Submitted by the experts from Canada

Document FRAV-02-12
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

This document is a conceptual draft intended for review and discussion purposes only. Nothing in this document should be construed as a position, implied or explicit, of the FRAV informal group or any of its participants or stakeholders.

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 driving systems. 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 encounter when in automated mode.

1.4. *"Operational design domain"* refers to the specific conditions under which a given driving automation system or feature thereof is 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.

Commented [RJ1]: Edited to reflect SAE J3016 definition

[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.

[3] Definition from SAE J3016:2016

Submitted by the experts from Canada

Document FRAV-02-12
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

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

Commented [RJ2]: Are we limiting this to traffic scenarios? There could be scenarios to test sub-systems or components.

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

Commented [RJ3]: Do we want to limit this to avoidance of injury death? We might also want to avoid causing damage (no injury/death).
Interpretation of the word "causing" :
There could be 'no-win' scenarios where we want to see how it might limit injuries/damage as a human driver might in those situations.

2. System Safety

2.1. Activation and use of the automated driving system shall only be possible when the operating domain falls within the boundaries of the system's operational design domain.

2.2. When in automated driving mode,

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

Commented [RJ4]: Should include damage.
Interpretation of the word "causing":
There could be "no-win" scenarios (ie other vehicle runs a red light hits the AV) where the AV should take action to minimize damage/injury/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.

Commented [RJ5]: There are many cases where we "bend" or break the rules (in some cases the rules may also be conflicting), the system should have the flexibility to do the same in those cases. ie. Object on side of lane partially blocking it, must cross middle lines to go around

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

3.1.3. 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.

Commented [RJ6]: It may be easier to define the opposite? There are too many possibilities in the OD.
Define boundaries of ODD (could be complex and dependent on many variables but still needs to be defined for the system), all else is outside ODD.

Commented [RJ7R6]: Alternatively, perhaps what is intended is to see what characteristics of the OD are monitored to ensure it remains within the ODD

[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

Submitted by the experts from Canada

Document FRAV-02-12
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

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.

Commented [RJ8]: The system should be able to classify objects as unknown in the case they are not “reasonably expected”

Commented [RJ9]: There should be more detailed requirements for the ability to do this within a certain timeframe or distance.
If it can detect and/or classify it only at the last second or when it is very near to the vehicle it would be dangerous.

Commented [RJ10]: There should be a requirement regarding the ability to do this based on the location of object relative to vehicle (in front, behind, to the side).
Ie. A highway only system w/o lane change may not have sensors to the rear/sides

4.1.1.1. [Categorical definition of objects/events?]

4.1.2. The automated driving system shall detect conditions within its operational domain that fall outside the boundaries of its operational design domain as defined in paragraph 3.2.

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 domain.

4.2.1.1. The automated driving system shall execute such maneuvers without causing outcomes resulting in injury or death.

Commented [RJ11]: Should add damage,
Also see above related to “causing” and no-win situations

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].

Commented [RJ12]: Ideally there would be no time limit, the system would adapt before exceeding boundaries.
For certain situations where this occurs suddenly, the failsafe response may be to attempt to re-enter the ODD (slowing down, steer/change lane etc.) without needing to transition/minimal risk etc. unless it will lead to a collision

4.3.2. The automated driving system shall execute an emergency response when conditions for the execution of a failsafe response are not present or when a collision is imminent.

5. Human-Machine Interface/Operator Information

5.1. Vehicles equipped with automated driving systems that may request or require driver intervention (e.g., transition demand) shall detect if the driver is available to take over the driving task by continuously monitoring the driver.[6]

5.2. The vehicle shall clearly 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. Initiation of emergency maneuver

5.2.6. Status of driver availability

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

5.3.3. Initiation of an emergency maneuver

6. Failsafe Response

6.1. When in automated driving mode,

6.1.1. The vehicle shall automatically initiate a failsafe response or sequence of failsafe responses when the operational domain exceeds the boundaries of the system's operational design domain for a duration not to exceed [time limit].

6.1.2. Failsafe responses shall only be initiated when conditions permit their completion in compliance with paragraph 2.2. If a failsafe response cannot be completed, an emergency response shall be initiated.

6.2. Failsafe responses include:

6.2.1. Transition demand

Commented [RJ13]: Unsure the intent here:
If the system is activated?
Which system is activated or available?

Commented [RJ14]: Should we have a section for communication with Pedestrians (see GRE - AVSR)

Commented [RJ15]: Unsure of intent:
System is activated?
Turn/brake signals during normal driving?

Commented [RJ16]: See above comment on 4.3.1

Commented [RJ17]: Perhaps the ability to re-enter the ODD by slowing down, changing lane etc. would be less risky than a transition demand or MRM (provided it does not become a cyclical response)

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

Submitted by the experts from Canada

Document FRAV-02-12
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

6.2.2. Minimal risk maneuver

7. Emergency Response

7.1. When in automated driving mode,

7.1.1. The vehicle shall automatically initiate an emergency response when the operational domain exceeds the boundaries of the system’s operational design domain and a failsafe response cannot be completed or, if there is an imminent threat of collision

7.1.2. Emergency responses shall [not cause/minimize damage/injury/death] [obey traffic laws]

7.2. Failsafe responses include:

7.2.1. Maximum braking force

7.2.2. Evasive steering action

Commented [RJ18]: Upon completion of an emergency response what should the vehicle do?
If there is a collision – stop and contact authorities
If there is no collision – level 3 could be transition? Resume normal operation for level 4 & 5? MRM could be fallback but may not be necessary if threat is avoided.

Commented [RJ19]: Would need more thought on this point, while we don’t want to create damage/injury/death it may be necessary to minimize damage (ie swerve to hit car vs pedestrians).
Same for obeying traffic laws, it may be required to break them in some cases (as a human might do) but it could also cause more problems due to “unpredictable” behavior to other user (ie swerving into oncoming lane to avoid an oncoming car drifting on your side blocking the lanes)