated Driving.

1.7. *"VMAD scenario"* refers a configuration of traffic variables as defined within the VMAD traffic scenario database.

1.8. *"VMAD traffic scenario database"* is the proposed database or catalog of traffic conditions for validation of automated functions, that are reasonably foreseeable under which a vehicle can reasonably be expected to avoid causing an event resulting in injury or death.

2. System Safety

2.1. Activation and use of the vehicle in automated mode shall only be possible within the boundaries of the automated driving system's operational design domain.

2.2. When in automated driving mode,

2.2.1. The vehicle shall reasonably respond to conditions within its operational domain without causing an event resulting in injury or death;

2.2.2. The vehicle shall comply with all applicable road traffic laws except in cases where such compliance would conflict with paragraph 2.2.1.

~~2.2.2.~~2.2.3. The vehicle shall demonstrate adequate mitigation of risks (e.g. approaching ODD boundaries), safe driving behavior and good Human Machine Interface

2.3. [Functional requirements related to overall system design safety (e.g., CEL)?]

3. Operational Design Domain (ODD)

3.1. The vehicle manufacturer shall define the operational design domain of the vehicle, including (at a minimum):[5]

3.1.1. Roadway types

3.1.2. Geographic area

[3] Definition from SAE J3016:2016
[4] Definition from ACSF-24-05 (clean)
[5] FRAV will consider ISO/WD 34503: Road vehicles — Taxonomy for operational design domain for automated driving systems

3.1.3. Speed range

3.1.4. Environmental conditions

3.2. The vehicle manufacturer shall identify the conditions defined for the vehicle's operational domain that fall outside the vehicle's operational design domain.

4. Execution of Dynamic Driving Tasks

4.1. Object and Event Detection and Response (OEDR)

4.1.1. The automated driving system shall detect and classify objects and events that may be reasonably expected within its operational domain.

4.1.1.1. [Categorical definition of objects/events?]

4.1.2. The automated driving system shall timely detect and react on conditions within its operational domain that ~~fall outside~~indicates the approach of the boundaries of its operational design domain as defined in paragraph 3.2.[explanation: for safe driving it is needed that detection and reaction are before the actual exceedance of the ODD]

4.2. Normal Driving

4.2.1. The automated driving system shall execute longitudinal and lateral maneuvers in response to objects and events within its operational design domain.

4.2.1.1. The automated driving system shall execute such maneuvers without causing outcomes resulting in injury or death.[seems to be a repetition of 2.2.1]

4.2.1.2. The automated driving system shall execute such maneuvers without disrupting the normal flow of the surrounding traffic.

4.3. Other Driving

4.3.1. The automated driving system shall execute a failsafe response when the conditions defined for its operational design domain are not satisfied for a duration exceeding [time limit]. [we understand the desire to specify such a limit. Nevertheless we think this is not in line with the general objective to create performance based criteria. If the items 2.2.1, 2.2.2 and (new) 2.2.3 are met, this article could be skipped

4.3.2. The automated driving system shall execute an ~~emergency response~~Minimal Risk Maneuver when conditions for the execution of a failsafe response are not present.

5. Human-Machine Interface/Operator Information

5.1. Vehicles equipped with automated driving systems that may require driver intervention (e.g., transition demand) shall detect if the driver is available to take over the driving task by ~~continuously~~ [this word might be too stringent, for some applications "regularly" might be sufficient. This requirement might be met with the trhee proposed items under 2.2] monitoring the driver.[6]

5.2. The vehicle shall ~~clearly~~ unambiguously communicate to the user:

5.2.1. Status of the automated driving system

5.2.1.1. System availability

5.2.1.2. System mode active

5.2.1.3. System malfunction

5.2.2. Critical messages

5.2.3. Transition demand

5.2.4. Initiation of minimal risk maneuver

5.2.5. Status of driver availability

~~5.2.5.~~5.2.6. Probability that the automated systems reach the boundary of the ODD

5.3. The vehicle shall signal to other road users:

5.3.1. Intentions to undertake dynamic driving tasks in accordance with applicable traffic laws

5.3.2. Initiation of a minimal risk maneuver

6. Failsafe Response[in our opinion, accepting 2.2.1-2.2.3 would make 6 abundant.

6.1. When in automated driving mode,

6.1.1. The vehicle shall automatically initiate a failsafe response or sequence of failsafe responses in response to detection of conditions outside its operational design domain for a duration not to exceed [time limit].[as explained under 4.3.1 we think this item should be skipped]

6.1.2. Failsafe responses shall only be initiated when conditions permit their completion in compliance with paragraph 2.2.[this is a very tricky formulation. So, if completion in compliance with 2.2 is not possible, failsafe response shall not be initiated. This would be in conflict with 2.2 itself?!]

6.2. Failsafe responses include:

6.2.1. Transition demand

[6] Derived from ACSF-24-05 (clean), para. 2.6.2.

6.2.2. Minimal risk maneuver