Document FRAV-04-07
Submitted by the expert from SAE
4th FRAV session (September 2020)
21 August 2020

Secretary's note: The following is excerpted from an email submitted by the expert.

FRAV and VMAD have enormously complicated tasks and I think it is helpful to simplify matters wherever possible and where consistent with the goals set for these groups. I think that starts with adopting some established terminology and, only where necessary, creating new and different terms that will not be confused with the established ones.

Topic 1. Should ODD be defined as external operating conditions under which an ADS feature is specifically designed to function?

There is no need to redefine ODD because the concept as currently defined is clearly, if implicitly, intended to deal with external conditions. Internal design elements may be a factor to consider in developing functional requirements, but they are not "operating conditions." The SAE J3016 definition is not all-inclusive, but its intent is clearly to cover conditions under which the ADS is designed to function, not design elements inside the vehicle:

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.

The WP.29 Framework contains similar language (although, unfortunately, it uses the abbreviation "OD" interchangeably with "ODD"):

Operational Design Domain (ODD/OD)] (automated mode): For the assessment of the vehicle safety, the vehicle manufacturers should document the OD available on their vehicles and the functionality of the vehicle within the prescribed OD. The OD should describe the specific conditions under which the automated vehicle is intended to drive in the automated mode. The OD should include the following information at a minimum: roadway types; geographic area; speed range; environmental conditions (weather as well as day/night time); and other domain constraints;

To the extent that FRAV and VMAD feel the need for elaboration on how the different elements of an ODD can be described, the document that Matt has provided, A Framework for Automated Driving System Testable Cases and Scenarios, and the AVSC best practice on describing the ODD are helpful references.

If FRAV decides that there is a need to specify design constraints for inside the vehicle I strongly recommend that a different term be developed that cannot be easily confused with ODD. At least in English, I don't think "ODC" (operational design constraints) would be helpful because of its close similarity in wording to "ODD" but quite distinct meaning. Something as straightforward as "Internal vehicle design constraints" may work. That way, there would be no confusion in terms. "ODD" is likely to be used in very many FRAV and VMAD contexts (e.g., with regard to developing requirements for an ADS's ability to sense the presence of its ODD limits and ODD-specific scenarios for validation), and redefining that term or using one that is extremely similar to mean something different would complicate those tasks.

Topic 2. 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”.

System safety.

This term "system safety" has long had an established meaning dating back at least to MIL-STD-882, which originated decades ago. One definition that I found useful while at U.S. DOT comes from the FAA System Safety Handbook:

System safety is a specialty within system engineering that supports program risk management. It is the application of engineering and management principles, criteria and techniques to optimize safety. The goal of System Safety is to optimize safety by the identification of safety related risks, eliminating or controlling them by design and/or procedures, based on acceptable system safety precedence.

Rather than defining system safety, the reference to system safety in paragraph 9(a) in the WP.29 Framework seems to establish a very high-level principle for the outcome of a system safety program as applied to an automated vehicle:

System Safety: When in the 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.

The Framework then goes on (in paragraph 9(f)) to describe the methods for "Validation of system safety." I don't think there is any need to redefine system safety for FRAV purposes. I think it's best and simplest to just acknowledge its accepted meaning in engineering, note the very broad Framework principle relating to it, and proceed with determining how to flesh out the validation of that principle using the various validation elements noted in the Framework.

Functional safety vs. functional requirements

I think there is understandable confusion about functional safety and functional requirements. "Functional safety" is defined in different ways. An IEC document contains this definition:

Functional safety is the part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.

Functional safety is the detection of a potentially dangerous condition resulting in the activation of a protective or corrective device or mechanism to prevent hazardous events arising or providing mitigation to reduce the consequence of the hazardous event.

ISO 26262 defines functional safety as the absence of unreasonable risk of harm that may be caused by malfunctions in safety-related electrical or electronic systems in passenger vehicles over the life cycle of those systems. SOTIF, of course, refers to safety of the intended functionality rather than to hazards caused by malfunctions. Although functional safety is generally spoken of as referring only to safety related to the absence of malfunctions, the broader definition could include SOTIF as well.

However, "functional requirements" as defined by WP.29 should not be read as confined to functional safety. The WP.29 Framework in the annex that sets out FRAV's work priorities for "functional requirements" says with regard to "description of work":

This work item should cover the functional requirements for the combination of the different functions for driving: longitudinal control (acceleration, braking and road speed), lateral control (lane discipline), environment monitoring (headway, side, rear), minimum risk manoeuvre, transition demand, HMI (internal and external) and driver monitoring. This work item should also cover the requirements for Functional Safety.

The Framework goes on to provide under the heading of "corresponding principles/elements":

a. System safety

b. Failsafe Response

c. HMI /Operator information

d. OEDR (Functional Requirements)

The simplest reading, then, of what WP.29 intended with regard to functional requirements is that FRAV develop requirements for each of the listed subject areas. Some requirements (how the vehicle actually performs various functions such as failsafe response, OEDR, longitudinal and lateral control, etc.) can be expressed as "performance requirements" because they actually measure the vehicle's performance and specify a performance metric. Others can be thought of as "process requirements" because they require that certain very general engineering processes (possibly including ISO 26262 on functional safety and SOTIF) be used. The Framework's paragraph on "Validation for System Safety" supports this distinction (with my note in the middle suggesting how the two types of requirements are stated separately):

f) 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. {Note: requirements before this note can be thought of as process requirements that can be audited; requirements after this note can be thought of as performance requirements that can be validated through testing} 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;

I think the process/performance distinction will aid FRAV's discussions and fit well with VMAD's distinctions between the audit pillar (process) and the various testing pillars of validation methods (performance).

Topic 3. John notes the proposal to differentiate 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. Please provide views on whether FRAV should try this (or another) method for considering safety requirements under Document 5.

With all due respect, I do not think that the proposed distinction between functional and operational requirements is helpful and I find it quite confusing. As explained above under Topic 2, the WP.29 Framework provides a broad description of "functional requirements" and neither the Framework nor the terms of reference for FRAV distinguish "operational requirements." I think the better and more logical way to distinguish two major categories of functional requirements is to speak of process requirements (design and validation process, including the validation and hazard analysis methods used to meet the Framework's principles) and performance requirements (demonstration of the ADS's behavioral competencies in normal driving, performance during crash avoidance situations, and performance of fallback strategies using simulation, test track, and/or on-road testing). This distinction seems to fit the purpose of the functional/operational distinction that was proposed, but also seems to fit better with the idea that functional requirements is the general category assigned to FRAV and not a sub-category itself.