Document FRAV-04-06
Submitted by the experts from China
4th FRAV session (September 2020)
21 August 2020

System Safety: Round 3

This document supersedes FRAV-03-05-Add.5. This document requests comments pursuant to discussions during the 3rd FRAV session.

Topic 1

During the 3rd session, FRAV discussed the proposition that ADS may have "internal" design constraints (such as use of seat belts as a prerequisite to use of the ADS). Stakeholders suggested that ODD should be limited to "external" vehicle operating conditions for clarity.

Should ODD be defined as external operating conditions under which an ADS feature is specifically designed to function?

Proposal:

China agrees that "ODD Should be defined as external operating conditions under which an ADS feature is specifically designed to function". And on this basis, the terms and definitions of ODC should be added to Document 5.

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

"Operational Design Conditions (ODC)" means all operating conditions under which an ADS feature is specifically designed to function, including, but not limited to, operational design domain (ODD) , vehicle status, driver and passenger status.

Topic 2

FRAV agreed during its 2nd session that "system safety refers to the system design and presence of requisite capabilities and to general safety performance of the vehicle in operation" (FRAV-02-02). FRAV reiterated this view during the 3rd session when discussing the System Safety chapter of Document 5. Stakeholders suggested that other Document 5 chapters are subsets of "system safety" (or conversely, that "system safety" is the overall purpose of Document 5).

The FRAV Terms of Reference includes two mandates: development of "functional (performance) requirements" and to "also cover the requirements for Functional Safety".

FRAV has discussed Safety of the Intended Functionality (SOTIF, i.e., ensuring that a function fulfills its intended purpose) and Functional Safety (i.e., that foreseeable failures in safety-critical functions are managed).

During the consideration of ODD, Germany raised a question regarding "features", "functions", and definition of the terms and their use. The concept of "functions" as separate from "features" arose again in the exchanges on the System Safety chapter. During the 3rd session, OICA noted that features can share all or part of the ADS (i.e., system-level) hardware and software.

Please provide views on clarifying Document 5 with regard to "system safety", "system design", "operational performance", SOTIF, Functional Safety, "functions", "functional requirements", and "performance requirements".

Proposal:

1. Agree that "system safety" is the overall purpose of Document 5. "System safety" should be an overall concept, including functional safety, information security, and expected functional safety, as well as the functional requirements and performance requirements of the system.

2. "Operational performance" is not used in Chapters 4 and 5, so there is no way to understand the meaning of this term. If it is equivalent to "performance requirements", it is not recommended to introduce new terms.

3. It is necessary to clarify the difference between "features" and "functions". The current content is difficult to understand the difference between them.

Topic 3

During the 3rd session, the FRAV leadership suggested differentiating functional requirements (e.g., system design, presence of requisite capabilities, SOTIF, Functional Safety) and operational requirements (e.g., safety performance in operation, performance specifications for driving behavior, fallbacks, user interactions) for clarity. The "System Safety" chapter (possibly under another name) would focus on functional performance while the remaining Document 5 chapters would address operational performance.

The leadership proposal aimed to create a path for starting work on specific requirements by late September (when VMAD anticipates needing such support from FRAV). FRAV has a list of 142 candidate requirements gathered during its 2nd session (circulated last February). The proposal suggested developing ODD elements, "functional performance requirements", and "operational performance requirements" simultaneously when considering each candidate.

For example, one candidate requirement states, "The system shall be able to detect and identify lane markings." Under the proposal, FRAV would consider the lane-marking proposal in terms of these three aspects:

- Does the proposal suggest an element for inclusion under ODD descriptions?
- Does the proposal suggest a function that should be present on an ADS?
- Does the proposal suggest an operational performance requirement?

Based upon the outcomes of this discussion (and FRAV's aim to draft high-level, performance-based, and technology-neutral provisions), FRAV would amend the relevant section(s) of Document 5.

The proposed method aims to enable FRAV to begin working on individual draft requirements by the end of September.

Please provide views on whether FRAV should try this (or another) method for considering safety requirements under Document 5.

Proposal:

Agree with the example method.

As mentioned above, the definition of "operational requirements" is not clear, nor is it reflected in the three aspects of the examples. If "operational requirements" can already be expressed by "functional requirements" and "performance requirements", it is not recommended to introduce new terms.