9. Tagung Automatisiertes Fahren

21. – 22. November 2019, München

Definition von Bestehens-/Versagenskriterien für das partikuläre Testen von automatisierten Fahrfunktionen

Moritz Lippert*, Björn Klamann*, Christian Amersbach* und Hermann Winner†

Themenkreis: Absicherung und Freigabe
Schlagwörter: UNICAR*agil*, Absicherung, Freigabe, Sicherheitsnachweis, Testfallgenerierung, Testkriterien

Zusammenfassung: Der Absicherungsaufwand automatisierter Fahrzeuge spielt für deren Freigabe und Markteinführung eine zentrale Rolle. Konventionelle Methoden zur Absicherung erlauben derzeit keine Einführung des automatisierten Fahrens auf öffentlichen Straßen. Neben neuen Methoden wie dem szenariobasierten Ansatz, der den Absicherungsaufwand auf Gesamtsystemebene reduzieren soll, besteht die Möglichkeit, das Gesamtsystem in Subsysteme aufzuteilen und diese unabhängig voneinander abzusichern. Im Projekt PEGASUS wurde bereits eine Methodik entwickelt, die das Gesamtsystem in funktionale Ebenen dekomponiert und auf diese Weise den Testparameterraum reduziert. Für eine höhere Kontrollierbarkeit des Parameterraums wird das Gesamtsystem im Projekt UNICARagil in mehrere Module unterteilt. Dieses Paper zeigt Herausforderungen dieser beiden Ansätze auf und stellt eine Methodik zur Definition von partikulären Bestehens- und Versagenskriterien vor, um diesen Problemen zu begegnen. Mithilfe von bewährten Methoden zur Fehler- und Gefahrenanalyse werden zunächst Versagensursachen auf Basis von zuvor definierten Sicherheitszielen abgeleitet. Anhand dieser Versagensursachen werden anschließend Sicherheitsanforderungen und daraus abgeleitet Bestehens- und Versagenskriterien definiert. In diesem Paper wird diese Methodik darüber hinaus an einem Beispiel angewendet sowie eine Definition von Schwellwerten zur Testbarkeit der abgeleiteten Kriterien anhand eines ausgewählten Anwendungsfalls vorgestellt.

1 Motivation

Einer der größten, bislang ungelösten Herausforderungen bei der Freigabe von hochautomatisierten Fahrzeugen (HAF, Level 3 oder höher nach [1]) ist der Sicherheitsnachweis. Die Frage „*Wie sicher ist sicher genug?*“ ist nach wie vor Teil verschiedener Forschungsprojekte, da eine ganzheitlich akzeptierte Antwort noch nicht gefunden wurde. Darüber hinaus muss die Erfüllung der Sicherheitsanforderungen der HAF nachgewiesen werden, wodurch die Entwickler in die sog. *Freigabefalle* tappen [2, S. 437].

Der szenariobasierte Testansatz wird derzeit als einer der vielversprechendsten Ansätze zur Bewältigung dieser Herausforderung diskutiert [3]. Dieser Ansatz bringt jedoch neue Herausforderungen mit sich, da die entstehende, hohe Zahl an Einflussparametern zu einer Parameterraumexplosion und somit zu einem sehr hohen Testaufwand führt. Dennoch hat das Testen von unabhängigen Teilfunktionen im Gegensatz zu Gesamtsystemtests das Potential, den Absicherungsaufwand von HAF zu reduzieren [4]. Um dieses Potential ausschöpfen zu können, müssen zunächst geeignete Bestehens- und Versagenskriterien zur Bewertung der partikulären Tests definiert werden.

* Wissenschaftlicher Mitarbeiter am Fachgebiet Fahrzeugtechnik der TU Darmstadt, Otto-Berndt-Straße 2, 64287 Darmstadt

(✉ {lippert, klamann, amersbach}@fzd.tu-darmstadt.de, ☎ +49 (0) 6151/16-24201).

† Hermann Winner ist Leiter des Fachgebiets Fahrzeugtechnik der TU Darmstadt, Otto-Berndt-Straße 2, 64287 Darmstadt (✉winner@fzd.tu-darmstadt.de, ☎ +49 (0) 6151/16-24200).

2 Stand der Technik

2.1 Sicherheitsanforderungen für HAF

Die Beantwortung der Frage „Wie sicher ist sicher genug?“ ist möglich, indem Sicherheitsanforderungen definiert werden. Dabei wird zwischen Sicherheitsanforderungen auf makroskopischer und mikroskopischer Ebene unterschieden.

2.1.1 Makroskopische Sicherheitsanforderungen für HAF

Junietz et al. [5] analysieren die Risikoakzeptanz involvierter Interessensgruppen, um makroskopische Sicherheitsanforderungen für HAF zu definieren. Diese Anforderungen basieren bspw. auf Unfallraten pro gefahrenem Kilometer anstatt auf spezifischen Fahrsituationen. Dazu nutzen sie die aktuelle Sicherheit des heutigen Straßenverkehrs als Referenz und wenden bekannte Konzepte aus anderen Bereichen, wie z.B. ALAREP (as low as reasonably possible), MEM (minimum endogenous mortality) und GAMAB (globalement au moins aussi bon) an. Sie folgern daraus, dass die Risikoakzeptanz der verschiedenen Interessensvertreter von dem Marktanteil der HAF abhängig ist. Bei einem Marktanteil von ca. 10 % folgt daraus eine dominierende Rolle der Sicherheitsanforderungen basierend auf dem Teil der Gesellschaft, der die HAF nicht nutzt. Somit müssten HAF 1,3-mal so sicher sein wie der heutige Verkehr (auf deutschen Autobahnen). Ein steigender Marktanteil würde die geforderte Sicherheit allerdings weiter erhöhen.

Liu et al. [6] nutzen zur Bestimmung von Risikoakzeptanzraten für HAF eine Umfrage. Das Ergebnis ist eine vier- bis fünffach höhere, geforderte Sicherheit der HAF im Vergleich zur heutigen Verkehrssicherheit. Dabei wird sich auf den chinesischen Straßenverkehr bezogen, ohne einen Marktanteil der HAF zu berücksichtigen.

2.1.2 Mikroskopische Sicherheitsanforderungen für HAF

Mikroskopische Sicherheitsanforderungen sind spezifische Sicherheitsanforderungen bspw. für individuelle Fahrzeuge, Komponenten oder auch Fahrsituationen. Diese können unter verschiedenen Sicherheitsaspekten betrachtet und definiert werden [7, S. 11].

2.1.2.1 Verhaltenssicherheit

Die Verhaltenssicherheit beschreibt wie sich ein System im Betrieb verhalten sollte, damit keine Gefährdung von diesem ausgeht. Prinzipiell wird das Verhalten eines Fahrzeugs in dessen Bewegung sowie Interaktion mit der Umwelt und anderen Verkehrsteilnehmern ausgedrückt. Nolte et al. [8] definieren den Begriff „Äußerliches Verhalten“ detaillierter, um das sichtbare Verhalten eines Fahrzeugs zu beschreiben und auf diese Weise den Einfluss auf den umgebenden Verkehr und die damit verbundenen Gefahren besser verstehen zu können. Da „Sicherheit“ eine Abwesenheit von Gefahren impliziert, beschäftigt sich die Verhaltenssicherheit mit gefahrenfreien, sichtbaren Handlungen von automatisierten Fahrzeugen. Somit liefern die Verkehrsregeln einen ersten regulatorischen Rahmen für das Verhalten von HAF, der durch weitere rechtliche Einschränkungen erweitert wird. Innerhalb dieses regulatorischen, gesetzlichen Rahmens muss ein automatisiertes Fahrzeug in der Lage sein, die aus den vorliegenden Fahrszenarien resultierenden Fahraufgaben zu bewältigen.

Im Projekt UNICAR*agil* wird die Verhaltenssicherheit genutzt, um Anforderungen basierend auf verschiedenen Straßenkategorien zu definieren. Diese Anforderungen müssen von den Fähigkeiten eines HAF erfüllt werden, damit eine Freigabe für die Streckenabschnitte innerhalb der jeweiligen Straßenkategorie erfolgt.

Die Absicherung einer Kategorie resultiert gleichzeitig in einer Absicherung aller korrespondierender Streckenabschnitte, sodass eine schrittweise Freigabe erlaubt wird. Auf diese Weise kann die Verhaltenssicherheit einen Beitrag zur Reduzierung des Absicherungsaufwands leisten, da Kategorie für Kategorie getestet wird [9].

2.1.2.2 Funktionale Sicherheit

Die funktionale Sicherheit betrachtet systematische und zufällige Fehler von Komponenten sowie deren Behandlung. Nach ISO 26262 [10] wird eine Gefahrenanalyse und Risikobewertung (HARA, Hazard Analysis and Risk Assessment) durchgeführt, um mögliche Gefahren zu identifizieren und dem Risiko entsprechende ASIL (Automotive Safety Integrity Level) zuzuweisen. Zur Vermeidung von unzumutbarem Risiko werden Sicherheitsziele, die Sicherheitsanforderungen auf einer allgemeineren Ebene darstellen, abgeleitet. Die Sicherheitsziele werden dann auf Sicherheitsanforderungen beeinflusster Komponenten heruntergebrochen. In der ISO 26262 werden für die HARA verschiedene Methoden wie die FTA (Fault Tree Analysis, Fehlerbaumanalyse) oder FMEA (Failure Mode and Effect Analysis, Fehlermöglichkeits- und -einflussanalyse) empfohlen. Neben diesen haben sich darüber hinaus weitere Methoden etabliert. Stolte et al. [11] nutzen bspw. die STPA (System Theoretic Process Analysis, Systemtheoretische Prozessanalyse) für die Ableitung von Sicherheitszielen und –anforderungen für Antriebssysteme von HAF.

2.1.2.3 Passive Sicherheit

Die passive Sicherheit beschäftigt sich mit der Reduzierung der Unfallschwere, sodass die involvierten Personen so wenig Schaden wie möglich im Fall einer Kollision nehmen. Per Gesetz werden für eine notwendige Typenzulassung minimale Unfallsicherheitsanforderungen vorgeschrieben. Darüber hinaus definieren Gesellschaften wie Euro/US NCAP (New Car Assessment Program, Neuwagen-Bewertungs-Programm) zusätzliche Anforderungen, die zum einen Testspezifikationen und zum anderen Bewertungskriterien beinhalten. Diese Anforderungen werden kontinuierlich bis hin zu aktiven Sicherheitsmaßnahmen von HAF erweitert [12, S. 59-65].

2.1.2.4 Gebrauchssicherheit

Die Gebrauchssicherheit adressiert die Interaktion zwischen Fahrzeugen und mit dem Fahrzeug interagierenden Personen. Ein Beispiel von Gebrauchssicherheit ist die sog. Mode-Confusion [13]. Darüber hinaus beschreibt sie die Einhaltung des tolerierten Risikos bei Interaktionen mit dem System außerhalb der Ausführung der eigentlichen Hauptfunktion. Hierzu zählen bspw. Reparaturen oder Wartungen bei denen Personen vor Gefahren wie scharfen Kanten oder vor elektrischem Schock geschützt werden.

2.1.2.5 IT-Sicherheit

Neben den zuvor genannten Sicherheitsaspekten muss bei einem Sicherheitsnachweis von HAF die IT-Sicherheit berücksichtigt werden, da diese die Sicherheitsanforderungen beeinflusst und umgekehrt [14]. Eine Definition von IT-Sicherheitsanforderungen wird auf Basis der SAE J3061 [15] vorgenommen.

2.2 Aktuelle Testkonzepte und die Freigabefalle

Das Sicherheitskonzept aktueller FAS (Fahrerassistenzsysteme, SAE Level 1 & 2) stützt sich auf die permanente Kontrolle des/der menschlichen Fahrers/Fahrerin über das Fahrzeug. In der Entwicklung von FAS wird angenommen, dass der/die Fahrer/in das System dauerhaft beobachtet und jederzeit eingreifen kann,

sowohl um das System zu deaktivieren als auch zu überlagern. Dieses Vorgehen wird dann von Testfahrern/Testfahrerinnen erprobt und abgesichert [2, S. 428 ff]. Weiterhin wird angenommen, dass alle sicherheitsrelevanten E/E-Komponenten nach der ISO 26262 [10] entwickelt sowie abgesichert werden, um die maximalen Fehlerraten nicht zu überschreiten.

Ist der/die Fahrer/in allerdings nicht mehr permanent in der Verantwortung über das Fahrzeug, wie es bei HAF der Fall ist, aber auch bei einschreitenden Notsystemen, müssen geeignet niedrige Falsch-Positiv-Raten sichergestellt werden. Die abschließende Freigabe von jedem FAS basiert nach wie vor auf Realfahrtests, gleichwohl das Testen in virtuellen Simulationsumgebungen in den letzten Jahren mehr und mehr Einzug erhalten hat. Christiansen stellt dar, dass für die Absicherung eines SAE Level 2 Systems 12 Mio. Testkilometer erforderlich sind, um die Erfüllung von Sicherheits-, funktionalen, Qualitäts- und Komfortanforderungen nachzuweisen [16].

Eine Anwendung der beschriebenen Testkonzepte auf HAF ist ohne Anpassungen nicht möglich. Da der/die Fahrer/in die Fahraufgabe nicht länger erfüllen muss, kann die Kontrollierbarkeit als wichtiger Bestandteil der HARA nicht wie bisher ausgewertet werden [17]. Darüber hinaus sind Degradationsmodi von HAF zu berücksichtigen, wohingegen bei einem/r menschlichen Fahrer/in von einer ganzzeitig vollen Verfügbarkeit der Fahrfähigkeiten ausgegangen wird. Koopman und Wagner [17] empfehlen, die Kontrollierbarkeit von HAF mit C3, der höchsten Ausprägung, zu klassifizieren. Hieraus resultieren höhere ASIL-Klassifikationen für die verschiedenen Komponenten eines Systems und damit auch ein höherer Absicherungsaufwand gegenüber kontrollierbareren Systemen. Ein weiteres Problem ist die statistische, streckenbasierte Absicherung von HAF. Nach Wachenfeld und Winner [2] sind für einen streckenbasierten Sicherheitsnachweis auf Autobahnen ca. 7 Mrd. Testkilometer im Realverkehr notwendig, sodass hier auch von der *Freigabefalle* gesprochen wird. Dieser Zahl liegt die Annahme zugrunde, dass ein automatisiertes System doppelt so sicher ist wie ein/e menschliche/r Fahrer/in. Als Metrik wird die Anzahl an Kilometern zwischen zwei tödlichen Unfällen verwendet. Kalra und Paddock [18] schätzen den Testaufwand von SAE Level 5 HAF, basierend auf statistischen Daten aus den USA, auf über 11 Mrd. Kilometer, also in derselben Größenordnung. Aus diesem Grund ist die Absicherung solcher Systeme ökonomisch nicht möglich.

2.3 Szenariobasierter Ansatz

Während große Teile der zurückgelegten Strecke nicht herausfordernd für HAF sind und deshalb keinen weiteren Beitrag zu einem Sicherheitsnachweis liefern, treten kritische, herausfordernde Situationen und Szenarien nur selten sowie stochastisch verteilt auf. Indem diese kritischen Szenarien identifiziert und simulativ oder auf Testgeländen reproduziert werden, kann der Testaufwand für eine Absicherung potentiell reduziert und somit die Freigabefalle überwunden werden. Dieser szenariobasierte Ansatz wird in verschiedenen Forschungsprojekten verfolgt [z.B. 19-21].

Ulbrich et al. [22] und Menzel et al. [23] definieren für die Absicherung von HAF eine Terminologie und Anforderungen zur Definition von (Test-)Szenarien. Diese Szenarien können mit unterschiedlichen Ansätzen generiert werden [24 - 27] oder aus vorhandenen Daten wie FOT (Field Operation Tests) oder Unfalldatenbanken identifiziert werden [z.B. 28]. Pütz et al. [29] schlagen eine allgemeine Datenbank zur Speicherung von Testszenarien vor.

2.4 Parameterraumexplosion

Einer der größten Herausforderungen bei dem szenariobasierten Ansatz ist die hohe Anzahl von Einflussparametern, die beim Testen berücksichtigt werden müssen. Alleine das einfache funktionale Szenario *Fahrstreifenwechsel* führt mit den noch grob diskretisierten Parametern in Tabelle 1 zu 10^7 möglichen Parame-

terkombinationen und entsprechend vielen konkreten Testfällen. Unter der Annahme einer Dauer von 5 s pro Testfall und einem Echtzeitfaktor von 1 würden die Absicherungstests für dieses eine Szenario alleine über ein Jahr dauern. Amersbach und Winner [4] analysieren die Parameterraumexplosion für ein exemplarisches Testset von 9 funktionalen Szenarien detaillierter.

Tabelle 1: Beispielhafter Parameterraum

Parameter	**Mögliche Werte**
Typ des Objektfahrzeugs	≥ 3
Abstand zu Objektfahrzeug	≥ 10
Geschwindigkeit des Objektfahrzeugs	≥ 5
Beschleunigung des Objektfahrzeugs	≥ 5
Geschwindigkeit des Egofahrzeugs	≥ 5
Beschleunigung des Egofahrzeugs	≥ 5
Kurvenkrümmung	≥ 5
Wetter	≥ 5
Helligkeit	≥ 5
Reibwert	≥ 3

2.5 Partikuläres Testen

Werden Subsysteme einzeln und individuell an Stelle des Gesamtsystems getestet, dann wird vom partikulären Testen gesprochen. Diese Subsysteme können bspw. einzelne funktionale Ebenen einer funktional dekomponierten Fahrfunktion [30] oder Module von HAF [z.B. 9, S. 22 f.] sein. Da die meisten Parameter nicht alle funktionalen Ebenen oder Module beeinflussen, hat das partikuläre Testen das Potential, den Absicherungsaufwand mithilfe dieser Parameterraumeinschränkung signifikant zu reduzieren [4]. Die *Helligkeit* hat bspw. nur Einfluss auf die funktionalen Ebenen *Informationsaufnahme* und *Informationsverarbeitung* und bedarf daher keiner Verwendung auf weiteren funktionalen Ebenen als Testparameter.

Ein notwendiger Bestandteil für das partikuläre Testen ist die Definition von Bestehens-/ Versagenskriterien. Während die Definition von Bestehens-/ Versagenskriterien für das Gesamtsystem HAF für viele Fälle offensichtlich ist – bspw. ist eine physisch vermeidbare Kollision ein eindeutiges Versagenskriterium – gestaltet sich die Definition von partikulären Kriterien schwieriger. Darüber hinaus müssen diese Kriterien für eine finale Absicherung von HAF in einer realen oder virtuellen Umgebung testbar sein.

3 Bestehens-/Versagenskriterien für das Testen automatisierter Fahrzeuge

Dieser Beitrag fokussiert sich auf die in Kapitel 2.1.2 beschriebene Verhaltens- sowie funktionale Sicherheit und adressiert damit die Sicherheit von HAF mithilfe von speziell für diesen Anwendungsfall konzipierten Methoden. Für die vorgestellten Methoden der passiven Sicherheit und Gebrauchssicherheit wird die Annahme getroffen, dass diese nach dem aktuellen Stand der Technik für HAF ausreichend sind, gleichwohl verschiedene technische Lösungen anzupassen sind.

Das Testen von HAF basiert auf spezifischen Testkriterien, die explizit für eine eindeutige Auswertung der Testfälle definiert werden müssen. Sicherheitsziele (SZ), die aus Sicht der Verhaltenssicherheit abgeleitet werden, sind für eine Definition solcher Testkriterien noch nicht ausreichend. Für die Definition eindeutiger Bestehens-/Versagenskriterien für HAF sind weitere Schritte notwendig.

Stolte et al. [31] entwickelten eine Methodik zur Ableitung von Sicherheitszielen basierend auf der HARA eines automatisierten, unbemannten Fahrzeugs. Basierend auf der Item-Definition werden Fehlfunktionen abgeleitet, die zu Gefahren und letztendlich zu gefährlichen Szenarien führen. Diese Szenarien dienen als Grundlage für eine ASIL-Bewertung, sodass Sicherheitsziele für das automatisierte System, wie sie exemp-

larisch in Tabelle 2 dargestellt sind, definiert werden können. Aufgrund der allgemeinen Charakteristik einer HARA bzgl. Gefahren unterscheiden sich die abgeleiteten Sicherheitsziele in ihrer Granularität.

Tabelle 2: Sicherheitsziele für den unbemannten Betrieb eines Fahrzeugs nach [31, Tabelle 1]

ID	**Sicherheitsziel**
SZ01	Ein unbeabsichtigter und nicht erlaubter Betriebsmoduswechsel muss verhindert werden.
SZ03	Eine Lenkbetätigung außerhalb der Spezifikation muss verhindert werden.
SZ08	Eine unbeabsichtigte langsame Beschleunigung muss verhindert werden.
SZ09	Eine Verzögerung in den Stillstand muss sichergestellt werden.
SZ12	Ein Überfahren von Seitenstreifenmarkierungen muss verhindert werden.

Die Zuordnung von Sicherheitszielen zu Modulen oder funktionalen Ebenen ist aufgrund der unterschiedlichen Granularität nicht direkt möglich. SZ12 ist bspw. auf Systemebene definiert, während sich SZ03 auf einer tieferen, spezielleren Ebene des automatisierten Fahrzeugs befindet. SZ12 ist folglich von geringerer Granularität als SZ03 und trägt somit mehr implizite Informationen mit sich. Sicherheitsziele mit geringer Granularität resultieren deshalb in einer hohen Anzahl von Testkriterien, die über viele Module oder funktionale Ebenen verteilt sind. Methoden zur direkten Ableitung von spezifischen Testkriterien auf Subsystemebene basierend auf den Sicherheitszielen speziell zur Erfüllung der Verhaltenssicherheit von HAF sind den Autoren dieses Papers bislang nicht bekannt. Eine andere Möglichkeit wäre die Ableitung von Bestehens-/Versagenskriterien auf der Ebene der Sicherheitsziele. In diesem Fall würde SZ12 ein Testkriterium auf Systemebene benötigen, was wiederum zur beschriebenen Parameterraumexplosion führt.

Zur potentiellen Nutzung des Ansatzes des partikulären Testens zur Reduzierung des Testaufwands für eine Absicherung von HAF, werden adäquate Tests inklusive konkreter Bestehens-/Versagenskriterien benötigt. Zusätzlich zur Zerlegung des automatisierten Fahrzeugs in funktionale Ebenen wie es Amersbach und Winner [30] beschreiben, wird der modulbasierte Ansatz von Woopen et al. [9] verfolgt. Auf diese Weise ist die entwickelte Methodik auf verschiedene Zerlegungen eines Systems anwendbar. Die entwickelten Bestehens-/Versagenskriterien auf Subsystemebene sollten eine fehlerfreie Integration in das Gesamtsystem ermöglichen. Dafür werden Sicherheitsziele auf Systemebene als Basis für die Zerlegung zu präzisen Bestehens-/Versagenskriterien verwendet, ohne dabei die Sicht der Verhaltenssicherheit zu verlieren. Neben diesen Vorteilen wird eine explizite Zuordnung von Sicherheitszielen zu einzelnen Modulen automatisierter Fahrzeuge möglich. Daraus resultieren die Verfolgbarkeit und Transparenz einzelner Kriterien, wie sie im nächsten Kapitel abgeleitet werden.

4 Partikuläre Bestehens-/Versagenskriterien

Eine Ableitung von Bestehens-/Versagenskriterien von anfänglich für das Gesamtsystem definierten Sicherheitszielen auf Subsystemebene, wie z.B. Module oder funktionale Ebenen, erfordert eine zureichende Methodik. Diese muss sicherstellen, dass möglichst alle Bestehens-/Versagenskriterien, die zur Einhaltung eines Sicherheitsziels erforderlich sind, generiert werden. Zur Generierung von Fehlerursachen (faults) bzw. Kausalfaktoren anhand von Fehlerwirkungen (failures) ist die FTA ein verbreitetes und anerkanntes Werkzeug. Leveson et al. [32] beschreiben außerdem die STPA als eine Methode, die anhand eines funktionalen Regelkreises systematisch Kausalfaktoren für potentielle Gefahren an den Schnittstellen herleitet. Beide Analysewerkzeuge werden in der im Folgenden dargestellten Methodik als erster Schritt zur Ableitung partikulärer Kausalfaktoren von Sicherheitszielen angewendet. Sie können jedoch auch durch andere Top-Down-Methoden ersetzt oder ergänzt werden. Nach diesem Schritt liegen die Kausalfaktoren auf Subsyste-

mebene vor. Für diese werden Sicherheitsanforderungen definiert, die das Auftreten der Kausalfaktoren verhindern. Im letzten Schritt werden die Bestehens-/Versagenskritierien formuliert, die in einem Test die Einhaltung bzw. Verletzung einer Sicherheitsanforderung bewerten. Durch Anwendung der beschriebenen und in Abbildung 1 dargestellten Methodik werden die auf Gesamtsystemebene definierten Sicherheitsziele anhand der definierten Bestehens-/Versagenskriterien auf Subsystemebene testbar.

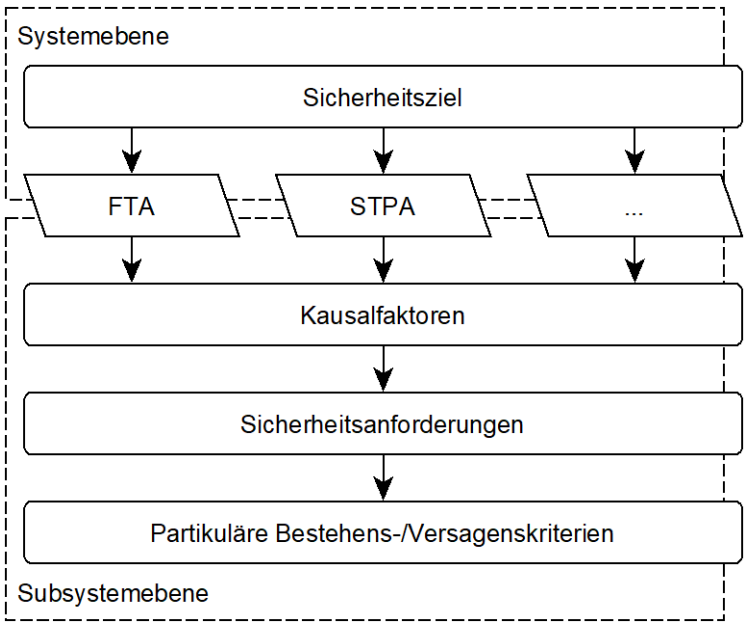

Abbildung 1: Methodik zur Ableitung von partikulären Bestehens-/Versagenskriterien

Im vorliegenden Beispiel wird die STPA zur Ableitung eines Sicherheitsziels auf funktionale Ebenen verwendet. Das Sicherheitsziel „Überfahren einer durchgezogenen Fahrstreifenmarkierung (FSM) muss vermieden werden“ ist dem SZ12 von Stolte et al. [31] nachempfunden. Der in Abbildung 2 dargestellte Regelkreis, wie er in der STPA zu definieren ist, bildet die nach Amersbach und Winner [30] vorgestellten funktionalen Dekompositionsebenen ab. Neben den als Blöcke dargestellten Ebenen sind die jeweiligen Schnittstellen angegeben. Diese Schnittstellen werden in der STPA hinsichtlich vierer Fehlerkategorien, sogenannter unsicherer Regelbefehle, die potentiell Gefahren hervorrufen, analysiert.

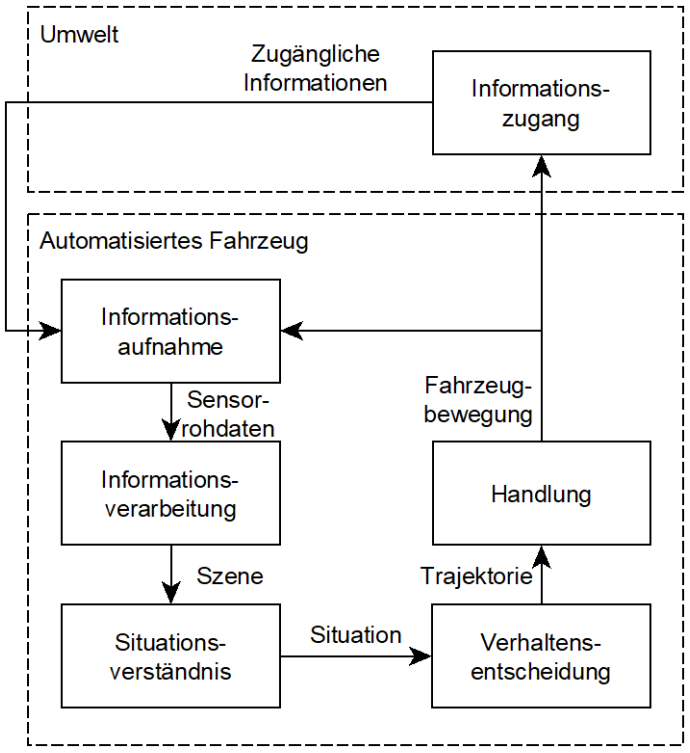

Abbildung 2: Regelkreis für die funktionalen Dekompositionsebenen

Abbildung 3 zeigt beispielhaft mögliche unsichere Regelbefehle bzw. Aktionen, die zur Verletzung des Sicherheitsziels SZ12 führen, und deren Ableitung zu Bestehens-/Versagenskriterien. Für den dabei analysierten Ausgang der funktionalen Dekompositionsebene *Informationsaufnahme* ergeben sich die beiden dargestellten unsicheren Aktionen. Die sich daraus ergebenden Sicherheitsanforderungen und Bestehens-/Versagenskriterien sind in Abbildung 3 für eine einfachere Rückverfolgbarkeit in gleicher Farbe dargestellt. Für die unsichere Aktion, dass keine verarbeitbaren Sensorrohdaten über die durchgezogene Linie zur Verfügung gestellt werden, lässt sich ein abgedeckter Sensor als eine Fehlerursache ableiten. Daraus leiten sich die Sicherheitsanforderungen „Der Sensor darf während des Betriebs nicht verdeckt sein“ bzw. „Ein verdeckter Sensor muss im Betrieb erkannt werden“ ab. Beide Sicherheitsanforderungen erfordern weitere Sicherheitsanforderungen, die dafür sorgen, dass weiterhin das übergeordnete Sicherheitsziel eingehalten wird. Ein Beispiel hierfür sind Anforderungen an das *Sichere Anhalten* [9], das im Fall von Funktionseinschränkungen, wie einen erkannten verdeckten Sensor, ein geeignetes Notmanöver in den Stillstand einleitet. Im letzten Schritt der beschriebenen Methode erfolgt die Definition der Bestehens-/Versagenskriterien. Dazu wird die Sicherheitsanforderung im ersten Schritt invers formuliert und für spezifische Testfälle ggf. noch weiter detailliert.

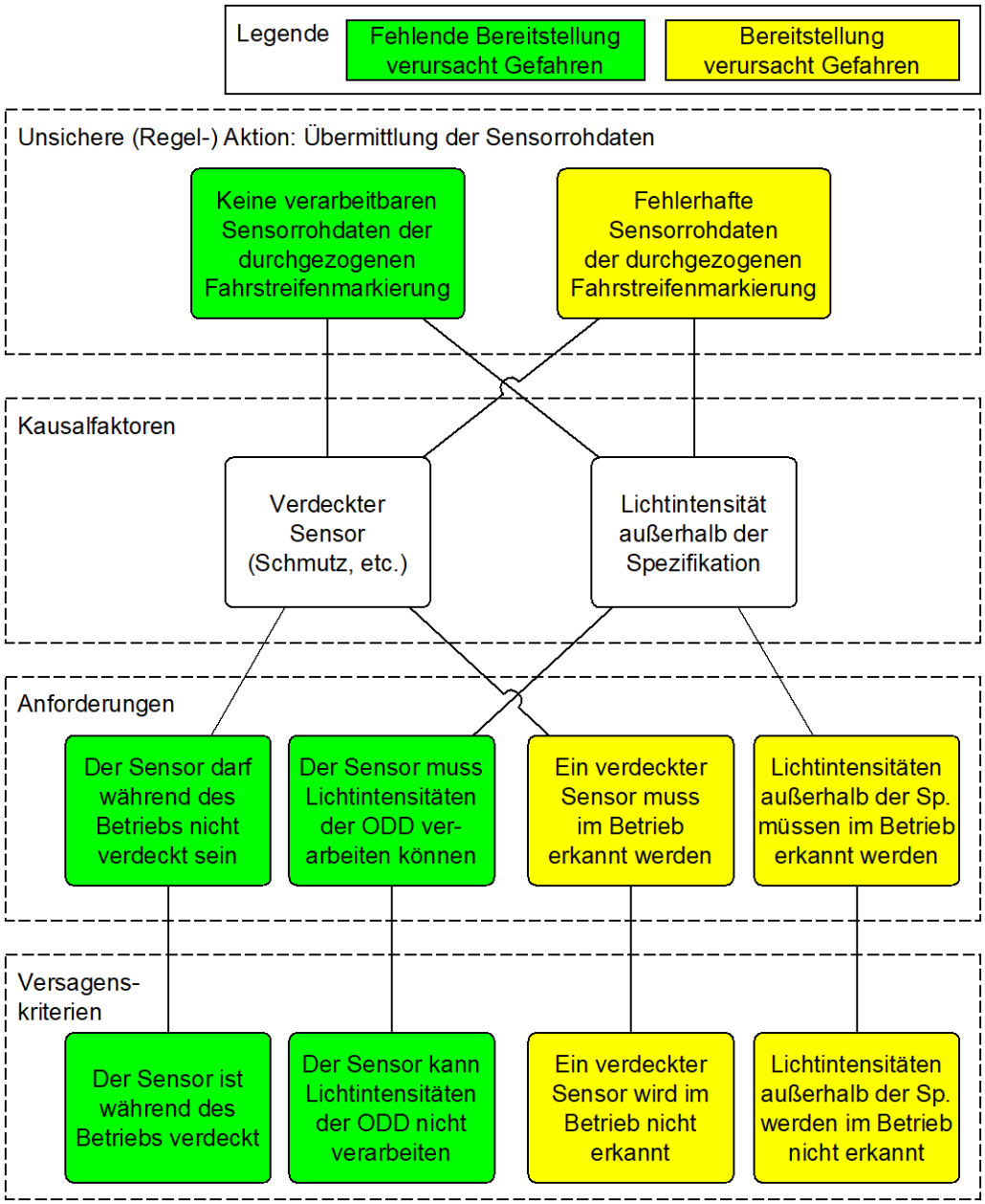

Abbildung 3: Ermittlung von Bestehens-/Versagenskriterien mit STPA

Im nächsten Beispiel wird die im Projekt UNICAR*agil* verwendete Modularchitektur [9] für die Absicherung genutzt. Anhand einer FTA werden Kausalfaktoren ausgehend vom selben Sicherheitsziel auf Modulebene abgeleitet. Module beinhalten Hardware- sowie Softwarekomponenten und können mit diesen ggf. mehrere funktionale Dekompositionsebenen abbilden. Darüber hinaus kann es auch Module geben, die keine Funktion der Fahraufgabe übernehmen, da sie z.B. nur zur Unterhaltung der Insassen eingesetzt werden und somit keine der vorgestellten funktionalen Dekompositionsebenen repräsentieren. Somit sind für Module zusätzliche Sicherheitsanforderungen zu definieren, die sich nicht anhand der Sicherheitsziele für die Fahraufgabe ableiten lassen. Die vorgestellte Methodik konzentriert sich jedoch auf die Problematik zur Absicherung von HAF und behandelt diese daher nicht weiter. Vergleichbar zur funktionalen Dekomposition wird durch Aufteilung des Gesamtsystems ebenso eine Verkleinerung des Parameterraums der einzelnen Subsysteme erreicht, sodass dieser Raum überblick- und kontrollierbarer wird. Für Entwickler und Tester werden Fehler dadurch u.a. einfacher aufdeckbar.

Zur Aufdeckung von möglichst vielen und detaillierten Kausalfaktoren auf Modulebene ist es im Allgemeinen hilfreich das Modul anhand einer detaillierten Beschreibung so gut wie möglich zu kennen. Trotzdem ist es bei der vorgestellten Methodik entscheidend, Kausalfaktoren möglichst allgemein zu formulieren. Daraus resultiert, dass die Struktur für zukünftige Entwicklungen ggf. mit geänderten Modulen wiederverwendbar ist, sofern die funktionale Architektur weitgehend bestehen bleibt. Zusätzlich wird eine höhere Vollständigkeit erreichbar, da Kausalfaktoren nicht zu früh zu detailliert beschrieben werden und damit nicht weiter in mehrere zusätzliche Kausalfaktoren heruntergebrochen werden können. Sobald keine weiteren allgemeinen Kausalfaktoren mehr gefunden werden, wird die modulare Architektur zur Zuweisung von Kausalfaktoren zu jeweils einem Modul verwendet. Die Zuweisung eines Kausalfaktors zu mehreren Modulen ist zu vermeiden, da nicht sichergestellt werden kann, dass die Module dann unabhängig voneinander betracht- und absicherbar sind.

Der Ausschnitt eines Fehlerbaums, wie in Abbildung 4 dargestellt, zeigt, wie das Sicherheitsziel zu Kausalfaktoren bis herunter auf Modulebene abgeleitet wird. Die dargestellten Module repräsentieren jeweils mehrere funktionale Dekompositionsebenen, weshalb sich trotz desselben Sicherheitsziels teilweise andere Kausalfaktoren ergeben. Im Beispiel enthält das Modul Stammhirn u.a. Sensorik, einen Algorithmus zur Durchführung eines sicheren Haltemanövers und einen Regler, wodurch die funktionalen Ebenen *Informationsaufnahme*, *Informationsverarbeitung*, *Verhaltensentscheidung* und *Handlung* adressiert werden. Aufgrund dessen ist es auch möglich, Module zu dekomponieren, wodurch der Testaufwand ggf. weiter reduziert werden kann. Zusätzlich ist anzunehmen, dass sich durch FTA andere Kausalfaktoren ergeben als durch STPA, weshalb ggf. eine Kombination der Methoden notwendig ist. Trotzdem deckt das dargestellte Beispiel ebenfalls den Kausalfaktor „Sensor verdeckt“ auf. Die Unterscheidung in nicht detektieren und falsch detektieren der FSM ist notwendig, da dies zu verschiedenen Kausalfaktoren auf den weiteren Ebenen führt. Die Definition der dazugehörigen Sicherheitsanforderungen und Bestehens-/Versagenskriterien wird wie im vorherigen Beispiel zur STPA beschrieben vorgenommen.

Die entwickelten Bestehens-/Versagenskriterien sind im ersten Schritt nur qualitativ beschrieben (z.B. durch Beschreibungen wie „falsch“ oder „fehlerhaft“). Zur Entscheidung, ob ein Test bestanden ist oder nicht, ist es notwendig, Metriken für die entsprechenden Bestehens-/Versagenskriterien zu entwickeln und diesen zulässige bzw. nicht zulässige Werte zuzuordnen. Dies ist besonders entscheidend zur Umsetzung automatisierter Tests und der automatisierten Auswertung. In Anbetracht der hohen Anzahl notwendiger Testfälle eines HAF sind Tests ökonomisch nur in automatisierter Form realisierbar und müssen für einen belastbaren Sicherheitsnachweis objektiv bewertet werden. Neben den externen Werten, wie die vom Modul zur Verfügung gestellten Ausgangsdaten, können auch interne Werte relevant für eine Absicherung des Moduls sein.

Für diese sind ebenfalls Metriken und zulässige Werte zu definieren, wofür ggf. zusätzliche Schnittstellen bei Tests notwendig sind, die die entsprechenden Informationen zur Verfügung stellen.

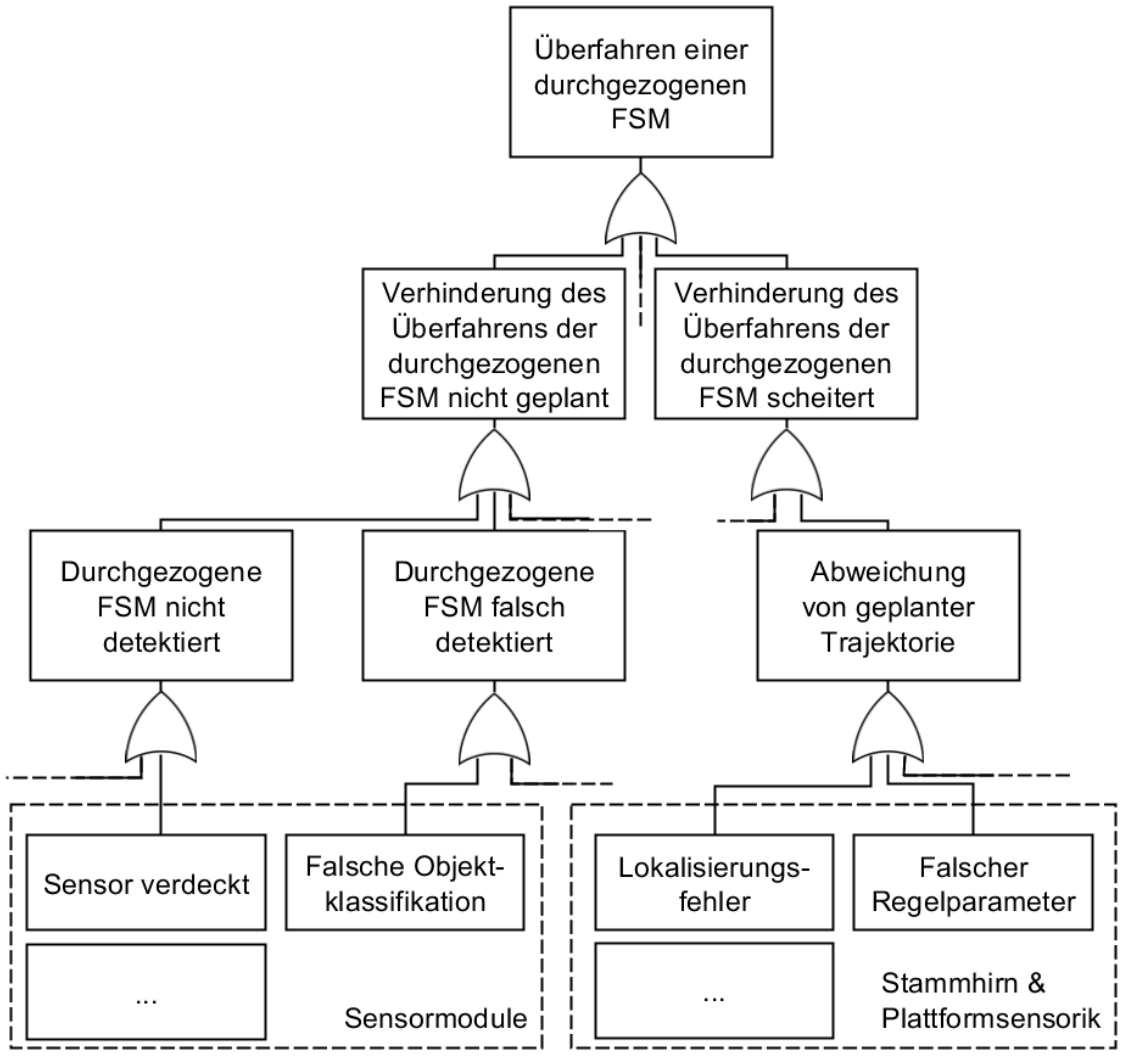

Abbildung 4: Beispielhafter Fehlerbaum zur Zerlegung von SZ in Kausalfaktoren auf Modulebene

Die zulässigen Werte von Modulen hängt stark vom Aufbau des Gesamtsystems und der Funktion bzw. Leistungsfähigkeit anderer Module ab. Andere Module können bestimmte Anforderungen an das betrachtete Modul stellen oder nur eine gewisse Leistungsfähigkeit erbringen. Zur Definition quantitativer Bestehens-/Versagenskriterien sind daher die Anforderungen und Spezifikationen (z.B. in Form einer Item Definition) frühzeitig festzulegen. Da die zulässigen Werte empfindlich gegenüber Änderungen z.B. an den Anforderungen reagieren, steht dies im Konflikt mit dem Entwicklungsprozess und dem Austausch oder den Änderungen von Modulen nach dem Freigabeprozess. Ein offensichtliches Beispiel, wie zulässige Werte definiert werden können, ist die Ableitung der zulässigen Latenzzeiten. Für das Gesamtsystem kann beispielsweise ein Weg bzw. eine Zeit definiert werden, in der das Fahrzeug nach Erkennung z.B. einer Notbremssituation zum Stillstand kommen muss. Hierzu kann ein Eventbaum entwickelt oder teilweise die bereits entwickelten Strukturen aus der durchgeführten FTA oder STPA verwendet werden. Die Ableitung zulässiger Werte vom Sicherheitsziel startet damit, dass z.B. die Berührung der Linie als Kriterium verwendet wird. Verwendet man nun den zuvor erstellten Fehlerbaum lässt sich daraus ableiten, dass das Ausweichen einer durchgezogenen Linie fehlschlägt, wenn diese berührt wird. Im nächsten Ast ist der mögliche Kausalfaktor, dass von der geplanten Trajektorie abgewichen wurde. Hierfür lassen sich zulässige Werte damit ableiten, dass z.B. Verbindungen zur Lokalisierung durch AND-Operatoren gezogen werden. Die zulässigen Werte sind dann so zu definieren, dass die Summe der einzuhaltenden Unsicherheiten klein genug bleibt und eine Linie nicht berührt wird.

5 Zusammenfassung

Die Absicherung automatisierter Fahrfunktionen erfordert mit bisherigen Methoden weiterhin einen nicht ökonomischen Aufwand. Neben dem szenariobasierten Testansatz versprechen die funktionale Dekomposition sowie die modulare Absicherung als partikuläre Testmethoden eine weitere Reduktion des Testaufwands. Dazu ist es notwendig für die definierten Subsysteme Testfälle und Testkriterien zu bestimmen, die die Absicherung des Gesamtsystems sicherstellen. Die vorliegende Arbeit geht dabei den ersten Schritt systematisch Testkritierien von Gesamtsystemebene auf Subsystemebene abzuleiten. Es wurde gezeigt, dass insbesondere die für automatisierte Fahrfunktionen notwendige Verhaltenssicherheit mit dieser Methode adressiert wird. Die Verhaltenssicherheit, für die in vorherigen Arbeiten Sicherheitsziele auf Systemebene entwickelt wurden, wird mit der gezeigten Methode auf Subsystemebene testbar. In der Methode kommen bewährte Analysewerkzeuge wie FTA und STPA zum Einsatz. Die damit entwickelten Kausalfaktoren auf Subsystemebene werden durch die Formulierung von Sicherheitsanforderungen adressiert und daraus folgend Bestehens-/Versagenskriterien definiert. Zu diesen Kriterien sind zulässige bzw. nicht zulässige Wertebereiche festzulegen. Für die Methode wurden mehrere Beispiele aufgezeigt und analysiert. Die teils grobe Formulierung von Sicherheitszielen macht es jedoch schwierig, Zahlenwerte für die entwickelten Kausalfaktoren zu definieren. Die dazu aufgezeigten Möglichkeiten sind ausführlicher in weiteren Arbeiten auszuarbeiten. Zusätzlich stellt sich aufgrund des hohen Aufwands der Methode die Frage nach einer möglichen Automatisierbarkeit. Im nächsten Schritt sind für das partikuläre Testen Testfälle auf Subsystemebene zu definieren und die Bestehens-/Versagenskriterien ggf. für die Testfälle zu detaillieren. Darüber hinaus ist es möglich, Sicherheitsziele bestimmten Streckenkategorien zuzuordnen, sodass Module bzw. das dekomponierte Gesamtsystem für jede Kategorie individuell freigegeben werden können.

Danksagung

Diese Forschungsarbeiten wurden im Rahmen der Projekte „UNICAR*agil*“ (FKZ 16EMO0286) und „PEGASUS“ durchgeführt. Wir bedanken uns für die finanzielle Unterstützung des Projekts „UNICAR*agil*“ durch das Bundesministerium für Bildung und Forschung (BMBF) und des Projekts „PEGASUS“ durch das Bundesministerium für Wirtschaft und Energie (BMWi).

Literatur

[1] Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE J3016, 2014

[2] W. Wachenfeld und H. Winner, “The Release of Autonomous Vehicles”, in Autonomous Driving: Technical, Legal and Social Aspects, H. Winner, M. Maurer, J. C. Gerdes, and B. Lenz, Eds., Berlin, Heidelberg: Springer, 2016, pp. 425–449

[3] W. Wachenfeld, P. Junietz, H. Winner, P. Themann, und A. Pütz, Safety Assurance Based on an Objective Identification of Scenarios. San Francisco, CA, USA, 2016.

[4] C. Amersbach und H. Winner, “Functional Decomposition - A Contribution to Overcome the Parameter Space Explosion during Validation of Highly Automated Driving (Accepted)”, in 26th International Technical Conference and exhibition on the Enhanced Safety of Vehicles (ESV), 2019

[5] P. Junietz, U. Steininger, und H. Winner, “Macroscopic Safety Requirements for Highly Automated Driving”, Transportation Research Record, 2019

[6] P. Liu, R. Yang, und Z. Xu, “How Safe Is Safe Enough for Self-Driving Vehicles?”, Risk analysis, 2018

[7] WAYMO, On the Road to Fully Self-Driving: Waymo Safety Report, 2017

[8] M. Nolte et al., “Towards a skill- and ability-based development process for self-aware automated road vehicles”, in IEEE ITSC 2017: 20th International Conference on Intelligent Transportation Systems: Mielparque Yokohama in Yokohama, Kanagawa, Japan, October 16-19, 2017, Piscataway, NJ: IEEE, 2017, S. 1–6

[9] T. Woopen et al., “UNICARagil - Disruptive Modular Architectures for Agile, Automated Vehicle Concepts”, in 27th Aachen Colloquium Automobile and Engine Technology 2018, 2018, S. 1–32

[10] ISO 26262: Road vehicles – Functional safety, 2011

[11] T. Stolte, G. Bagschik, und M. Maurer, “Safety goals and functional safety requirements for actuation systems of automated vehicles”, in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC): IEEE, 2016, S. 2191–2198

[12] T. M. Gasser, A. Seeck, und B. W. Smith, “Framework Conditions for the Development of Driver Assistance Systems”, in Handbook of Driver Assistance Systems, H. Winner, S. Hakuli, F. Lotz, und C. Singer, Eds., Cham: Springer International Publishing, 2016, S. 35–68

[13] H. Winner und N. L. Merkel, “Mode-Confusion und Inkompatibilitäten in der Migrationsphase des automatisierten Fahrens”, in 8. Darmstädter Kolloquium 7./8. März 2017 Technische Universität Darmstadt Herausgeber: H. Winner und R. Bruder, 2017, S. 53–64

[14] E. Schoitsch, C. Schmittner, Z. Ma, und T. Gruber, “The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles”, in Advanced Microsystems for Automotive Applications 2015: Springer, 2016, S. 251–261

[15] Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE J3061, 2016

[16] M. Christiansen, In geheimer Mission: auf Abnahmefahrt mit der neuen Mercedes E-Klasse, W213. [Online] Verfügbar: http://5komma6.mercedes-benz-passion.com/in-geheimer-mission-auf-abnahmefahrt-mit-der-neuen-mercedes-e-klasse-w213/. Zugriff am: 12. Juli 2017

[17] P. Koopman und M. Wagner, “Autonomous vehicle safety: An interdisciplinary challenge”, IEEE Intell. Transport. Syst. Mag., vol. 9, no. 1, S. 90–96, 2017

[18] N. Kalra und S. M. Paddock, “Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?”, 2016. [Online] Verfügbar: http://www.rand.org/pubs/research_reports/RR1478.html

[19] German Aerospace Center (DLR), PEGASUS - Project Homepage. [Online] Verfügbar: https://www.pegasusprojekt.de/en/about-PEGASUS. Zugriff am: 04. März 2019

[20] AVL LIST GMBH, About the project – Enable S3. [Online] Verfügbar: https://www.enable-s3.eu/about-project/. Zugriff am: 04. März 2019

[21] D. Zhao et al., “Accelerated Evaluation of Automated Vehicles Safety in Lane-Change Scenarios Based on Importance Sampling Techniques”, (eng), IEEE transactions on intelligent transportation systems : a publication of the IEEE Intelligent Transportation Systems Council, vol. 18, no. 3, S. 595–607, 2017

[22] S. Ulbrich, T. Menzel, A. Reschka, F. Schuldt, und M. Maurer, “Defining and substantiating the terms scene, situation, and scenario for automated driving”, in Intelligent Transportation Systems (ITSC), 2015 IEEE 18th International Conference on Intelligent Transportation Systems, 2015, S. 982–988

[23] T. Menzel, G. Bagschik, und M. Maurer, “Scenarios for development, test and validation of automated vehicles”, in 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, S. 1821–1827

[24] M. Althoff und S. Lutz, “Automatic Generation of Safety-Critical Test Scenarios for Collision Avoidance of Road Vehicles”, in 2018 IEEE Intelligent Vehicles Symposium (IV), 2018, S. 1326–1333

[25] M. O’Kelly, H. Abbas, und R. Mangharam, “Computer-aided design for safe autonomous vehicles”, in Resilience Week (RWS), 2017, 2017, S. 90–96

[26] H. Abbas, M. E. O'Kelly, A. Rodionova, und R. Mangharam, "A Driver's License Test for Driverless Vehicles", Mechanical Engineering Magazine Select Articles, vol. 139, no. 12, S13 - S16, 2017

[27] G. Bagschik, T. Menzel, und M. Maurer, "Ontology Based Scene Creation for the Development of Automated Vehicles", in 2018 IEEE Intelligent Vehicles Symposium (IV), 2018

[28] W. Wachenfeld, P. Junietz, R. Wenzel, und H. Winner, "The worst-time-to-collision metric for situation identification", in 2016 IEEE Intelligent Vehicles Symposium (IV): 19.-22. Juni 2016, Piscataway, NJ: IEEE, 2016, S. 729–734

[29] A. Pütz, A. Zlocki, J. Bock, und L. Eckstein, "System validation of highly automated vehicles with a database of relevant traffic scenarios", in 12th ITS European Congress, 2017

[30] C. Amersbach und H. Winner, "Functional Decomposition: An Approach to Reduce the Approval Effort for Highly Automated Driving", in 8. Tagung Fahrerassistenz, 2017

[31] T. Stolte, G. Bagschik, A. Reschka, und M. Maurer, "Hazard analysis and risk assessment for an automated unmanned protective vehicle", in 2017 IEEE Intelligent Vehicles Symposium (IV), 2017, S. 1848–1855

[32] N. G. Leveson und J. P. Thomas, STPA Handbook. [Online] Verfügbar: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. Zugriff am: 16. Juni 2019