Document FRAV-04-10
Submitted by the experts from Japan
4th FRAV session (September 2020)
18 June 2020

Secretary's note: This input by the experts from Japan responded to an initial draft request for comments sent to the FRAV stakeholders on 8 June 2020. The initial draft raised significant reservations and therefore was superseded by a revised request for comments (FRAV-03-05-Add. 5). At the request of the experts from Japan, this response is reproduced for the 4th FRAV session.

System Safety: Opening Discussion

This document opens the discussion on the System Safety chapter of Document 5. The document proposes starting points for drafting the initial paragraphs based upon certain logical (but not necessarily correct) assumptions drawn from the AV Framework Document (FRAV/2019/34/Rev.2) and the FRAV discussions to date.

The FRAV secretary's request is to comment on the following proposals and/or signal any objections.

Chapter preamble structure

The ODD chapter opens with 1) a statement on the scope of the chapter (i.e., description of an ODD), 2) a statement on the overall requirement (i.e., the manufacturer should provide ODD descriptions), and 3) a statement on the purpose of the requirement (i.e., to inform decisions on applicable requirements and scenarios under the assessment method). The FRAV secretary proposes to follow this basic structure for the System Safety chapter.

> Proposal 1
>
> The chapter should open with statements describing:
>
> - Chapter scope
> - Overall requirement
> - Purpose(s) of the overall requirement

Initial considerations

Assuming that Proposal 1 is acceptable, the following provides an initial basis for discussing revisions to Document 5.

The AV Framework Document offers two statements on "system safety":

1) System Safety: When in the automated mode (OD), the automated vehicle should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations.
2) Validation for System Safety: Vehicle manufacturers should demonstrate a robust design and validation process based on a systems-engineering approach with the goal of designing automated driving systems free of unreasonable safety risks and ensuring compliance with road traffic regulations and the principles listed in this document. Design and validation methods should include a hazard analysis and safety risk assessment for Automated Driving System (ADS), for the OEDR, but also for the overall vehicle design into which it is being integrated and when applicable, for the broader transportation ecosystem. Design and validation methods should demonstrate the behavioural competencies an Automated/autonomous vehicle would be expected to perform during a normal operation, the performance during crash avoidance situations and the performance of fall back strategies. Test approaches may include a combination of simulation, test track and on road testing.

Chapter scope

The "validation" paragraph appears to state the general intent for the section: "the vehicle manufacturer should demonstrate" system safety. The Framework Document provides further details, but the suggestion is to keep the opening statement simple. FRAV will add details further in the chapter. In addition, FRAV

appears agreed that the focus of our work concerns the requirements for an ADS, inherently covering its subcomponents or functions and its performance when installed on a vehicle.

> Proposal 2
>
> The statement on the scope of the chapter should read:
>
> This chapter concerns manufacturer demonstrations of ADS System Safety.

Overall requirement

The System Safety chapter would define the requirements that a manufacturer should respect to ensure a satisfactory demonstration. Again, the Framework Document provides additional details; however, the following proposal submits that "free of unreasonable safety risks" covers all these additional details. For example, an ADS incapable of ensuring compliance with road traffic regulations is unlikely to qualify as "free of unreasonable safety risks". Moreover, FRAV has identified such items as candidates for further discussions as requirements. In line with FRAV's "high-level first" approach, the proposal suggests reducing the overall requirement to its essential aim.

> Proposal 3
>
> Statement on the overall "system safety" requirement should read:
>
> For the assessment of vehicle safety, the vehicle manufacturer should demonstrate that the ADS is free of unreasonable safety risks in accordance with the provisions of this chapter.

[Overall requirement]

4.2. of the current text of the System Safety section of Document 5 is the overall requirement considering the AV Framework Document and should be included in high-level description of the overall requirement. Therefore, 4.2. of the current text should be overall requirement text.

And we think 4.4.6. is to breakdown the meaning of "reasonably preventable". So, 4.4.6. should be a sub-paragraph of 4.2. and we need one more sub-paragraph to breakdown the meaning of "reasonably foreseeable".

Reasonably preventable can be defined as avoidable by a competent and careful human driver and reasonably foreseeable stands for forecastable based on physics principles with a relevant exposure.

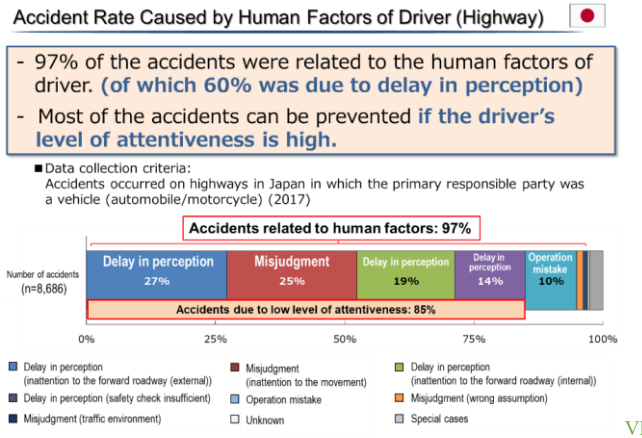
So free of accident reasonably foreseeable and preventable is equivalent with free of crashes that are forecastable based on physics principles, that result in injury or death, with a relevant exposure and that are avoidable by a competent and careful human driver.

With regards to setting the criterion as the state of the arts automated driving technology, it seems to be impossible to do so, because no automated driving technology has been introduced to the market.

Japan proposes to change "in equal or safer performance than a human driver" to "in equal or safer performance than a competent and careful human driver" and "The nominal operation of the ADS shall" to "When in the automated driving mode, ADS shall" in paragraph 4.4.6..

In reality the most of accidents are caused by human factor such as distraction. Because of the free of distraction of AD system, with the AD system with better capability than competent and careful human driver, the traffic society can get the big safety benefit from AD.

Document FRAV-04-10
Submitted by the experts from Japan
4th FRAV session (September 2020)
18 June 2020



VMAD-04-04

Regarding the second sentence of 4.4.6.,

[The overall safety target shall be at least as good as manual driving, i.e. P (accident with fatalities)< 10-8 /h and P(accident with light or severe injuries) <10-7/h.]

We are doubtful if it works well or not, because it is difficult to assume the accident occurrence ratio of ADS at this moment. So, we propose to set the appropriate human driver performance model in order to compare to ADS performance instead of this criterion.

Regarding [destruction of property,] of 4.2.,

[destruction of property,] is too broad meaning. It is necessary to clarify.

Regarding 4.4.4.,

4.2. describes "shall not cause any traffic accidents [incidents/events] ", 4.4.4. describes "shall not cause any traffic collision". These statements seem similar, but different terms are used and it leads to ambiguity. Japan propose to delete 4.4.4. to avoid confusion.

Purpose of the requirement

The aim of the "purpose" statement is to capture why a manufacturer should demonstrate system safety within the context of the NATM. In this regard, stakeholders may wish to offer views on the relationship between the "system safety demonstration" and the VMAD "pillars".

The Framework Document appears to highlight two distinct elements concerning a) the ADS design and b) its validation through testing. FRAV may wish to consider structuring the System Safety chapter in terms of these two high-level elements. One subsection might focus on requirements to ensure that safety risks have been identified and mitigated through a "systems engineering" approach to functional safety. A separate subsection might focus on requirements to ensure that the ADS and its features have been adequately tested through "a combination of simulation, test track and on-road testing". Therefore, the following proposal suggests stating the purpose of the system-safety demonstration requirement in these terms.

Document FRAV-04-10
Submitted by the experts from Japan
4th FRAV session (September 2020)
18 June 2020

Proposal 4

The statement on the purposes of the requirement to demonstrate system safety should read:

> The manufacturer should demonstrate that the ADS satisfies the functional safety requirements described in this document and its performance has been sufficiently validated through a combination of simulation, track, on-road, and other available test methods.

[Purpose of the requirement]

Purpose of the overall requirement is described in the AV Framework Document. Therefore, the text below should be "purpose of the requirement" paragraph.

3. Safety Vision

"WP.29 recognizes that for automated/autonomous vehicles to fulfil their potential in particular to improve road transport, then they must be placed on the market in a way that reassures road users of their safety. If automated/autonomous vehicles confuse users, disrupt road traffic, or otherwise perform poorly then they will fail."

Summary

Taken together, the proposals stipulate that the System Safety chapter provides requirements that a manufacturer should satisfy to demonstrate that its design and its validation methods have resulted in an ADS that is free of unreasonable risks to safety.

The FRAV secretary requests the stakeholders to consider these four proposals and provide initial comments on or before 18 June. The secretary will then report back to the group in a draft Addendum 6 to FRAV-03-05.

Document FRAV-04-10
Submitted by the experts from Japan
4th FRAV session (September 2020)
18 June 2020

Further reference

For information, the following provides the current text of the System Safety section of Document 5.

4.	System Safety [System Behavior]
4.1.	It is necessary to clearly define the split in responsibilities between the driver and the ADS.
4.2.	When in automated mode, the automated/autonomous vehicle should be free of unreasonable safety risks to the driver and other road users and ensure compliance with road traffic regulations. This level of safety implies that an automated/autonomous vehicle shall not cause any non-tolerable risk [introduce unreasonable risks], meaning that automated/autonomous vehicle systems, while in automated mode, shall not cause any traffic accidents [incidents/events] resulting in [destruction of property,] injury or death that were reasonably foreseeable and preventable.
4.3.	In terms of its alignment with the NATM structure, System Safety is closely associated with the Audit phase(s) under development by VMAD where manufacturer documentation provides a basis for an assessment of vehicle system design safety and safe performance across traffic scenarios applicable to the vehicle.
4.4.	Requirements under consideration include:
4.4.1.	The Automated Driving System (ADS) shall react to unforeseen situations in a way that minimizes risk.
4.4.2.	The vehicle shall demonstrate adequate mitigation of risks (e.g. approaching ODD boundaries), safe driving behavior and good Human Machine Interface.
4.4.3.	The system shall minimize the risks to vulnerable road users (VRU) in the case of an imminent collision (e.g., hit vehicle instead of VRU)
4.4.4.	When in the automated driving mode, the vehicle shall not cause any traffic collision that are rationally [reasonably] foreseeable and preventable. Any avoidable accident shall be avoided.
4.4.5.	When in automated driving mode, the automated vehicle drives and shall replace the driver for all the driving tasks for all the situations which can be reasonably expected in the ODD.
4.4.6.	[~~The nominal operation of~~ When in automated driving mode, the ADS shall result in equal or safer performance than a competent and careful human driver. i.e. achieve a neutral or positive risk balance.] [~~The overall safety target shall be at least as good as manual driving, i.e. P (accident with fatalities)< 10-8 /h and P(accident with light or severe injuries) <10-7/h.~~] The appropriate human driver performance model shall be set in order to compare to ADS performance.
4.4.7.	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.
4.4.8.	If an update renders the system obsolete or otherwise no longer supported, it shall not permit activation

Commented [J1]: [destruction of property,] is too broad meaning. It is necessary to clarify. Is there any background for this proposal?

Commented [J2]: 4.2. describes "shall not cause any traffic accidents [incidents/events] ", 4.4.4. describes "shall not cause any traffic collision". These statements seem similar, but different terms are used and it leads to ambiguity. Japan propose to delete 4.4.4. to avoid confusion.

Commented [J3]: Japan thinks 4.4.6. is to breakdown the meaning of "reasonably preventable". So, 4.4.6. should be a sub-paragraph of 4.2. and we need one more sub-paragraph to breakdown the meaning of "reasonably foreseeable".
Reasonably preventable can be defined as avoidable by a competent and careful human driver and reasonably foreseeable stands for forecastable based on physics principles with a relevant exposure.
So free of accident reasonably foreseeable and preventable is equivalent with free of crashes that are forecastable based on physics principles, that result in injury or death, with a relevant exposure and that are avoidable by a competent and careful human driver.

Commented [J4]: We do not think it work well with this concept and we think it is better to set the appropriate human driver performance model in order to compare to ADS performance.