System Safety: Round 2

The "opening discussion" raised a number of fundamental issues (including the scope of the FRAV and VMAD activities). As a result, the initial proposals did not indicate a path towards reaching consensus. Points raised included:

- The importance of ensuring that an ADS complies with traffic regulations,
- Mixed views on whether compliance with traffic regulations is a performance requirement and/or a system-safety requirement,
- Concern that "free of unreasonable safety risks" does not necessarily address compliance with traffic regulations and particularly interactions with public agents (police, emergency responders, etc.),
- Use of the AV Framework Safety Vision[1] to describe the purpose of the system-safety requirements,
- Addressing collisions caused by an ADS and avoidance or mitigation of collisions caused by other road-user actions,
- The path from high-level requirements to second, third, and further levels of detail as may be warranted,
- Determining the performance limits for "preventable" (avoidable) collisions,
- The relationship between "system safety" and "functional safety",
- The scope of "system safety" as an overarching concept that encompasses the other chapters of Document 5.

The collective input suggests a need to differentiate "system-safety requirements" and the requirements that would be defined under the remaining chapters of Document 5 (execution of driving tasks, HMI, safe fallbacks, etc.). This document suggests a possible approach.

The FRAV Terms of Reference specifically mandate "requirements for Functional Safety" in addition to "functional (performance) requirements". As defined under ISO 26262, functional safety broadly refers to managing responses to system failures. In various ways, the WP.29 discussions make a distinction between performance requirements and requirements related to system design, failure detection and response, and safety of complex electronic systems. The AV Framework Document (albeit under an item assigned to VMAD) speaks in these terms about "system safety".

Germany raised questions regarding a possible relationship between ADS "features" and ADS "functions". In addition, Germany submitted a discussion paper regarding "Safe System Behavior: From Requirements to Concrete Specifications" (FRAV-03-03). Multiple comments, including from Russia and Japan, noted that system safety broadly covers ADS capabilities that control driving behaviors/performance. The SAE definition of the Dynamic Driving Task refers to the functions necessary to operate a vehicle in traffic.

These elements suggest a distinction between the functions that should be integrated into the design of an ADS and the required performance of an ADS in operating a vehicle. For example, the ALKS regulation specifies following distances at different speeds. These performance requirements objectively require that a system be able to detect a lead vehicle and determine its distance from that vehicle. Functional safety would require the detection of a failure in this capability given its importance to safety.

Therefore, this document suggests defining the scope and purpose of the System Safety chapter in terms of ADS functions and functional safety. FRAV agreed that ODD description elements would be informed or derived from performance requirements. Similarly, system-safety requirements could be derived from performance requirements. A performance requirement to maintain a safe distance from a preceding vehicle (presumably based upon vehicle speed, road adhesion, and other factors) would logically imply certain ODD description elements (ADS feature speed range, road-surface conditions) and functional safety elements (presence and monitoring of function(s) for the detection of a lead vehicle, calculation of distance from the lead vehicle, condition of road surface).

---

[1] "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." "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."

This "triangular approach" (ODD description, system safety, and performance requirements) suggests four principle advantages.

First, the approach clarifies the roles of ODD description elements, system-safety requirements, and performance requirements in determining technical requirements for an ADS. ODD elements and system-safety functional requirements can be derived and justified by performance requirements.

Second, many, if not most, Document 5 requirements could be broad enough to cover wide ranges of ADS. For example, a performance requirement based on the notion that an ADS feature should not be available for use outside its ODD means that an ADS should be able to detect the ODD conditions and boundaries. A failure in the detection function(s) should prevent the feature from being used. Because the ODD description would define the conditions, Document 5 would not necessarily have to define detailed system-safety and performance requirements (i.e., specifying requirements for diverse arrays of possible ADS configurations and operational conditions). Technical requirements for a specific ADS could be objectively derived from the ODD description (e.g., not designed for use in rain = should have a function to detect rain, should not operate in rain, should meet following-distance requirements for dry roads).

Third, the approach facilitates differentiation between system-level and feature-level (i.e., ODD-specific) requirements. The approach differentiates between "functions" (i.e., system capabilities required to operate a vehicle in accordance with performance requirements) and "features" (i.e., ADS applications designed for use under specified conditions).

Fourth, FRAV could proceed to develop performance requirements under the remaining chapters while gradually defining and justifying ODD description elements and system-safety (functional safety) requirements. To the extent that a performance requirement relies on certain information regarding the ODD or relies on a function in good working order, the ODD and System Safety elements could be defined. This approach provides a way to organize further work and build out Document 5 in a logical, coherent manner.

With this in mind, this document proposes the following as a possible starting point for defining the scope and purpose of the System Safety chapter. The co-chairs have agreed to hold the 3rd FRAV session via web conference on 28 July. Comments on this proposal would be very welcome prior to the session in order to understand whether the approach merits further consideration.

3. Definitions

3.3.3. (ADS) function means a capability integrated into the design of an ADS to enable fulfillment of one or more performance requirements, including the means to detect a failure in the function.

3.3.4. Object and Event Detection and Response (OEDR) means the ADS function(s) designed to monitor the driving environment via object and event detection, recognition, classification, and response preparation.

3.3.6. User monitoring means the ADS function(s) designed to assess user performance of such roles as may be required to fulfill the requirements defined in this document.

5. System Safety

5.1. This chapter concerns requirements for ADS system safety, including functional safety.

5.2. For the assessment of vehicle safety, the vehicle manufacturer should describe the ADS functions designed to satisfy the requirements of this chapter.

5.3. The purpose of this chapter is to ensure that an ADS integrates functions necessary to ensure fulfillment of the [performance] requirements established in this document, including the means to ensure safety in the event of a failure in such functions.