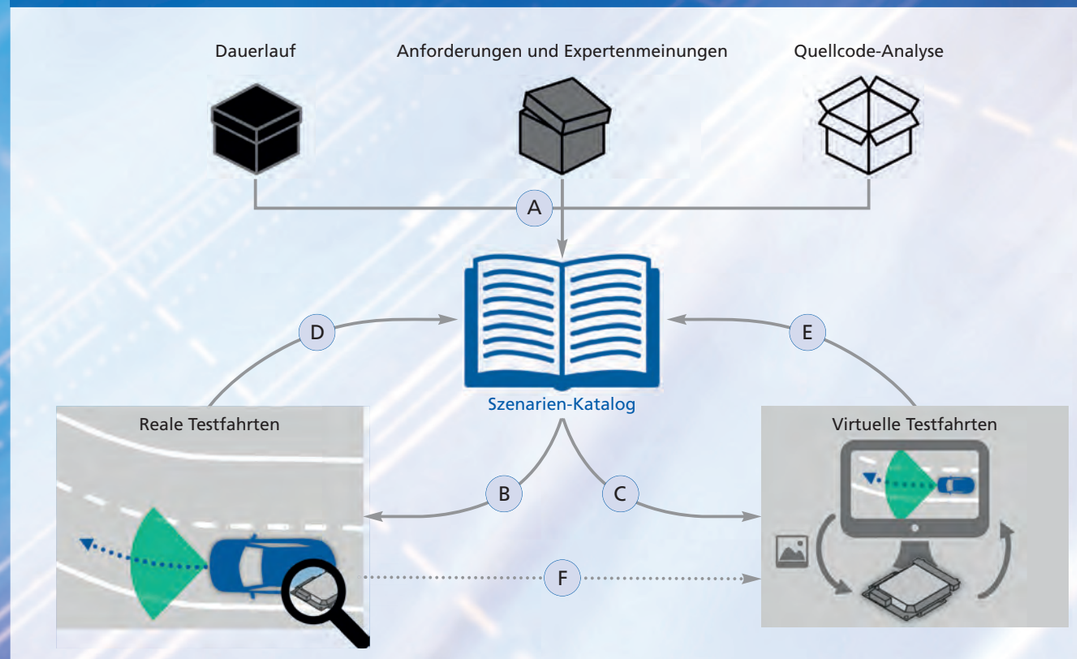
Robuste Assistenzsysteme

Iterative Absicherungsstrategie

Wie lassen sich softwaregesteuerte Assistenzsysteme für autonome Fahrzeuge effizient absichern? Da sich Verkehrsgeschehen und Umweltbedingungen vorab kaum vollständig in Systemspezifikationen erfassen lassen, sind robuste Softwaresysteme gefragt. Der Weg dahin führt über virtualisierte Tests auf Basis iterativ erweiterbarer Szenarien-Kataloge.



Schematische Darstellung des Absicherungsansatzes. A–F = Vorgehensweisen (siehe Text).

Womit werden Passagiere autonomer Fahrzeuge ihre neu gewonnene Zeit verbringen? Ob mit Büroarbeit, Onlineshopping oder Wellness bleibt dem Fahrgast überlassen. Klar ist aber, dass Autofahrer nur dann die Hand vom Lenkrad nehmen werden, wenn sie der Technik hundertprozentig vertrauen.

Es wird nicht mehr genügen, aktive Assistenzsysteme gemäß ISO 26262 auf den Fall eines Systemversagens auf funktionaler Ebene vorzubereiten. Sie müssen für das automatisierte Fahren auch gegen situative Fehlinterpretation abgesichert werden. Der Haken: Verkehrsszenarien, Wetter- und Lichtverhältnisse sind zu heterogen, um vorab alle Eventualitäten in Systemspezifikationen erfassen zu können. In der Softwarewelt hat diese Problematik einen Namen: funktionale Unzulänglichkeit.

Die Antwort darauf heißt Robustheit. Robuste Software muss auch in ungewöhnlichen Situationen definiert arbeiten und sinnvolle Reaktionen auslösen. Übertragen auf das autonome Fahren liefe das darauf hinaus, die Robustheit der softwaregesteuerten Assistenzsysteme trotz der zwangsläufig unvollständigen Spezifikationen auf ein gesellschaftlich akzeptables Niveau zu bringen – also bei allem Pragmatismus stets das höchstmögliche Sicherheitsniveau anzustreben.

Äquivalenzklassenbasierte Szenariobeschreibung

Aktuelle Fachaufsätze zeigen das Ausmaß dieser Aufgabe. So führt etwa der Darmstädter Professor Hermann Winner an einem wahrscheinlichkeitsbasierten Absicherungsansatz für einen Autobahnautomaten vor, dass schon für diese vergleichsweise einfache Anwendung **2,4 • 10^8 Kilometer** Fahrstrecke nötig wären, um nachzuweisen, dass Fahrzeuge mit diesem System auf Autobahnen maximal halb so viele Unfälle mit Personenschäden verursachen wie Fahrzeuge ohne den Autobahnautomaten.

Zur Absicherung gilt es zu klären, mit welcher Wahrscheinlichkeit **P** ein System eine Metrik **M** erfüllt. Aufgrund des Einsatzortes d_E **= Autobahn** ist diese Wahrscheinlichkeit bedingt durch: **P(M|Autobahn)**.

Soll das Systemverhalten abseits der Autobahn mitbetrachtet werden, ist der Einsatzort d_E **= Nicht-Autobahn**. Die Gesamtwahrscheinlichkeit zur Erfüllung der Metrik wird dadurch zu P_{ges}**(M) = P(M|Autobahn) • P(Autobahn) + P(M|Nicht-Autobahn) • P(Nicht-Autobahn)**.

In Testfahrten könnte sich herausstellen, dass der Einsatzbereich Nicht-Autobahn in die zwei unterschiedlichen Teile „innerorts“ und „außerorts“ aufgeteilt werden muss.

Verhält sich das zu testende System jeweils innerhalb eines klassifizierten Bereichs äquivalent, so lässt sich die Dimension Einsatzort in drei Äquivalenzklassen aufteilen: d_E **= {Autobahn, innerorts, außerorts}**.

Im Zuge einer Testkampagne könnte sich ergeben, dass das System auf trockener Straße einwandfrei arbeitet, auf nasser Straße aber häufig versagt. Dies ließe sich dann durch die Einführung einer weiteren Dimension Straßenbeschaffenheit d_S **= {trocken, nass}** in die Beschreibung aufnehmen. Damit wären bereits sechs Szenarien in der Metrik zu prüfen.

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 zu

$P_{ges}(M) = \sum P(M|S_i) \cdot P(S_i)$,

wobei sich die Anzahl an Szenarien i aus der Mächtigkeit an Äquivalenzklassen aller Dimensionen zu $i = \prod |d_n|$ ergibt. Die Bestimmung $P(M|S_i)$ bedarf im Experiment konkreter Testfälle, die jeweils ein Szenario repräsentieren. Die Gesamtsumme verschiedener Szenarien dient als Referenzgröße der Anzahl unterschiedlicher Testfälle und ist für die belastbare Absicherung des Systems essentiell.

Iterative Erweiterung der Szenario-Beschreibung

Diese Äquivalenzklassen-motivierte, iterativ verfeinerte Szenario-Beschreibung kann nun in einem anwendungsorientierten Prozess zur Absicherung autonomer Systeme angewandt werden, der in der Grafik links visualisiert ist.

Im Zentrum der iterativen Absicherungsstrategie steht ein Szenarien-Katalog, der sich aus drei Quellen (A) speist: Ereignisse aus Dauerläufen und Felderprobungen, bei denen das System nicht wie erwartet reagiert hat. Konstruierte Szenarien auf Basis von Systemspezifikationen und Experteneinschätzungen. Und weitere, aus statischen Quellcode-Analysen generierte Szenarien.

Dieser Szenarien-Katalog dient sowohl der Systematisierung realer Testfahrten (B) als auch zur Parametrierung virtueller Testfahrten (C). Letztere haben den Vorteil, dass sie von der Verfügbarkeit teurer Versuchsfahrzeuge entkoppelt und auf beliebig vielen Rechnern parallel durchführbar sind. Auch lassen sich kritische Situationen, die bei Testfahrten auftreten, nach Bedarf reproduzieren und abwandeln. Aus diesen Variationen können Entwickler neue Szenarien herleiten, diese analysieren und sie in den Katalog einfließen lassen (D, E). So ist die kontinuierliche Verbesserung der Testabdeckung gewährleistet. Zur Absicherung der domänenübergreifenden Gesamtsimulation von Assistenzsystemen ist es erforderlich, die einfließenden Modelle (F) im Abgleich realer und virtueller Fahrversuche zu validieren. Erst der Vergleich erlaubt verlässliche Aussagen zur Genauigkeit der Gesamtsimulation und zu den Gültigkeitsbereichen der Modelle. Zudem führt er nach und nach zu einer immer exakteren, umfassenderen Grundlage für die virtuelle Erprobung von Assistenzsystemen. Virtualisierung wird dadurch zum Schlüssel für steigende Qualität bei zugleich sinkendem Kosten-, Zeit- und Organisationsaufwand.

AUTOREN

Marius Feilhauer betreut die Entwicklung von Simulationsmodellen für Fahrerassistenzsysteme im Bereich Test und Validierung bei der **ETAS GmbH**.

Dr. Jürgen Häring ist Leiter des Produktmanagements im Bereich Test und Validierung bei der **ETAS GmbH**.