

Mastering complexity: Integrated safety process for modern vehicle systems

03/12/2025 Functional safety and the safety of the intended functionality are essential pillars when it comes to developing safe, modern vehicle systems. Due to increasingly complex assistance systems and autonomous driving, functional safety is becoming increasingly important. The experts at Porsche Engineering put their many years of experience into practice helping customers develop modern, safety-conforming systems from the initial draft to release.

The relationship between functional safety (FuSa) and the safety of the intended functionality (SOTIF) can be understood as two sides of the same coin: The two together result in one valuable whole. Both sides play a decisive role in modern driver assistance systems, or ADAS (advanced driver assistance systems) for short, as well as in autonomous driving (AD). FuSa addresses the classic question: What happens if a software or hardware component fails?

The idea of functional safety ensures that the system does not cause an unacceptable risk if internal

malfunctions arise, such as a sensor failure or a software error. This is based on a process of structured analysis in which all relevant software and hardware errors are examined and evaluated for their effects. Effects rated as safety-critical are mitigated by technical and procedural measures. The functional safety methods are applied consistently, this being both during the concept phase and in the series implementation phase. SOTIF, the safety of the intended functionality, addresses another, equally important question: What happens if the system operates without failures but fails to master a real operating situation? This concerns the acceptability of risks that arise from the limitations of the function itself, for example when a vehicle camera is blinded by the sun or an algorithm does not detect a cyclist in a complex driving scene.

SOTIF is an exploratory discovery process in which iterations are the central tool for gradual improvement of the function design and knowledge generation. In order to achieve the overall safety of the system, FuSa and SOTIF are systemically interconnected and complement each other.

“FuSa ensures that hardware and software work reliably. SOTIF ensures that the capabilities of these reliable components are sufficiently specified and proven to operate safely in the real world,” explains Marek Hudec, Senior Manager of System Safety at Porsche Engineering. “This is because a system can be safe from the traditional FuSa standpoint, but still not safe enough from a SOTIF standpoint due to performance limitations.”

Iterative approach for SOTIF

Despite the similarity, there are differences in the process steps between FuSa and SOTIF, because an iterative approach with exploratory analysis and test methods is generally preferred to achieve SOTIF (see box on page 38). “What that means is that the developers specify, test and revise the system design until an acceptable residual risk is reached,” reports Dennis Müller, Development Engineer at Porsche Engineering. Porsche Engineering offers its customers a comprehensive solution portfolio that includes both safety methods—SOTIF and FuSa—to manage the complex development and verify and validate of driver assistance systems and autonomous driving functions.

“Among other services, we support our customers in applying the relevant standards such as ISO 26262 (FuSa) and ISO 21448 (SOTIF). This includes their implementation in existing development processes, execution of the hazard and risk analyses, drawing up safety concepts, and supporting the entire safety lifecycle,” explains Müller. “At Porsche Engineering, we ensure safety-conformated development in accordance with FuSa and SOTIF through clearly defined, integrated processes with clearly dedicated responsibilities. This guarantees conformity to standards and provides traceability.“

Porsche Engineering has many years of expertise throughout the entire development chain: From drawing up requirements to simulating and testing real vehicles, Porsche Engineering uses state-of-the-art simulation and test methods, including ones for developing warning functions, parking systems, and (partially) autonomous driving functions. As an example, one out of many results of this expertise is the modular software component called “Guardian”. It is designed to facilitate the transition from

advanced Level 2 systems to highly automated Level 3 driving. It offers a robust, safe, and standard-conforming solution for the implementation of safety components for autonomous driving systems. By analyzing real driving data, potentially critical situations and special cases—referred to as corner cases and edge cases— are identified exploratively and used for data-driven scenario generation. As the responsibility of the system increases, the challenges the system is facing also become bigger. As far as functional safety is concerned, these challenges primarily consist of the fact that degradation and warning concepts can no longer rely solely on the driver, who bears sole responsibility for all vehicle maneuvers during assisted driving (Level 1) and semi-automated driving (Level 2).

This will change from Level 3 on: In this case, the systems must be able to handle failures autonomously, as the driver will no longer have a constant duty of attention. Only if the systems reach their limits must it be possible to intervene after an appropriate warning period. In principle, therefore, safe operability must continue to be guaranteed when failures occur, at least for a certain period of time - this makes the leap from Level 2 to Level 3 challenging. As a side effect, the number of redundancies in vehicle electronics is increasing rapidly—and so are the associated development workload and costs. With regard to SOTIF, the challenge lies in the depth and breadth of the set of all possible operating scenarios that the function needs to be able to master.

“These include the continuously changing vehicle environment, the behavior of road users, and unforeseeable events, which are referred to as unknown unsafe scenarios,” says Hudec. To deal with this complexity, systems are initially designed for a defined operational design domain (ODD). The scenarios to be safely mastered are thus restricted to a systematically derived space, which is divided into discrete individual scenarios by means of a scenario portfolio. The system must ensure that the approach to the boundary of this space is detected at an early stage so that either control can be handed over to the driver or the vehicle can be stopped safely within the boundaries of the ODD. “This approach is extremely important for driver assistance development: The more responsibility a system assumes for the actual driving, the more critical it becomes to consider the safety aspects of FuSa and SOTIF,” explains Müller.

Improved safety due to redundancy

One example from practice that illustrates the different but complementary approaches of FuSa and SOTIF is an SAE Level 3 situation for automated driving on the highway in which the driver completely relinquishes responsibility. When it comes to managing hardware or software failures, FuSa is required: Suppose that the radar sensor that measures the distance to the vehicle in front has a hardware defect and is no longer providing data. This example of a fault could lead to the function relying on outdated or invalid sensor data and possibly risking a rear-end collision. That is why the experts at Porsche Engineering use deductive and inductive safety analyses to identify such failures; the analyses must be verified by safety mechanisms. In this specific case, for example, redundancy would be useful to prevent this local individual failure from leading to “global unavailability” of the sensor data, at least until the point in time when the driver again takes responsibility for driving.

SOTIF comes into play when it is a matter of mastering performance limits for automated driving on the highway. For example, vehicle detection must be designed in such a way that all other vehicles around or approaching the vehicle, including all motorcycles, are detected. However, due to the general, technically inherent performance limits of the sensors used, the vehicle may not correctly detect certain narrow silhouettes and approach trajectories under unfavorable light or weather conditions. Although the hardware and software are working flawlessly, this could cause the function to initiate a lane change that could result in a collision risk with an overtaking motorcycle. In this case, the SOTIF processes stipulate that the design must be analyzed and validated across all operating scenarios and that the weaknesses identified are corrected with the next design iteration (specification update followed by implementation update). For example, additional cameras and lidar sensors could be installed in the rear section or the sensor fusion algorithms could be optimized.

“The biggest challenge is no longer just in the system itself, but in the almost infinite complexity of reality. It is not possible to test every conceivable scenario in advance, but it is necessary to achieve sufficient coverage of the range of operation. The development process is just as complex as one would expect. SOTIF provides the framework for understanding the limits of the system and designing them safely even when all system components are functioning perfectly,” Müller explains.

Providing qualitative and quantitative evidence that a system is safe requires large amounts of test data, a considerable amount of which is generated through simulations. The biggest challenge is dealing with unknown unsafe scenarios—dangerous situations that were not taken into account during development due to insufficient specifications or that could occur due to changes in operating conditions. To discover and minimize these is the core objective of SOTIF and represents a great challenge when developing the systems. “At Porsche Engineering, we offer our customers not only individual test services, but also close and long-term cooperation to meet the enormous demands placed on ADAS/AD development and to put safe, robust, and reliable functions on the road,” promises Hudec.

Methods such as AI-based recognition of corner cases or specially trained AI models will increasingly provide developers with support for this in the future. It is already clear today the use of AI in safety-critical systems will require even more complex verification procedures in the future. This topic is addressed by the new international standard draft ISO/PAS 880, which deals with the safety of AI when it is part of the end product. Another innovation is the international draft standard ISO/TS 5083, which focuses specifically on the topic of safety of autonomous driving functions of the vehicle and takes into account not only the vehicle on-board components, but considers also the off- board components and its effect on the overall safety. This is referred to as holistic safety. The safety-oriented V2X communication between vehicles and with the infrastructure not only brings with it new safety-enhancing possibilities, but also new potential sources of faults and new dependencies. These too must be safeguarded with the same consistency—a demanding process that the experts at Porsche Engineering devote themselves to on a daily basis.

Summary

The requirements placed on the functional safety of vehicles are significantly due to the widespread use of assistance systems. The performance of the correctly implemented system in corner cases is the main focus of SOTIF. Among other things, Porsche Engineering uses data-driven and AI-based methods to master complexity and thus bring reliable systems on the road.

Info

Text first published in Porsche Engineering Magazine, issue 1/2025.

Text: Ralf Bielefeldt

Copyright: All images, videos and audio files published in this article are subject to copyright. Reproduction in whole or in part is not permitted without the written consent of Dr. Ing. h.c. F. Porsche AG. Please contact magazin@porsche-engineering.de for further information.

MEDIA ENQUIRIES



Sandro Kälin

Head of Communications Porsche Schweiz AG
+41 41 487 91 16
sandro.kaelin@porsche.ch



Siraya Schäfer

Press and Public Relations Specialist, Porsche Schweiz AG
+41 41 487 91 47
siraya.schaefer@porsche.ch

Link Collection

Link to this article
https://newsroom.porsche.com/it_CH/2025/innovation/porsche-engineering-functional-safety-deleoping-modern-vehicle-systems-41260.html

External Links
https://newsroom.porsche.com/en/innovation/porsche-engineering.html