# FRAV

# Session 7
# Status Review and Session Orientation

Web Conference

17 November 2020

# Today's Agenda

1. Adoption of the agenda

2. Adoption of the reports of the previous sessions

3. FRAV status and consensus to date

4. Comments and updates to Document 5

5. Definitions ("user" and "foreseeable")

6. Elaboration of the five starting points

7. ADS level of safety and performance limits

8. Next steps and deliverables

# Adoption of the Agenda

**FRAV**

| Agenda item | | | Documentation |
|---|---|---|---|
| 1. | Adoption of the agenda | 12:30-12:40 | FRAV-07-01 |
| 2. | Adoption of the report of the previous sessions | 12:40-12:50 | FRAV-05-02 <br> FRAV-06-02 |
| 3. | FRAV status and consensus | 12:50-12:55 | FRAV-07-03 (Co-chairs) |
| 4. | Document 5 updates | 12:55-13:15 | FRAV-07-06 (Japan) |
| 5. | Definitions | 13:15-13:35 | |
| 6. | Elaboration of ADS safety requirements | 13:35-14:15 | FRAV-07-08 (Japan) <br> FRAV-07-09 (OICA/CLEPA) |
| 7. | ADS level of safety and performance limits | 14:15-14:50 | FRAV-07-07 (Japan) <br> FRAV-07-10 (Japan) |
| 8. | Next Steps and Deliverables | 14:50-15:00 | |

# Today's Agenda

1. Adoption of the Agenda

2. Adoption of the reports of the previous sessions
   - FRAV-05-02
   - FRAV-06-02

3. FRAV status and consensus to date

4. Comments and updates to Document 5

5. Definitions ("user" and "foreseeable")

6. Elaboration of the five starting points

7. ADS level of safety and performance limits

8. Next steps and deliverables

# Today's Agenda

1. Adoption of the Agenda

2. Adoption of the reports of the previous sessions
   - FRAV-05-02
   - FRAV-06-02

3. FRAV status and consensus to date

4. Comments and updates to Document 5

5. Definitions ("user" and "foreseeable")

6. Elaboration of the five starting points

7. ADS level of safety and performance limits

8. Next steps and deliverables

# Review of FRAV Points of Consensus (cont.)

1. "*Automated Driving System*" (ADS) means the hardware and software that are collectively capable of operating a vehicle on a sustained basis.
2. FRAV requirements specifically regard the ADS and its performance in the operation of a vehicle.
3. Operational Design Domain (ODD) refers to the operating conditions under which an ADS is designed to function.
4. ADS may be designed to function under more than one discrete set of operating conditions (i.e., more than one ODD).
5. "*(ADS) feature*" means an application of ADS hardware and software designed specifically for use within an ODD.
6. An ADS may have one or more features as defined by their unique ODD.
7. "*Operational Design Domain*" means the operating conditions under which an ADS feature is specifically designed to function.
8. In operation, the ADS continuously controls the vehicle motion, monitors the vehicle environment, interacts with other road users, and determines responses to road and traffic conditions (collectively known as the Dynamic Driving Task (DDT)).
9. The ADS has functions that collectively perform the entire DDT while the ADS is in use.
10. The ADS monitors the functions and safely manages failure modes when detected.
11. The ADS functions enable the features to operate the vehicle within the ODD of the feature.
12. An ADS feature may use all or some of the functions of the ADS.
13. ADS features may share ADS functions.
14. An ADS should be assessed based on its intended use(s) and limitations on the use of its features.
15. ADS requirements should be technology-neutral and performance-based.

# Review of FRAV Points of Consensus (cont.)

**FRAV**

16. ADS requirements should be applicable across the anticipated diversity of configurations (i.e., features and functions).
17. ADS assessments require information specific to the configuration of the ADS (i.e., features, functions, ODD, other usage specifications).
18. Manufacturers provide the information specific to the ADS design and intended uses.
19. FRAV will define mandatory requirements for ADS descriptions (i.e., ODD elements, other usage specifications).
20. The manufacturer description of the ADS provides a means to determine the application of the ADS performance requirements.
21. The NATM process should begin with a review of the ADS description to verify fulfillment of the mandatory description requirements and to determine the application of the performance requirements.
22. The ADS requirements should be derived from the following safety perspectives:
    • The ADS should drive safely.
    • The ADS should interact safely with the user.
    • The ADS should manage safety-critical situations.
    • The ADS should safely manage failure modes.
    • The ADS should maintain a safe operational state.

**No comments received since the last session.**

**If there are reservations, concerns, or questions regarding these points, please convey them to the FRAV secretary. FRAV will address the issues at a future session.**

# Today's Agenda

1. Adoption of the Agenda

2. Adoption of the report of the last session

3. FRAV status and consensus to date

4. Comments and updates to Document 5

5. Definitions ("user" and "foreseeable")

6. Elaboration of the five starting points

7. ADS level of safety and performance limits

8. Next steps and deliverables

# Document 5 Updates

FRAV

- For ease of use, Germany has proposed to separate the background section from Document 5.

- Proposal
  - Follow the 1998 Agreement approach by separating the background on FRAV discussions and justifications for decisions as a "technical report" (FRAV-xx-04)
  - Remainder of text in Document 5 (FRAV-xx-05)

> **Clarification: Document 5 uses "should" rather than "shall". D5 is not a draft regulatory text. D5 is our internal discussion tool. D5 will provide the basis for drafting formal proposals in separate documents when FRAV decides to do this**

# Document 5 Updates

**FRAV**

> 1.14.2. FRAV discussed the issues surrounding the term "system safety". FRAV discussed the difference between requirements and methods such as in "functional requirements" and the methods described under "functional safety" standards. FRAV concluded that use of the term "functional" results in ambiguity and risks confusion between requirements and methods. As a result, FRAV preferred the term "performance requirements" to address functional and operational safety requirements.

- Concern over interpretation of *"functional and operational safety requirements"*.

- To avoid confusion with Functional Safety, propose to replace with **"functional and operational requirements for ADS performance"**.

# Document 5 Updates

1.14.4. ~~FRAV discussed methodologies for defining the ADS performance limits.~~ FRAV considered four general ~~approaches:~~
- A "careful and competent ~~driver model"~~
- ~~A~~ "state-of-the-art" ~~method~~ based on technological feasibility
- A "safety envelope" ~~method,~~ and
- A "positive risk balance" compared with human driver.

FRAV concluded that the group should begin with conceptual starting points to guide an iterative process towards defining high-level performance requirements applicable across ADS configurations. FRAV agreed to continue consideration of possible methods for defining performance thresholds.

Japan proposed six criteria for assessing the approaches to setting performance limits (FRAV-04-13):

- Limits conducive to road transport improvement
- Limits would be performance based
- Limits would be technology neutral
- Limits would be measurable
- Limits conducive to social acceptance
- Feasibility of the limits

**FRAV discussed principles for ADS levels of safety.**

bases

human driver"

Insert "statistical" before "positive…"

Japan proposed to assess the principles from six perspectives (FRAV-04-13):
- Conducive to road transport improvement
- Applicable to performance-based assessments
- Applicable to technology-neutral requirements
- Definable in measurable terms
- Conducive to social acceptance
- Feasibility

# Document 5 Updates

1.15.3. Japan suggested that stakeholders rate the proposed methodologies for setting performance limits using its table of proposed criteria (FRAV-05-04).

Japan suggested that stakeholders rate the proposed principles using its table of six perspectives (FRAV-05-04).

3.3.2. *"(ADS) feature"* means an application of ADS hardware and software designed specifically for use within an ODD.

Japan: "hardware and software" is already included in the ADS definition. Therefore, "hardware and software" is not necessary here.

Japan noted the circular reference between the definitions of features and ODD. *At this point, this circularity appears unavoidable since a feature is defined by the ODD and ODD describes conditions for a feature.*

3.3.5. "Operational Design Domain (ODD)" means the operating conditions under which an ADS feature is specifically designed to function.

# Document 5 Updates

> 3.2.4. *"Dynamic driving task (DDT)"* means all of the real-time operational and tactical functions required to operate a vehicle in on-road traffic~~means the real-time functions collectively required to operate a vehicle in on-road traffic~~.

> 4.2. The automation of driving obligates manufacturers, safety authorities, and other stakeholders in road transportation to ensure that Automated Driving Systems perform safely in traffic.

Japan proposes to use the SAE J3016 definition.

Japan: It shall be ensured that automated driving systems perform safely in traffic.

*Proposal:*

*"An Automated Driving System must perform safely in the complex traffic environment"*

*Update pursuant to decisions on "level of safety" principles.*

# Document 5 Updates

| | |
|---|---|
| **4.7.** | As a result, stakeholders anticipate a wide variety of ADS applications carefully designed to operate within their performance limits. |

Japan proposal to replace "limits" by "criteria".

*Counterproposal: "capabilities".*

*"criteria" refers to standards by which something is assessed or judged.*

*The intent of the paragraph is to refer to limits of the ADS capabilities, not the requirements established for performance. This paragraph provides context for why ADS should be assessed according to their specific uses and limitations on their use.*

# Today's Agenda

1. Adoption of the Agenda
2. Adoption of the report of the last session
3. FRAV status and consensus to date
4. Comments and updates to Document 5
5. Definitions
   1. User
   2. Foreseeable
6. Elaboration of the five starting points
7. ADS level of safety and performance limits
8. Next steps and deliverables

# Driver/User/Operator?

- ## User-in-charge
  - ### A person qualified and fit to operate a vehicle either in the vehicle or <u>having a line-of-sight</u> to the vehicle
    - Liable for conduct unrelated to the DDT (e.g., insurance, maintenance, reporting crashes, child use of seat belt)
  - ### <u>Excludes operators in remote control centers</u>

- ## J3016
  - ### "Remote driver": A driver who is not seated in a position to manually exercise in-vehicle braking, accelerating, steering, and transmission gear selection input devices (if any) but is able to operate the vehicle [perform the DDT].
  - ### User can be within the vehicle, within line of sight of the vehicle, or beyond line of sight of the vehicle.

# Driver/User/Operator?

- *"ADS vehicle"* means a vehicle equipped with an ADS.
- *"User"* means a human being responsible for the ADS vehicle who is qualified, fit, and capable of performing the DDT.
- *"User-in-charge"* means a user in or with a line of sight to the vehicle.
- *"Remote operator"* means a user other than a user-in-charge.

> **Proposal to add these terms and definitions to Document 5 for use as needed.**
>
> **(As always, the definitions can be revised as we gain experience using them.)**

# Definition of "foreseeable"

- In FRAV-06-11, Germany proposed that FRAV define this concept
  - "This term needs to be defined: foreseeable by whom? ADS with sensors, expert driver, neural network, programmer of ADS?"

- As a regulatory principle, a requirement is something defined by a safety authority (or, in our case, safety authorities)
  - In requiring ADS to address "foreseeable" situations, the requirement should specify "foreseeable" objectively.

- We have two main tools for defining foreseeable:
  - ODD conditions
  - Traffic scenarios

# Definition of "foreseeable"

**FRAV** 🇺🇳

- ## ODD conditions
  - ### In the mandatory ADS description, the manufacturer defines the conditions under which each feature is designed to operate.
  - ### The ODD conditions FRAV includes in Chapter 5 of Document 5 are all "foreseeable" because we have identified them.

- ## VMAD defines the Scenario Catalogue as a "minimum baseline/non-exhaustive inventory" of traffic situations.
  - ### The catalogue may be "minimum" in the sense of a limited number of scenarios.
  - ### The catalogue may also be "minimum" in the omitting highly detailed logical or concrete scenarios for certain traffic situations.
  - ### Open issue whether the Catalogue includes crash mitigation scenarios.

# Definition of "foreseeable"

**FRAV**

- Starting points
  - "The ADS should not cause any traffic accidents that are reasonably foreseeable and preventable."
  - "The ADS shall not cause a collision due to its own driving behavior."[1]
- *"Traffic scenario"* means a representation of one or more real-world driving situations that may occur during a given vehicle trip as defined in the Scenario Catalogue.
  - *"Trip"* means the traversal of an entire travel pathway by a vehicle from the point of origin to a destination.
- *"ODD condition"* means an element identified within the ADS description as relevant to an ADS feature.
- The ADS driving response to a [collision-avoidable] traffic scenario and/or ODD condition should not cause a collision.[1]

[1] For clarity, "cause" means that the ADS behavior was the critical factor in the collision.

# Today's Agenda

1. Adoption of the Agenda

2. Adoption of the report of the last session

3. FRAV status and consensus to date

4. Comments and updates to Document 5

5. Definitions

6. Elaboration of the five starting points
   - FRAV-07-09 (OICA/CLEPA)
   - Scope and purpose of starting points

7. ADS level of safety and performance limits

8. Next steps and deliverables

# Performance Requirement Starting Points

1. **ADS should drive safely.**  (Ensure safe behavior of the ADS as "the driver")

2. **ADS should interact safely with the user.**  (Ensure safe use of ADS and safe interactions with the user such as transfers of control, user override, etc.)

3. **ADS should manage safety-critical situations.**  (Differentiate between normal driving and emergency situations to ensure safe responses to the latter)

4. **ADS should safely manage failure modes.**  (Ensure safe responses to system malfunction, physical damage, etc.)

5. **ADS should maintain a safe operational state.**  (Ensure safety throughout the useful life of the ADS, such as safety critical updates, response to obsolescence)

# Orientation for the following slides

**FRAV**

- Goal: Reach a common understanding of the starting points

  - Which kinds of issues belong under each starting point

  - Facilitate future organization of work

- Based on MLIT and OICA/CLEPA work on 142 candidates

  - Modified for purposes of consistency with starting points

  - Simplified as examples to illustrate what goes where

- Seeking comments/questions related to scope of starting point

  - Not seeking approval of items as specific proposals

  - Items provided as guidance for work on FRAV-06-04 and 142 candidates

# ADS should drive safely.

1. The ADS should respect traffic rules.

2. The ADS driving behavior should be consistent with surrounding traffic conditions.

3. The ADS feature should adapt its behavior to adverse and/or uncertain driving conditions.

4. The ADS should signal safety-related status information to other road users.

5. The ADS driving response to a [collision-avoidable] traffic scenario and/or ODD condition should not cause a collision.

6. The ADS should initiate a safe fallback response when the conditions of its ODD are not met.

# ADS should interact safely with the user.

**FRAV**

1.  Activation of an ADS feature should not be possible unless the conditions of its ODD are met.

2.  The user should be able to override the ADS feature.

3.  The ADS should prevent misuse.

4.  The ADS should provide timely feedback to the user.

5.  The ADS should be tolerant of errors in user inputs.

6.  Prior to initiation of a transition to full control, the ADS should determine the availability and readiness of the user-in-charge to assume control of the DDT.

7.  Upon initiation of a transition of full control to the user-in-charge, the ADS should suspend user-in-charge activities other than driving enabled by the ADS.

8.  The ADS should ensure a safe transition of full control to the user.

9.  Pursuant to a transition, the ADS may not deactivate until the user is fully in control of the DDT.

# ADS should manage safety-critical situations.

**FRAV**

1. The ADS should be capable of performing minimal risk maneuvers.

2. A minimal risk maneuver should place the vehicle in a minimal risk condition.

3. A minimal risk maneuver should be initiated as conditions (TBD) warrant.

4. Pursuant to a minimal risk maneuver, the ADS may not deactivate until the vehicle has reached a minimal risk condition.

5. In the event of a collision, the ADS should revert to a minimal risk condition and deactivate.

6. The ADS should initiate an MRM in response to a user failure to safely perform the DDT in completion of a transition to full control.

# ADS should safely manage failure modes.

1. The ADS should detect failure modes.

2. The ADS should initiate a safe fallback response upon detection of an unsafe operational state and deactivate upon completion.

3. An ADS feature may function in the presence of failures that do not impact its performance.

# ADS should maintain a safe operational state.

1. The ADS should be disabled while in an unsafe operational state.

2. Following a collision, activation of the ADS should not be possible until its safe operational state has been verified.

# Today's Agenda

1. Adoption of the Agenda
2. Adoption of the report of the last session
3. FRAV status and consensus to date
4. Comments and updates to Document 5
5. Definitions
6. Elaboration of the five starting points
7. ADS level of safety and performance limits
   - FRAV-07-07 (Japan)
8. Next steps and deliverables

# Today's Agenda

1. Adoption of the Agenda
2. Adoption of the report of the last session
3. FRAV status and consensus to date
4. Comments and updates to Document 5
5. Definitions
6. Elaboration of the five starting points
7. ADS level of safety and performance limits
8. Next steps and deliverables

# Next session

- ## Next session 8 December
  - ### Review updates to Document 5 pursuant to the 7th session
  - ### Consider comments on the next-level starting points
  - ### Consider "level of safety" principle
  - ### Last "educational presentations" on performance limit methods
- ## Provide submissions by 4 December to facilitate 8th session preparations
- ## Preferences/availability for January session(s)