Komplexität beherrschen: Integrierter Sicherheitsprozess für Fahrzeugsysteme

03/12/2025 Funktionale Sicherheit und die Sicherheit der beabsichtigten Funktion sind wesentliche Säulen der sicheren Entwicklung moderner Fahrzeugsysteme. Durch immer komplexere Assistenzsysteme und das autonome Fahren gewinnen sie zunehmend an Bedeutung. Mit jahrelanger Erfahrung unterstützen die Expertinnen und Experten von Porsche Engineering Kunden bei der Entwicklung von modernen, sicherheitskonformen Systemen von der ersten Konzeption bis zur Freigabe.

Das Verhältnis von Funktionaler Sicherheit (Functional Safety, FuSa) zur Sicherheit der beabsichtigten Funktion (Safety of the Intended Functionality, SOTIF) lässt sich wie die zwei Seiten einer Goldmedaille verstehen: Beides zusammen ergibt das wertvolle Ganze. Beide Seiten spielen bei modernen Fahrerassistenzsystemen, kurz ADAS (Advanced Driver Assistance System), sowie dem autonomen Fahren, kurz AD (Autonomous Driving), eine entscheidende Rolle. FuSa stellt dabei die klassische Frage: Was passiert, wenn eine Software- oder Hardware- Komponente ausfällt?

Das Konzept der Funktionalen Sicherheit sorgt dafür, dass das System durch interne Fehler, wie beispielsweise einen Sensorausfall oder einen Software- Fehler, kein unvertretbares Risiko verursacht. Dahinter steht ein strukturierter Analyseprozess, bei dem alle relevanten Software- und Hardware-Fehler auf Auswirkungen untersucht und bewertet werden. Als sicherheitskritisch bewertete Auswirkungen werden durch technische sowie prozessuale Maßnahmen gemindert. Hierbei werden die Methoden der Funktionalen Sicherheit durchgängig, das heißt sowohl in der Konzeptionsphase der Systemarchitektur als auch im Serienentwicklungsprozess angewendet. SOTIF, die Sicherheit der beabsichtigten Funktion, stellt eine weitere, ebenso wichtige Frage: Was passiert, wenn das System zwar fehlerfrei funktioniert, aber eine reale Betriebssituation nicht beherrscht? Hier geht es um die Akzeptierbarkeit von Risiken, die durch die Grenzen der Funktion selbst entstehen, zum Beispiel wenn eine Fahrzeugkamera von der Sonne geblendet wird oder ein Algorithmus einen Radfahrer in einer komplexen Fahrszene nicht erkennt.

SOTIF ist ein explorativer Entdeckungsprozess, bei dem Iterationen das zentrale Werkzeug zur schrittweisen Verbesserung der Funktionsauslegung und Wissensgenerierung sind. Zum Erreichen der Gesamtsicherheit des Systems sind FuSa und SOTIF systemisch miteinander verbunden und ergänzen sich.

„FuSa stellt sicher, dass Hardware und Software zuverlässig arbeiten. SOTIF sorgt dafür, dass die Fähigkeiten dieser zuverlässigen Komponenten ausreichend spezifiziert und abgesichert sind, um in der realen Welt sicher zu agieren“, erklärt Marek Hudec, Leiter Fachdisziplin Systemsicherheit bei Porsche Engineering. „Denn: Ein System kann funktional sicher sein, aber aufgrund von Leistungsbeschränkungen dennoch nicht sicher genug im Sinne der SOTIF.“

Iterativer Ansatz bei SOTIF

Trotz der Ähnlichkeit gibt es Unterschiede in den Prozessschritten zwischen FuSa und SOTIF, denn zum Erreichen von SOTIF wird in der Regel ein iterativer Ansatz bevorzugt mit explorativen Analyse- und Testmethoden (siehe Kasten Seite 38). „Das bedeutet: Die Entwicklerinnen und Entwickler spezifizieren, testen und überarbeiten die Auslegung des Systems so lange, bis ein vertretbares Restrisiko erreicht ist“, berichtet Dennis Müller, Entwicklungsingenieur bei Porsche Engineering. Um beispielsweise die komplexe Entwicklung und Absicherung von Fahrassistenzsystemen und autonomen Fahrfunktionen zu bewältigen, bietet Porsche Engineering seinen Kunden ein umfassendes Lösungs-Portfolio, das beide Sicherheitsmethoden SOTIF und FuSa beinhaltet.

„Wir unterstützen unsere Kunden unter anderem bei der Anwendung der relevanten Normen wie ISO 26262 (FuSa) und ISO 21448 (SOTIF). Dies umfasst die Implementierung in bestehende Entwicklungsprozesse, die Durchführung von Gefahren- und Risikoanalysen, die Erstellung von Sicherheitskonzepten und die Begleitung des gesamten Safety-Lifecycles“, erklärt Müller. „Bei Porsche Engineering gewährleisten wir die sicherheitskonforme Entwicklung nach FuSa und SOTIF durch klar definierte, integrierte Prozesse mit festgeschriebenen Verantwortlichkeiten. Das garantiert Normenkonformität und lückenlose Nachverfolgbarkeit.“

Porsche Engineering verfügt über langjährige Expertise entlang der gesamten Entwicklungskette: Von der Anforderungserstellung über die Simulation bis hin zur realen Fahrzeugerprobung werden modernste Simulations- und Testmethoden genutzt, unter anderem für die Entwicklung von Warnfunktionen, Parksystemen und (teil)autonomen Fahrfunktionen. Hierbei setzen die Experten-Teams unter anderem auf die modulare Softwarekomponente „Guardian". Sie wurde entwickelt, um den Übergang von fortschrittlichen Level-2-Systemen zum hochautomatisierten Fahren gemäß Level 3 zu erleichtern. Sie bietet eine robuste, sichere und standardkonforme Lösung für die Implementierung von Sicherheitskomponenten für autonome Fahrsysteme. Durch die Analyse von realen Fahrdaten werden potenziell kritische Situationen und Grenzfälle, sogenannte „Corner Cases" und „Edge Cases", explorativ identifiziert und für die datengetriebene Szenarien- Generierung verwendet. Mit steigender Verantwortlichkeit des Systems werden auch die Herausforderungen an das System immer größer. In puncto Funktionale Sicherheit bestehen sie vorrangig darin, dass sich Degradations- und Warnkonzepte nicht mehr allein auf die Fahrerin oder den Fahrer verlassen können, der beim assistierten Fahren (Level 1) und beim teilautomatisierten Fahren (Level 2) alleine die Verantwortung für alle Fahrzeugmanöver trägt.

Dies ändert sich ab Level 3: Hier müssen die Systeme selbstständig mit Fehlern umgehen können, da die permanente Aufmerksamkeitspflicht der Fahrerin oder des Fahrers ab diesem Level entfällt. Nur wenn die Systeme an ihre Grenzen stoßen, muss nach einer angemessenen Vorwarnzeit eingegriffen werden können. Grundsätzlich muss also die sichere Betriebsfähigkeit beim Auftreten von Fehlerzuständen weiterhin gewährleistet werden, zumindest für eine gewisse Zeit – infolgedessen ist der Sprung von Level 2 zu Level 3 anspruchsvoll. Die Anzahl der Redundanzen in der Fahrzeugelektronik nimmt stark zu – und damit steigen auch der Entwicklungsaufwand und die -kosten. Bezogen auf SOTIF besteht die Herausforderung in der Tiefe und Breite der Menge aller möglichen Betriebsszenarien, die die Funktion beherrschen soll.

„Dazu zählen unter anderem die sich kontinuierlich ändernde Fahrzeugumgebung, das Verhalten der Verkehrsteilnehmerinnen und -teilnehmer sowie unvorhersehbare Ereignisse, sogenannte Unknown Unsafe Scenarios", sagt Hudec. Um diese Komplexität zu beherrschen, werden Systeme zunächst für einen definierten Betriebsbereich (Operational Design Domain, ODD) ausgelegt. Somit werden die Absicherungsszenarien auf einen systematisch abgeleiteten Raum eingegrenzt, der durch ein Szenarienportfolio in diskrete Einzelszenarien aufgeteilt wird. Das System muss sicherstellen, dass die Annäherung an die Grenze dieses Bereichs frühzeitig erkannt wird, damit die Übergabe an die Fahrerin bzw. den Fahrer oder das sichere Anhalten des Fahrzeugs noch innerhalb des abgesicherten Auslegungsraums möglich ist. „Für die Fahrerassistenzentwicklung ist dieser Ansatz enorm wichtig: Je mehr Verantwortung ein System für das eigentliche Fahren übernimmt, desto kritischer wird die Betrachtung der Sicherheitsaspekte von FuSa und SOTIF", erklärt Müller.

Mehr Sicherheit durch Redundanz

Ein konkretes Beispiel aus der Praxis, um die unterschiedlichen, aber komplementären Ansätze von FuSa und SOTIF zu verdeutlichen, ist eine SAE-Level-3- Situation für automatisiertes Fahren auf der

Autobahn, bei dem die Fahrerin oder der Fahrer die Verantwortung vollständig abgibt. Geht es um die Beherrschung von Hardware- oder Software-Ausfällen, ist die FuSa gefragt: Angenommen, der Radarsensor, der den Abstand zum vorausfahrenden Fahrzeug misst, hat einen Hardware- Defekt und liefert keine Daten mehr. Dieser exemplarische Fehlerfall könnte dazu führen, dass sich die Funktion auf veraltete oder invalide Sensordaten verlässt und unter Umständen ein Auffahrunfall droht. Die Expertinnen und Experten bei Porsche Engineering identifizieren daher solche Fehler durch deduktive und induktive Sicherheitsanalysen, die durch Sicherheitsmechanismen belegt werden müssen. In diesem konkreten Fall wäre beispielsweise eine Redundanz zielführend, damit dieser lokale Einzelfehler nicht zur „globalen Nichtverfügbarkeit" der Sensordaten führt, zumindest bis zu dem Zeitpunkt, zu dem die Fahrerin oder der Fahrer wieder selbst die Fahrverantwortung übernimmt.

Geht es um die Beherrschung von Leistungsgrenzen beim automatisierten Fahren auf der Autobahn, greift SOTIF. Zum Beispiel muss die Fahrzeugerkennung so ausgelegt sein, dass alle anderen Fahrzeuge, die sich rund um das eigene Fahrzeug befinden oder sich ihm annähern, erkannt werden, also auch alle Motorräder. Aufgrund der generellen, technisch bedingten Leistungsgrenzen der benutzten Sensoren könnte es jedoch in der Praxis vorkommen, dass das Fahrzeug bestimmte schmale Silhouetten und Annährungs-Trajektorien unter ungünstigen Licht- oder Wetterbedingungen nicht korrekt erkennt. Obwohl die Hardware und die Software fehlerfrei arbeiten, könnte dies dazu führen, dass die Funktion einen Spurwechsel einleiten möchte, der ein Kollisionsrisiko mit einem überholenden Motorrad zur Folge haben könnte. In diesem Fall sehen die SOTIF-Prozesse vor, dass die Auslegung über alle Betriebsszenarien analysiert und validiert wird und die erkannten Schwächen mit der nächsten Auslegungsschleife (Update der Spezifikation und somit auch Umsetzung) behoben werden. Dabei könnten beispielsweise zusätzliche Kameras und Lidar-Sensoren im Hinterwagen eingebaut oder die Algorithmen der Sensorfusion optimiert werden.

„Die größte Herausforderung liegt nicht mehr nur im System selbst, sondern in der fast unendlichen Komplexität der Realität. Man kann nicht jede denkbare Situation vorab testen, muss aber eine ausreichende Abdeckung des Betriebsbereichs erreichen. Entsprechend aufwendig ist der Entwicklungsprozess. SOTIF stellt das Leitwerk, um die Grenzen des Systems zu verstehen und sicher zu gestalten, auch wenn alle Systemkomponenten perfekt funktionieren", erläutert Müller.

Den qualitativen und quantitativen Nachweis zu führen, dass ein System sicher ist, erfordert große Mengen von Testdaten, die zu einem erheblichen Teil mittels Simulation erbracht werden. Die größte Herausforderung ist der Umgang mit „Unknown Unsafe Scenarios" – also gefährlichen Situationen, die bei der Entwicklung aufgrund unzureichender Spezifikation nicht berücksichtigt wurden oder durch geänderte Bedingungen im Betriebsbereich auftreten könnten. Diese zu entdecken und zu minimieren, ist das Kernziel von SOTIF und eine große Herausforderung in der Entwicklung der Systeme. „Wir bei Porsche Engineering bieten unseren Kunden nicht nur einzelne Testdienstleistungen, sondern eine enge und langfristige Zusammenarbeit, um die enormen Anforderungen an die ADAS/AD-Entwicklung zu meistern und sichere, robuste und zuverlässige Funktionen auf die Straße zu bringen", verspricht Hudec.

Methoden wie die KI-basierte Erkennung von Corner Cases oder speziell trainierte KI-Modelle werden

die Entwicklerinnen und Entwickler zukünftig zunehmend dabei unterstützen. Schon heute steht fest: Die Absicherung von Systemen mit KI-Komponenten wird zukünftig noch komplexere Nachweisverfahren erfordern. Einen diesbezüglichen Rahmen soll unter anderem der neue internationale Normentwurf ISO/PAS 8800 definieren, der sich mit der Absicherung Künstlicher Intelligenz, die Teil vom Endprodukt ist, beschäftigt. Ebenfalls neu ist der internationale Normentwurf ISO/TS 5083, der speziell auf das Thema Absicherung autonomer Fahrfunktionen des Fahrzeugs fokussiert und dabei das Zusammenspiel relevanter Komponenten intern und extern (neu) berücksichtigt (sogenannte Holistic Safety). Die sicherheitsgerichtete V2X-Kommunikation von Fahrzeugen untereinander und mit der Infrastruktur bringt nicht nur neue sicherheitserhöhende Möglichkeiten mit sich, sondern auch neue potenzielle Fehlerquellen und Abhängigkeiten. Auch diese müssen mit der gleichen Konsequenz abgesichert werden – ein anspruchsvoller Prozess, dem sich die Expertinnen und Experten bei Porsche Engineering täglich widmen.

Zusammengefasst

Die Anforderungen an die Funktionale Sicherheit von Fahrzeugen steigen aufgrund der Verbreitung von Assistenzsystemen deutlich an. Die Performance des korrekt implementierten Systems in Grenzfällen steht bei SOTIF im Mittelpunkt. Porsche Engineering nutzt unter anderem datengetriebene und KI-basierte Methoden, um die Komplexität zu beherrschen und somit zuverlässige Systeme auf die Straße zu bringen.

Info

Text erstmals erschienen im Porsche Engineering Magazin, Ausgabe 1/2025.

Text: Ralf Bielefeldt

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/de_CH/2025/innovation/porsche-engineering-funktionale-sicherheit-entwicklung-moderne-fahrzeugsysteme-41258.html

External Links
https://newsletter.newsroom.porsche.com/prod/pag/NewsletterNewsroom.nsf/NewsletterActions?ReadForm&action=subscribe&language=PCH-de
https://newsroom.porsche.com/de/innovation/porsche-engineering.html