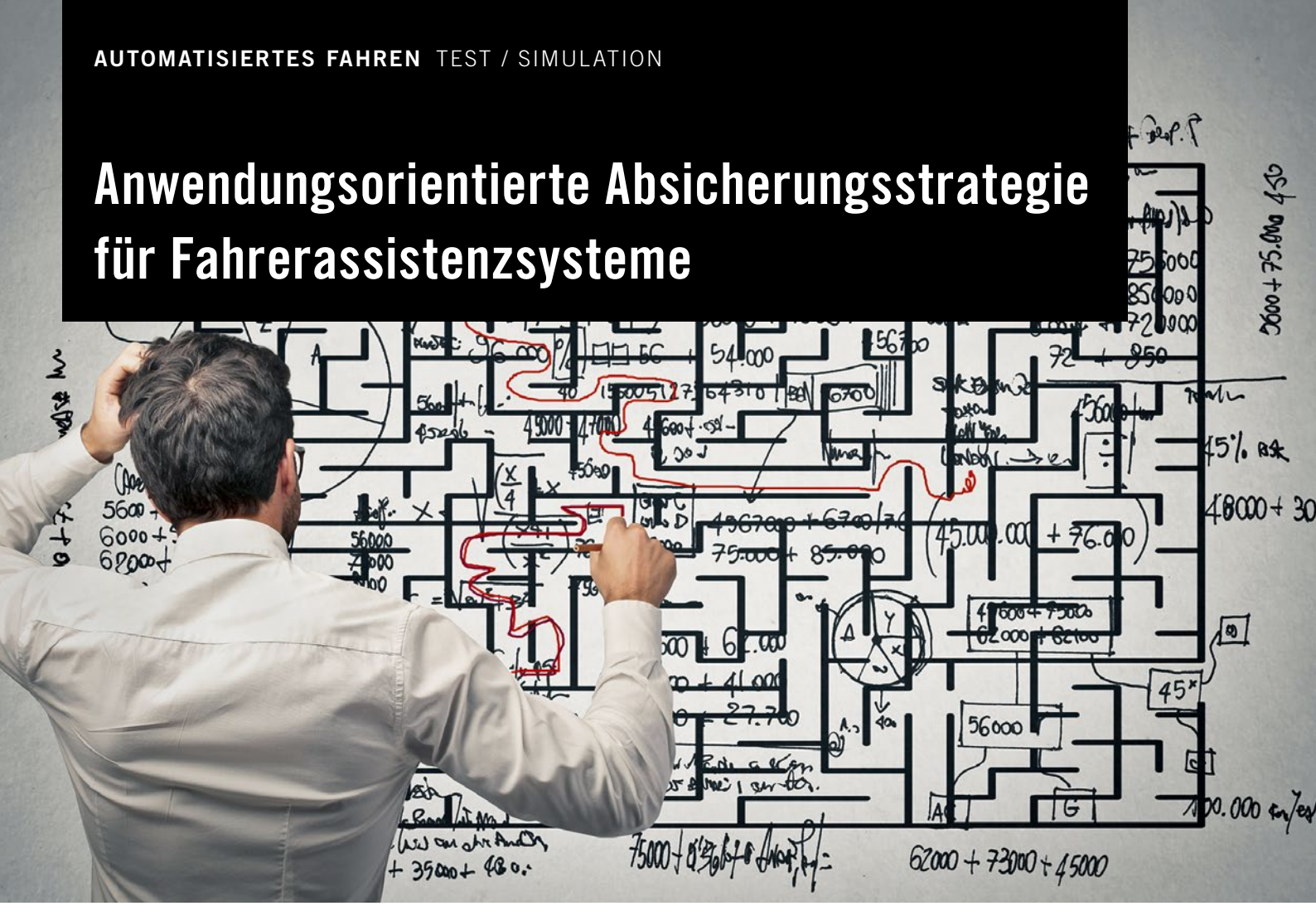
Anwendungsorientierte Absicherungsstrategie für Fahrerassistenzsysteme



© olly I fotolia

AUTOREN

Marius Feilhauer, M. Sc.
entwickelt Simulationsmodelle für Fahrerassistenzsysteme im Bereich Test und Validierung bei der Etas GmbH in Stuttgart.

Dr.-Ing. Jürgen Häring
ist Leiter des Produktmanagements im Bereich Test und Validierung bei der Etas GmbH in Stuttgart.

Die Ergänzung realer Testfahrten mit Simulationen bietet ein enormes Potenzial, den Absicherungsprozess effizient zu gestalten. Dabei gilt es, die Tests ständig mit dem realen Verkehrsgeschehen abzugleichen und den zugrundeliegenden Szenarienkatalog iterativ zu erweitern.

DIE ZUKUNFT IM BLICK

Noch ist unklar, wie Autofahrer die Zeit nutzen werden, die autonom fahrende Fahrzeuge ihnen verschaffen. Manche werden ihren Blick in die Ferne schweifen lassen, andere Zeitung lesen, E-Mails beantworten oder am Laptop spielen. Wieder andere werden das Steuer in der Hand behalten, weil sie Lust am Fahren haben. Sollte sie ihnen vergehen, kann der Autopilot ja immer noch übernehmen.

All das setzt voraus, dass die Passagiere den aktiven Fahrzeugsystemen vertrauen. Mit jedem Schritt in Richtung des automatisierten Fahrens wächst die Verantwortung der Fahrzeughersteller und ihrer Entwickler. Es bedarf zuverlässiger Absicherungsstrategien für autonome Fahrzeuge, die anstelle des Fahrers das Verkehrsgeschehen beobachten, es analysieren und auf dieser Basis die komplette Fahraufgabe übernehmen.

DIE KOMPLEXE UMGEBUNG LÄSST SICH NICHT VORAB SPEZIFIZIEREN

Die Erfordernisse dieser Systemabsicherung gehen über jene Anforderungen an die funktionale Sicherheit hinaus, die in der ISO 26262 definiert sind. Denn es genügt nicht, die aktiven

Assistenzsysteme auf den Fall eines Systemversagens auf funktionaler Ebene vorzubereiten. Vielmehr gilt es, sie gegen situative Fehlinterpretation abzusichern. Jedoch lassen sich im Rahmen einer vorab erstellen Systemspezifikation nicht alle Eventualitäten des realen Verkehrsgeschehens erfassen. Zu umfangreich sind die unterschiedlichsten Verkehrsszenarien im Stadtverkehr, auf Landstraßen und Autobahnen. Hinzu kommen vielfältige Wetterbedingungen, wie Nebel oder Schneetreiben, unterschiedliche Lichtverhältnisse und in verschiedenen Ländern jeweils eigene Verkehrsregeln und kulturelle Konventionen.

Diese Problematik wird in [1] als „funktionale Unzulänglichkeit" beschrieben. Im Rahmen der Softwarequalität wird eine entsprechende Problematik durch den Begriff „Robustheit" beschrieben. Robustheit charakterisiert die „Eigenschaft einer Betrachtungseinheit (…), auch in ungewöhnlichen Situationen definiert zu arbeiten und sinnvolle Reaktionen durchzuführen" [2]. Diese Beschreibung zeigt, dass sich im Umfeld von Softwaresystemen im Allgemeinen nicht alle Zustände mit akzeptablem Aufwand vorab identifizieren lassen. Übertragen auf die Absicherung der Assistenzsysteme impliziert dies einerseits, dass sich eine vollständige Unfallfreiheit nicht per se realisieren lässt. Andererseits führt es zu der Frage, wie sich die Robustheit autonomer Systeme auf ein gesellschaftlich akzeptables Niveau bringen und kontinuierlich verbessern lässt.

VERLÄSSLICHE ABSICHERUNGSSTRATEGIEN SIND GEFRAGT

Hier stellen wahrscheinlichkeitsbasierte Absicherungsansätze ein Mittel dar, um die Robustheit und den Nutzen der Assistenzsysteme bewerten zu können. Ob diese Ansätze gesellschaftliche Akzeptanz finden, kann hier nicht abschließend beantwortet werden. Der Vorsitzende des deutschen Ethikrats, Peter Dabrock, plädiert in [3] für ein pragmatisches Herangehen. Statt vorab in „manische Beschäftigung mit Gedankenexperimenten" zu verfallen, sei es ratsam, den Transformationsprozess hin zum automatisierten Fahren anhand jeweils aktualisierter Dokumentationen immer wieder aufs Neue zu prüfen und zu bewerten.

Pragmatismus in der ethischen Bewertung entbindet Fahrzeugentwickler aber nicht vom Anspruch, Systeme auf höchstmöglichem Sicherheitsniveau zu realisieren. In [4] wird exemplarisch ein wahrscheinlichkeitsbasierter Absicherungsansatz eines Autobahnautomaten vorgestellt. Daraus geht hervor, dass es schon in diesem vergleichsweise einfachen Anwendungsfall einer Fahrstrecke von $2{,}4 \cdot 10^8$ Kilometern bedarf, um nachzuweisen (bei 5 % Irrtumswahrscheinlichkeit), dass Fahrzeuge mit dem Assistenzsystem auf Autobahnen höchstens halb so viele Unfälle mit Personenschäden verursachen, wie Fahrzeuge ohne solche Systeme.

ÄQUIVALENZKLASSEN-BASIERTE SZENARIOBESCHREIBUNG

Ziel einer solchen Absicherung ist der Nachweis, mit welcher Wahrscheinlichkeit P ein System eine Metrik M erfüllt (die Metrik M könnte beispielsweise lauten: Mit dem Assistenzsystem ausgestattete Fahrzeuge dürfen nur halb so viele Unfälle mit Personenschaden verursachen wie Fahrzeuge ohne das Assistenzsystem). Aufgrund des Einsatzortes d_E=Autobahn ist die Wahrscheinlichkeit bedingt durch $P\,(M \mid \text{Autobahn})$.

Soll das Systemverhalten auch außerhalb der Autobahn betrachtet werden, so ergibt sich der Einsatzort d_E= Nicht-Autobahn. Dadurch ergibt sich die Gesamtwahrscheinlichkeit zur Erfüllung der Metrik, **GLEICHUNG 1**.

Gl. 1
$$P_{ges}(M) = P(M \mid \text{Autobahn}) \cdot P(\text{Autobahn}) + P(M \mid \text{Nicht-Autobahn}) \cdot P(\text{Nicht-Autobahn})$$

Zeigt sich in Testfahrten, dass sich der Bereich Nicht-Autobahn in die Bereiche Innerorts und Außerorts aufteilen lässt, innerhalb derer sich das System jeweils äquivalent verhält (Äquivalenzklassen, vgl. [2]), so lässt sich die Dimension Einsatzort vollständig in die drei Äquivalenzklassen d_E={Autobahn, Innerorts, Außerorts} aufteilen. Die Betrachtung der Metrik ist somit auf dem klassifizierten Parameterraum vollständig.

Bei detaillierter Untersuchung einer Testkampagne könnte sich herausstellen, dass das System auf trockener Straße einwandfrei arbeitet, auf nasser Straße jedoch häufig versagt. Dieser Erkenntnisgewinn kann durch die Einführung einer weiteren Dimension Straßenbeschaffenheit d_S={trocken, nass} in die Beschreibung aufgenommen werden. Damit ergeben sich sechs Szenarien, in denen die Metrik überprüft werden muss.

Allgemein lässt sich ein Szenario S als die Kombination je einer Äquivalenzklasse jeder Dimension definieren $S=[d_1, d_2, \ldots, d_n]$. Die Gesamtwahrscheinlichkeit zur Erfüllung der Metrik ergibt sich allgemein für n Dimensionen d_n, **GLEICHUNG 2**,

Gl. 2
$$P_{ges}(M) = \sum_i P(M \mid S_i) \cdot P(S_i)$$

wobei sich die Anzahl i an Szenarien aus der Mächtigkeit an Äquivalenzklassen aller Dimensionen zu $i=\prod \mid d_n \mid$ ergibt.

Die Bestimmung $P\,(M \mid S_i)$ bedarf im Experiment konkreter Testfälle. Ein Testfall ist ein Repräsentant eines Szenarios (vgl. [5]). Bei der Auswahl der Testfälle können Methoden aus dem Bereich der Softwarequalität verwendet werden. Die Gesamtsumme unterschiedlicher Szenarien dient als Referenzgröße der Anzahl unterschiedlicher Testfälle und ist für eine belastbare Absicherung des Systems essenziell.

ITERATIVE ERWEITERUNG DER SZENARIOBESCHREIBUNG

Diese äquivalenzklassen-motivierte, sich iterativ verfeinernde Szenariobeschreibung kann nun in einem anwendungsorientierten Prozess zur Absicherung von autonomen Systemen angewandt werden, der in **BILD 1** visualisiert ist.

Im Zentrum der iterativen Absicherungsstrategie steht ein Szenarienkatalog. Drei qualitativ unterschiedliche Quellen (A) liefern Informationen zum Aufbau des Katalogs. In diesen fließen einerseits Ereignisse aus Dauerläufen und Felderprobungen ein, in denen das System nicht wie erwartet reagiert hat. Andererseits lassen sich für den Katalog weitere Szenarien konstruieren, wobei neben Systemspezifikationen auch Experteneinschätzungen herangezogen werden können. Zusätzlich können statische Quellcodeanalysen weitere Szenarien liefern.

Mit einem solchen Szenarienkatalog wird nicht nur ein Ablaufplan zur Syste-

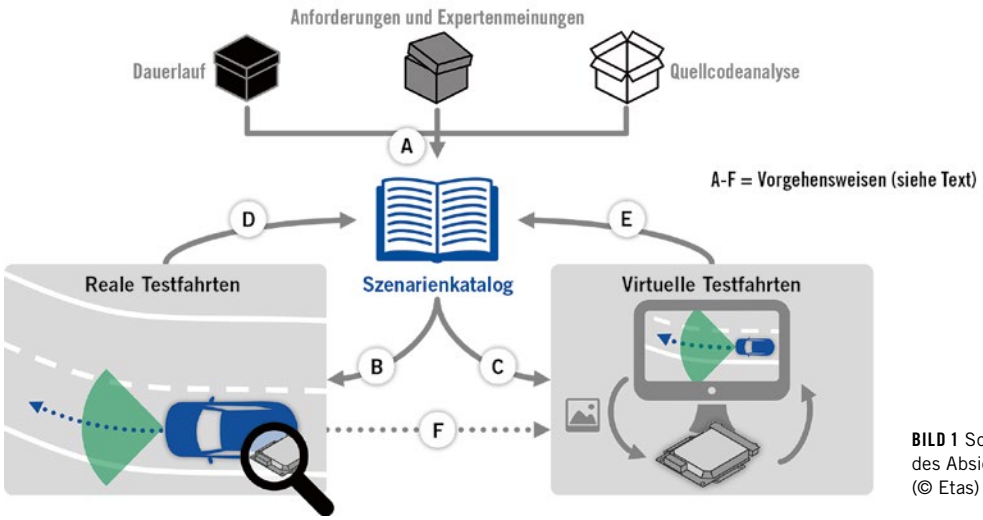


BILD 1 Schematische Darstellung des Absicherungsansatzes (© Etas)

matisierung realer Testfahrten gewonnen (B). Vielmehr kann er zudem als Parametrierung virtueller Testfahrten dienen (C), die gleich mehrere Vorteile miteinander verbinden. Diese Tests können parallel auf beliebig vielen Rechnern ausgeführt werden. Sie sind also nicht von der Verfügbarkeit teurer Versuchsfahrzeuge abhängig. Zum reduzierten Kosten-, Zeit- und Organisationsaufwand kommt ein weiterer Vorteil: Kritische Situationen, die in Testfahrten aufgetreten sind, lassen sich im virtuellen Versuch frei nach Bedarf reproduzieren und abwandeln.

Durch die systematische oder zufällige Variation von Repräsentanten eines Szenarios in Testfahrten können neue Szenarien identifiziert werden, innerhalb derer das System nicht die gewünschte Reaktion zeigt. Nach deren Analyse können die neu entdeckten Szenarien konsequent in den Katalog zurückfließen (D und E). Diese Überführung erlaubt eine kontinuierliche Verbesserung der Testabdeckung. Bleibt diese Transition aus, so sind die in Testfahrten erkannten Probleme wertlos.

Voraussetzung für eine domänenübergreifende Gesamtsimulation von Assistenzsystemen ist die zuverlässige Validierung der zugrundegelegten Modelle. Dafür ist es nötig, die einzelnen Szenarien im realen und virtuellen Fahrversuch miteinander abzugleichen (F). Der Vergleich erlaubt verlässliche Aussagen zur Genauigkeit der Gesamtsimulation sowie zu den Gültigkeitsbereichen der Modelle. Darüber hinaus entsteht auf diese Weise nach und nach eine immer exaktere und umfassendere Basis für die virtuelle Erprobung von Assistenzsystemen.

SIMULATION ALS SCHLÜSSEL ZUR ABSICHERUNG VON SYSTEMVARIANTEN

Werden bei solchen Tests Fehler des Fahrerassistenzsystems entdeckt und beseitigt, ändert sich auch das zu testende System bei realen Testfahrten sowie $P_{ges}\ (M)$. Das erscheint zunächst problematisch, da bisher erhobene Messungen nicht mehr ohne weitere Argumentation zur Validierung herangezogen werden können. Damit stellt sich die Frage, ob der Szenarienkatalog bei Anpassungen des Systems transformierbar ist, **BILD 2**.

Zur Beantwortung der Frage muss überprüft werden, ob die eingeführten Äquivalenzklassen weiterhin äquivalent sind und wie sich $P\ (M \mid S_i)$ ändert. Ein Lösungsansatz stellt die modellbasierte Simulation dar. Denn wenn das Verhalten des Fahrerassistenzsystems auf Basis der Szenarien validiert und die Gültigkeitsbereiche der zugrundeliegenden Modelle definiert sind, kann auch das veränderte System anhand der validierten Modelle in der Simulation bewertet werden, sofern sich die Anpassungen des Systems innerhalb des Modell-Gültigkeitsbereichs bewegen. Diese Transformierbarkeit ist der Schlüssel zur Absicherung auftretender Systemvarianten.

In [6] wird beispielsweise ein physikalisch motiviertes Modell der Umfeldsensorik beschrieben. Dieses Modell kann für unterschiedliche Einbauorte eines Ultraschallsensors für spezifische Szenarien S_i validiert werden. Dadurch ergibt sich ein validierter Gültigkeitsbereich dieses Modells. Somit werden Änderungen des

BILD 2 Ist ein Szenarienkatalog bei Anpassungen des Systems transformierbar? (© Etas)

Einbauortes des realen Sensors in der Simulation bewertbar und das Modell lässt sich zur Überprüfung der Äquivalenzklassen sowie zur Bewertung von $P(M \mid S_i)$ des angepassten Systems verwenden.

FAZIT

Der dargestellte iterative Ansatz ist eine praxistaugliche Absicherungsmethodik, mit der Entwickler der Herausforderung funktionaler Unzulänglichkeit autonomer Fahrzeuge begegnen können. In den zentralen Szenarienkatalog gehen Wissen, Erfahrungen und Erkenntnisse aus Dauerläufen ein. Die gesammelten, einer gemeinsamen Beschreibung folgenden Szenarien können sowohl zur Parametrierung realer als auch virtueller Fahrversuche dienen. Die Konsistenz der Beschreibung realer und virtueller Test erlaubt es zudem, Szenarien als Validierungsgrundlage der Simulation zu nutzen. Damit bietet sich die vorgestellte Methodik an, um Prüfverfahren für sicherheitsrelevante Assistenzsysteme in autonomen Fahrzeugen zu dynamisieren und sie um eine lernende Dimension zu erweitern. Es handelt sich um einen transparenten und nachvollziehbaren Ansatz zur robusten Auslegung autonomer Fahrfunktionen.

LITERATURHINWEISE

[1] Wilhelm, U.; Ebel, S. ; Weitzel, D.: Funktionale Sicherheit und ISO 26262. Validierung von Systemen mit funktionaler Unzulänglichkeit. Bd. 3. In: Winner, H.; Hakuli, S.; Lotz, F.; Singer, C. (Hrsg.): Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort. Wiesbaden: Springer Vieweg, 2015, S. 85-103

[2] Liggesmeyer, P.: Software-Qualität: Testen, Analysieren und Verifizieren von Software. 2. Auflage. Heidelberg: Spektrum, Akademischer Verlag, 2002

[3] Dabrock, P.: Ethische Dilemmata unterlaufen oft Akzeptanz von autonomen Fahrzeugen: Ethik und autonomes Fahren. In: Tagesspiegel vom 23.03.2017

[4] Winner, H.: Quo vadis, FAS?, Bd. 3. In: Winner, H.; Hakuli, S.; Lotz, F.; Singer, C. (Hrsg.): Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort. Wiesbaden: Springer Vieweg, 2015, S. 1167-1186

[5] Schmidt, A.: Einführung in die algebraische Zahlentheorie. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg, 2007, S. 7

[6] Feilhauer, M. ; Häring, J.: Ein echtzeitfähiges Multi-Sensor Modell zur Validierung von Fahrerassistenzsystemen in einer virtuellen Umgebung. In: 3. Internationale ATZ-Fachtagung Fahrerassistenzsysteme, 2017

DOWNLOAD DES BEITRAGS
www.springerprofessional.de/ATZextra

SPRINGERNATURE