Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung

Berichte der
Bundesanstalt für Straßenwesen

Fahrzeugtechnik Heft F 98

Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung

von

Alexander Weitzel
Hermann Winner
Cao Peng
Sebastian Geyer
Felix Lotz
Mohsen Sefati

Technische Universität Darmstadt
Fachgebiet Fahrzeugtechnik

Berichte der Bundesanstalt für Straßenwesen

Fahrzeugtechnik Heft F 98

bast

Die Bundesanstalt für Straßenwesen veröffentlicht ihre Arbeits- und Forschungsergebnisse in der Schriftenreihe **Berichte der Bundesanstalt für Straßenwesen.** Die Reihe besteht aus folgenden Unterreihen:

A - Allgemeines
B - Brücken- und Ingenieurbau
F - Fahrzeugtechnik
M - Mensch und Sicherheit
S - Straßenbau
V - Verkehrstechnik

Es wird darauf hingewiesen, dass die unter dem Namen der Verfasser veröffentlichten Berichte nicht in jedem Fall die Ansicht des Herausgebers wiedergeben.

Die Hefte der Schriftenreihe **Berichte der Bundesanstalt für Straßenwesen** können direkt bei der Carl Schünemann Verlag GmbH, Zweite Schlachtpforte 7, D-28195 Bremen, Telefon: (04 21) 3 69 03 - 53, bezogen werden.

Über die Forschungsergebnisse und ihre Veröffentlichungen wird in der Regel in Kurzform im Informationsdienst **Forschung kompakt** berichtet. Dieser Dienst wird kostenlos angeboten; Interessenten wenden sich bitte an die Bundesanstalt für Straßenwesen, Stabsstelle Presse und Öffentlichkeitsarbeit.

Ab dem Jahrgang 2003 stehen die **Berichte der Bundesanstalt für Straßenwesen** (BASt) zum Teil als kostenfreier Download im elektronischen BASt-Archiv ELBA zur Verfügung.
http://bast.opus.hbz-nrw.de

Impressum

Bericht zum Forschungsprojekt FE 82.0546/2012:
Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung

Fachbetreuung:
Tom Michael Gasser

Herausgeber
Bundesanstalt für Straßenwesen
Brüderstraße 53, D-51427 Bergisch Gladbach
Telefon: (0 22 04) 43 - 0 · Telefax: (0 22 04) 43 - 674

Redaktion
Stabsstelle Presse und Öffentlichkeitsarbeit

Druck und Verlag
Fachverlag NW in der
Carl Schünemann Verlag GmbH
Zweite Schlachtpforte 7, D-28195 Bremen
Telefon: (04 21) 3 69 03 - 53 · Telefax: (04 21) 3 69 03 - 48
www.schuenemann-verlag.de

ISSN 0943-9307
ISBN 978-3-95606-118-9

Bergisch Gladbach, November 2014

Kurzfassung – Abstract

Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung

Fahrerassistenzsystemen mit Umfeldwahrnehmung wird ein hohes Potenzial zur Unfallvermeidung zugeschrieben, wenn diese umfassender und intensiver in die Fahrdynamik von Fahrzeugen eingreifen und weiter vernetzt werden. Diese erweiterten Eingriffsmöglichkeiten erzeugen auch neue Risiken, welche vor der Genehmigung und Zulassung für den öffentlichen Straßenverkehr abgesichert werden müssen. Neuartig ist bei diesen Systemen, dass sie nur über eine Situationsrepräsentation die unfallvermeidenden Handlungen ableiten können. Somit kommt zum Risiko des Versagens von Systemkomponenten, das bereits durch die ISO-26262-Norm zur funktionalen Sicherheit adressiert ist, das Risiko aufgrund einer falschen Interpretation auftretenden, nicht situationsgemäßen Auslösung, z. B. durch Situationskonstellationen, die bei der Entwicklung nicht berücksichtigt wurden und daher in den Funktionsspezifikationen nicht enthalten sind. Um die Anforderungen an Absicherungsmethoden für diese Assistenzsysteme zu identifizieren, werden diese zusammengestellt und der Absicherungsaufwand mit bestehenden Methoden, bspw. aufbauend auf den Anforderungen der ISO 26262, bestimmt. Die Analyse zeigt, dass bisherige Ansätze sowohl hinsichtlich der objektiven Nachweisbarkeit der Vollständigkeit der theoretisch möglichen Situationen Lücken aufweisen als auch hinsichtlich des Umfangs der notwendigen Spezifikationen und deren Prüfung in Versuchen. Aufgrund des daher zu erwartenden Aufwands für den Nachweis eines sicheren Verhaltens der Systeme sind eine Priorisierung von Fahrsituationen und die Gewährleistung einer hohen Übertragbarkeit von Bewertungsergebnissen notwendig. Um die Vollständigkeitsproblematik zu adressieren, wird ein Ansatz vorgestellt, der eine objektive Bewertung und den Vergleich von Fahrsituationen ermöglicht. Abschließend werden die Erkenntnisse zusammengefasst und notwendige weitere Schritte für die Schaffung einer einheitlichen Absicherungsstrategie für Fahrerassistenzsysteme abgeleitet.

Approval strategies for advanced driving assistance systems

Driver Assistance Systems with surrounding perception systems, often called Advanced Driver Assistance Systems (ADAS), are attributed to have a high potential to reduce accidents. Therefore they are growingly interconnected and have increasing options to intervene in the driving dynamics of the vehicle. The expansion of intervention options are generating new risks, which needs to be evaluated to get approval for public traffic. Specific for these systems is that they derive the decision about the intervening action from a situation representation. In addition to the failure of components, which is addressed for example by the ISO 26262 standard, this adds the risk of an unintended reaction of the system. Causes of the unintended reaction are an incorrect interpretation of the situation, for example as a result of situations that have not been considered in the specification of the system. To identify the requirements for an approval method of ADAS, existing approaches are summed up and the effort with these methods, for example according to the requirements of ISO 26262, is quantified. The analysis reveals that existing methods have gaps concerning the verifiability of the completeness of possible situations and the scope of the requirements in connection with their approvability in testing. Due to the expected high effort for the approval of safe behavior of ADAS, prioritization and transferability of test results are necessary. To address the problem of completeness, an approach for an objective evaluation and comparison of driving situations is described. The overall findings are concluded and the necessary steps for the development of a unified approval strategy for Advanced Driving Assistance Systems are summarized.

Inhalt

1 Einleitung

Damit ein Fahrzeug für den Betrieb im öffentlichen Straßenverkehr freigegeben werden kann, muss gewährleistet werden, dass es den geltenden Sicherheitsanforderungen genügt.

Aus Kundensicht wird die „Sicherheit“ eines Fahrzeugs häufig anhand der sicherheitstechnischen Einrichtungen, beispielsweise der Anzahl von Airbags, bzw. der daraus resultierenden Bewertungen in standardisierten Test-Verfahren, beispielsweise der Euro-NCAP-Bewertung,[1] definiert.

Aus Sicht des Fahrzeugherstellers bzw. des Herstellers von Fahrzeugsystemen muss dagegen die Sicherheit eines Fahrzeugs allgemeiner betrachtet und nachgewiesen werden. Sowohl bei Stillstand als auch im Betrieb muss gewährleistet werden, dass die vom Fahrzeug ausgehenden Gefahren für den Nutzer und die Umgebung minimiert werden. Dies gilt auch bei Ausfällen oder Versagen von Systemen, bei vorhersehbarem Fehlgebrauch oder sogar Missbrauch, insoweit der Hersteller diesen vermeiden oder darauf Einfluss nehmen kann.

Bevor also eine Freigabe für den öffentlichen Straßenverkehr erfolgen kann, muss daher eine Absicherung erfolgen, die den Sicherheitsnachweis führt. Diese Absicherung muss für das Gesamtfahrzeug erfolgen und umfasst beispielsweise sowohl den Einklemmschutz der elektrischen Fensterheber als auch Fahrerassistenzsysteme mit Umfeldwahrnehmung, wie beispielsweise ein automatisches Notbremssystem. Die dazu benötigten Absicherungsmethoden können sich aber abhängig von der Funktion und deren potenziellen Risiken unterscheiden. Im Fokus des vorliegenden Berichtes stehen Fahrerassistenzsysteme mit Umfelderfassung.

2 Besonderheiten von Fahrerassistenzsystemen mit Umfeldwahrnehmung bei Test und Bewertung

Seit dem Beginn der Entwicklung des Automobils wird beständig daran gearbeitet, das Fahren komfortabler und sicherer zu machen. Insbesondere mit fortschreitendem Einsatz von elektrischen und elektronischen Komponenten und deren Vernetzung haben sich die Möglichkeiten dazu erheblich erweitert. Neben Funktionen auf Stabilisierungsebene (bspw. dem Antiblockiersystem – ABS und dem Elektronischen Stabilitätsprogramm – ESC) wurden im letzten Jahrzehnt auch verstärkt Systeme mit Umfeldwahrnehmung entwickelt, die den Fahrer bei Fahrmanövern unterstützen. Zu Beginn dieser Entwicklung standen Komfortsysteme, wie zum Beispiel Adaptive Cruise Control (ACC), im Vordergrund. Durch die beständige Evolution von Sensorik und Elektronik können inzwischen auch Sicherheitsfunktionen dargestellt werden, sodass vermehrt unfallvermeidende und unfallfolgenlindernde Systeme auf Basis von Umfeldsensoren entwickelt und in Serienfahrzeugen eingesetzt werden. Angesichts eines hohen technischen Niveaus der passiven Sicherheitssysteme in einem modernen Kraftfahrzeug und der bei Neufahrzeugen vorliegenden ESC-Ausrüstungsverpflichtung[2], wird umfelderfassenden Fahrerassistenzsystemen zur Unfallvermeidung, häufig auch „Aktive Sicherheitssysteme“ genannt, ein großes Potenzial zur weiteren Verringerung der Unfallzahlen zugeschrieben.[3]

Mit steigender Verbreitung und angesichts wachsender Vernetzung und damit steigender Komplexität sowohl der Systeme selbst als auch deren Anwendungsfälle werden Fragestellungen zu Absicherungsmethoden für diese Systeme immer wichtiger. Eine valide Absicherung der Fahrerassistenzfunktionen ist notwendig, um das Potenzial zur Unfallvermeidung nutzen zu können. Mit Erweiterung der Einsatzszenarien erhöhen sich zudem auch die Variationsparameter der Fahrsituationen. Dabei ist stets abzusichern, dass das potenzielle zusätzliche Risiko, welches von den Systemen im Fehlerfall ausgeht, innerhalb des gesellschaftlich akzeptierten Risikos bleibt. Das gesellschaftlich akzeptierte Risiko des Straßenverkehrs ist aber unter Umständen gar nicht explizit definiert, sondern wird durch den Stand der serientauglichen Sicherheitstechnik im Automobil, im Zusammenhang mit den Fahrerfähigkeiten, jeweils implizit bedingt.

Der Bericht analysiert die Herausforderungen bei der Absicherung von Fahrerassistenzsystemen mit Umfeldwahrnehmung. Dazu werden die Grundlagen der Absicherung mit den dazugehörigen Normen, Regelwerken und Richtlinien analysiert,

---

1 Euro NCAP (2013)

2 Verordnung EG 661/2009 (2009)

3 Bspw. HUMMEL et al. (2012), S. 55

Absicherungsansätze exemplarisch vorgestellt und durch Forschungsansätze, die absicherungsrelevante Themen behandeln, ergänzt. Ziel ist die Identifikation von Herausforderungen und potenziellen Hemmnissen bei der Entwicklung zukünftiger unfallvermeidender Systeme.

Damit versteht sich der Bericht als Ergänzung zu der ebenfalls aktuell geführten Diskussion der rechtlichen Aspekte zunehmender Fahrzeugautomatisierung[4] und als Anstoß zur Entwicklung eines effektiven und effizienten Vorgehens zur Absicherung von Fahrerassistenzsystemen mit Umfeldwahrnehmung mit hoher Relevanz für das reale Unfallgeschehen.

Eine umfassende vollständige Darstellung von Methoden zur Absicherung von komplexen elektrischen/elektronischen Systemen ist angesichts der großen Zahl existierender und teilweise seit mehreren Jahren bewährter Methoden im Rahmen dieses Berichtes nicht möglich und aus Sicht der Autoren auch nicht zielführend. Beschreibungen dazu sind zahlreich in vorhandener Literatur zu finden, auf die entsprechend im Text verwiesen wird. Dadurch sollen auch zukünftige Vertiefungen einzelner Aspekte erleichtert werden.

2.1 Besonderheiten bei Test und Bewertung

Fahrerassistenzsysteme mit Umfeldwahrnehmung, im Weiteren mit der Abkürzung FAS bezeichnet, unterstützen den Fahrer bei der Bewältigung der Fahraufgabe oder ergänzen ihn in Bereichen, in denen seine Leistungsfähigkeit dazu nicht ausreicht. Systeme, die die Stabilisierung des Fahrzeugs betreffen (bspw. ESC oder ABS), verwenden dabei Sensoren, die den fahrdynamischen Zustand des Fahrzeugs ermitteln, beispielsweise anhand der Gierrate und der Querbeschleunigung. Fahrerassistenzsysteme, die den Fahrer bei der Ausführung eines Manövers, zum Beispiel einem Fahrstreifenwechsel, unterstützen sollen, müssen zusätzlich über die maschinelle Wahrnehmung die Umgebung des Fahrzeuges erfassen. Daraus erfolgen eine Bewertung der aktuellen Fahrsituation und eine Prädiktion der weiteren Entwicklung dieser Situation.

Der schematische Ablauf einer Situationserfassung eines umfeldwahrnehmenden Fahrerassistenzsystems ist in Bild 1 dargestellt.

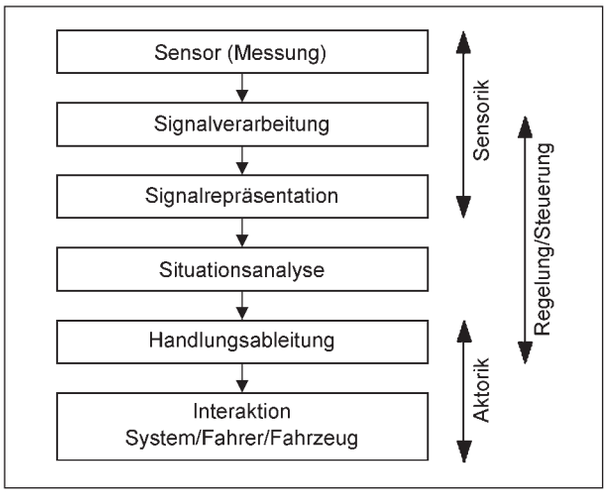

Bild 1: Schematischer Ablauf der Umfelderfassung[5]

Die einzelnen Elemente dieses Ablaufs sind jedoch bei realen Systemen nicht immer klar voneinander zu trennen. Ebenso kann dieser Ablauf auch nicht unbedingt an Bauteile gekoppelt werden, da die Kopplung von der Systemarchitektur des Fahrzeugs abhängig ist. Zudem kann die Fahrer-Fahrzeug-Interaktion einen großen Einfluss auf die Ergebnisse haben. Entsprechend ist eine Bewertung der Systeme meist nur als Ganzes durchführbar, wenn zum Beispiel der Nutzen oder die Risiken des Gesamtsystems beurteilt werden sollen.

Aus der Analyse dieses Ablaufs ergeben sich Problemstellungen für die Absicherung und Freigabe von FAS. Umfelderfassende Systeme müssen in der Lage sein, aus den durch die Sensorik bestimmten Messwerten die relevante Information zu identifizieren. Beschränkt durch die Qualität der Sensorik und durch die mit dem jeweiligen Messprinzip erfassbaren Merkmale sind diese Daten im Allgemeinen unvollständig und fehlerbehaftet. Diese Unvollständigkeit ist nicht per se negativ, sondern kann durchaus gezielt zur Reduktion der zu verarbeitenden Datenmenge genutzt werden. Ebenso können aufgrund von Annahmen über das Umweltverhalten auch nach der Messung bestimmte Daten ausgeschlossen oder vernachlässigt werden. Für eindeutig definierte Nutzfälle der Systeme, in denen beispielsweise die zu detektierenden Objekte eindeutig hinsichtlich der Messbarkeit mit dem Sensorkonzept identifizierbar sind,

4 GASSER et al. (2012)

5 Vgl. STILLER (2005), S. 8, und DARMS (2007), S. 9

kann bei dieser Vorgehensweise sichergestellt werden, dass alle in den Anforderungen definierten Objekte erfasst werden können. Für die Verwendung der Systeme im öffentlichen Straßenverkehr ist dabei jedoch einerseits die exakte Definition der Anforderungen, beispielsweise an zu erkennende Objekte, relevant und andererseits die Absicherung von funktionalen Unzulänglichkeiten und potenziellen Fehlerkennungen bzw. Fehlinterpretationen.

In beiden Fällen resultiert aus einer potenziell unvollständigen Abbildung aller denkbaren Anwendungsfälle durch die Anforderungen eine unbeabsichtigte, nicht situationsgerechte Bewertung durch das System. Deutlich wird diese Problematik beispielsweise bei der Gestaltung von Ersatzzielen für die Untersuchung von FAS. MARX et al. (2013) liefern hier ein Beispiel, wie durch umfangreiche Messungen an Realfahrzeugen ein repräsentativer Radarrückstrahlquerschnitt eines Pkw aus unterschiedlichen Richtungen ermittelt wird. Daraus werden Aussagen für die Mindestanforderungen an ein Zielobjekt für das Testen der Systeme abgeleitet. In diesem Beispiel werden mehrere Fahrzeuge aus unterschiedlichen Klassen vermessen, um einen repräsentativen Querschnitt des Realverkehrs abzubilden. Im Umkehrschluss lässt sich daraus ableiten, dass dieses repräsentative Kollektiv von Fahrzeugen auch durch die jeweilige Sensorik erfassbar sein muss, um im Realverkehr den gewünschten Nutzen zu gewährleisten.

Für die Bewertung eines Gesamtsystems müsste daher die Repräsentativität der gestellten Anforderungen bestimmt werden. Dies setzt jedoch die Verfügbarkeit umfangreicher statistischer Daten zu der jeweiligen Problematik (in diesem Beispiel der Fahrzeugbestand) voraus, welche theoretisch zudem von beliebiger Detailtiefe sein können (bspw. Farbgestaltung des Fahrzeugbestandes) als auch abhängig vom Einsatzbereich variieren (bspw. Betrieb des Fahrzeugs in versch. Ländern). Zudem können die Anforderungen bei dieser Vorgehensweise sehr umfangreich werden, sodass deren Absicherung in Versuchen einen hohen Aufwand bedeutet.

Dadurch ergibt sich die Herausforderung, welche Anforderungen an den minimalen Testsituationsumfang gestellt werden, damit dieser für eine objektive Absicherung von Systemen mit Umfeldwahrnehmung als ausreichend angesehen werden kann.

Um die Unterstützung des Fahrers zu ermöglichen, müssen die Systeme über eine Mensch-Maschine-Schnittstelle mit ihm interagieren. Die Qualität dieser Schnittstelle bestimmt damit maßgeblich das Unfallvermeidungs- oder -linderungspotenzial des Systems. Dadurch müssen Test- und Absicherungsverfahren auch diese Fahrereinbindung berücksichtigen und dadurch die Leistungsfähigkeit des Gesamtsystems Fahrer-Fahrzeug in seiner Umwelt messen und bewerten. Eine eindeutige Trennung von Fahrer und Systemreaktionen kann nur in klar abgegrenzten Bereichen vorgenommen werden. Die Komplexität der Absicherung wird dann durch das breite Spektrum an realen Fahrern hinsichtlich Fahrerfahrung, Konstitution, Ausbildungsstand, Reaktionsvermögen usw. erhöht.

2.2 Vorgehensweise

Um die Absicherung von Fahrerassistenzsystemen mit Umfeldwahrnehmung auch bei steigender Komplexität belastbar gewährleisten zu können, werden die unterschiedlichen Problemstellungen bei dieser Absicherung analysiert. Bestehende Normen und Richtlinien werden identifiziert und ein Vergleich mit Luft- oder Schienenverkehr abgeleitet. In der Folge werden bestehende Kontrollmechanismen für Straßenfahrzeuge diskutiert, um gegebenenfalls existierende Lücken aufzuzeigen. Die automobilspezifische Norm zur funktionalen Sicherheit, die ISO 26262 (2009), wird hinsichtlich der Anwendbarkeit auf die vorliegende Problematik geprüft um Grenzen oder Einschränkungen zu ermitteln.

Basierend auf der Funktionskette umfelderkennender Systeme werden Anwendungsfälle aus der Fahrerassistenzforschung dargestellt, die bestehende Problematiken weiter konkretisieren und diskutieren und teilweise Lösungsansätze für die Bereiche aufzeigen. Ebenso wird der theoretische Absicherungsaufwand basierend auf konventionellen, bekannten Methoden abgeschätzt.

Basierend auf diesen Erkenntnissen wird ein Ansatz entwickelt, der eine systematische Ableitung von Prüffällen und eine Bewertung der Relevanz ermöglicht.

Abschließend werden die gewonnenen Erkenntnisse diskutiert und potenzielle Forschungsthemen zur zukünftigen Entwicklung von Absicherungsstrategien für umfelderfassende Fahrerassistenzsysteme identifiziert.

3 Bestehende Normen und deren Übertragbarkeit

3.1 Konzept der funktionalen Sicherheit

Für die Freigabe eines Produktes ist immer der Nachweis zu führen, dass dieses auch ausreichend sicher ist. Betrachtet man darin das Teilgebiet der korrekten und sicheren Funktion des Produktes, wird dies als funktionale Sicherheit bezeichnet.[6] Für elektrische, elektronische und programmierbare elektronische Systeme im Allgemeinen fasst die technische Norm IEC/EN 61508 (2010) Anforderungen an deren sichere Gestaltung zusammen. Für bestimmte Teilgebiete existieren basierend auf dieser Norm spezifische Normen, die die jeweiligen Besonderheiten adressieren. Bild 2 zeigt schematisch Standards zur funktionalen Sicherheit in verschiedenen Bereichen.

Bei der Diskussion von technischen Normen im rechtlichen Kontext muss dabei zwischen den Rechtsnormen, beispielsweise auch EU-Richtlinien und Verordnungen, und technischen Normen, beispielsweise die genannte IEC/EN 61508, unterschieden werden.

Ausgehend von der Annahme, dass in anderen Verkehrssystemen ebenfalls die Absicherung und Freigabe elektronischer Systeme, die in die Fahrzeugführung eingreifen, notwendig sein müssten, wird ein Vergleich des öffentlichen Straßenverkehrs zu den Anwendungsfeldern Luftfahrt und Schienenfahrzeugtechnik durchgeführt. Dabei werden auch dort anzuwendende Normen diskutiert. Ziel ist es, einen Überblick über diese Fragestellungen in anderen Verkehrssystemen zu schaffen und dadurch den Einstieg in die Thematik zu erleichtern. Eine detaillierte Betrachtung aller Methoden, Vorschriften und Richtlinien würde die Zielsetzung dieses Berichtes weit überschreiten.

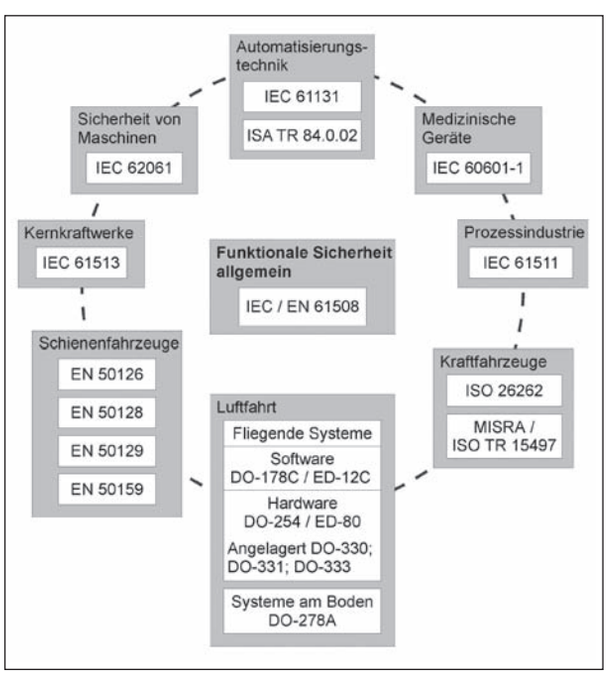

Bild 2: Bestehende Normen zur Funktionalen Absicherung elektrischer/elektronischer/programmierbarer Systeme[7]

Für eine weitere Detaillierung und Klassifizierung existierender Normen aus unterschiedlichen Anwendungsgebieten sei auf BÖRCSÖK (2011)[8] und STÄNDER et al. (2008)[9] verwiesen

3.2 Rechtliche Rahmenbedingungen zu Zulassungsverfahren und Normung

Bedingung für die Teilnahme am öffentlichen Verkehr mit einem Fahrzeug ist eine gültige Zulassung, die eine Fahrzeuggenehmigung voraussetzt (vgl. FZV (2011) § 3 Abs. 1). Die Fahrzeuggenehmigung stellt Anforderungen an das Fahrzeug, welche dieses erfüllen muss. Diese sind in entsprechenden Verordnungen oder Gesetzen der jeweiligen Staaten festgelegt. Ein Beispiel ist die Straßenverkehrszulassungsordnung (StVZO) (2012). Diese setzt teilweise wiederum harmonisierte Zulassungsbestimmungen, beispielsweise EG-Richtlinien, in nationales Recht um. In der StVZO wird ein von Kraftfahrzeugen gefordertes sicheres Verhalten definiert, sowohl allgemein (§ 30 StVZO Abs. 1) als auch spezifischer hinsichtlich besonders sicherheitsrelevanter Komponenten, beispielsweise der Bremsanlage (§ 41 StVZO) oder von Lenkeinrichtungen (§ 38 StVZO). Ein direkter Verweis auf technische Normen findet in diesen Verordnungen jedoch nur in Ausnahmefällen statt.[10] Eine Nennung von technischen Normen, die ggf. den allgemein

---

6 BÖRCSÖK (2011) ,S. 52

7 S. auch BÖRCSÖK (2011) und STÄNDER et al. (2008), S. 335

8 BÖRCSÖK (2011), S. 31 ff.

9 STÄNDER et al. (2008)

10 Bspw. bei der Definition von einzusetzenden Produkten wie Warnmarkierungen (vgl. StVZO (2012) § 52 Abs. 4 Abschnitt 1)

anerkannten Stand von Wissenschaft und Technik wiedergeben, wird in der Regel vermieden, auf Rechtsnormen, wie beispielsweise ECE-Regelungen, wird im Rahmen von Gesetzen jedoch verwiesen (vgl. StVZO, Anhang I).

Für die Darstellung der Abhängigkeiten zwischen Gesetzen, Verordnungen und technischen Normen, auf nationaler und europäischer Ebene, wird häufig die „Normenpyramide“ verwendet, die die Hierarchie der rechtlichen Normen beschreibt. In Bild 3 ist diese unter Einordnung der technischen Normen dargestellt.

Dabei werden EU- (bzw. EG-)Verordnungen unmittelbar mit ihrem Inkrafttreten verbindliche Rechtsvorschriften in allen Mitgliedstaaten.

Normen für die technische Sicherheit, beispielsweise die funktionale Sicherheit, und Zulassungsbestimmungen sind daher zunächst voneinander getrennt. Eine Verbindung wird durch das Produktsicherheitsgesetz (ProdSG) und das Produkthaftungsgesetz (ProdHaftG) hergestellt. Nach § 1 Abs. 1 ProdHaftG und § 4 ProdSG ist der Hersteller für die Fehlerfreiheit seiner Produkte verantwortlich. Er muss gewährleisten, dass das Produkt hinsichtlich seiner Konstruktion mindestens dem erforderlichen Sicherheitsstandard nach dem Stand von Wissenschaft und Technik zum maßgebenden Zeitpunkt entspricht.[11] Dieser Mindestsicherheitsstandard ist damit durch Normen und Richtlinien definiert. Implizit stellt dieser auch das akzeptierte Grenzrisiko[12] des Betriebs eines technischen Gerätes dar. Entsprechend muss der Hersteller im Schadensfall nachweisen können, dass er diesem genügt hat. Kann trotz korrekter Handhabung ein entsprechendes Risiko auf Basis des aktuellen Standes der Technik nicht ausgeschlossen werden, so ist der Hersteller zumindest verpflichtet, darauf hinzuweisen.[14]

In der Folge werden die Verkehrssysteme Luftfahrt und Schienenverkehr betrachtet und dafür vorliegende technischen Normen und deren angelagerte Umsetzungsrichtlinien, die die funktionale Sicherheit betreffen, diskutiert. Dabei wird der Begriff der Norm stellvertretend für die technische Norm verwendet.

3.3 Luftfahrt

3.3.1 Luftfahrzeug

Ein in der Luft befindliches Luftfahrzeug/Flugzeug ist in alle Raumrichtungen frei beweglich. Aufgrund der physikalischen Effekte ist eine ständige Zufuhr von Energie und der Erhalt einer Mindestgeschwindigkeit notwendig, um eine bestimmte Höhe zu halten.[15] Nur solange Bodenkontakt besteht, ist dies nicht der Fall. Für den Wechsel zwischen diesen Zuständen ist ein Start- und Landeplatz notwendig, der je nach Flugzeugtyp unterschiedlich hohen Anforderungen genügen muss. Aufgrund dessen sind Störungen oder Ausfälle, die die Energiezufuhr

11 ProdHaftG (1989), § 3 Abs. 3; vgl. auch BGH (2009)
12 S. hierzu BÖRCSÖK (2011), S. 51 ff., und S. 96 u. a.
13 In: STÄNDER (2011) nach LOSANO (2007)
14 ProdHaftG (1989), § 3 Abs. 3
15 Fluggeräte „leichter als Luft“ werden hierbei nicht betrachtet.

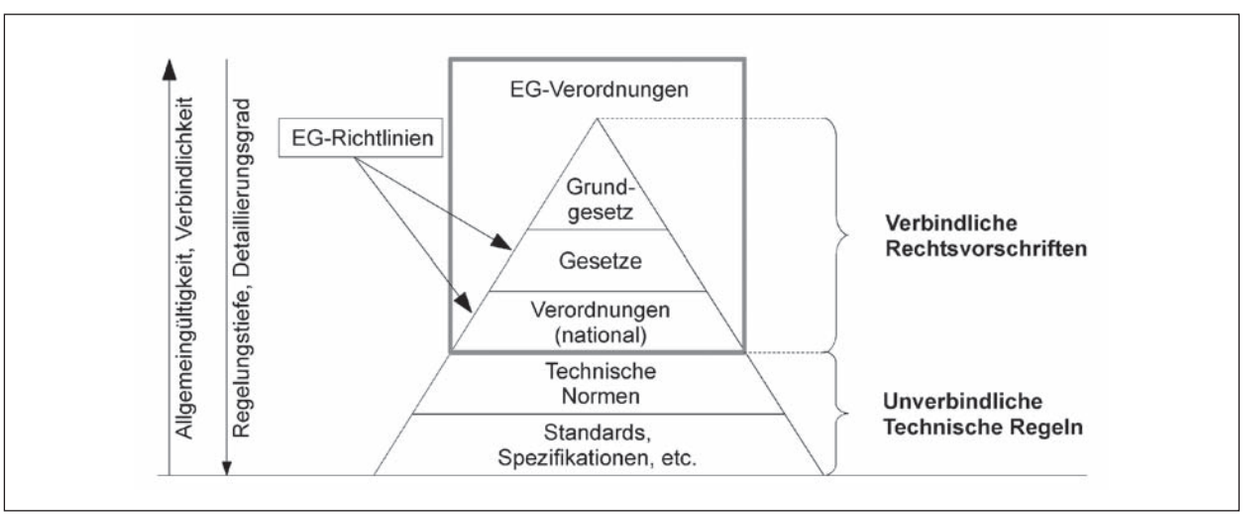

Bild 3: Normenpyramide des Rechts[13]

oder die Steuerung des Flugzeugs betreffen, unbedingt zu vermeiden, da nicht sichergestellt werden kann, dass bei einem Ausfall ein entsprechender Landeplatz erreicht und das Flugzeug sicher gelandet werden kann. Zumindest ist zu gewährleisten, dass bei einem Ausfall eine sichere Landung noch möglich ist.

Die Zulassung von Fahrzeugen für den Luftverkehr wird durch die European Aviation Safety Agency (EASA)[16] durchgeführt. Sie definiert die Standards, die zur Zulassung von Luftfahrzeugen erfüllt werden sollten, und legt Zertifizierungsvorschriften kategorisiert nach Luftfahrzeugtypen fest. Ein Beispiel für eine solche Zertifizierungsvorschrift ist die CS-25 für zivile Transportflugzeuge.[17] Diese sind jedoch nicht bindend.[18] Die jeweiligen genehmigenden Luftfahrtbehörden sind berechtigt, auch andere Zulassungswege anzuerkennen. Die EASA-Richtlinien[19] verweisen dabei beispielsweise direkt auf die Identifikation der Sicherheitsebenen nach DO-178.

Die DO-178B[20] (bzw. für Systeme am Boden die DO-278A) legt die Prozesse für die sichere Planung und Entwicklung, die Verifikation und die Qualitätssicherung von sicherheitskritischer Software fest. Sie verweist hinsichtlich der Fehlerdefinition und -quantifizierung auf das Federal Aviation Administration Dokument AC 25-1309-1A.[21] Darin findet sich die Fehlerzustandsbemessung (Failure Condition Classification) anhand der Kriterien Folgenschwere, Auftretenshäufigkeit sowie Vermeidungs-/ Entdeckungsmöglichkeiten wieder. Dazu werden Techniken wie die Functional Hazard Analysis (FHA) bzw. für qualitative Bewertung Fault Tree Analysis (FTA) und Failure Modes and Effects Analysis (FMEA) empfohlen. Die Vermeidungs-/ Entdeckungsmöglichkeiten sind weiter aufgeteilt in Flugpersonal, Bodenpersonal, regelmäßige Zustandskontrolle (insb. für latente Fehler) und den Nachweis, dass auch ohne diese Systeme ein Flug bzw. eine sichere Landung möglich ist.[22]

Die DO-178B beschreibt unter anderem Methoden zur Generierung von „Test-Cases“ für die Prüfung der Software und für die Bestimmung der „Test Coverage“, die die Abdeckung der Anforderungen in „Test-Cases“ nachweist.[23]

Bei der 2011 erfolgten Änderung zur neueren Version DO-178C/ED-12C wurden weitere, angelagerte Normen ergänzt, die Software Tools (DO-330), modellbasierte Entwicklung und deren Verifikation (DO-331), objektorientierte Technologien und formale Methoden (DO-333) adressieren.

Die auf luftfahrttechnische Software ausgerichtete DO-178B/C wird hier beispielhaft herangezogen. Aufgrund der Fokussierung auf Software stellt sie nur einen kleinen Ausschnitt der in der Luftfahrt verwendeten Prozesse und Abläufe dar. Weiterführend sollten hier die Prozesse nach den Standards ARP 4761 „Safety Assessment Process Guidelines & Methods“, ARP 4754A/ED-79 „Aircraft & System Development Processes“ und die DO-297/ED-124 „Guidelines for Integrated Modular Avionics“ analysiert werden. Nicht funktionale Anforderungen an avionische Systeme fassen beispielsweise PAULITSCH et al. (2009) zusammen.

3.3.2 Unfallanalyse

Im Luftverkehr ist eine strikte Nachverfolgbarkeit von Fehlern vorgesehen. Dazu wird eine umfangreiche Dokumentation des Betriebes gefordert, beispielsweise die Abgabe eines Flugplanes für bestimmte Flugarten, das Erstellen eines Hauptflugbuchs auf Flugplätzen[24] oder das Verfassen eines Flugbetriebshandbuches für Luftfahrzeuge in Luftfahrtunternehmen.[25] Zusätzlich werden sämtliche Unfälle durch eine unabhängige Stelle untersucht. In Deutschland führt dies die BFU (Bundesstelle für Flugunfalluntersuchung) durch und veröffentlicht umfangreiche Unfallberichte. Sie fassen das Unfallgeschehen zusammen und bewerten Unfallursachen und Unfallbeitragsfaktoren. Auch Vorfälle, die nur zu Sachschaden führen, werden dabei erfasst (Unfallmeldung nach § 5 LuftVO (2013); Anzeige von Unfällen und Störungen beim Betrieb ziviler Luftfahrzeuge nach § 5 LuftVO (2013) an die BFU).

---

16 www.easa.europa.eu

17 European Aviation Safety Agency (EASA) (2007)

18 Vgl. www.easa.europa.eu/rulemaking/faq/acceptable-means-of-compliance-AMC.php: Abruf am 28.11.2012

19 EASA (2012), Referenzierung über AMC 20-115

20 Radio Technical Commission for Aeronautics (RTCA) (1992), in Europa auch als ED-12 B/C

21 S. FAA (1988)

22 FAA (1988), S. 10 ff.

23 RTCA (1992), S. 30 ff.

24 LuftVG (2013) § 70

25 LuftBO (2013) § 37

3.3.3 Bediener

In modernen Flugzeugen wird der Pilot durch zahlreiche Systeme in der Ausführung seiner Aufgabe unterstützt. Diese „assistieren“ ihm, dem modernen Pkw vergleichbar, bei der Navigation, bei der Manöverdurchführung und der Stabilisierung des Luftfahrzeugs. Auf der Stabilisierungsebene wird die Leistungsfähigkeit des Luftfahrzeugs durch den „Flight Envelope“ begrenzt. Innerhalb dieses wird der Pilot durch elektronische Systeme, als „Electronic Flight Control“ (EFCS) bezeichnet, bei der Stabilisierung, der Lageregelung und der Bahnregelung unterstützt.[26] Piloten durchlaufen zudem eine intensive Ausbildung. Für das Führen eines Luftfahrzeugs müssen sie sowohl eine Pilotenlizenz als auch eine Berechtigung für das jeweilige Flugzeug-Baumuster vorweisen. Auch die Bewältigung kritischer Situationen ist Bestandteil der Ausbildung.[27] Lizenzen und Berechtigungen sind in regelmäßigen Zeitabständen zu erneuern. Insofern es sich um kommerziellen Luftverkehr handelt, übt der Pilot seine Tätigkeit als Beruf aus, er ist seinem Arbeitgeber, der häufig auch Eigentümer des Flugzeugs ist, direkt verpflichtet. Dieser kann Anweisungen erteilen, wie und in welchen Grenzen das Flugzeug bewegt werden muss.

3.3.4 Verkehrsraum und Umfeld

Der Luftraum wird gemäß der Definition der ICAO in Klassen A-G unterteilt, diese sind in der LuftVO analog hinterlegt.[28] Unterscheidungsmerkmal ist dabei, die Art der Luftraumkontrolle und ob Instrumentenflug-Verkehr (IFR) oder Sichtflug-Verkehr (VFR) durchgeführt wird. Der gesamte Luftraum ist in diese Klassen aufgeteilt, ein Beispiel zeigt Bild 4.

In Lufträumen mit großem Verkehrsaufkommen werden zudem Flugrouten und „Luftstraßen“ festgelegt. Allgemein wird der Luftraum ständig durch eine externe Institution, die Flugsicherung, überwacht und geplant. Diese gibt bestimme Wege mit Sicherheitszuschlägen für Flugzeuge frei, sodass die Annäherung an einen weiteren „Verkehrsteilnehmer“ nicht vorkommen sollte und an sich bereits eine kritische Situation darstellt. Typische Abstände sind 9,3 bis 27,8 km[30] in Längsrichtung, 92,6 km für nebeneinander fliegenden Flugzeuge und 610 m vertikaler Abstand im oberen Luftraum.[31] Werden diese Abstände unterschritten, kann diese Regelverletzung entweder durch ein Antikollisionssystem oder durch den Fluglotsen erkannt werden, die den Piloten warnen. Ein Beispiel hierfür ist das „Traffic Alert and Collision Avoidance System“ (TCAS). Es informiert den Piloten über ein sich näherndes Flugzeug und warnt bei einer drohenden Kollision innerhalb der nächsten 15 bis 35 Sekunden.[32] Die Überwachung erfolgt also durch mehrere unab-

---

26 S. KLUßMANN et al. (2004), S. 83 ff.

27 Bundesministerium für Verkehr (2009), deutsch, 2009, S. 86 ff.

28 Anlage 4 (zu § 10 Abs. 2 LuftVO), Luftraumklassifizierung und Flugverkehrsdienste

29 In Anlehnung an DFS (2012)

30 Die Angaben sind zur besseren Lesbarkeit von nautischen Meilen in Meter bzw. Kilometer umgerechnet.

31 KLUßMANN et al. (2004), S. 194

32 KLUßMANN et al. (2004), S. 287 ff.

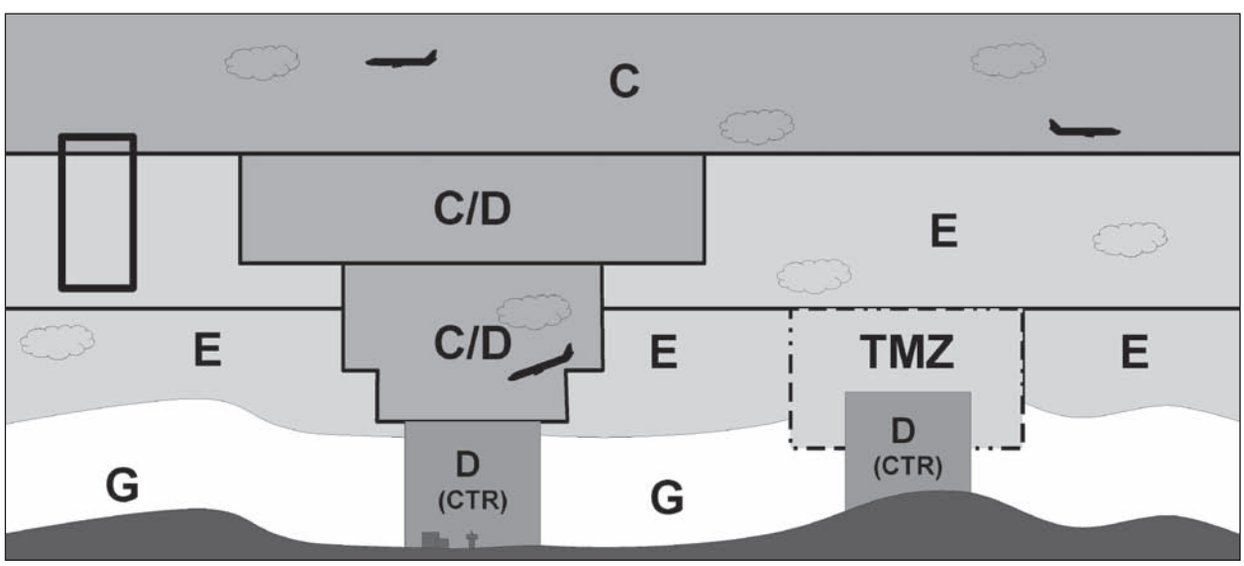

Bild 4: Luftverkehrsstruktur BRD[29]

hängige technische Systeme bzw. Personen. Nicht durch Menschen kontrollierte Objekte, die groß genug sind, das Luftfahrzeug zu gefährden, sind kaum zu erwarten.[33] Insofern kann der Luftraum als abgeschlossener, kontinuierlich überwachter Bereich betrachtet werden, der zudem auf umfangreicher Kommunikation zwischen den Beteiligten bzw. mit den überwachenden Stellen basiert.

3.4 Schienenverkehr

3.4.1 Fahrzeug

Beim Schienenfahrzeug kann der Bediener im Fahrzeug nur auf den longitudinalen Freiheitsgrad Einfluss nehmen. Zudem ist aufgrund des durch den geringen Reibwert langen Bremsweges eines Schienenfahrzeugs die Fahrt auf Sicht nur bei geringen Geschwindigkeiten möglich. Der Fahrzeugführer ist damit darauf angewiesen, dass der Fahrweg frei ist, dies kann durch ihn nicht kontrolliert werden. Eine Reaktion ist nur auf Signale möglich. Durch die daraus resultierende enge Verknüpfung von Fahrzeug und Verkehrssystem ist eine isolierte Betrachtung nur der fahrzeugrelevanten Sicherheitstechnik kaum durchführbar. Das Fahrzeug muss immer in der Infrastruktur und dem Betriebsablauf betrachtet werden. Normen und Richtlinien werden daher in der Folge auf das Gesamtsystem bezogen dargestellt. Ein Beispiel für diese Verknüpfung sind beispielsweise die zur technischen Sicherung eingesetzte Sicherheitsfahrschaltungen (SiFa), die beispielsweise das Überfahren von Signalen verhindern sollen.

Relevante Normen, die die Sicherheit von elektronischen oder elektrischen Systemen betreffen, sind die DIN EN 50126 (1999), die DIN EN 50128 (2011) und die DIN EN 50129 (2003). Diese werden aktuell überarbeitet mit dem Ziel, sie sowohl zueinander als auch zu der IEC 61508 in der aktuellen Fassung von 2010 zu harmonisieren.[34] Dazu werden beispielsweise die darin definierten „Safety Integrity Level“ (SIL) hinsichtlich ihrer Definition in der DIN EN 50126 bis 50129 angepasst.[35] Grundsätzlich sind in den Sicherheitsnormen der DIN EN 50126 aber ebenso Gefährdungsstufen festgelegt, die die Folgenschwere von Fehlern definieren. Ebenso folgt die Produktauslegung dem V-Modell. Bezieht man sicherheitsrelevante Kommunikationssysteme ebenfalls ein, so ist zusätzlich die DIN EN 50159 (2003) zu berücksichtigen. Bild 5 zeigt die unterschiedlichen Normen des Gesamtsystems Bahnanlage in ihrer Zuordnung bzw. Abhängigkeit zueinander.

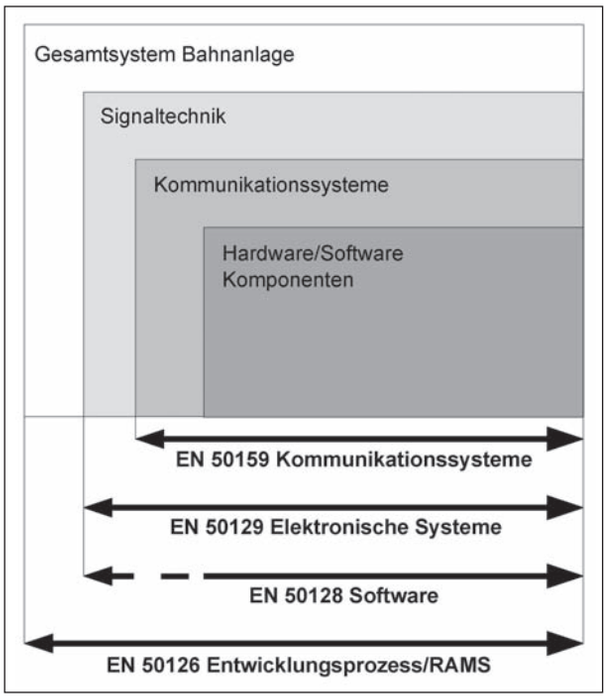

Bild 5: 5012X – Normensuite in der Schienenfahrzeugtechnik[36, 37]

Die Umsetzung der Normen bei der realen Zulassung von Fahrzeugen für den Schienenverkehr ist in der Sicherheitsrichtlinie Fahrzeug (SIRF)[38] definiert. Darin ist festgelegt, wie der Nachweis der funktionalen Sicherheit bei Schienenfahrzeugen zu erfolgen hat. Sie verweist direkt auf die EN 50126, 50128 und 50129 und definiert für die Einteilung in Sicherheitsanforderungsstufen ein an die IEC 61508 angelehntes Bewertungsverfahren.[39] Dieses bezieht neben den üblichen Kategorien Expositionswahrscheinlichkeit, Schadensschwere und Vermeidungsmöglichkeiten auch eine Expositionszeit ein. Ebenso werden die Bewertungsgrundlagen detaillierter definiert.

---

33 Ausnahme bilden unter Umständen Vogelschwärme, insbesondere bei kleineren Flugzeugen, und „Sonderereignisse“ wie beispielsweise Vulkanasche in der Atmosphäre.

34 Vgl. GRIEBEL (2012)

35 Vgl. GRIEBEL (2012)

36 In Anlehnung an GRIEBEL (2012), S. 3, und WESTERKAMP (2004,) S. 6

37 RAMS: Abkürzung für Zuverlässigkeit, Verfügbarkeit, Instandhaltung und Sicherheit (Reliability, Availability, Maintainability, Safety)

38 Eisenbahn-Bundesamt (2012)

39 Eisenbahn-Bundesamt (2012), S. 2

Schaden (S) = S_A x S_V	
Anzahl S_A	
Einer	1 Person
Mehrere	1 < x < 10 Personen
Viele	> 10 Personen
Verletzungsgrad S_V	
Leichtverletzte (LV)	Gefährdung führt zu einem Unfall mit leichten Verletzungen (Prellungen, Frakturen) unterhalb von 2 Tagen Krankenhausaufenthalt und ohne irreversible Folgeschäden.
Schwerverletzte (SV)	Gefährdung führt zu einem Unfall mit mindestens 2 Tagen Krankenhausaufenthalt und/oder irreversible Folgeschäden (bis zu 50 % Behinderung).
Tote	Gefährdung führt zu Unfall mit tödlichen Verletzungen (Tod erfolgt innerhalb von 30 Tagen nach dem Unfall) oder zur sofortigen Todesfolge.

Tab. 1: Schadensschwere Bewertung nach SIRF[40]

Tabelle 1 zeigt einen Ausschnitt aus der SIRF zur Bewertung der Schadensschwere.

Ebenso werden die jeweiligen Kategorien mit entsprechenden Zahlenwerten belegt, eine Formel zur Verrechnung dieser Zahlenwerte definiert und eine Einstufungstabelle vorgegeben, anhand derer die Sicherheitsanforderungsstufe festzulegen ist.

Analog zu den Umsetzungsbestimmungen zur Zulassung in anderen Bereichen ist die Anwendung der beschriebenen Methoden nicht verpflichtend, eine Nachweisführung nach anderen Verfahren und Methoden ist möglich.

3.4.2 Unfallanalyse

Alle gefährlichen Ereignisse[41] (bspw. „Vorbeifahrt eines Zuges am Haltbegriff“) im Bahnbetrieb sind dem Eisenbahn-Bundesamt zu melden. Diese können Bahnbetriebsunfälle sein oder eine gefährliche Unregelmäßigkeit, die entweder fahrende Schienenfahrzeuge beeinträchtigt oder in Gefahr bringt oder von fahrenden Schienenfahrzeugen ausgeht. Bei schweren Unfällen[42] muss die Eisenbahn-Unfalluntersuchungsstelle des Bundes (EUB) eine Untersuchung durchführen, in den übrigen Fällen kann sie dies tun.[43] Die EUB, unter Leitung des Bundesministeriums für Verkehr, Bau und Stadtentwicklung (BMVBS), ist eine unabhängige Stelle zur Untersuchung von gefährlichen Ereignissen im Eisenbahnbetrieb. Die Ermittlung zur Unfallursache dient der Vermeidung der Wiederholung. Die im Rahmen dieser Untersuchung angefertigten Unfallberichte sind frei zugänglich.[44]

3.4.3 Bediener

Die Triebfahrzeugführer müssen auf der jeweiligen Triebfahrzeugbaureihe geschult sein und ihre Qualifikation regelmäßig nachweisen, in dieser Ausbildung sind auch Schulungen des Umgangs mit betrieblichen und technischen Unregelmäßigkeiten enthalten.[45] Sie werden bei der Ausführung ihrer Aufgabe durch technische Systeme innerhalb und außerhalb des Fahrzeugs kontrolliert. So sollen Sicherheitsfahrschaltungen und Zugbeeinflussungssysteme vermeiden, dass mehrere Züge gleichzeitig in den gleichen Streckenabschnitt einfahren.[46] Diese Systeme unterstützen auch den Triebfahrzeugführer, indem beispielsweise die Signale außerhalb des Fahrzeugs auch im Führerstand angezeigt werden und dieser bereits vor dem Erreichen des Signals darüber informiert wird, wie es gestellt ist.[47] Der Triebfahrzeugführer übt seine Tätigkeit in der Regel als Beruf aus, es ist also davon auszugehen, dass er diese häufig ausführt und dabei seinem Arbeitgeber, in den meisten Fällen dem Betreiber/dem Eigentümer des Fahrzeugs, direkt verpflichtet ist, sodass dieser Anweisungen erteilen kann, wie und in welchen Grenzen das Fahrzeug bewegt werden muss.

---

40 Eisenbahn-Bundesamt (2012), S. 3

41 Definition gemäß Eisenbahn-Bundesamt (2009), in Anlehnung an RL 2004/49/EG

42 ebd.

43 EUV (2007), § 2 Abs. 2

44 S. http://www.eisenbahn-unfalluntersuchung.de

45 Deutsche Bahn (2012)

46 S. PACHL (2011), S. 55 ff.

47 S. PACHL (2011), S. 67 ff.

Sind Streckenabschnitte mit moderner Leittechnik ausgestattet, können die Triebfahrzeugführer die Automatische Fahr- und Bremssteuerung (AFB) verwenden, die Freiinformationen und Geschwindigkeitsvorgaben in optimale Fahrprofile umgesetzt werden. Der Fahrer ist in diesem Fall für die Überwachung zuständig.

3.4.4 Verkehrsraum und Umfeld

Da eine Fahrt auf Sicht aufgrund der notwendigen Bremswege nicht möglich ist, müssen Schienenfahrzeuge im Raumabstand bewegt werden. Deswegen werden, ähnlich wie in der Luftfahrt, die Fahrzeugbewegungen durch eine externe Institution, die Fahrdienstleitung, überwacht und freigegeben. Sie sorgt dafür, dass sich nicht mehrere Fahrzeuge im gleichen Streckenabschnitt bewegen. Zudem handelt es sich jeweils um geplante Bewegungen des Verkehrs; Start und Ziel stehen bereits zu Beginn fest. Dadurch kann die allgemeine Überwachung mit einem vergleichsweise hohen Automatisierungsgrad erfolgen und menschliche Eingriffe sind nur noch bei Abweichungen oder Störungen erforderlich. Darüber sollen Kollisionen mit anderen Gleisverkehrsteilnehmern ausgeschlossen werden. Um zu vermeiden, dass sich beispielsweise Personen im Gleisbereich aufhalten, sind das Betreten von Gleisanlagen und das Umgehen von Schranken in der Eisenbahn-Bau- und Betriebsordnung (EBO) verboten.[48] In städtischen Bereichen sind zudem Bahnanlagen häufig so geführt oder gesichert, dass kein unbeabsichtigtes Eindringen in den Gleisbereich erfolgen kann (bspw. durch Zäune oder durch Geländeeinschnitte). Ebenso ist in der EBO § 17 eine regelmäßige Überwachung und Untersuchung der Bahnanlage vorgesehen, die sich nach der Belastung der Bahnanlage und der zulässigen Geschwindigkeit richten. Eine kontinuierliche Überwachung erfolgt jedoch nicht. In einigen Hochgeschwindigkeitszugnetzen sind die Strecken eingezäunt, um sowohl unbefugtes Betreten, beispielsweise durch suizidgefährdete Personen, zu verhindern als auch Tiere vom Gleiskörper fernzuhalten. Wie in Kapitel 3.4.1 bereits angesprochen, jedoch die Gestaltung des Verkehrsraumes, z. B. die Netzgestaltung, aber auch Elemente wie Weichen, Bahnübergänge und die dazugehörigen Normen streng genommen in allgemeine Sicherheitsbetrachtungen mit einzubeziehen.

Bei autonomen Schienenfahrzeugen ist der Gleiskörper abgeschlossen, d. h. mit räumlicher Trennung versehen, um Außeneinflüsse zu minimieren. Bahnsteige sind entweder mit zusätzlichen Türen an der Bahnsteigkante versehen, die einen Zugang zum Gleiskörper vom Bahnsteig nur dann ermöglichen, wenn ein Zug eingefahren ist, oder der Bahnsteigbereich wird kontinuierlich mit Kamera und HF-Sensoren überwacht.[49] Zusätzlich wird der Betrieb durch zentrale Leitstellen überwacht.

3.5 Öffentlicher Straßenverkehr

3.5.1 Fahrzeuge

Die Fahrzeuge im öffentlichen Straßenverkehr unterliegen ebenso einer Genehmigungspflicht wie andere Verkehrssysteme. Eine regelmäßige technische Kontrolle dieser zulassungsrelevanten Eigenschaften ist zumindest in Deutschland ebenfalls vorgeschrieben. Bezüglich sicherheitskritischer Software im automobilen Kontext existiert bereits seit Beginn der 90er Jahre die „Motor Industry Software Reliability Association“ (MISRA)[50], die Entwicklungsrichtlinien wie die 1994 erschienenen „Development Guidelines for Vehicle Based Software“[51] erstellt. In den folgenden Jahren sind weitere Dokumente hinzugekommen, die neue und erweiterte Programmiertechniken adressieren und beispielsweise auf modellgestützte Softwareentwicklung ausgerichtet sind.

Seit 2011 sind Richtlinien für die Gewährleistung der funktionalen Sicherheit von Hard- und Softwarekomponenten in der ISO 26262 zusammengefasst. Sie beschreibt eine Risikobewertung im frühen Entwicklungsstadium sicherheitskritischer Systeme und leitet daraus Anforderungen an den gesamten Lebenszyklus des Produktes ab.[52] Dieses Konzept findet sich sowohl im Schienenverkehr und der Luftfahrt wieder und stellt die Umsetzung der in der allgemeinen Norm IEC 61508 beschriebenen Methoden und Prozesse für die spezifischen Anwendungen dar.

Hinsichtlich der Zusammenhänge von Zulassungsbestimmungen und Umsetzungs- und Anwen-

---

48 Vgl. EBO § 62, § 63 und § 64

49 Am Beispiel der Nürnberger U-Bahn: www.rubin-nuernberg.de, Abruf am 28.11.12

50 Motor Industry Software Reliability Association(1995)

51 Motor Industry Software Reliability Association (1995), auch als ISO TR 15497 veröffentlicht

52 Eine ausführlichere Betrachtung der ISO 26262 findet sich in Kapitel 3.9.

dungsrichtlinien konnten keine analog zu Luftfahrt oder Schienenfahrzeugtechnik entwickelten Definitionen des Standes der Technik für die Zulassung gemäß den gesetzlichen Bestimmungen identifiziert werden, wie dies beispielsweise in der SIRF-100 und -400 der Fall ist. In ähnlicher Ausrichtung kann aber der „Code of Practice“[53] gesehen werden, der den Stand der Technik zur Bewertung der Kontrollierbarkeit von Fahrerassistenzsystemen mit Umfeldwahrnehmung im Fehlerfalle zusammenfasst und im Rahmen eines von der EU geförderten Projektes entstanden ist. Eine rechtliche Verknüpfung von Normen und der Zulassungsfähigkeit von Fahrzeugen ist über die in Kapitel 3.2 beschriebenen Zusammenhänge gegeben.

Eine gewisse Sonderstellung können dabei die EG-Richtlinien einnehmen, die direkt Fahrzeugfunktionen betreffen und diese durch regulatorischen Eingriff als verpflichtend für bestimmte Fahrzeugtypen vorschreiben. Ein Beispiel hierfür ist die gesetzliche Forderung von Notbremssystemen für Lkw in Neufahrzeugen ab dem Jahr 2013. Diese ist allgemein in der Verordnung EC 347/2012 definiert, diese wiederum ist über die EC 661/2009 der Richtlinie 2007/46/EC zugeordnet, welche die Zulassung von Kraftfahrzeugen allgemein regelt. In der EC 347/2012 sind die geforderten Reaktionen der geforderten Notbremssysteme explizit definiert, es werden Warnelemente, Mindestwarnzeitpunkte und die Geschwindigkeitsbereiche vorgegeben, in denen die Systeme arbeiten müssen. Ebenso werden Methoden vorgeschlagen, mit denen die Fehleranalyse und -bewertung erfolgen können, und Testsetups vorgegeben.[54] Damit ist dieses Beispiel für ein regulatorisches Dokument bereits sehr spezifisch und detailliert.

3.5.2 Unfallanalyse

Nur bei erheblichem Sachschaden oder Personenschaden kann sicher davon ausgegangen werden, dass ein Verkehrsunfall an öffentliche Stellen gemeldet wird. Diese Meldung erfolgt an die Polizei, die gegebenenfalls am Unfallort eine Beweisaufnahme durchführt. Die Zielsetzung dieser Beweissicherung ist meist die Klärung der Schuldfrage. Detailliertere Ursachenforschung wird durch Unfallforschungseinrichtungen durchgeführt, die in bestimmten Regionen Verkehrsunfälle bereits am Unfallort aufnehmen und die so gesammelten Daten auswerten.[55] Ebenso unterhalten einige Fahrzeughersteller eigene Unfallforschungsabteilungen.[56] Eine zentrale Unfalluntersuchungseinrichtung existiert in Deutschland nicht. Um für die Fahrzeugentwicklung eine ausreichend große Stichprobe aus dem Unfallgeschehen in Deutschland zu erhalten, bei der Unfälle mit Personenschaden detailliert erfasst werden, wurde im Jahr 1999 in den Großräumen Hannover und Dresden das GIDAS-Projekt initiiert.[57] Eine detaillierte deutschlandweite Untersuchung jedes einzelnen Verkehrsunfalles nach dem Vorbild von Luft- und Schienenverkehr ist aufgrund der hohen Anzahl aus volkswirtschaftlichen Gründen aber sicherlich nicht vertretbar und bei ausreichender Größe und Relevanz der genannten „GIDAS-Stichprobe“ auch nicht notwendig.

Wird dem Hersteller/Produktverantwortlichen eine potenzielle Gefährdung durch Fahrzeuge erst bekannt, wenn sich bereits Fahrzeuge in Kundenhand befinden, ist er verpflichtet, das Kraftfahrtbundesamt (KBA) zu informieren und die Gefahren zu beseitigen.[58] Bei diesen Rückrufaktionen wird er vom Kraftfahrtbundesamt unterstützt und auch überwacht.[59] Basierend darauf kann das KBA auch Rückrufe anordnen, wenn die vom Hersteller eingeleiteten Maßnahmen nicht als ausreichend schnell oder wirksam erachtet werden.

3.5.3 Bediener

Die Bediener von Pkw werden nur bei Erwerb der Fahrerlaubnis ausgebildet, danach muss die Befähigung nicht wieder nachgewiesen werden. Verpflichtende Weiterbildungen sind ebenso nicht vorgesehen. Die Fahrausbildung enthält keine gezielte Schulung für kritische Situationen und eine Unterweisung auf den jeweiligen Fahrzeugtyp ist jeweils auch nicht gefordert. Die einzige Möglichkeit, den Fahrer mit den zu erwartenden Fahrzeug-Systemreaktionen vertraut zu machen, ist die Bedienungsanleitung des Fahrzeugs. Diese Informationsquelle steht anderen möglicherweise betroffenen Verkehrsteilnehmern wie Fußgängern bereits nicht mehr zur Verfügung.

---

53 PREVENT (2009), im Rahmen des Response-3-Projektes

54 EC 347/2012 (2012)

55 Bspw. VuFO GmbH Verkehrsunfallforschung Dresden, und Verkehrsunfallforschung Medizinische Hochschule Hannover

56 Bspw. Audi Accident Research Unit (AARU) oder Daimler-Unfallforschung

57 GEORGI et al. (2006)

58 KBA (2013), S. 7

59 Vgl. KBA (2013)

Nur ein kleiner Anteil der Bediener führt die Tätigkeit als Beruf aus, dadurch ist davon auszugehen, dass sich die Fahrer hinsichtlich Ausbildungsstand, Erfahrung, Fertigkeiten und Fähigkeiten stark unterscheiden.

3.5.4 Verkehrsraum und Umfeld

Im Gegensatz zu Luftfahrt und Schienenfahrzeugtechnik ist der öffentliche Verkehrsraum nicht als geschlossener und kontrollierter Raum zu betrachten. Eine räumliche Trennung von Verkehrsteilnehmern analog zur Luftfahrt, in der Fahrzeuge bestimmte Voraussetzungen erfüllen müssen, um Verkehrsräume nutzen zu dürfen, existiert nur teilweise. Beispiel hierfür sind Autobahnen, die nur mit Kraftahrzeugen benutzt werden dürfen, die eine durch die Bauart bedingte Mindesthöchstgeschwindigkeit (vgl. § 18 Abs.1 StVO (2013)) aufweisen müssen, womit eine Teilnahme von Fußgängern und Radfahrern am Verkehr auf Autobahnen ausgeschlossen wird. Im innerstädtischen Umfeld jedoch sind die unterschiedlichsten Verkehrsteilnehmer zu erwarten, diese nutzen zudem teilweise den Verkehrsraum gemeinsam und dieser ist nicht kontinuierlich räumlich voneinander getrennt (bspw. Fußgänger, die die Fahrbahn überqueren, Fahrradfahrer, die von einem abgetrennten Radweg in die Fahrbahn einfahren).

Der Verkehrsraum wird nur in Ausnahmen durch eine externe Instanz kontinuierlich kontrolliert. Ein Beispiel ist die Verkehrsbeobachtung durch Verkehrsleitzentralen, die durch Kameras den Verkehrsfluss auf Streckenabschnitten beobachten, um Verkehrssteuerung wie beispielsweise die Freigabe des Seitenstreifes zu ermöglichen. Manöver der Verkehrsteilnehmer sind nur von den Entscheidungen des Bedieners abhängig. Zudem muss mit Regelverstößen der Verkehrsteilnehmer gerechnet werden. Um die Regeleinhaltung zu gewährleisten, wird durch die Polizei eine Verkehrsüberwachung durchgeführt und Verstöße sanktioniert. Eine Planung von Start und Ziel sowie der Route wird ebenfalls durch den Bediener festgelegt und kann jederzeit auch durch spontane Einzelentscheidungen geändert werden.

Der Straßenverkehr folgt dabei dem Prinzip der Fahrt auf Sicht, die Einhaltung von sich daraus ergebenden Sicherheitsabständen obliegt den Verkehrsteilnehmern. Selbst bei Einhaltung der Verkehrsregeln ergeben sich dabei vergleichsweise kurze für Kollisionsvermeidung notwendige Reaktionszeiten im Bereich von 1 bis 2 Sekunden.

3.6 Vergleich der Verkehrssysteme

Zur Zusammenfassung der Betrachtungen wird der von STÄNDER (2011, S. 25) vorgeschlagene Vergleich der Verkehrsträger anhand der beschriebenen Erkenntnisse angepasst und erweitert (s. Tabelle 2).

Da auch die Normen anderer Verkehrssysteme auf der IEC 61508 aufbauen oder deren Entstehung beeinflusst haben, finden sich die Konzepte funktionaler Sicherheit auch dort wieder. Entsprechend sind die in der ISO 26262 beschriebenen Abläufe der Produktdefinition und Risikoidentifikation mit hoher Ähnlichkeit im Bereich von Luft- und Schienenverkehr wiederzufinden. Hinsichtlich der bereits seit längerem veröffentlichten und vor kurzem zum zweiten Mal überarbeiteten DO-178 zeigt sich, dass bei der Überarbeitung weitere Normen hinzugekommen sind, die die bei der Entwicklung verwendeten Methoden und Werkzeuge und die Verifikation und Validierung von Modellen betreffen. Dieser Bereich ist im Automobil-Segment auch zu finden und wird beispielsweise durch die MISRA Guidelines[60] dargestellt.

Da in Luftfahrtnormen die Begrifflichkeit der „Testabdeckung“ bei der Softwareentwicklung bereits verwendet wird, könnten hier eventuell aus einer tiefergehenden Analyse des gesamten Entwicklungsprozesses und der damit verbundenen Normen auch Vorgehensweisen für die Bestimmung der Testabdeckung hinsichtlich der funktionalen Anforderungen weitere Erkenntnisse gewonnen werden.

Ebenso sind in der Luftfahrt und in der Schienenfahrzeugtechnik ergänzende Dokumente üblich, die den Stand der Technik bei der Umsetzung und Anwendung der Normen zusammenfassen und dabei Zulassungskonformität gewährleisten. Mit ähnlicher Zielsetzung ist im Rahmen eines von der EU geförderten Projektes in der Automobilindustrie der „Code of Practice“[61] entstanden. Dieser bezieht

---

60 Bspw. die Motor Industry Software Reliability Association (1995), weitere unter: http://www.misra.org.uk/Publications/tabid/57/Default.aspx

61 PREVENT (2009)

	Luftfahrt[62]	**Straßenverkehr**	**Eisenbahn**
Bewegungsoptionen	3-D (Raum)	2-D (Fläche)	1-D (Linie)
Bediener			
Verantwortlicher Fahrzeugführer	meist redundant	nicht redundant	nicht redundant
Professionalität der Fahrzeugführer	fast vollständig hauptberuflich	geringer Anteil hauptberuflich	fast vollständig hauptberuflich
Ausbildung			
Theorie	> 750 Stunden	> 21 Stunden	~ 800 Stunden
Praxis	> 1.500 Stunden[63]	> 9 Stunden[64]	~ 400 Stunden[65]
Schulung auf Fahrzeugtyp	Ja	Nein	Ja
Weiterbildung	Erforderlich	Nicht erforderlich	Erforderlich
Sicherheitskonzepte des Verkehrsablaufs			
Verkehrsraum abgeschlossen	Gesetzlich festgelegte Begrenzungen	In Sonderfällen	Gesetzlich festgelegte Begrenzungen
Fahrt auf Sicht	Nein, nur in Sonderfällen[66]	Ja	Nein, nur in Sonderfällen
Technische Vorrichtungen (Beispiele)	Kollisionswarnsysteme verpflichtend	Fahrbahnmarkierung, Lichtsignalanlagen, Beschilderung	Sicherheitsfahrschaltungen, punktförmige Zugbeeinflussung, AFB[67]
Externe Überwachung	Ja: Flugsicherung	Nein	Ja: Fahrdienstleitung, Betriebszentrale
Technische Rahmenbedingungen			
Dokumentation Fahrten/Betriebsstunden	Ja	Nein[68]	Überwachung der Laufleistung[69], automatische Fahrtenschreiber
Instandhaltung, Reparatur	Nur von zertifizierten Betrieben	Werkstätten, Selbsthilfe	Nur von zertifizierten Betrieben, dann auch kleine Werkstätten
Unfallanalyse	Jeder Unfall/schwere Störung, durch unabhängige staatliche Stelle	In Einzelfällen, durch zertifizierte Gutachter	Jeder Unfall/schwere Störung, durch unabhängige staatliche Stelle
Stückzahlen (in Europa)	10^3 (fallend)	10^6 (steigend)	10^3 (fallend, bei steigender Fahrleistung pro Triebfahrzeug)
Modellwechsel	ca. 20 Jahre	ca. 5-7 Jahre	ca. 20 Jahre für Triebfahrzeuge

Tab. 2: Vergleich der Bedingungen der Verkehrssysteme[70]

sich auf die ISO 26262, die andererseits nicht direkt mit den Zulassungsbestimmungen verknüpft ist. In der Nutzfahrzeugtechnik liegen im Falle des gesetzlich vorgeschriebenen Notbremsassistenten sehr umfangreiche Zulassungsbestimmungen seitens der EU vor, die detailliert Verhaltensweisen und Mindestsystemeigenschaften definieren.

Diese Schlussfolgerungen greifen jedoch nur einzelne Elemente heraus und haben keinen Anspruch auf Vollständigkeit. Eine tiefergreifende Analyse und der Vergleich existierender gesetzlicher Regularien und technischer Richtlinien in den verschiedenen Verkehrssystemen könnten hier weitere Erkenntnisse liefern.

62 Betrachtet wird hier aufgrund der deutlich höheren Verkehrsleistung vereinfachend nur der professionelle Luftverkehr.

63 Am Bsp. der Lizenz für Verkehrspiloten ATPL (Airline Transport Pilot Licence)

64 Am Bsp. der Fahrerlaubnisklasse B in der Bundesrepublik Deutschland

65 In Anlehnung an Empfehlungen der Lokführergewerkschaft GDL

66 Vgl. Kapitel 3.3.4

67 Automatische Fahr- und Bremssteuerung

68 Als Empfehlung zu Wartungs- und Instandhaltungszwecken

69 Zwecks Wartung- und Instandhaltung, teilweise Erfassung der Stromverbräuche

70 Basierend auf STÄNDER (2011), S. 25

Anhand der Analyse der Randbedingungen der verschiedenen Verkehrsträger können die Unterschiede in den Anforderungen der Absicherung zwischen dem Straßenverkehr und dem Luft- und Schienenverkehr abgeleitet werden. Es gibt keine übergeordnete Kontroll- und Planungsinstanz, die die Bewegungen der Verkehrsteilnehmer überwacht und auf das individuelle Fahrzeug Steuerungsmöglichkeiten besitzt. Zudem sind sowohl die Bewegungen im Straßenverkehr als auch auf makroskopischer Ebene als ungeplant zu betrachten. Bei Kraftfahrzeugen kann nicht a priori davon ausgegangen werden, dass die Fahrzeugführer mit dem jeweiligen Fahrzeug und dessen Systemen vertraut sind. Allerdings ist von starken Gewöhnungseffekten des Fahrers bei häufig anzutreffenden Systemen und häufig verwendeten Fahrzeugen auszugehen. Die Fahrer werden jedoch nicht obligatorisch für Not- und kritische Situationen ausgebildet oder geschult.

Die zu befahrenden Straßen sind kein abgeschlossener Raum, sodass mit Hindernissen und Störungen unterschiedlichster Art, wie beispielsweise einer Schafherde auf der Fahrbahn, gerechnet werden muss. Die verfügbaren Reaktionszeiten sind aufgrund der hohen erreichbaren Längs- und Querdynamik der Verkehrsteilnehmer und des begrenzten Raumes im Vergleich zu anderen Verkehrsträgern kurz.

Eine unabhängige technische Unfallforschung wird in Luft- und Schienenverkehr gesetzlich vorgeschrieben. Im öffentlichen Straßenverkehr gibt es keine zentrale Einrichtung zur unabhängigen technischen Unfallforschung für jeden Einzelfall. Allerdings kann für detailliertere Unfallbetrachtungen das GIDAS-Projekt herangezogen werden, welches mit ca. 2.000 erfassten Unfällen pro Jahr[71] eine Stichprobe von etwa 6,5 ‰ der Unfälle mit Personenschaden in Deutschland[72] nimmt.

3.7 Kontrollmechanismen der funktionalen Sicherheit im Straßenverkehr

Trotz dieser scheinbar geringeren Kontrolle und Regulierung sind prominente Fälle schwerwiegender unzureichender funktionaler Sicherheit kaum bekannt. Dafür sind zwei Ursachen denkbar. Als Grundannahme dient hier, dass die Hersteller von Fahrzeugen ein großes Interesse haben, funktionale Sicherheit zu gewährleisten, dies ist sowohl hinsichtlich der allgemeinen Verantwortung zu sehen als auch gesetzlich hinterlegt über die Regularien der Produkthaftung. Ein bewusstes Zuwiderhandeln birgt hier nicht nur die Gefahr mehrerer Produkthaftungsfälle zuungunsten des Herstellers, sondern zusätzlich einen erheblichen Reputationsverlust, der zudem noch deutlich vergrößert wird, wenn nachgewiesen werden kann, dass bewusst zuwidergehandelt wurde. Wie einschneidend die Folgen eines solchen Ereignisses für einen Hersteller sein können, selbst wenn es sich nur um einen bloßen Verdacht handelt, der sich im Nachhinein als unbegründet herausstellt, haben die Fälle des Audi 5000[73] und in neuerer Zeit die „Unintended Acceleration“-Problematik von Toyota[74] gezeigt. Hinzu kommt die Verantwortung von Führungskräften im Entwicklungsprozess zur Einhaltung der technischen Regeln, die bei nachweisbaren Zuwiderhandlungen direkte juristische Konsequenzen für die Einzelperson nach sich ziehen kann. Entsprechend liegt die Vermutung nahe, dass prominente Fälle nicht bekannt sind, weil sie durch die bestehenden Prozesse, Methoden und Maßnahmen wirkungsvoll vermieden werden konnten. Alternativ wäre es auch möglich, dass die entsprechenden Fälle bereits vor der gerichtlichen Klärung durch die beteiligten Parteien geklärt wurden und daher nicht publik geworden sind.

Theoretisch ist als zweite Ursache möglich, dass eine unzureichende funktionale Sicherheit bzw. in Erweiterung die funktionale Unzulänglichkeit aber unter Umständen gar nicht objektiv beobachtbar ist und deshalb nicht bekannt wird. Daher wird hier diskutiert, inwiefern diese Fälle bereits durch bestehende Mechanismen abgedeckt sein können.

Rückmeldungen über falsches Systemverhalten direkt aus Fahrer-/Nutzersicht sind darauf angewiesen, dass der Fahrer/Nutzer in der Lage ist, richtiges bzw. falsches/fehlerhaftes/unbeabsichtigtes Systemverhalten zu identifizieren und zuverlässig zu beurteilen.

Für bestimmte Märkte ergibt sich meist basierend auf durch den Fahrer wahrgenommenen scheinbaren Fehlern jedoch ein weiterer Kontrollmechanis-

---

71 GIDAS (2013)

72 Bezogen auf das Jahr 2012 mit 306.266 Verkehrsunfällen mit Personenschaden, Quelle: Statistisches Bundesamt (2012), S. 43

73 Vgl. Manufacturing the Audi Scare (2013)

74 FORKENBROCK (2011) und KIRCHHOFF et al. (2010)

mus, dass nämlich, wenn Eigentümer oder Fahrer einen Produkthaftungsfall vermuten und das jeweilige Rechtssystem hierfür hohe wirtschaftliche Entschädigungen ermöglicht, diese den Rechtsweg initiieren werden. Die USA sind hierfür ein Beispiel. Der wirtschaftliche Nutzen eines erfolgreichen Produkthaftungsprozesses kann dort so hoch sein, dass eine ausreichende Motivation besteht, solche Fälle seitens der Eigentümer bzw. Fahrer detailliert zu untersuchen. Dies kann ebenfalls zur Aufdeckung von Fehlern führen, setzt jedoch voraus, dass die Analyse der Ursachen von Experten durchgeführt wird bzw. werden kann. In Deutschland sind solche Fälle höchstens zu erwarten, wenn der dazugehörige Unfall zu einem schweren Personen- und Sachschaden führt. Ein Beispiel hierfür ist die umfangreiche Untersuchung der technischen Beitragsfaktoren des Lkw-Unfalls in Herborn.[75]

Bei heutigen Fahrerassistenzsystemen ist zudem der Fahrer mindestens überwachend an der Fahraufgabe beteiligt oder er muss Teile dieser selbst ausführen (Bsp. ACC: überwachend in Längs-, ausführend in Querrichtung). Daher wird angenommen, dass er jederzeit in der Lage ist, korrigierend einzugreifen, sodass kritische Situationen aufgrund von funktionalen Fehlern oder Unzulänglichkeiten nicht zu einem Unfall führen.

Allgemein ist eine nachträgliche objektive Betrachtung von gemeldeten Fällen nur möglich, wenn die Situation hinsichtlich der technischen und situativen Randbedingungen einwandfrei reproduzierbar ist. Insbesondere hinsichtlich der funktionalen Unzulänglichkeiten aufgrund von Einschränkungen des Sensorsystems jedoch besteht das Problem ja genau darin, dass die aus den Sensormessdaten wahrgenommenen Merkmale der Situation (und damit die bei der nachträglichen Analyse zur Verfügung stehenden gespeicherten Signale) eben nicht der realen Situation entsprechen.

Dieses Problem besteht auch für Eigendiagnosesysteme. Für eine zuverlässige Bewertung der korrekten Funktion ist eine Referenz notwendig, die mindestens ebenso zuverlässig sein muss. Für fahrzeuginterne Systeme werden zu Diagnosezwecken Vergleiche unterschiedlicher Erfassungs- bzw. Verarbeitungspfade herangezogen.[76] Für umfelderfassende Systeme sind diese Mechanismen nur einsetzbar, wenn beispielsweise mehrere Sensorsysteme eingesetzt werden, die in der Lage sind, dieselben Objekte zu erfassen, und zudem eine Zuverlässigkeitsbewertung der Erkennung liefern.[77]

Möglich ist die Ableitung einer Fehlervermutung aus Häufungsbetrachtungen von Ereignissen. Wird ein aktives Sicherheitssystem wie beispielsweise eine Notbremsassistenz innerhalb einer Fahrt deutlich häufiger als statistisch zu erwarten wäre ausgelöst, so kann davon ausgegangen werden, dass eine Fehlfunktion vorliegt und die Funktion abgeschaltet. Zudem ist eine A-Posteriori-Bewertung von kritischen Situationen denkbar. Wurde eine kritische Situation erkannt, die aus Funktionssicht unvermeidlich zum Unfall führen müsste, und erfolgt dieser Unfall dann nicht, kann ein Fehler vermutet werden. Inwiefern eine Häufigkeitsbetrachtung solcher Fälle beispielsweise durch eine Erfassung seitens der Hersteller durchgeführt wird, ist nicht bekannt.

Letztendlich ist dabei immer zu definieren (durch Gesetzgeber/Gesellschaft), welche Fehlerhäufigkeit bzw. welcher summierter zusätzlicher Schaden als vertretbar angesehen wird. Welche Herausforderungen damit bei der Einführung von Fahrerassistenzsystemen verbunden sein können, hat HOMANN unter ethischen Gesichtspunkten betrachtet und Lösungswege aufgezeigt.[78]

Anhand des aus dieser Diskussion abzuleitenden „gesellschaftlich akzeptierten Grenzrisikos“ kann und muss der Hersteller eines Produktes nachweisen, dass er innerhalb dieser „zulässigen Schadensmenge“ bleibt. Entweder indem die Schadensschwere gering ist und der Fehlerfall dafür häufiger eintreten darf, oder dadurch, dass ein Unfall mit großer Schwere sehr selten eintritt.

Das Grenzrisiko bedingt damit die Anforderungen an die Absicherung. Inwiefern jedoch die technisch durch den Stand der Technik definierten Grenzwerte für funktionale Sicherheit nach ISO 26262 auch beispielsweise auf nicht situationsgerechte Auslösungen von aktiven Sicherheitssystemen anwendbar sind, ist nicht eindeutig definiert.[79] Bei diesen Systemen kann zudem die Einschränkung des Einsatzbereiches aufgrund von Bedenken hinsichtlich

---

75 BREUER et al. (1991)

76 S. Kapitel 4.4

77 Eine detailliertere Diskussion dazu findet sich in Kapitel 4.4.6.

78 HOMANN (2005), S. 239 ff.

79 Vgl. EBEL et al. (2010) und Kapitel 3.9

der funktionalen Sicherheit auch den Nutzen der Systeme verringern.

Zusammenfassend festzuhalten ist, dass keine Beweise gefunden werden konnten, die das Funktionieren bestehender Regelmechanismen hinsichtlich der Absicherung von Fahrerassistenzsystemen in Frage stellen. Inwiefern dies auch für die Weiterentwicklung der Systeme und die damit verbundene steigende Komplexität und Vernetzung gilt, kann jedoch nicht beantwortet werden.

3.8 Resultierende Herausforderungen bei der Absicherung

3.8.1 Situationsvielfalt[80]

Der Straßenverkehr ist kein abgeschlossenes System. Die möglichen eintretenden Ereignisse haben eine hohe Zahl von Variationsparametern. Dies wird dadurch verstärkt, dass keine externe kontinuierliche Kontrolle des Betriebes durchgeführt wird. Durch die Möglichkeit des Weiterverkaufs von Fahrzeugen ist streng genommen die Beschränkung auf bestimmte Länder oder Kontinente nicht zulässig. Allerdings ist die Genehmigung von Fahrzeugen an EU- bzw. länderspezifische Bestimmungen geknüpft, sodass unter Umständen eine Neuzulassung notwendig ist. Der Großteil der Verantwortung liegt damit beim Fahrer, der oft auch Kunde des Fahrzeugherstellers bzw. des jeweiligen Händlers ist, von dem er das Fahrzeug erwirbt.

Eine Einschränkung des Betriebsbereiches durch Regelwerke ist dadurch praktisch nicht zu realisieren. Systemgrenzen können zwar durch Betriebsanleitungen dokumentiert werden, es ist jedoch nicht gewährleistet, dass der Kunde diese auch zur Kenntnis nimmt und respektiert. Kann ein Hersteller eine sowohl die unbewusste als auch die bewusste Fehlbedienung[81] („foreseeable misuse“[82]) jedoch nicht ausschließen, so muss er auch in diesen Fällen für Sicherheit sorgen.

3.8.2 Erkennbarkeit von Fehlern

Das Verkehrssystem Straßenverkehr wird nicht kontinuierlich extern überwacht. Dadurch können die meisten Fehler nur durch den Fahrer erkannt werden, dieser ist jedoch auf die Systeme unter Umständen nicht geschult und kann den Fehler daher gar nicht identifizieren. Eine Information des Fahrers über vorliegende Fehlerzustände durch Warnleuchten im Cockpit setzt voraus, dass aufgrund der vorliegenden Informationen einwandfrei eine (wiederholte oder dauerhafte) Fehlfunktion durch das Fahrzeug identifiziert werden kann. Zudem wird das Fahren eines Pkw in wesentlich geringerem Anteil (ca. 1-2 %) als Beruf ausgeführt.[83] Die „Professionalität“ und Erfahrung der Bediener und das Verständnis des Fahrers über zu erwartendes Fahrzeugverhalten können dadurch stark schwanken. Dieser Weg kann daher für eine zuverlässige Fehlererkennung nicht genutzt werden.

Alternativ kann eine Dokumentation des Betriebes zur Erkennung von Fehlern genutzt werden. Während dies in anderen Verkehrssystemen üblich ist, kann im öffentlichen Straßenverkehr davon ausgegangen werden, dass dies aus Kunden-/Bedienersicht nicht unbedingt erwünscht ist. Dem kann durch den Einsatz sogenannter „Trojanischer Pferde“[84] begegnet werden, bei dem neben einer für den Kunden sichtbaren Komfortfunktion eine Sicherheitsfunktion ohne Zugriff auf die Aktorik eingesetzt wird. Theoretische Auslösungen können im Entwicklungsspeicher des Fahrzeugs hinterlegt, später ausgelesen und dann damit abgeglichen werden, ob nach der Auslösung tatsächlich ein Unfall erfolgte oder ob es sich um eine nicht berechtigte Auslösung gehandelt hat. Ebenso können durch gesetzliche Verpflichtungen der Verwendung von Event-Data-Recordern[85] weiterführende Daten gesammelt werden.[86] Steht diese Informationsquelle nicht zur Verfügung, können Fehler unter Umständen erst entdeckt werden, wenn es zu Schadensfällen kommt, die eindeutig auf das System zurückgeführt werden können.

3.8.3 Unfallanalyse

Der Straßenverkehr ist kein abgeschlossenes System, die möglichen eintretenden Ereignisse haben

---

80 Für die Begriffsdefinition und Unterscheidung von Situation, Szenario usw. sei auf GEYER et al. (2013) verwiesen

81 Für eine detailliertere Diskussion sei auf GASSER (2012), S. 21 f., verwiesen.

82 ISO 26262 (2009b) S. 9

83 Schätzung auf Basis einer Statistik des Bundesverbandes Güterkraftverkehr Logistik und Entsorgung (BGL) e. V. der Fahrer im Güterkraftverkehr und der Führerscheinbesitzer in Deutschland im Jahr 2007 (BASt-Info 16/2007)

84 WINNER (2001)

85 Umgangssprachlich häufig auch als „Black Box“ bezeichnet

86 NHTSA (2012)

eine hohe Zahl von Variationsparametern. Eingetretene Ereignisse technischen Versagens, die nicht direkt aus dem Unfallverlauf ersichtlich sind, sind schwierig zu erkennen und zu erfassen. Zudem ist ihr Anteil am Gesamtunfallgeschehen gering, weil ein großer Anteil der Unfälle auf menschliches Versagen oder Verschulden zurückgeführt wird (bspw. > 90 % für Verkehrsunfälle in Deutschland[87]).

Es existiert keine zentrale unabhängige Nachverfolgung der technischen Ursachen von Fehlern, eine detaillierte unabhängige Bewertung jedes einzelnen Unfallereignisses wäre volkswirtschaftlich und angesichts der beschriebenen Verteilungen der Unfallursachen aktuell auch kaum zu rechtfertigen. Dies schränkt aber auch die Verbesserungsmöglichkeiten aufgrund von Erfahrungen aus dem Betrieb ein. Allerdings kann davon ausgegangen werden, dass die meisten Fahrzeughersteller eigene Sicherheitsforschungsabteilungen haben, in denen für Modelle der eigenen Marke Unfallanalysen durchgeführt werden.[88] Insbesondere bei neuen Systemen ist von Seiten des Herstellers eine erhöhte Aufmerksamkeit zu erwarten.

Eine Verbesserung der existierenden Datenlage zu Unfällen, die potenziell von Fahrerassistenzsystemen mit Umfeldwahrnehmung beeinflusst wurden, könnte hier Hersteller und Freigabeinstitutionen unterstützen, potenzielle bisher unentdeckte Gefährdungen zu identifizieren.

In einem ähnlichen Ansatz wie bei GIDAS[89] müsste dazu mindestens jeder Unfall, bei dem vor oder während des Unfalles ein Fahrerassistenzsystem mit Umfeldwahrnehmung aktiv war, erfasst werden. Der Datensatz sollte die dazugehörigen Situationsparameter sowie die technischen Merkmale des Assistenzsystems und, in sofern vorhanden, die vom System erfassten Umfelddaten in der Vorunfallphase enthalten.

Allerdings muss dabei berücksichtigt werden, dass die zu erwartende Menge durch fehlerhafte Funktion oder Entscheidung hervorgerufener Unfälle sehr klein gegenüber der aktuellen Unfallrate ist. Nur dann könnte man die Systeme ja überhaupt einsetzen! Dadurch sind die realen Fallzahlen vermutlich gering, sodass im Vergleich zu GIDAS größere Gebiete einbezogen werden müssten, um belastbare Unfallmengen zu erhalten.

3.8.4 Nutzenbetrachtungen

Der Aufwand einer zusätzlichen Unfallanalyse und die damit verbundenen Kosten sind nur zu rechtfertigen, wenn der Nutzen für Fahrzeug- und Systemhersteller, aus gesetzgeberischer Sicht oder für die Gesellschaft eindeutig identifiziert werden kann.

Folgt man der Argumentation von HOMANN (2005, S. 244), so ist eine hohe Transparenz für die gesellschaftliche Akzeptanz unbedingt notwendig. Detaillierte Daten zu fehlerhaften Reaktionen von automatisierten Systemen im Straßenverkehr könnten dazu Argumentationsbasis bei Akzeptanzfragen bieten, insbesondere dann, wenn diese von unabhängiger Stelle erhoben werden.

Ebenso ist auch ein allgemeiner Konsens hinsichtlich gesellschaftlich akzeptabler Grenzwerte für das Restrisiko aus fehlerhaftem Systemverhalten, welches nicht durch funktionale Sicherheit abgedeckt ist, sowohl gesellschaftlich als auch für Hersteller und Zulieferer notwendig, um das maximale Potenzial unfallvermeidender Systeme nutzen zu können.[90]

In dieser Diskussion ist jeweils eine Betrachtung der Nutz- und Fehlerfälle notwendig. Wird beispielsweise aufgrund von Unsicherheiten bei der Bemessung des Risikos im Falle von funktionalen Unzulänglichkeiten der Einsatzbereich oder Funktionsumfang eines aktiven Sicherheitssystems reduziert, verringert sich damit auch der Anteil der Unfälle, die dann noch verhindert werden können. Das Unfallvermeidungspotenzial des Systems kann, zumindest für unfallvermeidende Systeme, aus dem Verhältnis von durch das System vermiedenen Unfällen zu möglicherweise durch das System erst ausgelösten Unfällen definiert werden.[91] Dieses Schaden-zu-Nutzen-Verhältnis muss dabei für alle sinnvoll unterteilbaren Gruppen von potenziellen Nutzern/Geschädigten sehr klein gegen eins bleiben (s. Formel 1).

$$SN_{Gruppe} = \frac{n_{Unfälle,\,erzeugt}}{n_{Unfälle,\,vermieden}} << 1 \qquad (1)$$

87 Statistisches Bundesamt (2012) S. 43, S. 248 ff.

88 Bspw. Audi Accident Research Unit (AARU) oder Daimler-Unfallforschung

89 S. GIDAS (2013)

90 GASSER et al. (2012), S. 25 ff.

91 Vgl. auch GASSER et al. (2012), S. 25 ff.

Dabei muss gewährleistet werden, dass die entstehenden zusätzlichen Kosten und der finanzielle Nutzen aus vermiedenen Unfällen nicht durch unterschiedliche Gruppen getragen werden. Aktuell ist dies nicht zwingend gegeben, weil die Kosten eines Unfalls grundsätzlich durch den Einzelnen getragen werden müssen, während eine geringere Unfallzahl gesamtgesellschaftlichen Nutzen bringt. Im Umkehrschluss muss sichergestellt werden, dass der Nutzen der Systeme den potenziell zusätzlichen Schaden auch finanziell auffängt. HOMANN diskutiert dazu Ansätze, wie diese Problematik angegangen werden könnte.

Sind dabei die Fehlerfälle von denselben Faktoren abhängig wie die Nutzfälle und voneinander direkt abhängig, verändert sich das Schaden-Nutzen-Verhältnis nicht. Der Gesamtnutzen sinkt jedoch, weil absolut weniger Unfälle vermieden werden. Für eine objektive Bewertung muss daher auch immer ein Absolutbezug (bspw. die Absolutzahl der Unfälle) gegeben werden. Welche Wirkungsgrade als akzeptierbar gelten, kann letztendlich nur aus der gesellschaftlichen Diskussion bzw. dem Vergleich zu ähnlichen Problematiken ermittelt werden.

3.8.5 Schlussfolgerungen

Hinsichtlich der Herausforderungen bei der Absicherung von Fahrerassistenzsystemen mit Umfeldwahrnehmung für den öffentlichen Straßenverkehr werden die folgenden Schlüsse gezogen:

- Es ist eine große Zahl von möglichen Fahrsituationen für die Risikobewertung zu betrachten. Beschränkungen des Einsatzgebietes eines Pkw als Absicherungsstrategie bzw. zur Risikominderung unterliegen nach dessen inverkehrbringen keiner externen Kontrolle mehr.
- Die Funktion muss für ein breites Kollektiv an Fahrern ausgelegt und anwendbar sein, welches hinsichtlich mehrerer Faktoren stark variiert. Ebenso muss dieses Kollektiv auch bei der Absicherung repräsentiert werden, um beispielsweise die Kontrollierbarkeit zu gewährleisten. Dabei gibt es nach aktuellem Kenntnisstand keinen Mechanismus, den Fahrer auf diese Situationen prophylaktisch und wirksam vorzubereiten. Allerdings kann er unter Umständen bereits analoge Situationen anderer Ursache erlebt haben. Ein Beispiel hierfür ist der fehlerhafte Eingriff eines Spurhalteassistenten, der hinsichtlich des Lenkradmomentes bzw. des Querversatzes mit einer Seitenwindböe vergleichbar sein kann.
- Nach Auslieferung bestehen Kontrollmöglichkeiten durch die Initiierung eines Rückrufs, diese sind jedoch zumeist mit hohen materiellen und Imageschäden verbunden. Daher muss die Funktion bzw. das System bereits zum Zeitpunkt der Freigabe für den Verkauf einen hohen Reifegrad aufweisen. Die Datenbasis für die Identifikation und Definition dieses Reifegrades kann jedoch streng genommen nur im realen Betrieb und damit in Kundenhand geschaffen werden. Es ergibt sich ein „Kausalitätsdilemma“. Durch umfangreiche Messfahrten wie beispielsweise in der „Kundennahen Fahrerprobung“[92] kann dieses Problem gelöst werden, allerdings ist der Aufwand hierfür hoch. Die Identifikation des notwendigen minimalen Situationskollektivs für die Absicherung und die Übertragbarkeit der gewonnenen Daten auf möglichst viele unterschiedliche Systemausprägungen- oder -varianten ist daher für die zukünftige Entwicklung von Fahrerassistenzsystemen mit Umfeldwahrnehmung notwendig. Zusätzlich wird zur Risikobemessung eine Relevanzbewertung benötigt.

3.9 ISO 26262[93]

Für die Definition einheitlicher Standards für die Absicherung der funktionalen Sicherheit von elektronischen/elektrischen Komponenten im Automobilbereich wurde aus der allgemeinen Norm IEC 61508 die spezifischere ISO 26262 abgeleitet. Die erste verbindliche Version wurde im Jahre 2011 veröffentlicht. Eine Analyse und Diskussion von Gemeinsamkeiten und Unterschieden zwischen der IEC 61508 und der ISO 26262 mit Schwerpunkt auf den Hardware-Fehlermetriken finden sich in BINFET-KULL (2010, S. 375 ff.) und in BÖRCSÖK (2011, S. 35). BINFET-KULL betrachtet dabei insbesondere die Übertragbarkeit der Sicherheitsintegritätsbewertungen zwischen den Normen.

Ebenso wie in der „Mutternorm“ IEC 61508 enthält die ISO 26262 Anforderungen an die Entwicklung sicherheitskritischer Komponenten und Systeme über den gesamten Produktlebenszyklus. Das Vorgehen orientiert sich am allgemeinen V-Modell der Produktentwicklung. Bild 6 stellt den allgemeinen Ablauf schematisch dar. Bereits zu Beginn der Ent-

92 FACH et al. (2010), S. 434

93 Kapitel basierend auf WEITZEL (2013), S. 13 ff.

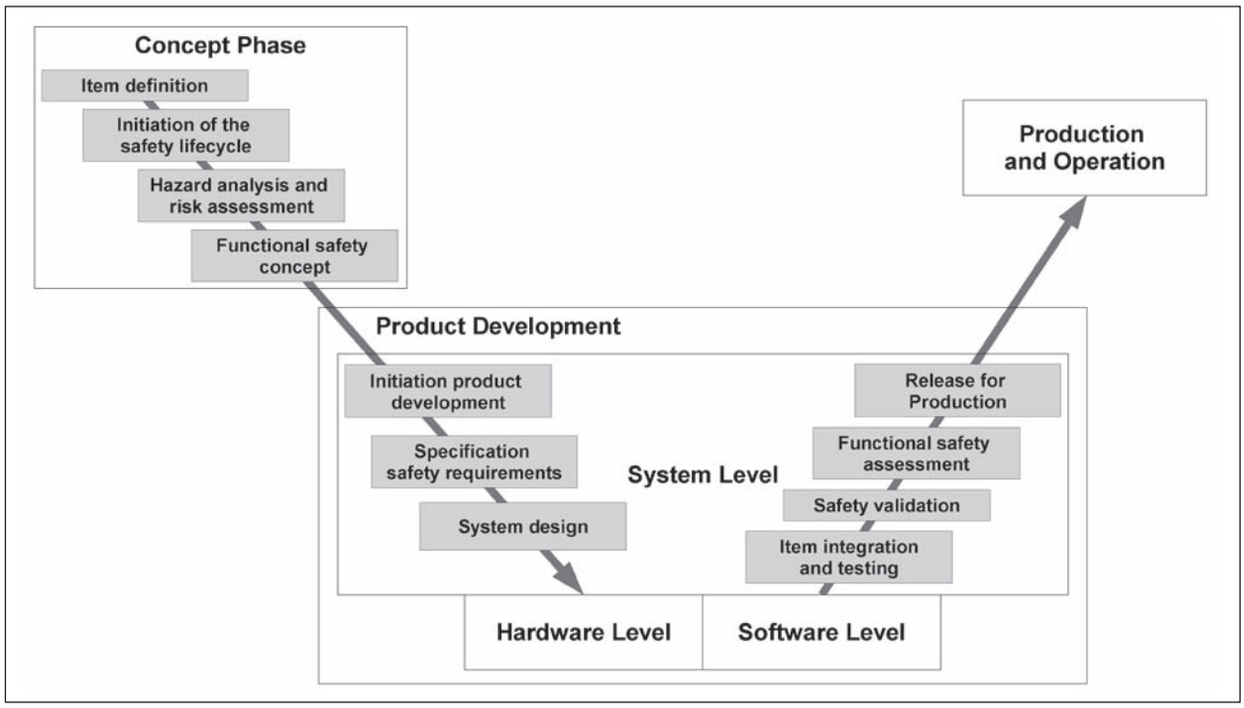

Bild 6: Vereinfachter schematischer Ablauf der Entwicklung sicherheitskritischer E/E-Komponenten nach ISO 26262[94]

Class	**S0**	**S1**	**S2**	**S3**
Description	No injuries	Light and Moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries
Reference for single injuries (from AIS scale)	Damage that cannot be classified safety-related **AIS 0**	more than 10% probability of **AIS 1-6** (and not S2 or S3)	more than 10% probability of **AIS 3-6** (and not S3)	more than 10% probability of **AIS 5-6**

Tab. 3: Einteilung der Severity-Stufen nach ISO 26262[95]

wicklung von Systemen, in der Konzeptphase, sind die Gefahren, die durch das System entstehen können, abzuschätzen und die resultierenden Risiken zu quantifizieren. Basierend darauf werden die Sicherheitsziele festgelegt und damit die Anforderungen an Methoden, Qualitätssicherung und Überwachung sowohl während der folgenden Entwicklung als auch im späteren Betrieb definiert.

Im Rahmen der „Hazard Analysis and Risk Assessment“ werden potenzielle Gefährdungen in den Kategorien Expositionswahrscheinlichkeit (Exposure), Schadensschwere (Severity) und Kontrollierbarkeit (Controllability) in 3 oder 4 Stufen eingeteilt. Tabelle 3 zeigt dies am Beispiel der Schadensschwere (Severity).

Aus der Kombination der Bewertungen in diesen drei Kategorien wird dann anhand der „ASIL Determination Matrix“ (s. Tabelle 4) das resultierende geforderte „Automotive Safety Integrity

		C1	**C2**	**C3**
S1	**E1**	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	**E1**	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	**E1**	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Tab. 4: ASIL-Bestimmungsmatrix

94 Vgl. ISO 26262 (2009b), S. vi
95 ISO 26262 (2009b), S. 20

Level“ (ASIL) (Einteilung A bis D) ermittelt. In der niedrigsten Ausprägung ist ein Qualitätsmanagement (QM) ausreichend.

Hinsichtlich der Anforderungen an die Ausfallsicherheit der Hardware bedeutet ASIL D beispielsweise, das die maximale Fehlerrate geringer als 10^{-8} pro Betriebsstunde sein muss.

Aus den ASIL leiten sich dann die Sicherheitsziele („Safety Goals“) ab, die die Sicherheitsanforderungen enthalten. Diese sind in der weiteren Produktentwicklung zu berücksichtigen bzw. bedingen das Vorgehen in den weiteren Schritten.

Insbesondere bei neuen Systemen liegt in dieser frühen Phase nur die funktionale Definition des betreffenden Items vor. Die Bewertung muss daher auf Basis von Abschätzungen erfolgen, sie kann durch Ergebnisse aus Entwicklungsstudien sowie durch Erfahrungen von bereits getesteten Systemen gestützt werden.[96]

Im Anschluss an die Risikobewertung definiert die ISO 26262 Prozessschritte, notwendige Informationen sowie die Dokumentation, die zur Einhaltung der gestellten Sicherheitsziele und zum normengerechten Entwickeln benötigt werden.

Durch dieses Vorgehen werden Sicherheitsanforderungen von Beginn des Entwicklungsprozess einbezogen. Entwicklungs- oder auch Programmiermethoden und Techniken werden dann in der Folge an den Sicherheitsanforderungen orientiert ausgewählt. Ebenso sind die jeweiligen Schritte zu dokumentieren.

3.9.1 Anwendungsgrenzen

Hinsichtlich des Anwendungsgebietes ist die ISO 26262 auf die Elektronik- und Elektrik-Komponenten eines Fahrzeugs bis 3,5 t beschränkt. Die Norm adressiert die fehlerfreie Funktion von elektrischen/elektronischen/programmierbaren Systemen. Nicht situationsgerechte Reaktionen von Fahrerassistenzsystemen mit Umfeldwahrnehmung werden jedoch nicht nur durch Versagen oder fehlerhafte Funktion von Komponenten hervorgerufen. Auch bei korrekter Funktion innerhalb der Spezifikationen kann durch eine unvollständige Situationswahrnehmung oder aufgrund nicht eintretender Prädiktions- bzw. Modellannahmen eine nicht situationsgerechte Reaktion des Systems auftreten. In der ISO 26262 werden nur Systeme adressiert, die quasi schwarz-weiß klassifiziert sind. Entweder sind sie in einem Zustand, der die Spezifikation erfüllt, und damit sind Gefährdungen, in der ISO 26262 als „Hazards“ bezeichnet, ausgeschlossen oder sie versagen aufgrund des Ausfalls von Bauteilen oder Design-/Programmierfehlern und liegen damit außerhalb der Spezifikation. Umfeldinterpretierende Assistenzsysteme hingegen können weder so eindeutig spezifiziert noch so getestet werden, dass nicht-situationsgerechte Reaktionen nur außerhalb der Spezifikation auftreten. Ähnlich wie die deterministische klassische Physik um eine statistische Physik (Quantenmechanik, Chaostheorie) ergänzt wurde, muss auch hier eine neue Betrachtungsweise Einzug in die Sicherheitsbewertungen halten. Auf der obersten Ebene, der Risikobetrachtung und der ASIL-Einstufung spielt dieser Unterschied noch keine Rolle, da es unerheblich ist, ob ein Hazard aufgrund „klassischer“ Versagensmechanismen ausgelöst wurde oder ob er zur systeminhärenten statistischen Funktionseigenschaft gehört. Somit eignet sich die ISO 26262 grundsätzlich gut als Ausgangspunkt. Allerdings sind die Methoden für die Vermeidung des Auftretens ungewünschter Hazards für die neue Systemklasse prinzipbedingt ungeeignet.

Aktuell sind keine Methoden bekannt, wie die dadurch entstehende Betrachtungslücke mit vertretbarem Aufwand zumindest so weit zu füllen ist, das für den Einsatz umfelderfassender und -interpretierender Systeme mit hohem Gefahrenpotenzial (insbesondere bei höher automatisiertem Fahren) ein hinreichendes Sicherheitsniveau erreicht werden kann.

Wird die nicht situationsgerechte Reaktion des Systems aus Sicht des Betroffenen (bspw. des Fahrers, aber auch anderer Verkehrsteilnehmer) betrachtet, so kann davon ausgegangen werden, dass sowohl bei funktionalen Fehlern als auch bei funktionalen Unzulänglichkeiten die Auswirkungen auf das Fahrzeug und damit der Eindruck für den Betroffenen vergleichbar sind.[97] EBEL et al. (2010, S. 396) gründen auf diese Annahme den dort vorgestellten ganzheitlichen Ansatz, der eine vergleichende Bewertung der Auswirkungen sowohl von technischen Fehlern als auch von funktionalen Unzulänglichkei-

---

96 ISO 26262 (2009b), S. 3

97 Mit dem Unterschied, dass Fehler vermutlich seltener auftreten als funktionale Unzulänglichkeiten und daher keine Gewöhnung bzw. kein Lernprozess im Umgang damit absolviert werden kann.

ten zulässt. Inwiefern dabei allerdings das zugrunde liegende akzeptierte Grenzrisiko in beiden Fällen gleichgesetzt werden darf, wird dort bereits angezweifelt.[98]

3.10 Weitere Normen zu FAS mit Umfeldwahrnehmung

Neben der ISO 26262, die sich allgemein auf sicherheitskritische elektrische/elektronische Systemen bezieht, existieren bezüglich Fahrerassistenzsystemen mit Umfeldwahrnehmung zahlreiche Normen, die deren Funktionsbereiche und/oder -umfänge definieren und Mindestanforderungen bezogen auf das Produkt (bspw. eine Fahrstreifenwechselassistenzfunktion) formulieren. Diese Normen definieren dann teilweise auch Testverfahren, mit denen die Anforderungserfüllung überprüft werden kann.

Sie beziehen sich jeweils auf konkrete Funktionsausprägungen. Die beschriebenen Testprocedere decken den Nachweis der grundsätzlichen Funktion in exakt definierten Fällen ab. Zum Nachweis der funktionalen Sicherheit ist dies aber als nicht hinreichend anzusehen, zumal es auch nicht Zielsetzung der genannten Normen ist.

Tabelle 5 enthält eine Übersicht über aktuelle funktionsorientierte Normen zu Fahrerassistenzsystemen mit Umfeldwahrnehmung.

4 Bestehende Entwicklungs- und Absicherungsstrategien

Zur Absicherung und Bewertung von Fahrerassistenzsystemen wird eine Vielzahl von verschiedenen Methoden eingesetzt. Um eine Einordnung der existierenden Verfahren zu ermöglichen, erfolgen eine Zuordnung hinsichtlich der Anwendbarkeit und Einsatzzweckes anhand des V-Modells der Produktentwicklung unter Berücksichtigung der Anforderungen aus der ISO 26262[99] und Einbeziehung von darin bzw. im angelagerten „Code of Practice“[100] genannten Verfahren.

In der frühen Phase der Produktentwicklung kann beispielsweise eine Hazard-and-Operability-Study angewendet werden, um mögliche Fehlerquellen und deren Auswirkungen auf Prozessebene zu betrachten. Mit steigender Konkretisierung und Umsetzung werden dann Risikobewertungsmethoden wie beispielsweise die Failure-Mode-and-Effect-Analysis (FMEA) oder die Fault-Tree-Analysis (FTA) möglich. Diese werden auch in der Norm vorgeschlagen. Um diese Verfahren zum Einsatz brin-

98 EBEL et al. (2010), S. 396
99 ISO 26262 (2009a)
100 PREVENT (2009)

Norm	Titel	Jahr
ISO/DIS 11270	Lane Keeping Assistance Systems – Performance requirements and test procedure	Draft Status
ISO 15622	Adaptive Cruise Control Systems – Performance requirements and test procedures	2010
ISO 15623	Forward vehicle collision warning systems – Performance requirements and test procedures	2002
ISO 17361	Lane departure warning systems – Performance requirements and test procedures	2007
ISO 17386	Manoeuvring Aids for Low Speed Operation (MALSO) – Performance requirements and test procedures	2010
ISO 17387	Lane Change Decision Aid Systems (LCDAS) – Performance requirements and test procedures	2008
ISO 22178	Low Speed Following (LSF) systems – Performance requirements and test procedures	2009
ISO 22179	Full Speed Range Adaptive cruise control (FSRA) systems – Performance requirements and test procedures	2009
ISO/FDIS 22839	Forward vehicle collision mitigation systems – Operation, performance, and verification requirements	2013
ISO 22840	Devices to aid reverse manoeuvres – Extended-Range Backing Aid Systems (ERBA)	2010

Tab. 5: Aktuelle funktionsbeschreibende Normen von Fahrerassistenzsystemen mit Umfeldwahrnehmung

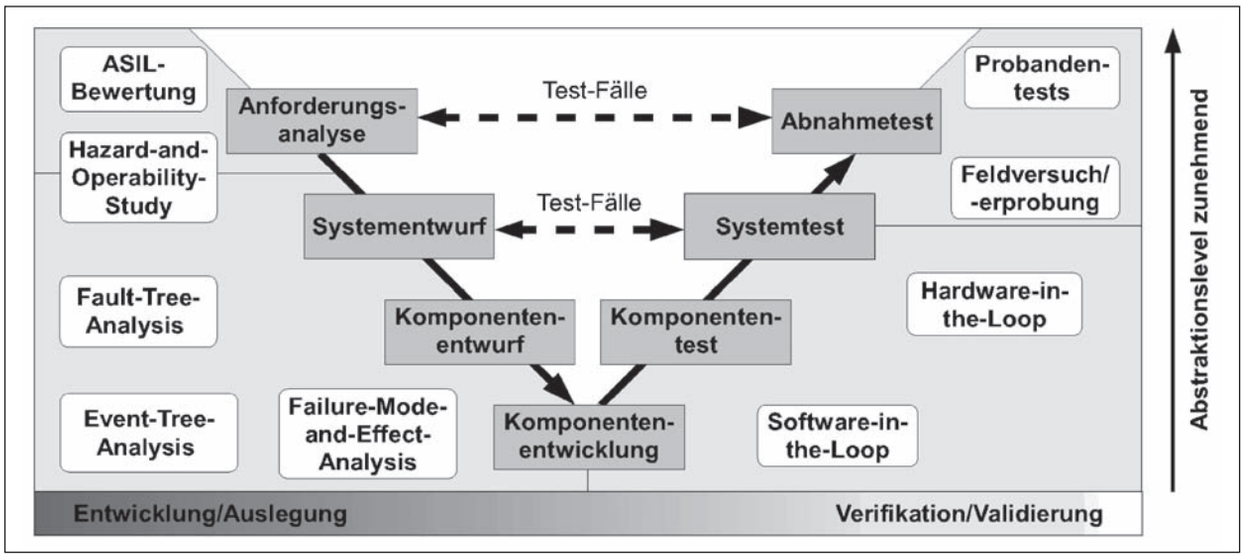

Bild 7: Einordnung von Sicherheitsbewertungsmethoden im Entwicklungsprozess[101]

gen zu können, sind Kenntnisse über die Struktur der Funktion, gegebenenfalls deren Module sowie dazugehörige Spezifikationen notwendig.

Im nächsten Schritt werden bei der Entwicklung der Komponenten, die die vorher definierten Funktionen abbilden, Hardware- und Software-in-the-Loop (HiL, SiL)[102]-Techniken eingesetzt. Diese können auch bei der Prüfung des Gesamtsystems[103] zum Einsatz kommen, werden hier jedoch häufig zusätzlich durch Probandentests oder Field-Operational-Tests[104] ergänzt. Sie sollen die anhand der Systemanforderungen definierten Test-Fälle adressieren, abbilden und die korrekte Funktion des Gesamtsystems in seinem späteren Einsatzgebiet überprüfen.

Bild 7 enthält eine Übersicht von Bewertungsmethoden mit ihrer Einordnung in den Produktentwicklungsprozess.

In allen Phasen werden ergänzend Expertenbewertungen herangezogen,[105] um die systematischen Verfahren zu ergänzen, insbesondere dann, wenn eine eindeutige Abgrenzung mit den vorliegenden Methoden nicht möglich ist oder der Aufwand hierfür sehr hoch wäre.

4.1 Differenzierung der Absicherungsansätze

Das V-Modell folgt einer Top-Down-Strategie, die ausgehend von den allgemein formulierten Produktanforderungen eine schrittweise Detaillierung vornimmt. Diese führen auf dem linksseitigen Ast zum Entwurf und der Entwicklung der Einzelkomponenten bei sinkendem Abstraktionsgrad des Systems. Wie in Kapitel 3.9 dargestellt, stellen Normen der funktionalen Sicherheit innerhalb dieses Vorgehens spezifische Anforderungen an die Definition, Dokumentation und Prüfung der Sicherheitsanforderungen. Diese sind dann im rechtsseitigen Ast jeweils zuerst auf den jeweiligen Entwicklungsstufen nachzuweisen, um anhand dieser Einzelergebnisse in Kombination mit dem abschließenden Systemtest die funktionale Sicherheit des Gesamtproduktes nachweisen zu können. Zur Absicherung werden also sowohl Ansätze zur Gewährleistung der Anforderungserfüllung für Einzelkomponenten als auch des Gesamtsystems benötigt. Dabei steigt mit abnehmendem Abstraktionsgrad die Abhängigkeit der Methoden von der konkreten hard- und softwaretechnischen Ausführung der Komponenten an. Unter Umständen sind die notwendigen Prüfmethoden direkt von der Art des gewählten Sensortyps oder der Softwarearchitektur abhängig. Mit der zunehmenden Spezifizierung sinkt auch die Übertragbarkeit auf andere ähnliche Problemstellungen und wird mit zunehmender Spezifizierung eingeschränkt. Im Rahmen dieser Arbeit wird daher eine Übersicht über Herangehensweisen zur Gewährleistung einer sicheren Funktion von Fahrerassis-

101 In Anlehnung an BÖRCSÖK (2011), S. 58, und MAURER (2012), S. 45
102 STRASSER et al. (2010), S. 2
103 In Anlehnung an SCHICK et al. (2008), S. 2
104 FACH et al. (2010), S. 429
105 FACH et al. (2010), S. 429

tenzsystemen bei abstrakter Betrachtung gegeben. Dabei wird keine Vollständigkeit angestrebt, sondern einerseits die Problematiken, die aus den Besonderheiten von Fahrerassistenzsystemen mit Umfelderfassung hervorgehen, beschrieben und diese zusätzlich vor dem Hintergrund aktueller Forschungsansätze diskutiert.

Differenziert werden Verfahren, die einzelne Komponenten der abstrakten Funktionsstruktur von Fahrerassistenzsystemen der aktiven Sicherheit mit Umfeldwahrnehmung adressieren, und Verfahren, die die Absicherung des Gesamtsystems auf höchster Abstraktionsebene betreffen.

4.2 Verfahren in der Entwicklungs- und Auslegungsphase

Hinsichtlich der angewandten und bewährten Verfahren in der Entwicklungs- und Auslegungsphase wurden von STÄNDER (2011, S. 30 ff.) eine umfangreiche Betrachtung und Bewertung durchgeführt, in denen sich die in Bild 7 dargestellten, bekannten Verfahren wiederfinden. Dort findet auch eine Bewertung der Verfahren nach Vor- und Nachteilen statt. Die Vorgehensweise der ASIL-Bewertung ist in Kapitel 3.9 beschrieben.

4.3 Verfahren in der Verifikations- und Validierungsphase

Zu Beginn der Verifikation und Validierungsphase kommen zahlreiche virtuelle Testmethoden zum Einsatz. Dies ermöglicht den Test von prototypischen Systemen in der Komponentenentwicklung, sodass Probleme frühzeitig identifizierbar werden und dadurch kostengünstig lösbar sind. Zudem können mit virtuellen Testmethoden eine hohe Anzahl unterschiedlichster Test-Fälle mit vergleichsweise geringem Aufwand durchlaufen werden. Häufig angewendete Verfahren folgen dem „X-in-the-Loop“-Ansatz. Näher erläutert werden sollen in diesem Zusammenhang mit absteigendem Abstraktionsgrad die drei Beispiele Model-in-the-Loop (MiL), Software-in-the-Loop (SiL) sowie bei Verfügbarkeit von prototypischen Komponenten eines Systems die Hardware-in-the-Loop-Methode. In allen Ansätzen werden Teile des Gesamtsystems Fahrer-Fahrzeug-Umwelt simuliert. Die Qualität der Ergebnisse hängt damit von der Güte der verwendeten, aus der Simulation erzeugten Eingangsdaten ab. Von SCHICK et al. (2008) wird dazu eine Methode vorgestellt, die diese Ansätze innerhalb einer Simulationsumgebung miteinander verknüpft und auf einen bestehenden Versuchsszenarienkatalog zurückgreift.

4.3.1 Model-in-the-Loop (MiL)

Bei Model-in-the-Loop-Simulationen wird keine einsatzbereite Hard- oder Softwareimplementierung benötigt. Die Bewertung, Entwicklung und Optimierung erfolgen auf Basis von Simulationsmodellen, die die Systemstruktur und das Systemverhalten hinreichend genau abbilden. Damit handelt es sich um eine rein simulationsgestütze Methode ohne direkte Einbindung von realen Komponenten oder Situationselementen.[106] HOLZMANN (2006, S. 109) verweist darauf, dass eine Unterscheidung zwischen MiL und SiL auch meist nur im angelsächsischen Sprachgebrauch durchgeführt wird.[107]

Aufgrund dessen eignet sich die Methode sehr gut für frühe Entwicklungsphasen wie beispielsweise Systementwurf und Komponentenentwurf[108], aber auch zur Spezifikation von Komponenten (modellbasierte Spezifikation[109]).

4.3.2 Software-in-the-Loop (SiL)

Bei der weiteren Implementierung und Konkretisierung der Funktion wird die Software erstellt. Dieser reale Code kann dann ebenfalls wieder im Rahmen einer Simulation geprüft und optimiert werden. Die Simulationsumgebung umfasst weiterhin nur virtuelle Elemente, ist daher rein rechnergestützt. Fahrzeughardware wird nicht benötigt.[110] Eine Betrachtung des Zusammenspiels von Softwarekomponenten, die später gegebenenfalls auf verschiedenen Steuergeräten dargestellt werden, ist möglich. Aussagen über hardwarebedingte Effekte sind abhängig von der Qualität der Abbildung dieser Eigenschaften in der Simulation (bspw. hinsichtlich Übertragungsgeschwindigkeiten und Übertragungsqualtität).

Die SiL-Simulation kann angewendet werden, sobald eine Implementierung der konkreten Software der Fahrerassistenzfunktion vorliegt, sie unterstützt die Komponentenentwicklung.[111]

---

106 HOLZMANN (2006), S. 104

107 HOLZMANN (2006), S. 104

108 SCHICK et al. (2008), S. 3

109 SCHÄUFFELE et al. (2010), S. 214 ff.

110 HOLZMANN (2006), S. 104 f.

111 SCHICK et al. (2008), S. 3

4.3.3 Hardware-in-the-Loop (HiL)

Mit weiterer Konkretisierung des Produktes werden Prototypen der Komponenten hergestellt. Diese Hardware mit der dazugehörigen Software kann dann ebenso mit einem „In-the-Loop“-Ansatz getestet werden. Dabei wird beispielsweise zur Stimulanz einer Kamera ein Videofilm eingesetzt und dadurch eine reale Umgebung simuliert.[112] Eine der Herausforderungen dabei ist, dass die virtuellen und realen Stimulanzen so miteinander synchronisiert werden müssen, dass eine plausible Umgebungsrepräsentation erzeugt wird. Damit können Funktionen geprüft, verifiziert und, sofern der Validitätsnachweis der Simulationsumgebung vorliegt, auch Produkteigenschaften validiert werden.

4.4 Absicherung auf Systemebene[113]

Die beschriebenen Test- und Prüfverfahren dienen dazu, die funktionale Sicherheit eines mehr oder weniger konkreten Systementwurfs zu prüfen und gegebenenfalls Anpassungen vorzunehmen.

Bei der Entwicklung von Fahrerassistenzsystemen müssen insbesondere Herausforderungen zur Systemkomplexität und Systemzuverlässigkeit berücksichtigt werden.

Die Systemkomplexität der Fahrerassistenzsysteme lässt sich hinsichtlich zweier Aspekte betrachten. Einerseits muss bei den komplexen Fahr- und Unterstützungsaufgaben (wie z. B. moderne Kreuzungsassistenzsysteme) an vielfältige Situationen gedacht werden, bei denen ein sicheres Systemverhalten zu erwarten ist.[114] Andererseits werden diese Aufgaben durch mehrere Busse, Subbusse und mit einer Vielfalt von Steuergeräten realisiert, die viele unnötige Abhängigkeiten zu anderen Systemen entstehen lassen.[115] Dies kann zu einem nicht mehr durchschaubaren System und zu einer schwierigen Fehlererkennung führen. Außerdem werden die klare Trennung der Arbeitsbereiche der Funktionen und dementsprechend die Absicherung der Funktionalität beeinträchtigt.[116] Aus diesen Gründen muss die Beherrschung der steigenden Systemkomplexität bei der Entwicklung der Fahrerassistenzsysteme bereits in der Designphase betrachtet werden und somit wird dies hier als eine Herausforderung definiert.

Die Fahrerassistenzfunktionen, im Besonderen diejenigen, die in den Regelkreis Fahrer-Fahrzeug-Umwelt oder direkt in die Fahrdynamik eingreifen, müssen trotz hoher Komplexität möglicher Fahrsituationen und trotz potenzieller Fehlfunktionen weiterhin zuverlässig und sicher bleiben. Hiermit lässt sich eine weitere Herausforderung für die Systemsicherheit und Systemzuverlässigkeit identifizieren.

In den folgenden Kapiteln werden die Maßnahmen zur Erfüllung der identifizierten Herausforderungen diskutiert.

4.4.1 Beherrschung von Systemkomplexität

Zur Beherrschung der steigenden Systemkomplexität müssen die Abhängigkeiten der Fahrerassistenzsysteme zu anderen Systemen sowie die vielfältigen Wechselwirkungen getroffener Entscheidungen untersucht werden.[117] Diese definieren, zusammen mit der Qualität, den Kosten und der Funktionalität, ein Optimierungsproblem, welches durch eine geeignete Systemarchitektur zum bestmöglichen Kompromiss geführt werden kann.[118] Die optimale Architektur kann durch Einsatz der Architekturprinzipien wie Standardisierung, Hierarchisierung und Modularisierung erreicht werden.[119] Dabei wird die Struktur des Systems hinsichtlich des Zusammenwirkens und der Vernetzung der Systemelemente und der Abhängigkeiten zu anderen Systemen untersucht.

Da die Fahrerassistenzfunktionen oft durch die Zusammenarbeit mehrerer Steuergeräte realisiert werden, spielt hier Vernetzung eine sehr große Rolle. REIF et al. (2012, S. 166) hat die Vernetzungsmöglichkeiten der Steuergeräte hinsichtlich der funktionsorientierten und der zonenorientierten Ansätze dargestellt. Während die Steuergeräte beim funktionsorientierten Ansatz je nach Einsatzzweck verschiedenen Funktionsbereichen, als Domänen bezeichnet, zugeordnet werden, erfolgt ihre Vernetzung bei zonenorientiertem Ansatz hinsichtlich der räumlichen Aspekte.[120]

---

112 SCHMIDT (2012), S. 208 ff.

113 Verantwortlicher Autor des Kapitels 4.4 ist Herr MOHSEN SEFATI, M. Sc.

114 Vgl. EBEL et al. (2010), S. 393

115 Vgl. REICHART et al. (2012), S. 88

116 S. Kapitel 3.9 und 4.5.3

117 Vgl. REICHART et al. (2012), S. 86

118 In Anlehnung an BÄKER (2005), S. 20

119 Vgl. REICHART et al. (2012), S. 84

120 Die ECUs werden da platziert, wo sie räumlich gesehen am besten liegen.

Die Vernetzung von Steuergeräten aufgrund der Zuordnung zu einer Funktionsdomäne weist viele Vorteile auf. Die Hauptvorteile sind hier die klare Trennung der Funktionsbereiche und geringe bis gar keine gegenseitige Beeinflussung, die eine Reduzierung der Komplexität zur Folge hat. Darüber hinaus können einzelne Domänen bezüglich Sicherheitsanforderungen unabhängig voneinander entwickelt werden.[121]

Die letzte Entwicklungsstufe von funktionsorientierter Vernetzung der Steuergeräte lässt sich durch „Domänenleitrechner“ bezeichnen. Dabei wird jeder Domäne ein dezidierter Master-Rechner zugeteilt, der die Informationen aller Sensoren zentral auswertet[122] und entsprechende Befehle an „intelligente Aktoren“ weiterleitet. So wird die Realisierung eines Multi-Sensor-Systems durch Sensordatenfusion möglich, bei der die unterschiedlichen Messdaten zusammengeführt werden. Hiermit finden die Beobachtung, Erkennung und Plausibilisierung der Sensordaten nur einmal zentral statt, sodass keine unterschiedlichen Interpretationen des aktuellen Fahrzustands innerhalb der Domäne entstehen können. Bei der Entwicklung komplexerer Fahrerassistenzsysteme hat eine solche zentrale Einheit zur Umgebungserfassung eine große Bedeutung. Dabei kann der Sichtbereich eines Sensors mit anderen Sensoren erhöht werden, sodass die in den Sicherheitszielen definierten Standards erfüllt werden können. Die Daten aus den unterschiedlichen Sensoren werden in einem konsistenten Modell zusammengeführt und anschließend die notwendigen Informationen aus dem Modell extrahiert. Ein weiterer Vorteil zentraler Einheiten besteht darin, dass Schwächen des einen Systems durch ein anderes ausgeglichen werden können und dadurch gegenseitige Störeingriffe nicht mehr vorhanden sind. Es werden gleiche Auswertealgorithmen verwendet und die Regler müssen nicht mehr unabhängig voneinander eingestellt werden.[123]

4.4.2 Zuverlässigkeit trotz Fehlfunktion

Sofern fehlerhafte Verhaltensweisen bei Fahrerassistenzsystemen zu schweren Unfällen führen können, ist bei diesen Systemen ein hoher Systemintegritätsgrad erforderlich. Das bedeutet unter anderem, dass solche Systeme im Fehlerfall weiterhin aktiv bleiben müssen (fehleroperativ), wenn ein Wechsel in den sicheren Ruhezustand (fehlersicher) auf Grund eines direkten Eingriffs beispielweise in die Fahrdynamik nicht möglich ist oder wenn kein sicherer Abschaltzustand (fehlerpassiv) für das System existiert.[124] Um dies zu erreichen, sind Mechanismen im System vorzusehen, die Fehlfunktionen einzelner Komponenten im ersten Schritt erkennbar und im zweiten Schritt kompensierbar machen. Diese Notwendigkeiten führen wiederum zu zusätzlichen Anforderungen an die Architektur des Systems.[125]

4.4.3 Fehlererkennung

Der erste Schritt eines fehlertoleranten Systems besteht darin, den Fehler zu erkennen. Dies wird durch Sensordatenplausibilisierung[126] erreicht. Hierzu werden, ausgehend von den eingesetzten Systemen, die erwünschten Funktionen untersucht. Auf dieser Basis werden der Informationsbedarf und die Anforderungen an die Sensordatenplausibilisierung abgeleitet. VERSMOLD et al.[127] schlagen drei Stufen der Fehlererkennung mit Hilfe von Sensordatenplausibilisierung vor. Diese Stufen werden in Serie hintereinander geschaltet, um einen möglichst großen Umfang von Fehlern zu erkennen.

1. Einzelsignalplausibilisierung: Ist beispielweise durch physikalisch basierte Gradienten-, Rausch-, Pegel- oder Grenzwertüberwachung realisierbar. Bei der Einzelsignalplausibilisierung wird der Fehler erst sehr spät erkannt und Methoden wie Rauschüberwachung benötigen eine gewisse Zeit zur Fehlererkennung.

2. Redundanzgestützte[128] Plausibilisierung: Diese sind durch den Vergleich vorhandener redundanter Sensoren realisierbar. Mit dieser Methode sind geringe Abweichungen, die durch Messrauschen und Fertigungstoleranzen verursacht werden, zulässig. Nachteil dieser Methode ist, dass nicht erkennbar ist, welcher von den redundanten Sensoren defekt ist.[129]

3. Modellgestützte Plausibilisierung: Diese ist durch den Vergleich unterschiedlicher Signale,

---

121 Vgl. REIF et al. (2012), S. 166

122 Weitere Information im Kapitel 4.4.6

123 Vgl. REIF et al. (2012), S. 166

124 Vgl. ISERMANN (2008), S. 568

125 Vgl. BÄKER (2005), S. 82

126 Siehe Kapitel 4.4.6

127 VERSMOLD et al. (2004), S. 1598

128 Redundanzen werden im folgenden Kapitel näher betrachtet.

129 Hierzu müssen mindestens drei Sensoren eingesetzt werden (siehe „Physikalische Redundanz“ im Kapitel 4.4.4).

für die ein modellbasierter Zusammenhang existiert, realisierbar.

Mit den oben dargestellten Methoden kann der Fehler detektiert und dadurch bestimmt werden, ob etwas nicht korrekt funktioniert. Dies bedeutet aber nicht zwingend, dass ein bestimmter Ausfall unbedingt erkennbar wird und der Fehler lokalisiert werden kann. Ist die fehlerhafte Komponente erkennbar und kann der Fehler lokalisiert werden, ist eine Fehlerisolation möglich. Hierfür können Methoden wie zum Beispiel die modellbasierte Diagnose eingesetzt werden.

4.4.4 Kompensierung des Fehlers und Verbesserung der Zuverlässigkeit

Die Informationen aus der Fehlererkennung werden zum Fehlermanagement weitergeleitet. Dabei werden Notlaufstrategien (Rekonfigurationsstrategien) auf Basis der gelieferten Informationen, des Grads der Fehlerauswirkung und möglichersicherheitskritischer Zustände aktiviert. Hier kann zwischen folgenden Notlaufstrategien unterschieden werden:[130]

- harte oder weiche Übernahme/Umschaltung,
- Änderung des Betriebszustandes,
- fehlertolerante Regelung (Rekonfiguration der Regelung z. B. anderer Regler, andere Regelparameter oder andere Hilfsstellgrößen).

Neben den Notlaufstrategien kann eine Verbesserung der Zuverlässigkeit verschiedener Komponenten durch Kompensierung bzw. Vermeidung der Fehler mit Hilfe von unterschiedlichen Maßnahmen erfolgen. In Tabelle 6 sind mögliche Maßnahmen gemäß der Bewertung nach REICHART dargestellt.[131]

Wie in Tabelle 6 zu erkennen ist, wird die Schaffung von Redundanzen für die bei FAS besonders relevanten elektrischen/elektronischen Komponenten mit gut bis sehr gut bewertet. Im Folgenden werden unterschiedliche Redundanzarten betrachtet.

Physikalische Redundanz (Hardware-Redundanz)

Die physikalische Redundanz ist die einfachste Art der Redundanz. Hierbei wird die betrachtete Komponente durch eine oder mehrere Komponenten (identisch oder diversitär) ergänzt. Es existieren grundsätzlich zwei physikalische Redundanzarten, „statische Redundanz“ und „dynamische Redundanz“. Beim typischen Fall der statischen Redundanz werden zwei oder mehrere zueinander parallele Komponenten eingesetzt, die dasselbe Eingangssignal messen und alle aktiv sind. Grundsätzlich erfolgt bei stationärer Redundanz eine Überprüfung auf Widerspruch. Sofern noch genügend widerspruchsfreie Signalinstanzen vorliegen, kann weiter das Signal geliefert werden. Das heißt, wenn das Überprüfungsprinzip Widerspruchfreiheit ist, reicht es aus, zwei parallele Komponenten zueinander einzusetzen. Alternativ werden drei Komponenten eingesetzt und ihre Ausgänge werden zu einem „Voter“ geführt, in dem aufgrund von Mehrheitsentscheidung festgelegt wird, welches Signal korrekt gemessen wird.

---

130 Vgl. ISERMANN (2008), S. 569

131 In Anlehnung an REICHART (1998)

Verbesserung der Zuverlässigkeit durch	Komponenten				
	mechanisch	hydraulisch	elektrisch	elektronische Hardware	Software
Überdimensionierung	++	+	+	+	0
Wartung	++	++	+	0	+
Schutzmaßnahmen	++	++	+	++	0
Verschleißreduzierung	++	+	+	0	0
Redundanz	0	+	+	++	+
statisch	0	+	+	++	0
dynamisch	0	0	+	++	+
diversitär	0	0	0	++	++
++ sehr gut, + gut, 0 neutral					

Tab. 6: Maßnahmen zur Verbesserung der Zuverlässigkeit

Im Gegensatz dazu ist bei der dynamischen Redundanz im Normalzustand nur eine Komponente in Betrieb und bei Auftreten des Fehlers wird auf die Reserveeinheit umgeschaltet. Hier kann man noch zwischen kontinuierlich aktiver Reservekomponente (Hot Stand-by) oder inaktiver Reservekomponente (Cold Stand-by) unterscheiden.[132]

Ein Beispiel für die physikalische Redundanz ist der E-Gas-Fahrpedalsensor von HELLA für X by-Wire. Hierbei wird die Pedalposition durch dreifache berührungslose induktive Aufnehmer gemessen.[133]

Analytische Redundanz (modellgestützte Redundanz)

Bei analytischer Redundanz wird mit Hilfe eines analytischen Modells ein Teil der Messgrößen berechnet. Mit der Betrachtung des Unterschiedes zwischen den berechneten und gemessenen Größen kann überprüft werden, ob im System ein Fehler aufgetreten ist. Die Modelle können sowohl für Signale als auch Prozesse erstellt werden. Bei den Signalmodellen kommen Analysemethoden wie Korrelation, Spektralanalyse und Waveletanalyse zur Anwendung. Zur Erstellung der Prozessmodelle können Methoden wie Parameterschätzung, neuronale Netze, Zustandsschätzer und Paritätsgleichungen eingesetzt werden.[134]

Ein Beispiel für die analytische Redundanz ist der Gierraten-Sensor für ESP. Hierbei wird die Gierrate aus der Querbeschleunigung und der Differenz der Drehzahlsignale des linken und rechten Rades einer Achse über Prozessmodelle rekonstruiert.[135]

Redundanzen bei Steuergerätearchitekturen

Hinsichtlich des Aufbaus der Steuergeräte kann an weitere Varianten der Redundanz gedacht werden. In heutigen Steuergräten werden mehrere Microcontroller eingesetzt.

Zur Verbesserung der Fehlersicherheit der Steuergeräte durch Redundanz sind unterschiedliche Strategien erkennbar. Eine Strategie dabei ist, eine identische Redundanz mit identischen Geräten, identischen Algorithmen und identischen Codegeneratoren zu schaffen. Dabei besteht aber das Risiko, dass wegen des Duplikats der Steuergeräte auch Fehler dupliziert werden. Um dieses Problem zu lösen, muss von redundanten Steuergeräten eine möglichst große Unterschiedlichkeit gefordert werden. Dieses Konzept ist unter „diversitäre Redundanz“ bekannt und kann realisiert werden, indem unterschiedliche Prozessoren mit möglichst unterschiedlichen Compilern, sogar unterschiedlichen Betriebssystemen, eingesetzt werden. Ein weiterer sinnvoller Weg ist, mit unterschiedlichen algorithmischen Ansätzen zu arbeiten. Wie aber soll darauf reagiert werden, wenn zwei Steuergeräte keine gleichen Ergebnisse liefern? Hierzu ist eine dreifache diversitäre Redundanz nötig, bei der sich drei Steuergeräte gegenseitig überwachen. Ein abweichendes Steuergerät wird dann von den anderen beiden Steuergeräten als fehlerhaft erkannt.[136] Eine weitere Möglichkeit zur Fehlererkennung der Steuergeräte besteht darin, durch zusätzliche Rechenzeit Berechnungen zu wiederholen und die Ergebnisse zu vergleichen. Dieses Konzept heißt „temporale Redundanz“ und ist nur für diejenigen Fehler geeignet, die für kurze Zeit auftreten.[137]

Allen genannten Redundanzstrategien ist gemeinsam, dass ein absolutes „Richtig“ oder „Falsch“ angenommen wird und ein Widerspruch von Ergebnissen als Fehler gewertet werden kann. Bei der inhärenten Unsicherheit der Situationsinterpretation umfelderfassender Fahrerassistenzsysteme reicht diese Betrachtung nicht mehr aus. Probabilistische Ansätze können zwar die Unsicherheit beschreiben, doch bleibt offen, wie daraus eindeutige Handlungen abgeleitet werden, wenn dafür mehrere widersprechende Optionen infrage kommen.

4.4.5 Weitere Absicherungsmöglichkeiten

Eine weitere Absicherungsmethode lässt sich aus der Gewährleistung der Rechenaufgaben in Steuergeräten ableiten. Hierzu muss die Hardwarestruktur der Steuergeräte so ausgewählt werden, dass die Berechnungsverfahren möglichst nicht abgebrochen oder abgeschaltet werden. Beispielsweise muss beim Einsatz von eingebetteten Steuergeräten für rechenintensive Aufgaben darauf geachtet werden, dass diese hinsichtlich Verfügbarkeits- und Sicherheitsaspekten nicht als unkritisch beurteilt werden können. Diese Art von Steuer-

---

132 Vgl. ISERMANN (2008), S. 566
133 S. HELLA (2003)
134 In Anlehnung an ISERMANN (2006)
135 Vgl. ISERMANN (2008), S. 572
136 Vgl. BORGEEST (2010), S. 298
137 Vgl. HOFFMANN (2013), S. 99

geräten führt neben Sensorauswertung und Algorithmenberechnung auch die Ansteuerung der Aktoren mit hoher elektrischer Leistung aus. In solchen Fällen werden die Lastschaltelemente mit den zugehörigen Treibern in separaten Modulen mit oder ohne eigene Intelligenz ausgelagert. Gegenüber eingebetteten Steuergeräten sind Semi-embedded-Steuergeräte von der Ansteuerung der Aktoren entlastet und haben keine Treiberbausteine. Diese Steuergeräte bieten eine höhere Rechenleistung und eignen sich deshalb besser für die rechenaufwendigen Fahrerassistentenfunktionen. Der Einsatz von Rechenknoten beispielweise mit einer Doppelprozessorarchitektur und einer hohen Rechenleistung bietet weitere Möglichkeiten, bei denen ein Prozessor die wichtigen Berechnungsergebnisse des Hauptprozessors überwacht.[138]

Eine weitere Absicherungsmethode im Hard-/Softwareverbund ist die in der ISO 26262 erwähnte „Dekomposition". Bei dieser Methode wird das Risikopotenzial, welches durch den Zugriff des Fahrerassistenzsystems auf Aktoren entsteht, so auf die beteiligten Steuergeräte verteilt, dass nicht jedes ein hohes ASIL-Level erreichen muss, insofern das Gesamtsystem die Sicherheitsanforderungen erfüllen kann.[139]

4.4.6 Integrität von umfelderfassenden Sensorsystemen[140]

Wegen der zahlreichen verschiedenen Fahrsituationen von Fahrzeugen sind die Anwendungsfälle für Fahrerassistenzsysteme auch vielfältig und unterschiedlich. Diese Vielfältigkeit macht es praktisch unmöglich, einen Sensor zu finden, der bei allen Anwendungsfällen eine zuverlässige vollständige Umfeldwahrnehmung oder eine für die unterschiedlichen Funktionen ausreichend genaue Messung schaffen kann. Die Funktionstüchtigkeit einer Kamera im sichtbaren Wellenlängenbereich beispielsweise wird abends durch die niedrige Helligkeit der Umgebung begrenzt, während die Funktionalität der Infrarot-Kamera während des Tages durch die Reflexion der Wärmestrahlung der Sonne an der Straße oder den anderen Oberflächen stark beeinträchtigt werden kann. Auf der anderen Seite hängt, wie im Kapitel zuvor beschrieben, die Qualität von Messung und Wahrnehmung auch von der Qualität der Sensorik, den Merkmalen des Messprinzips (z. B. ausgewählter Frequenzbereich der Welle, Modulation usw.) und Informationsverlusten bei der Datenbearbeitung ab. Unsicherheiten der Messergebnisse und der Wahrnehmung sind deshalb unvermeidbar. Diese können aber aufgrund der Verwendung falsch gemessener Werte aus unsicherer Wahrnehmung und Messung zur Fehlinterpretation des Umfelds und gegebenenfalls weiter zur Unsicherheit bei dadurch ausgelösten Aktionsentscheidungen führen.

Ungeachtet dieser Unvermeidlichkeit der Unsicherheit können jedoch die Auswirkungen auf die Unsicherheit eines Umfeldsensors qualitativ analysiert und weiterhin die Einflussfaktoren herausgefunden werden. Durch die Analyse der Auswirkungen auf die Unsicherheit bzw. die qualitative Bewertung der Einflussfaktoren auf Integrität der Messergebnisse kann einerseits der Wirkungsbereich jeder Funktion eines Fahrerassistenzsystems abgeleitet und definiert werden und andererseits kann eine weitere Datenverarbeitung oder Datenfusion, die auf die Verminderung der Einflüsse eines oder mehrerer Einflussfaktoren zielt, durchgeführt werden. Beispielsweise werden bei komplementärer Datenfusion die Daten von Umfeldsensoren, die von den möglichst unterschiedlichen Einflussfaktoren beeinflusst werden, ausgewählt und fusioniert.

Bevor die Auswirkungen auf einen Umfeldsensor oder die Einflussfaktoren für einen Umfeldsensor weiter betrachtet werden, muss die Unsicherheit eines Sensors genau definiert werden. In der Statistik kann die Beurteilung eines Klassifikators in einer Wahrheitsmatrix bzw. falsche und richtige Klassifikationen dargestellt werden. Darin werden die vier möglichen Fälle als „falsch positiv", „falsch negativ", „richtig positiv" und „richtig negativ" definiert. Unter dem Begriff „falsch/richtig" versteht man eine falsche oder richtige Beurteilung des Klassifikators. Da es sich um eine Ja/Nein-Frage handelt, werden die Antworten zu der vorliegenden Frage als „positiv/negativ" bezeichnet.[141]

Bei der Diskussion der Unsicherheit eines Umfeldsensors kann der Status der Umfeldwahrnehmungen auch durch die vier Fälle repräsentiert werden. D. h., „falsch positiv" beschreibt eine Wahrnehmung, bei der ein Objekt, das tatsächlich nicht existiert, detektiert wird, während „falsch negativ" die Situation, bei der ein existiertes Objekt nicht wahr-

---

138 In Anlehnung an REICHART et al. (2012)

139 Vgl. SCHAFFNER (2011)

140 Verantwortlicher Autor des Kapitels 4.4.6 ist Herr PENG CAO, M. Sc.

141 SHESKIN (2004), S. 282

genommen wird, darstellt. D. h., bei „falsch positiv“ wird ein Geisterobjekt falsch generiert und bei „falsch negativ“ wird ein relevantes Objekt falsch vernachlässigt. Außerdem wird eine richtige Detektion eines Verkehrsobjekts durch „richtig positiv“ gekennzeichnet. Und der Status „keine Detektion der Inexistenz“, der für die Sicherheit eines Umfeldsensors unwichtig ist, wird als „richtig negativ“ benannt. Sowohl „falsch positiv“ als auch „falsch negativ“ können zu unsicheren Fahrzuständen führen. Aber natürlich bedeutet ein „richtig positiv“ auch nicht eine absolut zuverlässige Wahrnehmung. Bei „richtig positiv“ können auch Messfehler, die zur falschen Zustandsinformation des detektierten Objekts führen können, auftreten. Die drei unterschiedlichen Unsicherheiten werden im Folgenden weiter erklärt.

Um die Einflussfaktoren auf einen Umfeldsensor zu finden, müssen zuerst die Wirkungsprinzipien eines Umfeldsensors im Ziel von einer Aufzählung der Auswirkungsmöglichkeiten analysiert werden. Ein allgemeines Funktionsblockdiagramm eines Umfeldsensors ist in Bild 8 dargestellt. Die Umfeldsensoren werden normalerweise nach den Wirkungsprinzipien in zwei Gruppen unterteilt. Einige Umfeldsensoren sorgen für die Strahlung und beleuchten die zu detektierenden Gegenstände. Durch die reflektierte Strahlung kann ein Sensor dieser Gattung ein Objekt detektieren und die erwünschten Messgrößen daraus ableiten. Ein typisches Beispiel dieser Art von Sensoren ist das Radar. Andere Sensoren nehmen direkt die von den Gegenständen reflektierten Fremdstrahlungen auf, um die gewünschten Informationen zu erhalten. Beispielsweise gehört die Kamera zu dieser Gattung.

Trotz der unterschiedlichen Signalquellen kann der Vorgang des Signalempfangs immer in einem gleichen abstrakten Modell zusammengefasst werden. Das Nutzsignal wird zuerst in der Atmosphäre von äußerem Rauschen gestört und dann von der Antenne und dem Empfänger empfangen. Im Empfangsvorgang wird wieder inneres Rauschen hinzugefügt. Danach wird das empfangene Signal gefiltert. Das bearbeitete Signal wird danach zwei weiteren Funktionsblöcken zugeführt. Auf dem einen Pfad wird das Signal bei der Detektion verwendet, um die relevanten Gegenstände zu erkennen. Auf der anderen Seite wird das Signal mit den Informationen über die relevanten Gegenstände zusammen zum Signalverarbeitungsblock geschickt, damit die Koordinaten und die Fahrzustände von jedem relevanten Gegenstand erfasst werden können. Durch die Verarbeitung werden im Sensor die direkt gemessenen Werte, beispielsweise relativer Abstand, relative Geschwindigkeit oder Azimutwinkel, bestimmt. Diese Werte werden eventuell noch durch geometrische Berechnungen nachbearbeitet, um beispielsweise durch Ableitung oder Offsetkompensation die gewünschten Werte, wie relative Geschwindigkeit oder relativer Abstand, in fahrzeugfeste x- und y-Richtung als Ausgänge des Sensors zu erhalten.

Aus dem Funktionsblockdiagramm in Bild 8 geht hervor, dass der „falsch positive“ Fehler und der „falsch negative“ Fehler bei der Funktion „Detektion“ auftreten können.

142 BENZ (2004), S. 21

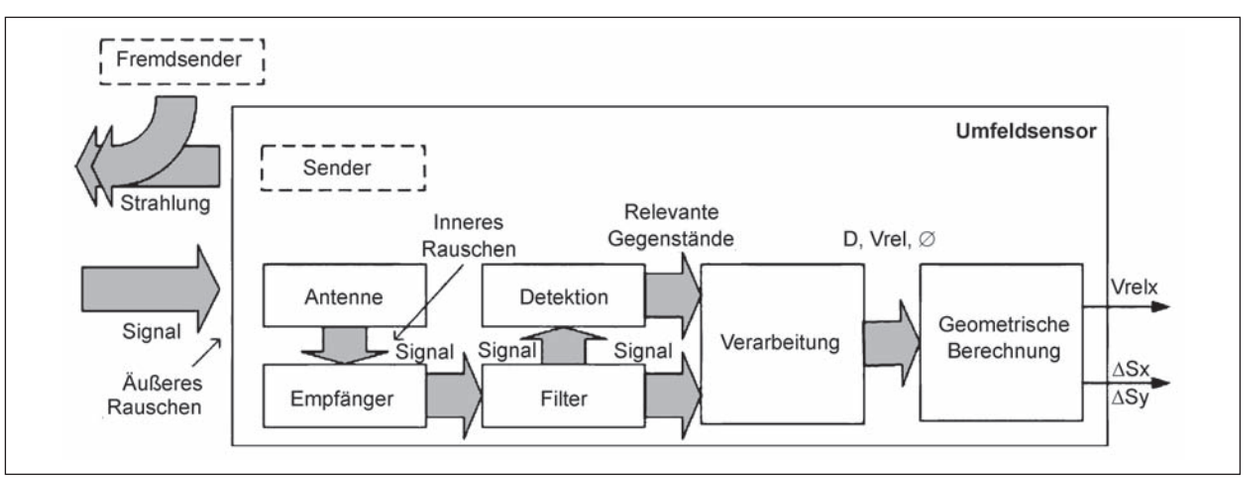

Bild 8: Allgemeines Funktionsblockdiagramm eines Umfeldsensors[142]

Ein großer Unterschied zwischen den Umfeldsensoren und den konventionellen Sensoren ist, dass die Umfeldsensoren außer den geometrischen Messungen noch die Detektion zur Aufgabe haben. Aber bei den unterschiedlichen Umfeldsensoren sind die Arten der Detektion durch unterschiedliche Wirkungsprinzipien begründet.

Grundsätzlich können die gegenwärtigen Detektionsansätze in der Umfeldsensorik in zwei Gruppen, die auf die Verarbeitung der elektromagnetischen Wellen basierende (z. B. Radar, Lidar usw.) und die auf die Bildverarbeitung basierende Detektion (z. B. Kamera, 3D-Time-of-Flight usw.) unterteilt werden. Die Ursachen für „falsch positive“ und „falsch negative“ Fehler werden daher für diese beiden Gruppen getrennt, anhand der jeweiligen Wirkungsprinzipien hergeleitet.

Falsch negative und falsch positive Fehler bei der Detektion mit elektromagnetischen Wellen

Die Detektion mit elektromagnetischen Wellen funktioniert durch einen Vergleich der Leistung der reflektierten Wellen mit einer Schwelle. Wenn die Leistung der von anderen Verkehrsobjekten reflektierten Wellen höher als die vordefinierte Schwelle ist, wird dies als eine Detektion beurteilt. Dieser Vorgang kann nicht nur im zeitlichen Bereich, sondern auch im Frequenzbereich durchgeführt werden. Z. B. bei der Detektion der anderen Verkehrsobjekte auf der Straße durch ein Continuous-Wave-Radar wird das Nutzsignal zusammen mit dem Rauschen in einem Messzyklus des Sensors über eine Fourier-Transformation im Frequenzbereich dargestellt. Liegt die Leistung einer der Frequenzlinien über einer vordefinierten Schwelle, dann wird die Detektion eines Objekts angenommen. Deswegen sind die Leistung des Nutzsignals und die Leistung des Rauschens bzw. das Verhältnis zwischen der Leistung von Nutzsignal und von Rauschen, welches bei Signalverarbeitung als Signal-to-Noise-Ratio (SNR) bezeichnet wird, bei der Detektion dieser Gattung als Eingänge der Funktion relevant.

Die Rauschsignale bestehen wie zuvor beschrieben aus zwei unterschiedlichen Gruppen, dem äußeren Rauschen und dem inneren Rauschen. Das äußere Rauschen, das am häufigsten von Störungen aus der Umgebung verursacht wird und in den Empfänger gelangt, kann als stochastisches Signal betrachtet werden. Grundsätzlich sind die zufällig auftretenden atmosphärischen Störungen White Noise, aber ihre charakteristischen Größen (z. B. Störpegel, Feldstärke) können wegen der unterschiedlichen Fahrumgebungen und Fahrsituationen geändert werden. Beispielsweise in dichten Verkehrssituationen oder Industriegebieten wird das äußere Rauschen verstärkt. Das Rauschen dieser Gattung wird zum Nutzsignal addiert und die Summe vom Empfänger empfangen.

Neben dem äußeren Rauschen muss auch das innere Rauschen berücksichtigt werden. Das innere Rauschen entsteht durch störende Signale innerhalb des Empfängers. Abhängig von den unterschiedlichen Wirkungsprinzipien der Empfänger ist der Verlauf des inneren Rauschens im Frequenz- oder Zeitbereich unterschiedlich. Ein Beispiel hierfür ist das Rauschen aufgrund der thermischen Bewegung der Elektronen in einem ohmschen Widerstand. Das Rauschen kann nach dem zentralen Grenzwertsatz der Statistik durch eine stochastische Größe mit einer Gaußverteilung im Zeitbereich und als frequenzunabhängiges („weißes“) Spektrum dargestellt werden.[143]

Außerdem ist das Entstehen des inneren Rauschens nicht nur vom Empfänger, sondern auch von allen Filtern, die als die nächste Kaskade des Empfängers angeschlossen werden, abhängig. Da das äußere Rauschen mit dem Nutzsignal auch vom Empfänger empfangen wird, durchläuft es ebenfalls die Filter. Deshalb wird der Verlauf der zwei Rauscharten im Zeit- und Frequenzbereich entsprechend den Filtern beeinflusst. Aber natürlich ist das Ziel des Einsatzes der Filter das Erreichen einer möglichst niedrigen Stärke des Rauschens, unter Berücksichtigung geringer Verzerrung des Nutzsignals. In LUDLOFF (2002, S. 5-1 ff.) und in SKOLNIK (2008, S. 6.24 ff.) wird eine Vielzahl von Filtertypen zur Verbesserung der Signalqualität des Radars vorgestellt. Da sich diese auf die „klassischen“ Anwendungen, wie Wetterradar oder Luftfahrtbeobachtung beziehen und nicht auf die im Automobilbereich verwendeten Konzepte übertragen werden können, wird hier nicht weiter darauf eingegangen.

Die Leistung des Nutzsignals kann auch von äußeren Einflussgrößen beeinflusst werden. Vor allen anderen Einflussgrößen steht die Entfernung

---

143 LUDLOFF (2002), S. 3-6

bzw. der Abstand. Die Welle breitet sich in der Atmosphäre in Kugelform aus. Die Energiedichte schwächt sich mit dem Quadrat des Abstandes ab. Nach der Reflexion breitet sich die reflektierte Welle wieder kugelförmig aus. Dies führt am Empfänger zu einer Energiedichte, die umgekehrt proportional zur vierten Potenz des Abstands ist. Ferner wird bei der Energieeffizienz der Reflexion der Rückstrahlquerschnitt betrachtet. Der Rückstrahlquerschnitt ist eine relevante Kenngröße für die Darstellung der Eigenschaften der Wellenreflexion auf der Oberfläche eines Verkehrsobjekts. Er bestimmt das Verhältnis zwischen der reflektierten Leistungsdichte und der eingestrahlten Leistungsdichte der Welle. Der Rückstrahlquerschnitt ist nicht nur von den Eigenschaften der Reflexionsoberfläche (z. B. geometrische Größen, Material oder Lacke), sondern auch stark von dem Aspektwinkel und der Frequenz der Welle abhängig. Deswegen sind die relative Position des Egofahrzeugs zu dem beobachteten Verkehrsobjekt und das Frequenzband, das ein Umfeldsensor benutzt, auch wichtige Einflussfaktoren auf den Rückstrahlquerschnitt bzw. die Leistung der reflektierten Strahlung.

Eine andere Einflussgröße des Nutzsignals ist die Durchlässigkeit. Der Energieverlust der Welle in der Atmosphäre steigt auch mit der Strecke, den die Welle zurückgelegt hat. Die Durchlässigkeit der Welle in der Atmosphäre ist von dem Frequenzbereich der Welle abhängig. Das Frequenzband, welches ein Umfeldsensor nutzt, ist für die Durchlässigkeit entscheidend, aber natürlich kann die Durchlässigkeit auch von der Witterung beeinflusst werden. Beispielweise wird die Welle stark gedämpft, wenn der Durchmesser des Wassertröpfchens in der Atmosphäre in der Größenordnung der Wellenlänge ist.

Das Nutzsignal kann auch von selbst beeinflusst werden. Die Aufgabe der Umfeldsensoren ist, die relevanten Verkehrsobjekte zu detektieren. Allerdings wird die Strahlung überall im Erfassungsbereich ausgesendet. Die nicht relevanten Reflektoren (z. B. Pfosten oder andere Infrastrukturbauteile) können ebenfalls die Strahlung reflektieren und zur Störung beitragen. Der Unterschied zwischen der Störung aus einem Nutzsignal und der Störung aus einem Rauschen ist, dass die Störung aus einem Nutzsignal nicht durch eine Verlängerung der Messdauer abgeschwächt werden kann. Die direkt reflektierte Strahlung kann einfach durch einen Vergleich mit der physikalischen Begrenzung, z. B. die Position der Fahrbahngrenze oder die mögliche Geschwindigkeit, ausgeschlossen werden. Aber die reflektierten Strahlungen, die aufgrund der Mehrwegeausbreitung, speziell durch die Reflexion der Fahrbahn oder Seitenbebauung, zu einer Phasenverschiebung mit einer Länge vom ungeraden Vielfachen der halben Wellenlänge führen, sorgen für eine starke Beeinträchtigung des Detektionsverhaltens.

Außer diesen äußeren Einflussfaktoren ist zudem die Bestimmung der Beurteilungsschwelle wichtig. Die Schwelle hat immer gegenseitige Wirkungen auf den „falsch positiven“ Fehler und den „falsch negativen“ Fehler. Wenn die Schwelle zu hoch eingestellt wird, sinkt die Wahrscheinlichkeit des „falsch positiven“ Fehlers. Aber in diesem Fall wird die Wahrscheinlichkeit des „falsch negativen“ Fehlers angehoben. Wenn die Schwelle niedriger eingestellt wird, gibt es eine entsprechende Wirkung in der Gegenrichtung. Deshalb ist die Einstellung der Schwelle immer das Ergebnis von einem Kompromiss zwischen dem „falsch positiven“ Fehler und dem „falsch negativen“ Fehler.

Bei der Detektion dieser Gattung, in einer Abtastperiode, ist das Ergebnis boolscher Art: detektiert und nicht detektiert. Werden mehrere Messzyklen herangezogen, so wird die Rate der „falsch Positiven“ erheblich reduziert, wenn man für die Detektion eine Bestätigung innerhalb eines zumeist heuristisch gebildeten Zustandsfensters verlangt. Ebenso lassen sich so genannte „Drop-outs“ durch Tracking beheben und somit die „falsch negativen“ Detektionen senken. Daher wird auch die „Drop-out-Rate“[144] als weitere charakteristische Größe für Darstellung der Unsicherheit der Detektion verwendet.

Falsch negative und falsch positive Fehler bei der Detektion mit Bildverarbeitung

Die Detektion der zweiten Gattung bzw. die auf die Bildverarbeitung basierende Detektion funktioniert durch eine digitale Verarbeitung eines von einer Kamera aufgenommenen Bildes. Bei der Detektion sind der „falsch positive“ Fehler und der „falsch negative“ Fehler stark von den Algorithmen der Bildverarbeitung abhängig. Beispielweise gehören die im Einsatz verwendeten A/D-Wandler, Detektoren und auch Filtermasken zur Signalverarbei-

144 WINNER (2012b), S. 125

tungskette. Physikalisch kann die Detektion auch vom Bildaufnehmer und von Lichtverhältnissen beeinflusst werden. In Situationen mit hellen Lichtverhältnissen, z. B. durch eine Reflexion der Sonnenstrahlung oder eine starke Gegenbeleuchtung, kommt das Sensorpixel auf dem Bildaufnehmer schnell in die Sättigung. Dies führt zu einer Abschattung des anderen sichtbaren Lichtes, und die Kontraste können nicht gewährleistet werden. Natürlich kann der Effekt durch eine High-Dynamic-Resolution-Kamera abgeschwächt, aber nicht ausgeschlossen werden. Ein „falsch negativer" Fehler kann auch auftreten, wenn die aufgenommene Kontur eines Objekts nicht dem zugrunde liegenden Detektionsmuster entspricht. Dies kann aufgrund tatsächlich geometrischer Abweichungen, eines ungünstigen Betrachtungswinkels, einer (teilweisen) Sichtverdeckung oder der teilweisen diffusen Reflexion bei Dunkelheit entstehen. Beim „falsch positiven" Fehler wurde das Erkennungsmuster nicht selektiv genug gewählt, sodass von anderen als den beabsichtigten Objekten erzeugte Muster erkannt werden. Beispiele sind Dehnungsfugen, die als Fahrstreifenmarkierung „missverstanden" werden, oder Schlagschatten, die für sowohl kanten- als auch flächenbasierte Operatoren eine Herausforderung darstellen.

Messfehler bei „richtig positiver" Detektion

Unabhängig von der Art der Detektion existiert eine dritte Gattung der Unsicherheit, der Messfehler bei „richtig positiver" Detektion. Natürlich ist der Messfehler vom empfangenen Signal abhängig. Die ermittelten Zustandswerte eines Objektes können außerhalb der Spezifikation liegen, sei es aufgrund von Rauschen oder durch Aliaseffekte. Solche Einflüsse auf Messergebnisse sind bei unterschiedlichen Messprinzipien und Modulationen unterschiedlich. Prinzipiell lassen sich durch einige empirischen Formeln, bei denen die relevanten Attribute des Rauschens und Nutzsignals (z. B. Signal-to-Noise-Ratio (SNR) bei Radar oder Lidar) als Unbekannte definiert werden, die Auswirkungen abschätzen oder können durch Monte-Carlo-Verfahren getestet werden. Die zumeist durch falsche Zuordnung entstehenden Alias-Fehler lassen sich nur mit präzisem Wissen über die verwendete Sensor- und Auswertetechnik modellieren. Dabei können auch physikalische Ursachen, wie die Mehrwegeausbreitung, die Winkelauswertung von korrekt detektierten Objekten erheblich verfälschen.

Die Koordinaten der Objekte in einem kartesischen Koordinatensystem werden normalerweise nicht direkt von einem Umfeldsensor gemessen, sondern durch eine weitere Transformation aus dem Koordinatensystem des Sensors in ein geeigneteres Koordinatensystem übertragen. Beispielweise werden von einem Radarsensor der Radialabstand, die relative Radialgeschwindigkeit und der Azimutwinkel im Allgemeinen erfasst und diese aus dem Polarkoordinatensystem auf die x- und y- Richtungen des Fahrzeugkoordinatensystems transformiert. Deswegen wird der Einfluss der Signalfehler auf die Messung zuerst nach unterschiedlichen Wirkungsprinzipien der Messungen generiert und danach in das kartesische Koordinatensystem propagiert („error propagation"). Bei der Propagation können die Verteilung, der Mittelwert und die Varianz der Messungsfehler geändert werden.

Außer den grundsätzlichen Wirkungsprinzipien müssen auch die Leistungsfähigkeit und die Mehrzielfähigkeit eines Umfeldsensors sowohl bei den Messungen als auch bei der Detektion berücksichtigt werden. Sie beziehen sich auf die folgenden Fähigkeiten eines Umfeldsensors: die Messauflösung in jeder Dimension bzw. das „Zellvolumen" der Messungen, Trennfähigkeit[145], maximale Anzahl der verfolgten Verkehrsobjekte, Sichtverdeckung, Latenzzeit sowie EMC („Electromagnetic Compatibility"). Neben den Umwelteinflussfaktoren können viele unsichere Anwendungsfälle aus diesen Fähigkeiten abgeleitet werden, z. B. beim dichten Verkehr könnte ein unsicherer Zustand eintreten, falls das Maximum der Anzahl der Objekte, die verfolgt werden können, oder die Trennfähigkeit des Sensors überschritten werden.

4.5 Bewertung der Fahrer-Fahrzeug-Interaktion und Absicherungsansätze

Anhand der Situationsanalyse und gebunden an Kritikalitätsmaße, die zur Quantifizierung der aktuellen Gefährdungslage dienen, wird durch ein Fahrerassistenzsystem eine Aktion eingeleitet. Bei einem unfallvermeidenden System ist dies beispielsweise ein Eingriff in Längs- und Querdynamik über Lenk- oder Bremsaktoren.

145 WINNER (2012b), S. 146

Die Korrektheit und Angemessenheit dieses Eingriffs wird in realen Fahrsituationen in-situ von den beteiligten Personen beurteilt. Entspricht die Aktion der Intention und der Erwartungshaltung beispielsweise des Fahrers, so erfolgt subjektiv ein korrekter Eingriff, widerspricht sie der Intention, wird sie vermutlich als subjektiv falsch bewertet. Diese subjektive Bewertung kann sowohl abhängig von der beteiligen Person sein als sich auch über den Situationsverlauf ändern. Probandenversuche zeigen, dass Probanden bei nachträglicher Einschätzung von Situationen das eigene Verhalten nicht korrekt wiedergeben können[146] bzw. plausible konsistente Handlungen nachträglich konstruieren.[147] Zusätzlich zur subjektiven Bewertung ist auch eine objektive Bewertung möglich. Da die beteiligten Personen und Fahrzeuge, die die Situationsentwicklung direkt beeinflussen, dabei in Wechselwirkung stehen und der weitere Situationsverlauf von den getroffenen Entscheidungen abhängt, ist dies nur bei vergleichsweise einfachen Entscheidungen (bspw. Ausweichen oder Bremsen) nach Abschluss der Situation, also a-posteriori, möglich. Bei komplexen Situationen ist bereits die Definition eines gewünschten objektiven Idealverhaltens schwierig, weil dazu alle theoretisch möglichen Situationsentwicklungen miteinander rekombiniert werden müssen und selbst dann eine geänderte Fahrerreaktion nicht ausgeschlossen werden kann.

Für die Absicherung für den öffentlichen Straßenverkehr sind daher Untersuchungen mit Fahrereinbindung notwendig. Testverfahren ohne Fahrereinbindung sind nicht in der Lage, das zusätzliche Unfallvermeidungspotenzial und bspw. die Milderung von Falschauslösungen durch einen Fahrereingriff zu betrachten. Dabei muss entsprechend eine Eindeutigkeit der Situation für System und Fahrer hergestellt werden. Dies gilt sowohl für die Nutzenbewertung als auch für die Kontrollierbarkeit im Falle einer Falschauslösung. Um repräsentative Daten zu ermitteln, werden dazu neben Expertenbewertungen häufig Probandenversuche durchgeführt.

4.5.1 Werkzeuge zur Untersuchung von FAS mit Fahrereinbindung

Verschiedene Verfahren kommen dabei zum Einsatz, wobei im Bereich unfallvermeidender Systeme die Gefährdungslage für Probanden eine entscheidende Rolle bei der Auswahl geeigneter Verfahren spielt. Insbesondere bei der Bewertung der Kontrollierbarkeit, bei der gemäß ISO 26262 und dem angelagerten „Code of Practice“ das Unfallkriterium herangezogen wird, stehen realitätsnahe Versuchsmethoden im Zielkonflikt mit den Sicherheitsanforderungen an den Versuchsaufbau.[148]

Unproblematisch ist die Gewährleistung der Sicherheit bei Versuchen im Fahrsimulator, dabei kommen statische und dynamische Simulatoren zum Einsatz und die Darstellung einer Situation ist bis zum Unfall möglich. FACH et al. (2010, S. 428) beispielsweise setzen einen dynamischen Fahrsimulator zur Kontrollierbarkeitsbewertung einer Bremsenfunktion ein. Ein großer Vorteil ist dabei, dass kein funktionstüchtiges reales Versuchsfahrzeug benötigt wird, dadurch sind Bewertungen bereits in der frühen Entwicklungsphase möglich. Bei der Übertragung auf ein reales System und Gesamtfahrzeug ist zusätzlich die Validität der verwendeten Simulationsmodelle nachzuweisen.

Bei steigenden Realitätsanforderungen und fortschreitender Produktentwicklung können dann Versuche mit realen Fahrzeugen durchgeführt werden. Um dabei kontrollierte Bedingungen zu erreichen, gezielt bestimmte Situationen zu untersuchen und aufgrund der Sicherheitsanforderungen müssen jedoch auch dabei künstliche Szenerien geschaffen werden. BOCK (2012, S. 76) beschreibt dazu eine Methode, bei der dem Fahrer über eine Augmented-Reality-Darstellung während einer realen Fahrt auf einem abgesperrten Gelände eine Fahrsituation virtuell eingespielt wird, auf die das Fahrzeug/Fahrerassistenzsystem durch ein Vehicle-in-the-Loop-System (ViL) auch wie in der Realität reagiert.

Bei weiterer Erhöhung des geforderten Realitätsgrades werden die virtuellen Szenerieelemente durch reale ersetzt. Beispielsweise werden entgegenkommende Fahrzeuge mit instruierten Fahrern verwendet, parkende Fahrzeuge aufgestellt, Verkehrszeichen, Schutzplanken oder Lichtsignalanlagen hinzugefügt. Sind das Gefährdungspotenzial und die Komplexität gering, erhöht dies zwar den Aufwand, es kann jedoch auf existierende Technologien zurückgegriffen werden. Zahlreiche Verfahren verwenden diesen Ansatz für Test und Bewer-

146 MUTTART (2005), S. 2

147 Bspw. KOBIELA (2011), S. 257, S. 259

148 Vgl. auch BREUER (2012), S. 56

tung von Fahrerassistenzsystemen. Beispielhaft zu nennen sind hier die Fahrerintentionserkennung[149], Überholassistenz[150] und Fahrstreifenwechselmanöverassistenz[151].

Werden in der darzustellenden Fahrsituation jedoch Komponenten benötigt, mit denen im Verlauf eine Kollision nicht ausgeschlossen werden kann, oder ist diese sogar beabsichtigt, werden spezielle Zielobjekte benötigt. Diese müssen sich realistisch bewegen, gegebenenfalls kollisionstolerant sein oder die Kollision aktiv vermeiden und zudem realistisch für Sensorik und Probanden sein. Hinzu kommen Zusatzanforderungen, wie die Vermeidung von Beschädigungen am (potenziell noch prototypischen) Versuchsträger oder die schnelle Wiederherstellung der Einsatzfähigkeit nach dem Versuch. Entsprechend gibt es eine Vielzahl von Zielobjekten, die unterschiedliche Verkehrsteilnehmer darstellen[152], selbstbewegt[153] oder fremdbewegt[154], kollisionstolerant[155] oder kollisionsvermeidend[156] sind. In extremen Ausprägungen wird dann für den Test von Fahrerassistenzsystemen eine Vielzahl von Objekten miteinander kombiniert, um eine möglichst realistische Fahrumgebung zu erschaffen.[157]

Auch wenn die Realitätsnähe abhängig vom Aufwand der Darstellungsverfahren zunimmt, ist die Übertragbarkeit von Ergebnissen auf den Realverkehr jeweils zu diskutieren. Insbesondere bei Bewertungen des Gesamtsystems muss der Nachweis, dass es sich um eine realitätsnahe Darstellung handelt, hinsichtlich aller Situationsmerkmale geführt werden, anhand derer die vorliegende Sensorik und der Fahrer die Situation erfassen. Für kollisionstolerante Zielobjekte beispielsweise ist dieser Nachweis insbesondere hinsichtlich der Eignung für die eingesetzten Sensorik[158] und des Bedrohungseindrucks des Fahrers notwendig.

Können die Versuche im realen Straßenverkehr durchgeführt werden, entfällt dieser Nachweis, allerdings muss hier die Repräsentativität der Daten bezogen auf das spätere Nutzungsprofil sichergestellt sein. Zudem sind nur Versuche möglich, bei denen bereits vorher nachgewiesen werden kann, dass eine Gefährdung des Fahrers oder anderer Verkehrsteilnehmer ausgeschlossen ist. NEUKUM et al. (2008) beschreiben hierzu ein Verfahren, bei dem zusätzlich der Beifahrer als Versuchsleiter über Zusatzpedale verfügt, um im Notfall eingreifen zu können.

4.5.2 Bewertungskriterien

Bewertungskriterien für die Leistungsfähigkeit der Interaktion bei der Fahrzeugführung durch Fahrer und Fahrzeug werden sowohl für den Vergleich verschiedener Warn- und Eingriffsmöglichkeiten oder auch unterschiedlicher Kombinationen dieser Elemente zu Warn- und Eingriffsstrategien als auch für den Vergleich von Gesamtsystemen benötigt. Während im ersten Fall die Auslöse- und Eingriffszeitpunkte festgelegt und in allen Versuchen gleich sind, können diese im zweiten Fall variieren. In allen Fällen, bei denen eine Fahrerreaktion notwendig ist, muss der letztmögliche Eingriffszeitpunkt des Fahrers während der Testsituation erreicht werden. Ebenso ist eine hohe Dringlichkeit der Handlung notwendig, um realistische Fahrerreaktionen zu erhalten.[159]

Anhand objektiver Messdaten wird eine Bewertung durchgeführt. Als Kriterien werden Bewegungsgrößen herangezogen, die die Prädiktion des Auftretens eines Unfalls erlauben und zur weiteren Differenzierung die Minderung der Unfallschwere durch die Reaktion von Fahrer und System bewerten. Ein Beispiel hierfür ist für längsdynamische Systeme der Geschwindigkeitsabbau innerhalb eines festgelegten Beurteilungszeitraums.[160]

Zusätzlich werden Kenngrößen wie die Blickzuwendungszeiten, Reaktionszeiten und Umsetzzeiten erfasst. Auch der subjektive Eindruck des Probanden wird durch Befragung und oder psychophysische Bewertungsmethoden (Herzfrequenz, Hautleitwert) erfasst und bewertet. Dies ist insbesondere für Akzeptanzbetrachtungen hilfreich.

Für den Nachweis der Sicherheit eines Systems im Nutz- und Falschauslösungsfall wird das Unfallkriterium (es kommt zur Kollision/es kommt nicht

---

149 KOBIELA (2011)
150 HOHM (2010)
151 HABENICHT (2012)
152 Bspw. in ROEHDER et al. (2010), S. 170
153 Bspw. SEINIGER et al. (2013)
154 BERTRANDT (2008) und SCHULTE (2011), Vortrag
155 Bspw. in NITZ (2010), S. 97, und WAAGMEESTER (2010)
156 HOFFMANN (2008), S. 21 ff., und DIEBOLD (2003), S. 30
157 TSS (2013)
158 MARX et al. (2010)
159 MUTTART (2005), S. 3 ff.
160 HOFFMANN (2008), S. 32 ff., und WINNER et al. (2013)

zur Kollision) als ausreichend[161] angesehen. Eine detailliertere Betrachtung der Vorkollisionsphase erlaubt es jedoch, auch für Testverfahren, bei denen es prinzipbedingt nicht zu einer Kollision kommen kann, die aber aufgrund der hohen Realitätsnähe für Kontrollierbarkeitsversuche sehr gut geeignet sind, Aussagen zu treffen.[162]

4.5.3 Begrenzung des Arbeitsbereiches

Kann eine fehlerhafte oder nicht situationsgerechte Auslösung nicht ausgeschlossen werden oder kann kein eindeutiger Nachweis der Kontrollierbarkeit dieser Fälle geführt werden, kann der Arbeitsbereich des Fahrerassistenzsystems begrenzt werden (s. hierzu auch Kapitel 4.4). Dazu werden die Eingriffsstärke oder die Eingriffsdauer begrenzt, um das Risiko zu senken, indem die Schwere des potenziellen Schadens reduziert wird. Wird dies auf

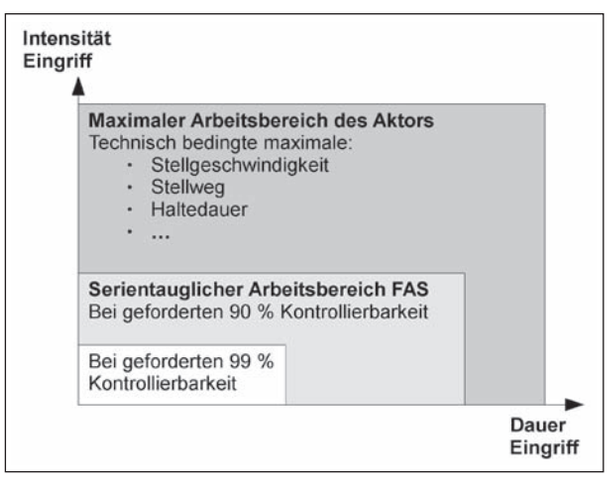

Bild 9: Begrenzung des Arbeitsbereiches hinsichtlich Eingriffsdauer und Eingriffsschwere[163]

Soft- und Hardwareebene dicht am Aktor-Steuergerät durchgeführt, kann damit auch ein Großteil der Fehler in der weiteren Verarbeitungskette abgefangen und dadurch abgesichert werden.[164] Bild 9 stellt diesen Ansatz beispielhaft für zwei unterschiedliche benötigte Kontrollierbarkeitsstufen dar.

4.6 Absicherungsansätze auf Basis des Gesamtsystems Fahrer/ Fahrzeug/Umwelt

Im rechten Ast des V-Modells (s. Bild 7) werden die Einzelkomponenten schrittweise zum Gesamtsystem kombiniert und dabei jeweils auf die Erfüllung der im linken Ast erarbeiteten Anforderungen geprüft. Auf höchster Ebene werden dann abschließend Abnahmetests durchgeführt, mit denen die Erfüllung der übergreifenden Systemanforderungen nachgewiesen werden soll.

Dabei ergibt sich eine Zweiteilung der Testziele. Zum einen müssen zur Validierung im Sinne des V-Modells alle funktionalen Anforderungen eines Gesamtsystems oder eines einzelnen Moduls hinsichtlich ihrer Erfüllung überprüft werden, zum anderen muss im Rahmen der ISO 26262 sichergestellt werden, dass das dadurch ausgelöste Systemverhalten nicht zu einer Risikoerhöhung für eine Gruppe der Verkehrsteilnehmer beiträgt,[165] wobei sich die anzuwendenden Teststrategien hierbei grundsätzlich unterscheiden können.

Beiden Ansätzen ist jedoch gemein, dass im Rahmen des V-Modells im ersten Schritt relevante Anwendungsfälle, im Engl. als „use-Cases“ bezeichnet, für das zu entwickelnde System zu definieren sind, die im Bereich von Fahrerassistenzsystemen in der Literatur überwiegend als Verkehrsszenarien[166] dargestellt sind. Diese haben sich vor allem bei komplexen Fahrerassistenzsystemen mit Umfeldwahrnehmung bewährt, da dort aufgrund der Vielzahl an möglichen Situationsparametern eine vollständige Anforderungsdefinition mit vertretbarem Aufwand a priori nicht möglich ist.[167] Durch Definition von Anwendungsfällen kann diese Parametervielfalt gezielt eingeschränkt werden. Diese funktionalen Anforderungen bedingen über die „Item-Definition“ und die darauf aufbauende „Gefährdungsanalyse und Risikoabschätzung“ den Betrachtungsraum für die funktionale Sicherheit nach ISO 26262.[168]

Inwiefern der Anwendungsfall-Ansatz auch auf die Definition von Absicherungsfällen bei assistiertem

---

161 FACH et al. (2010), S. 431

162 FACH et al. (2010)

163 In Anlehnung an EBEL et al. (2010), S. 397

164 EBEL et al. (2010), S. 397

165 Diese zweigeteilte Betrachtung wird ebenfalls von der Norm IEEE-SA Standards Board (1998) (S. 44) für Software- und Systemtests unterstützt, wobei in sog. „Positiv“-Testen (d. h. eine erfolgreiche Verarbeitung von Daten zur Erfüllung einer Funktion) und „Negativ“-Testen unterschieden wird (d. h., dass falsche und unplausible Daten als solche erkannt und entsprechende Gegenmaßnahmen eingeleitet werden).

166 Für die Begriffsdefinition und Unterscheidung wird auf GEYER et al. (2013) verwiesen.

167 S. SAUST (2009), S. 2

168 S. ISO 26262 (2009b), Kapitel 5.4 und Kapitel 2.8

und teilautomatisiertem Fahren übertragen werden kann und welche Herausforderungen sich bei der Weiterentwicklung zu manöverbasierten Systemen ergeben, wird daher in den folgenden Kapiteln diskutiert.

4.6.1 Übertragbarkeit und Erweiterungsmöglichkeiten des Anwendungsfall-Ansatz zur Definition von Absicherungsfällen für assistiertes und teilautomatisiertes Fahren[169]

Generierungsmethoden von Anwendungsfällen

Der Begriff „Use-Case“ stammt ursprünglich aus der Softwaretechnik und bezeichnet ein Verfahren, das helfen soll, systematisch Systemgrenzen zu bestimmen sowie ein anwenderorientiertes Anforderungsprofil für eine zu entwickelnde Software zu erstellen.[170] Im Gegensatz zur klassischen Softwareentwicklung, in der die Nutzerziele zur Erstellung einer Anforderungsliste ausreichend sind, hat sich im automobilen Umfeld ein kontextbasierter Anwendungsfall-Ansatz bewährt, da ein Assistenzsystem die Nutzerziele in den unterschiedlichsten Verkehrssituationen erfüllen muss.[171] Nach DOMSCH et al. (2008)[172] sind Anwendungsfälle im Sinne von Referenzfahrsituationen ein erforderliches Hilfsmittel für das Anforderungsmanagement von FAS.

Hinsichtlich der Generierung von Anwendungsfällen finden sich in der Literatur zahlreiche Methoden, die sich auf eine systematische Variation von Situationsparametern stützen, wie sie beispielsweise in DOMSCH et al. (2008) beschrieben sind. Dabei wird die Verkehrsszene in Merkmale und jeweilige Merkmalsausprägungen unterteilt und diese im Anschluss, ähnlich der Kreativitätstechnik des morphologischen Kastens, variiert. Merkmale können hier beispielsweise die Anzahl und Anordnung der Fahrstreifen oder die räumliche und zeitliche Konstellation von beteiligten Verkehrsteilnehmern sein. Die funktionalen Anforderungen werden dabei durch das gewünschte Systemverhalten in der definierten Verkehrssituation bestimmt.

Der Vorteil dieses Verfahrens liegt darin, dass prinzipiell alle möglichen Lösungen im Umfang des vorher durch Merkmalsdefinition aufgespannten Lösungsraumes gefunden werden. Der Nachteil dieser Vorgehensweise liegt jedoch in der Tatsache, dass je nach Anzahl der Merkmale und deren Ausprägungen eine sehr hohe Anzahl an Anwendungsfällen erzeugt wird und bestimmte Kombinationen zu nicht sinnvollen Lösungen führen können, die im Anschluss manuell aussortiert werden müssen. Vor diesem Hintergrund stellt sich die Frage, welchen Grad an Konkretisierung und Diversifizierung Anwendungsfälle besitzen müssen. Obwohl eine Antwort darauf der aktuellen Literatur nicht zu entnehmen ist, kann folgende Abschätzung gegeben werden: Trotz Unterstützung mit Software-Tools[173] aus dem Bereich des „Requirements Engineering“ sind das Extrahieren von konkreten funktionalen Anforderungen und das Erstellen von Pflichtenheften in textueller Form bisher nur auf Basis einer manuellen Betrachtung verschiedener Einsatzszenarien und der dazugehörigen Beschreibung des gewünschten Systemverhaltens möglich. Aus diesem Grund muss die Anzahl der Anwendungsfälle insoweit beschränkt werden, dass das beteiligte Entwicklerteam unter Berücksichtigung der Projektressourcen noch in der Lage ist, die Szenarien mit wirtschaftlich vertretbarem Aufwand zu erstellen und auszuwerten. Das Ergebnis dieses Zielkonfliktes zwischen einer möglichst hohen Anforderungsabdeckung und der dafür verfügbaren Ressourcen ist, dass nicht die vollständige Variation aller möglichen Situationsparameter für die Eignung der Anwendungsfälle ausschlaggebend ist, sondern möglichst wenige komplementäre und dafür systemrelevante Anwendungsfälle.

Dies zeigt die Notwendigkeit auf, den Parameter „Relevanz“ für Anwendungsfälle zu quantifizieren. Eine Möglichkeit, dies zu tun, erschließt sich vor allem für Assistenzsysteme der aktiven Sicherheit unter Nutzung von Verkehrsunfallstatistiken. Um das zu entwickelnde System an der gesamten Wirkkette des Unfallhergangs auszurichten und effektive Warn- und Eingriffsstrategien abzuleiten, sind insbesondere die ursächlichen Fahrerfehlhandlungen von Interesse, wie sie in In-Depth-Untersuchungen, wie z. B. VOLLRATH et al. (2006), gegeben sind. Durch eine Zusammenfassung solcher Daten hinsichtlich häufiger Unfallursachen und -konstellationen ist es möglich, eine

---

169 Verantwortlicher Autor des Kapitels 4.6.1 ist Dipl.-Ing. Felix LOTZ.

170 S. OMASREITER et al. (2004)

171 S. OMASREITER et al. (2004)

172 Hier wird auch ein einheitliches Vokabular zur Definition von Verkehrsszenarien vorgestellt.

173 S. z. B. BRABAND (2007), S. 39 ff.

hohe Effizienz bzgl. der funktionalen Abdeckung der Anwendungsfälle zu erreichen. Ein möglicher Parameter der „Relevanz“ ergibt sich dabei aus dem Anteil aller statistisch erfassten schwerwiegenden Unfälle, die der Anwendungsfall adressiert. Im Gegensatz zu eingreifenden Systemen der aktiven Sicherheit, z. B. Kollisionsvermeidungssystemen, ist für automatisierte Fahrzeugkonzepte einer andauernden Fahrzeuglängs- und -querführung die Bildung eines Relevanzparameters von untergeordneter Bedeutung, da sie prinzipiell alle Situationen innerhalb einer aus Nutzersicht klar definierbaren situations- und systemgebundenen Grenze (z. B. Autobahnassistent) beherrschen müssen. Für eine weiterführende Betrachtung des Anwendungsfälle-Ansatzes für automatisiertes Fahren sei an dieser Stelle auf Kapitel 4.6.2 verwiesen.

Ermittlung von Test-Fällen zur Absicherung und Validierung

Bei Testfällen handelt es sich um eine Konkretisierung der Anwendungsfälle mit einer damit einhergehenden Vereinfachung bzgl. der betrachteten Parameter, da definierte Randbedingungen, wie z. B. die Ausgangsgeschwindigkeit der beteiligten Fahrzeuge, zur vollständigen Situationsbeschreibung vorausgesetzt werden müssen. Ergänzend dazu werden bei Test-Fällen konkrete Bestehens- oder Versagens-Kriterien aufgeführt („K.-O.-Kriterien“), z. B. eine Kollision mit einem anderen Verkehrsobjekt, sowie weitere Qualitätskriterien, wie z. B. die Güte geplanter Fahrzeug-Trajektorien, anhand derer eine Absicherung und Validierung des Gesamtsystems erfolgen.[174] Die Überprüfung solcher explizit definierten Fehlertoleranzen erfordert eine entsprechende quantitative Beschreibung dieser sowie der im Vorfeld der Verkehrssituation zugrunde gelegten Parameter, wie z. B. der genauen räumlichen und zeitlichen Konstellation der beteiligten Verkehrsobjekte. Im vorliegenden Kapitel wird aus diesen Gründen zwischen zwei Anwendungsfällen differenziert: einerseits Fälle, die die Anforderungsspezifikation unterstützen sowie den Systemkontext im Sinne einer Verkehrsszene qualitativ, jedoch durchaus im Rahmen von quantifizierbaren Grenzen, beschreiben, und andererseits Test-Fälle, die im Rahmen der definierten Grenzen vollständig quantifizierte Ausprägungen der betrachteten Kontextparameter darstellen.

Laut HORSTMANN (2005, S. 108) existieren drei allgemeine Prinzipien der Testfallermittlung: Bei der lastenheftbasierten Testspezifikation wird für jede definierte Anforderung mindestens ein Testfall erstellt, wobei eine quantitative Aussage hinsichtlich der Erfüllung der Systemverifikation möglich ist. Grundsätzlicher Nachteil dieser Vorgehensweise ist, dass keine Fehler gefunden werden, die durch eine mangelhafte Systemspezifikation entstehen. Dennoch ist dieses Vorgehen im Sinne des V-Modells notwendig, um das System hinsichtlich des intendierten funktionalen Umfangs und des Nutzens zu validieren. Für eine Absicherung des Systems gilt es jedoch, gerade diese „versteckten“ Fehler zu betrachten. HORSTMANN beschreibt, dass sich dafür die risikobasierte Testspezifikation eignet, d.h., auf Basis einer vorhergehenden Risikobetrachtung die Testpriorität auf Funktionsteile zu legen, von denen ein hohes Risiko ausgeht. Hinsichtlich der ISO 26262 würde dies bedeuten, dass den Testfällen, korrespondierend zu den Systemelementen mit der höchsten ASIL-Einstufung, auch die meisten Testressourcen zugeordnet werden. Im konkreten Falle hieße dies für das Gesamtsystem, dass eine höhere Anzahl an Testfällen für Verkehrssituationen vorzusehen ist, von denen ein hohes Risiko für beteiligte Verkehrsteilnehmer zu erwarten ist. Dadurch wird die Entdeckungswahrscheinlichkeit damit verbundener Fehler höher.

Die dritte Möglichkeit zur Testfallermittlung ist die schnittstellenbasierte Testspezifikation, die Gemeinsamkeiten mit strukturellen Testspezifikationsverfahren besitzt und sich somit auch für modellbasiertes und automatisiertes Testen eignet. Als bisher einziges bekanntes Verfahren ermöglicht dies in der Theorie, die Testabdeckung zu quantifizieren und ein System auf Basis einer Variation aller diskretisierten Eingangsinformationen und internen Zuständen eines Systems vollständig zu testen.[175] Dieses Spezifikationsverfahren wurde jedoch bisher nur auf Systeme angewendet, die verhältnismäßig einfache Verhaltensentscheidungen treffen, wie z. B. die Aktivierung eines elektrischen Fensterhebers[176] oder eine Pedalaktivierungserkennung für ACC[177]. Für die Anwendung auf FAS besteht hier die Schwierigkeit, kontinuierliche und räumliche Messgrößen, wie sie z. B. aus einem Radarsensor gewonnen werden, effizient für unterschiedliche

174 S. SAUST (2009), S. 97

175 Z. B. die „Klassifikationsbaummethode“ (CTM)

176 S. BENZ (2004)

177 S. BENZ (2004)

Verkehrsszenarien mit beliebigen Konstellationen der beteiligten Verkehrsobjekte zu diskretisieren.

Zusammenfassend ist festzuhalten, dass sich aus der funktionalen Sicht einerseits und der risikobasierten Absicherung eines Systems andererseits zwei unterschiedliche Strategien zur Ermittlung von Testfällen ergeben. Anwendungsfälle in Form von Referenzfahrsituationen unterstützen dabei den Prozess der Anforderungsdefinition und stellen in einem höheren Detaillierungsgrad analog zur lastenheftbasierten Testspezifikation passende Testfälle zur Systemverifikation und -validierung zur Verfügung. Für die Absicherung eines Fahrerassistenzsystems eignen sich diese nur bedingt, da dabei nicht zwingend eine Betrachtung des dabei vom System ausgehenden Risikos erfolgt. Zum Nachweis der funktionalen Sicherheit muss daher vielmehr eine risikobasierte Testspezifikation auf Basis der aus Anwendungsfällen gewonnenen Systemanforderungen erfolgen. Ob sich das modellbasierte Testen auch auf die Absicherung von Fahrerassistenzsystemen mit Umfelderfassung anwenden lässt, ist nach aktuellem Stand der Technik nicht zu beantworten. Hier besteht weiterer Forschungsbedarf.

4.6.2 Entwicklung eines Szenarienkatalogs zur Bewertung der technischen Realisierbarkeit eines hochautomatisierten manöverbasierten Fahrzeugführungskonzepts[178]

Wie im vorherigen Kapitel dargestellt, haben Forschungs- und Entwicklungsaktivitäten im Bereich der Fahrzeugautomatisierung in den vergangenen Jahrzehnten eine Vielzahl von Entwicklungswerkzeugen und -methoden hervorgebracht. Die von den entwickelten Systemen zu erfüllenden Anforderungen und somit die Entwicklungsrichtlinien werden meist in verschiedenen Arten von Katalogen (z. B. Use-Case-Kataloge, Situationskataloge, Szenarienkataloge etc.) dokumentiert, die durch unterschiedliche Herangehensweisen erstellt werden. Die beschriebenen Ansätze zur Reduktion des Umfangs dieser Kataloge und somit zur Reduktion des Entwicklungsaufwands bestehen in der Beschränkung auf die repräsentativsten Szenarien, auf spezielle Anwendungsfälle für einen bestimmten Funktionsumfang der Automation oder schlicht in der Auswahl der reproduzierbar darstellbaren Test-Fälle.

Diese Ansätze haben sich in der Vergangenheit bewährt und bilden daher den Stand der Technik im Bereich der Entwicklung von Fahrerassistenzsystemen, die gemäß der BASt-Nomenklatur[179] dem „assistierten“ Fahren zuzuordnen sind. Die beschriebenen Ansätze erreichen jedoch schnell ihre Grenzen, wenn es um die Entwicklung höherautomatisierter Fahrzeugführungskonzepte geht. Ein Beispiel für die „teilautomatisierte“ Fahrzeugführung, und damit für den nächsthöheren Automatisierungsgrad, ist das von der Deutschen Forschungsgemeinschaft geförderte Forschungsvorhaben „Conduct-by-Wire“ an der Technischen Universität Darmstadt. Die Idee von Conduct-by-Wire (CbW)[180] besteht darin, die Fahrzeugführung durch eine manöverbasierte Interaktion zwischen Fahrer und Automation von der Stabilisierungsebene auf die Bahnführungsebene anzuheben (vgl. Bild 10).

Die konventionelle kontinuierliche Interaktion zwischen Fahrer und Fahrzeug auf der Stabilisierungsebene wird durch eine ereignisbasierte Kommunikation über Manöverbefehle auf der Bahnführungsebene ersetzt. Der Fahrer eines CbW-Fahrzeugs kommuniziert seine Manöverbefehle über eine Manöverschnittstelle, die zudem eine Parametrierung der gewählten Manöver sowie bei Bedarf eine Interaktion auf der Stabilisierungsebene ermöglicht. Das CbW-Konzept basiert somit auf einer eindeutigen Aufgaben- und Verantwortungsverteilung zwischen den beiden handelnden Interaktionspartnern Fahrer (Manöverbeauftragung) und Automation (Manöverausführung).

Der Fokus des genannten Forschungsprojekts liegt auf der Untersuchung der Realisierbarkeit des CbW-Konzepts in dieser frühen Produktentwicklungsphase als Grundlage für eine prototypische Umsetzung in einem Versuchsfahrzeug. Ziel ist die Untersuchung der Fragestellung, ob die konventionelle Fahrzeugführung durch das CbW-Konzept ersetzt werden kann. Die Entwicklungsgrundlage bildet die Identifikation der von einem CbW-Fahrzeug zu absolvierenden Szenarien.[181] Aufgrund des in dem Projekt verfolgten ganzheitlichen Ansatzes sind die oben beschriebenen Kataloge nicht direkt anwendbar. Stattdessen sind alle potenziellen Szenarien zu betrachten, die ein CbW-Fahrzeug bewäl-

---

178 Verantwortlicher Autor des Kapitels 4.6.2 ist Dipl.-Ing. Sebastian GEYER.

179 Vgl. GASSER et al. (2012), S. 9

180 WINNER et al. (2005) und WINNER et al. (2006)

181 Die im Folgenden verwendeten Begriffe orientieren sich an der Nomenklatur von GEYER et al. (2013).

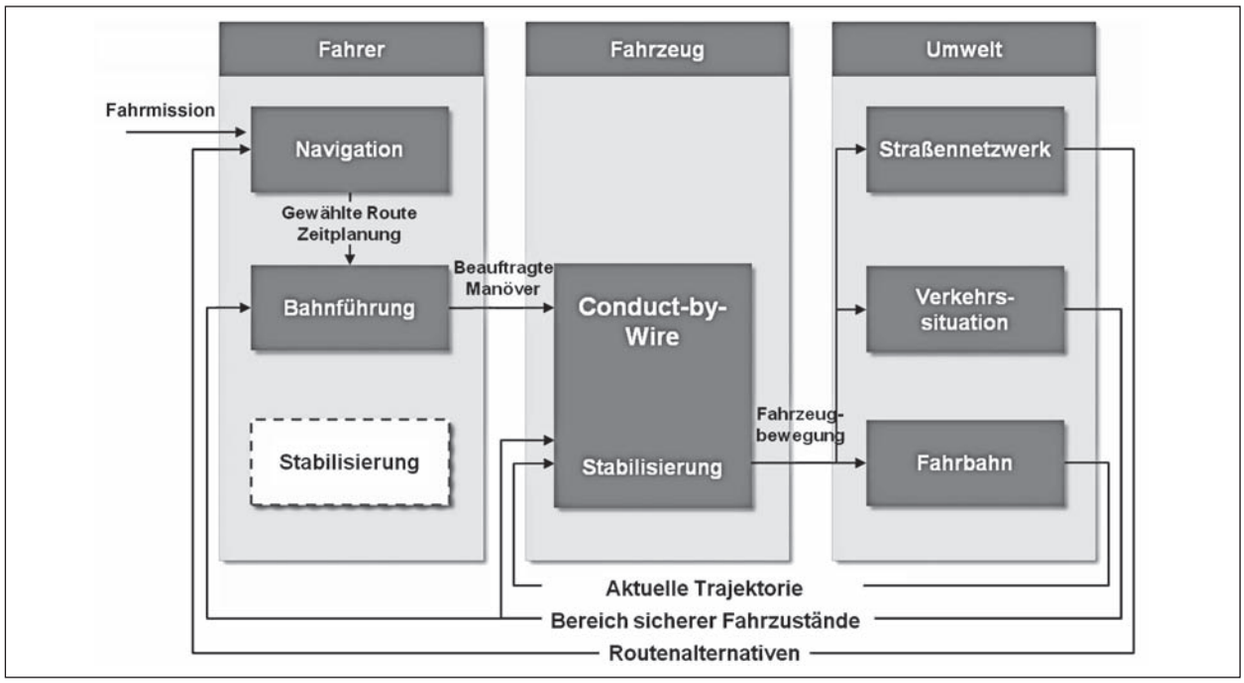

Bild 10: Manöverbasierte Fahrzeugführung nach dem CbW-Prinzip[182]

tigen muss. Die beschriebenen Maßnahmen zur Reduktion der Kataloge sind unzulässig, da unter Umständen relevante Ausprägungen oder Kombinationen vernachlässigt werden.

Bei der Entwicklung des für die CbW-Entwicklung zu Grunde gelegten Katalogs wird daher ein systematischer Top-down-Ansatz verfolgt, der gewährleistet, dass möglichst viele potenzielle Szenarien abgedeckt werden. Den Ausgangspunkt des in Bild 11 dargestellten Vorgehens bildet die systematische Identifikation von Szenerien beschreibenden Merkmalen. Diese werden aus den technischen Regelwerken für das Straßenwesen in Deutschland und der Straßenverkehrsordnung (StVO) abgeleitet. Erstere enthalten Vorschriften zur geometrischen Gestaltung und Verkehrsführung. Die Straßenverkehrsordnung liefert Merkmale wie Fahrbahnmarkierungen oder Typ und Platzierung von Verkehrszeichen sowie Verhaltensvorschriften. Aus diesen Regelwerken lassen sich zudem Implikationen von Gestaltungselementen sowie zulässige Kombinationen von Merkmalsausprägungen und Szenerien ableiten, wodurch die Zahl möglicher Variationen automatisch begrenzt wird.

Die auf diese Weise identifizierten Szenerien und deren beschreibende Parameter lassen sich einer der vier Klassen „Kreuzung“, „Kreisverkehr“, „Querverkehr“ und „Längsverkehr“ zuordnen. Die Auswahl der Merkmale orientiert sich an den für die Untersuchungspunkte dieses Forschungsprojekts relevanten Einflussfaktoren. So werden in dieser frühen Konzeptphase ideale Umweltbedingungen angenommen, sodass die Szenerie beeinflussende Faktoren wie Lichtverhältnisse oder der Fahrbahnzustand nicht berücksichtigt werden.

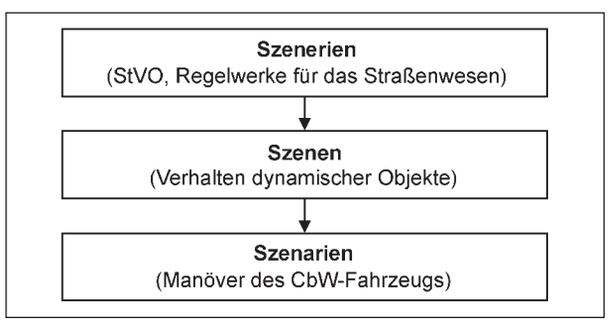

Bild 11: Methodik zur Erstellung des CbW-Szenarienkatalogs

Die auf diese Weise identifizierten Szenerieklassen treten im realen Straßenverkehr nur selten getrennt voneinander auf. Beispielswese stellt die Kombination einer Kreuzung mit Fußgängerüberwegen eine häufig auftretende Szenerie dar. Hinsichtlich einer möglichst vollständigen Abdeckung aller in der Realität auftretenden Szenerien kann in zwei Schritten vorgegangen werden. Zunächst werden alle Szenerien systematisch miteinander kombiniert und im zweiten Schritt nicht sinnvolle Kombinationen gestrichen bzw. die Zulässigkeit dieser

182 WINNER et al. (2005)

Kombinationen anhand der Regelwerke für das Straßenwesen in Deutschland und der Straßenverkehrsordnung (StVO) überprüft. Der entwickelte Szeneriekatalog wurde abschließend anhand von Videodaten von im Rhein-Main-Gebiet durchgeführten Messfahrten validiert.

Aufbauend auf dem Szeneriekatalog lassen sich Szenen durch Kombination mit dynamischen Objekten und Definition deren Verhaltens generieren. Die entwickelten Szenen lassen sich wiederum mit den vom CbW-Fahrzeug ausgeführten Manövern zu Szenarien verknüpfen.

Die Anwendung dieses Katalogs beschränkt sich, wie eingangs beschrieben, auf die Untersuchung der technischen Realisierbarkeit des CbW-Konzepts in einer sehr frühen Entwicklungsphase. Der Untersuchungsfokus richtet sich hierbei in erster Linie auf die kooperative Interaktion zwischen Fahrer und Automation und die Ableitung unterschiedlicher Systemausprägungen. Basierend auf diesen der Systemebene zuzuordnenden Betrachtungen, erfolgt die praktische Umsetzung auf der Funktionsebene. Hierzu zählen die Entwicklung des erforderlichen Funktionsumfangs der Automation sowie die Ermittlung der Anforderungen an die maschinelle Umfeldwahrnehmung. In all diesen Entwicklungsphasen bildet der beschriebene Katalog die Entwicklungsgrundlage. Damit kann in einer Frühphase der Entwicklung die technische Realisierbarkeit einer teilautomatisierten manöverbasierten Fahrzeugführung abgeprüft werden. Gleichwohl werden grundlegende Aspekte, wie die Betrachtung der funktionalen Sicherheit, noch nicht betrachtet. Im Hinblick auf eine spätere prototypische Realisierung, einen Funktionstest im öffentlichen Straßenverkehr oder gar den späteren Kundeneinsatz ist diese jedoch unerlässlich. Zudem bietet die Analyse der funktionalen Sicherheit, neben der grundsätzlichen technischen Realisierbarkeit, mögliches „Showstopper“-Potenzial. Doch wie testet man ein System, bei dem große Teile der Fahrzeugführungsaufgabe durch die Automation übernommen werden? Auch wenn im Falle von CbW der Fahrer jederzeit die Fahrzeugführung wieder übernehmen kann, stellt die von WINNER et al. (2010) beschriebene „Freigabefalle“ der vollautomatisierten Fahrzeugführung, neben den rechtlichen Rahmenbedingungen, eine große Herausforderung dar. Berücksichtigt man als weitere Randbedingung einen vertretbaren Entwicklungs- und Freigabeaufwand, ist aus Sicht des aktuellen Standes der Forschung und Technik keine Alternative zu der beschriebenen Beschränkung auf Anwendungsfälle erkennbar. So geben FLEMISCH et al. (2009, S. 23) einen Ausblick auf einen möglichen Testkatalog für die automatisierte Fahrzeugführung zur Untersuchung der Auswirkungen von Fehlfunktionen der Automation.

4.7 Schlussfolgerungen – Absicherungsmethoden

Zahlreiche Verfahren zur Absicherung beziehungsweise zur Bewertung der korrekten Funktion eines Fahrerassistenzsystems wurden dargestellt. Im Bereich von Sensorik und Steuerung lassen sich hinsichtlich der Ansätze und Methoden Parallelen erkennen. So werden beispielsweise Redundanzen angewendet, die entweder funktionsgleich oder auch disjunkt sein können. Die Architektur wird so gestaltet, dass sich Komponenten gegenseitig, teilweise modellgestützt, überwachen können. Die Sensoren führen Integritätsbewertungen der Messdaten durch und erlauben dabei über hinterlegte Fehlermodelle, die Qualität der eigenen Daten zu bewerten. Diese Daten können an die Steuergeräte weitergegeben werden, um sie dort in die Situationsbewertung einzubeziehen. Diese ständige Integritätsbewertung von Sensorsignalen ist aktuelles Forschungsthema und noch in der Entwicklung begriffen.

An der Schnittstelle zum Fahrer kann ebenfalls großes Potenzial zur weiteren Verbesserung der Sicherheit identifiziert werden. Zahlreiche Projekte beschäftigen sich mit der Bewertung der Interaktion zwischen Fahrer und Fahrzeug in kritischen Situationen, um sowohl den Nutzen der Systeme im Falle von berechtigten Auslösungen zu maximieren als auch die Auswirkungen im Fall von unberechtigten Auslösungen. Durch Letzteres kann die Einschränkung des Einsatzbereiches von Fahrerassistenzsystemen auf das notwendige Minimum begrenzt werden, sodass ein größerer Anteil des Gesamtfahrsituationskollektivs bzw. des Unfallkollektivs abgedeckt wird.

Existierende oder in der Entwicklung befindliche Verfahren, die auf das Gesamtsystem von Fahrer/Fahrzeug/Umwelt ausgerichtet sind, wurden ebenfalls betrachtet, diese zeigen sehr deutlich eine Problematik der dringend notwendigen Relevanzbewertung für die Begrenzung des zur Absicherung notwendigen Testaufwandes. Vermutlich wird auch bei Ansätzen basierend auf der Funktionskette diese Frage mit zunehmender Vernet-

zung von Systemen und bei der Ausrichtung auf immer komplexere Anwendungsszenarien auftreten. Einerseits sind eine möglichst spezifische Definition des Anwendungsfalls und die daraus resultierende Ableitung eines Test-Falles (im engl. auch „test-case“) notwendig, um belastbare Ergebnisse zu erhalten. Die Relevanz dieses Anwendungs- bzw. Test-Falles für den realen Verkehr muss aber jeweils nachgewiesen bzw. sogar quantifiziert werden. Sonst wird unter Umständen im Feld trotz exzellenter Funktions- und Sicherheitsbewertungen nur ein geringer Sicherheitsfortschritt erzielt. Durch die steigende Anzahl von Sensoren und in die Funktion einbezogener Parameter in modernen Fahrerassistenzsystemen mit Umfeldwahrnehmung steigt auch der Aufwand für die Definition von Szenarien, die Durchführung von Tests und den Relevanznachweis für das Feld beständig. Daher sind bei der Suche nach ergänzenden Methoden insbesondere Effizienz- und Effektivität, auch vor wirtschaftlichem Hintergrund, zu berücksichtigen.

5 Definition von Prüffällen[183]

5.1 Herleitung des theoretischen Testaufwandes bei konventionellen Testmethoden

Wie im vorhergehenden Kapitel identifiziert, ist die belastbare systematische Ableitung von Prüffällen für die Absicherung von Fahrerassistenzsystemen mit Umfeldwahrnehmung notwendig. Eine konventionelle Methode ist dabei der Dauerlauftest sowie Feldversuche im realen Straßenverkehr teilweise mit Probandeneinbindung.[184] Der hierfür notwendige Aufwand ist dabei direkt abhängig von der erwarteten Auslösehäufigkeit und darüber bezogen auf die Kilometerleistung zurückzulegenden Strecke zwischen den Systemauslösungen. In Tabelle 7 sind hierfür Beispiele dargestellt.

Zur Ermittlung der nötigen Testkilometer für die Prüfung des Nutzens eines Systems in realen Fahrsituationen wird hier beispielhaft eine Abschätzung vorgenommen.

Zuerst wird der Nutzen der Funktion anteilig am Unfallgeschehen ermittelt. Es wird davon ausgegangen, dass es sich um eine Funktion handelt, die die Unfälle mit Personenschaden adressiert. Angenommen wird, dass ein Viertel aller Unfälle Auffahrunfälle sind: $p_{Auffahrunfall}$ = 25 %.[187] Weiterhin angenommen, die besagte Funktion adressiert hinsichtlich der Systemgrenzen (beispielsweise der Geschwindigkeiten vor dem Aufprall, der Witterungsbedingungen usw.) drei Viertel der Unfälle ($p_{adressierte\ Unfälle}$ = 75 %) und kann diese in der Hälfte der Fälle sicher vermeiden ($p_{sicher\ vermieden}$ = 50 %).[188]

Die allgemeine Unfallhäufigkeit wird auf Basis der zurückgelegten Pkw-Kilometer bezogen auf die Anzahl der Unfälle mit Personenschaden ermittelt. Für das Anwendungsgebiet Deutschland ergibt sich die Jahreskilometerfahrleistung zu $s_{ges.\ Jahr}$ = 615 · 10^9 km[189] bei einem Fahrzeugbestand in 2012 von $n_{Pkw,BRD}$ = 42.927.647 Pkw[190]. Im Jahr

183 Kapitel in Anlehnung an WEITZEL (2013), S. 42 ff.

184 BREUER (2012), S. 58

185 Aus FACH et al. (2010), S. 424

186 Datenbasis ca. 300.000 Messungen auf ca. 2.000.000 km (ca. 20 % in USA) > 1.000 Fahrer (∅ eine Messung je ca. 6 km Fahrt)

187 Statistisches Bundesamt (2012), S. 8-9

188 Und in den anderen Fällen die Unfallfolgen lindern

189 KUNERT et al. (2012), S. 6

190 KBA-Webseite; Abruf am 15.02.2013

Messungen mit Systemauslösungen	Häufigkeit pro 10.000 km	km mit Auslösung
Aktiver Totwinkel-Assistent	0,4-0,7	15.000-25.000
Spurhalte-Assistent	500-800	12-20
Aktiver Spurhalte-Assistent	70-80	125-150
Abstands-Warnung	40-60	170-250
Pre-Safe-Bremse Stufe 1	0,1-0,2	50.000-100.000
Pre-Safe-Bremse Stufe 2	0	-
BAS Plus	0,5-1	10.000-20.000

Tab. 7: Häufigkeiten von Systemauslösungen[185, 186]

2011 geschahen in Deutschland $n_{Unfälle}$ = 306.266 Unfälle mit Personenschaden[191].

Daraus ergibt sich nach Formel 2 die Anzahl der Auffahrunfälle ($n_{Auf.unf.}$) mit Personenschäden in Deutschland.

$$n_{Auf.unf.} = n_{Unfälle} \cdot p_{Auf.unf.} \approx 76.500 \quad (2)$$

Formel 3 beschreibt die Anzahl von diesen Unfällen, die innerhalb der Systemgrenzen liegt ($n_{Auf.unf.\ adr.}$).

$$n_{Auf.unf.\ adr.)} = n_{Auf.unf.} \cdot p_{adr.Unf.} \approx 58.000 \quad (3)$$

Davon kann die Hälfte sicher vermieden werden, sodass sich die Anzahl sicher vermiedener Unfälle ($n_{Auf.unf.,\ sicher\ vermieden}$) nach Formel 4 ergibt.

$$n_{Auf.unf.sich.verm.} = n_{Auf.unf.adr.} \cdot p_{sich.verm.} \approx 29.000 \quad (4)$$

Die Distanz zwischen zwei zu den beschriebenen für die Funktion relevanten Unfällen ergibt sich daraus theoretisch gemäß Formel 5.

$$l_{Unfall} = \frac{s_{ges.\ Jahr}}{n_{Auf.unf.\ adr.}} = 10^7 \text{ km} \quad (5)$$

Eine weitere Begrenzung dieser Distanz kann noch vorgenommen werden, indem nur die Anteile des Gesamtkilometerkollektivs betrachtet werden, in denen die Funktion einen Nutzen bringen kann (Formel 6).

$$l_{Unf.Nutzen} = \frac{s_{ges.\ Jahr} \cdot p_{adr.\ Unf.}}{n_{Auf.unf.\ adr.}} = 7{,}5 \cdot 10^6 \text{ km} \quad (6)$$

Dabei wird zugrunde gelegt, dass sowohl die Unfallverteilung über dem Kilometerkollektiv konstant ist als auch der Nutzenanteil am Kilometerkollektiv gleich dem Anteil der beobachteten Unfälle ist.[192]

Die unfallvermeidende Fahrerassistenzfunktion wird also statistisch betrachtet nur alle 7.500.000 km eine gültige Auslösung aufweisen.

Soll der Nutzen eines solchen Systems im Realverkehr abgesichert werden, wäre eine Mindeststichprobe notwendig, bei der die Überschneidung der Expositionswahrscheinlichkeiten der Ereignisse kleiner als 5 % ist (Konfidenzniveau = 95 %). Dann kann die Hypothese „Die Unfallrate mit System ist mindestens um 50 % kleiner als ohne System“ angenommen werden.

Aufgrund dessen, dass das Unfallereignis selten eintritt und nur zwei Zustände eingenommen werden können (Unfall/kein Unfall), wird eine Poisson-Verteilung herangezogen. Es ergibt sich die Expositionswahrscheinlichkeit eines Ereignisses nach Formel 7[193] und 8.

$$P_\lambda(k) = \frac{\lambda}{k!} e^{-\lambda} \quad (7)$$

mit

$$\lambda = n \cdot p \quad (8)$$

Mit der Expositionswahrscheinlichkeit des Ereignisses p (bspw. dem Kehrwert der Distanz zwischen zwei Unfällen ($l_{Unf.\ Nutzen}$) und dem Stichprobenumfang n (bspw. die Beobachtungskilometer $l_{Beob.\ km}$) Diese Definitionen eingesetzt ergeben für $\lambda_{Absicherung}$ nach Formel 9:

$$\lambda_{Abs.} = l_{Beob.\ km} \cdot l_{Unf.Nutzen}^{-1} \quad (9)$$

Für den Nachweis des Unterschieds ist entsprechend der einseitige Test der 95%-Grenze für beide kumulativen Wahrscheinlichkeitsdichtefunktionen zu führen. Für die genannten Bedingungen ergibt sich diese Grenze zu rund 236 Mio. km.

Wird statt des Falls der korrekten Funktion des Systems die fehlerhafte/falsche/nicht situationsgerechte Auslösung betrachtet, kann ebenfalls die Einschränkung der Betrachtung auf die Begrenzungen des Einsatzbereiches des Systems anhand von $p_{adr.\ Unfälle}$ (bspw. hinsichtlich der Geschwindigkeit o. Ä.) vorgenommen werden.

Für die Bestimmung des notwendigen Kilometerkollektivs hinsichtlich der Absicherung dieses potenziellen Gefährdungsfalles durch eine unerwünschte Systemreaktion wird ein gesellschaftlich akzeptiertes Grenzrisiko als Referenz benötigt.[194]

Ein Ansatz, dieses zu bestimmen, ist der Vergleich des Nutzenanteils mit den Gefährdungsfällen. Dazu kann beispielsweise der Nachweis geführt werden, dass der Nutzen der Systeme deutlich größer als der potenzielle Schaden ist.[195]

Angenommen, dieses geforderte Verhältnis zwischen Nutzwert und potenziellem Zusatzschaden

---

191 Statistisches Bundesamt (2012), S. 43; Stand 01. Januar 2012

192 Treten Auffahrunfälle bspw. gehäuft auf Autobahnen auf, so kann der Anteil der BAB-Fahrten als Beschränkung verwendet werden.

193 Nach BORTZ (2005), S. 71

194 S. Kapitel 3.8.4

195 Vgl. GASSER et al. (2012), S. 11 und Kapitel 3.8.4

durch nicht situationsgerechte Auslösungen wird auf einen Unterschied von einer Größenordnung festgelegt. Dies entspricht in etwa der Änderung des Risikos, wie sie auch bei Absicherungsnormen wie ISO 26262 zwischen den Stufen häufig herangezogen wird. Dann ist der Absicherungsaufwand für diese unerwünschten Auslösungen mindestens um diesen Faktor größer. Im beschriebenen Beispiel müssten entsprechend 2,4 Mrd. Kilometer gefahren werden.

5.1.1 Eventbasierte Betrachtung

Neben der kilometerbasierten Betrachtung einer Auslösung, die davon ausgeht, dass der intendierte Auslösungsfall bzw. die fehlerhafte Auslösung des Systems an eine bestimmte Laufleistung gekoppelt werden kann, ist auch eine eventbasierte bzw. fahrtbasierte Betrachtung möglich. Dabei wird die Auftretenshäufigkeit an ein Ereignis gekoppelt, bspw. das Starten des Motors bzw. an die Fahrt an sich und ist damit von der Anzahl der Fahrten abhängig. Die Fahrtenzusammensetzung hinsichtlich spezifischer Ereignisse ist durch die durch das Nutzungskollektiv bedingten Situationen definiert. Auch der Unfall kann als Einzelereignis betrachtet werden, sodass hier die gleichen Überlegungen wie bei der kilometerbasierten Betrachtungsweise angestellt werden können, solange sichergestellt ist, dass im gewählten Fahrtkollektiv das potenziell auslösende Einzelereignis statistisch belastbar häufig auftreten wird.

Ausgehend davon, dass ein relevantes Nutzungskollektiv gewählt wurde und der Nachweis dieser Relevanz geführt werden kann, müssten in diesem alle eventbasierten Ereignisse in entsprechender Häufigkeit auftreten, sodass eine Unterscheidung gegenüber der kilometerbasierten Betrachtungsweise nicht vorgenommen werden muss.

5.1.2 Ungünstige Situationskonstellationen

Neben den statistisch relevanten kilometerbasierten Ereignissen und Fällen können zudem auch Konstellationen mit mehreren Einflussfaktoren auftreten, die entweder in dieser Kombination sehr viel häufiger auftreten als bei Annahme der statistischen Unabhängigkeit der Einzelfaktoren oder bei denen die Kombination der Einzelfaktoren zu einer Schadensvermehrung führt. Diese Konstellationen, im Sprachgebrauch der Systementwicklung teilweise als „pathologische Fälle“ bezeichnet, müssen im Vorhinein bekannt sein bzw. systematisch anhand der Systemspezifikationen herzuleiten sein. Ist dies nicht der Fall, können gegebenenfalls Langzeiterfahrungen und bekannt gewordene Fälle aus der Vergangenheit („kritisch aus Erfahrung“) herangezogen werden. Diese Situationen müssen dem Situationskollektiv ebenfalls hinzugefügt werden. Diese im Betrieb durch Dauerlauftests sowohl zu identifizieren als auch zu prüfen ist, angesichts des bereits vorgestellten Aufwandes für häufige Situationen, für diese seltenen Fälle vermutlich kaum darzustellen.

5.1.3 Anwendbarkeit existierender Beschleunigungsmechanismen

Bei der Untersuchung der Versagenshäufigkeit von Bauteilen und Komponenten werden in der Ingenieurwissenschaft unterschiedliche Methoden eingesetzt, die zu einem gehäuften Auftreten der zu betrachtenden Fälle führen sollen.[196]

Zwei Methoden werden hier hinsichtlich ihrer Eignung für die Reduzierung der benötigten Testkilometerleistung diskutiert.

Komponentenlebensdauertests

Bei der Lebensdauerprüfung von mechanischen und elektrischen Einzelkomponenten werden die Testzyklen gekürzt, indem entweder nur die kritischen Anteile des Belastungskollektivs ausgewählt werden oder indem beispielsweise die Lasten auf das Bauteil erhöht werden.[197] Dabei werden kritische Bauteile ausgewählt und diese isoliert getestet.

Zur Erhöhung des „Lastkollektivs“ für Fahrerassistenzsysteme mit Umfeldwahrnehmung nach dem Vorbild der Lebensdauertests könnte aus allen Variationsparametern jeweils die für die zu bewertende Eigenschaft am kritischsten wirkende Ausprägung herausgesucht, und diese zu einem allgemeinen „Worst-Case“ kombiniert werden. Dieser berücksichtigt jedoch nicht die Expositionswahrscheinlichkeit dieses Falles und ist damit für eine belastbare Risikobestimmung nicht geeignet, jedenfalls nicht ohne Relevanzbewertung. Ausgehend von der Vermutung, dass sich die Exposi-

196 Vgl. MEYNA et al. (2003), S. 192 ff.

197 MEYNA et al. (2003), S. 192 ff.

tionswahrscheinlichkeit der Kombination gefährlicher Situationsausprägungen aus der Multiplikation der Einzelwahrscheinlichkeiten ergibt, ist die Expositionswahrscheinlichkeit des „Worst-Case“ vermutlich sehr gering und damit dessen Relevanz für das Feld sehr gering.

Bei der Prüfung von Fahrerassistenzsystemen ist zudem der Versagensfall „nicht situationsgerechte Reaktion“ kein Ausfall einer einzelnen Komponente, sondern das Resultat einer inhärenten Unsicherheit/Ungewissheit (uncertainty) bei Erkennung oder Entscheidungsfindung des Gesamtsystems. Diese kann an unterschiedlicher Stelle des Systems entstehen. Kann eine Komponente identifiziert werden, die besonders anfällig für bestimmte Situationskonstellationen sind und dabei unabhängig von Einflüssen anderer Elemente ist, ließe sich diese isoliert betrachten.

Ansonsten muss eine Bewertung des Gesamtsystems stattfinden und das Belastungskollektiv alle Einzelkomponenten und deren Zusammenspiel adressieren. Zudem ist die Bewertung, wie in Kapitel 4.5 beschrieben, unter Umständen noch fahrerabhängig. Die Kürzung des notwendigen Kollektivs ist nur dann möglich, wenn besonders kritische Situationen für die Entscheidungsfindung und für das Zusammenspiel im Vorfeld identifizierbar sind. Muss die Betrachtung inklusive Fahrerreaktion erfolgen, kann dann versucht werden, diese Situationen gezielt entweder, in sofern aus Sicherheitsgründen vertretbar, im Realverkehr oder auf Testgeländen und in Simulatoren zu erzeugen. Die Belastbarkeit und Relevanz der Auswahl ist dabei jeweils nachzuweisen.

Beschleunigungsmechanismen wie die Erhöhung der Last sind aktuell nicht bekannt. Dazu müsste die „Belastung“ für das System definiert werden, indem beispielsweise besonders „reizüberflutete“ oder mehrdeutige Situationen herangezogen werden.

In Erweiterung können auch Situationslisten verwendet werden, in denen potenziell kritische Situationen gesammelt und hinsichtlich der zu erwartenden Expositionswahrscheinlichkeit bewertet werden. KEMMANN et al. (2005, S. 5) zeigen hierzu einen Ansatz, der diese Methode hinsichtlich der Kriterien Konsistenz, Vergleichbarkeit und Wiederverwendbarkeit optimiert.

Simulation und X-in-the-Loop

Eine bei der Entwicklung komplexer Systeme häufig angewendete Technik zur Aufwandsreduktion sind Simulationstechniken. Ergänzend hierzu können auch teilweise simulative Ansätze, wie in Kapitel 4.3 als „X-in-the-Loop“ dargestellt, herangezogen werden. Überträgt man diese Vorgehensweise auf die hier vorliegende Problemstellung, sind Test-Fälle zu definieren, in denen dann Teile der Umwelt bzw. des Systems selbst durch Simulation nachgebildet werden.

Um dabei Übertragbarkeit in die Realität gewährleisten zu können, muss ebenfalls die minimale Anzahl relevanter notwendiger Test-Fälle definiert werden. Zudem ist die Validität der Simulation unter Variation der Vielzahl von Situationsparametern nachzuweisen. Das Ergebnis der Test-Fälle hängt zudem unter Umständen von der Reaktion weiterer Verkehrsteilnehmer ab, denen entsprechend eine Art künstliche Intelligenz zugewiesen werden müsste. Entsprechend ergibt sich ein hoher Aufwand für die Erstellung und Validierung eines solchen ausreichenden Testumgebungsmodells.

Statistisch motivierte Ansätze

Alternativ existieren auch statistisch motivierte Ansätze. Dabei werden die Expositionswahrscheinlichkeiten der einzelnen Situationsfaktoren rekombiniert und daraus die Relevanz bestimmt.[198] Mit diesen Methoden kann die vollständige Abbildung aller theoretisch möglichen Situationen in statistischen Modellen angestrebt werden. Dabei sind die abgeleiteten Aussagen von den gewählten Situationsfaktoren und deren Diskretisierung abhängig. Die Belastbarkeit der Argumentation setzt voraus, dass die gewählten Fahrsituationsparameter als hinreichend vollständig bewertet werden können. Ein Bewertungsverfahren dafür ist zum aktuellen Zeitpunkt nicht bekannt. Ebenso ergibt sich aus der freien Rekombination der Einflussfaktoren, dass statistische Wechselwirkungen einbezogen werden müssen. Die Expositionswahrscheinlichkeiten der Situationsparameter sind unter Umständen direkt voneinander abhängig. So zeigt zum Beispiel FECHER (2005, S. 51 ff.) Abhängigkeiten des Abstandsverhaltens von Umgebungsfaktoren und Straßenklasse. Damit ist eine freie Rekombination

198 STÄNDER (2011), S. 133 ff.

von Situationsfaktoren streng genommen nicht zulässig, es sei denn, die Expositionswahrscheinlichkeit wird für jede explizite Einzelsituation bestimmt. Dies schränkt aber die Möglichkeit der Übertragbarkeit und Kumulation bei niedrigeren Detaillierungsgraden ein.

5.1.4 Statistische Rahmenbedingungen für Probandentests nach ISO 26262

Sollen für die Absicherung von Fahrerassistenzfunktionen gemäß ISO 26262 Versuche mit hoher Übertragbarkeit und Relevanz für das Feld durchgeführt werden, empfiehlt der „Code of Practice“[199] Probandenversuche. Dazu sind entsprechend den dort definierten Grenzen für die Absicherungsstufe C2 mindestens 20 gültige Versuche zu fahren.

In einer darauf basierenden Analyse der notwendigen Anzahl von Probanden am Beispiel einer Kontrollierbarkeitsbewertung zeigen WEITZEL et al. (2012, S. 18 ff.), dass bei diesem Ansatz bereits für die Absicherungsstufe C2 eine Probandenanzahl von mindestens 29 Personen notwendig ist. Dabei müssen zudem alle Versuche als kontrollierbar zu bewerten sein. Treten im Versuchskollektiv unkontrollierbare Ereignisse auf, erhöht sich die notwendige Probandenanzahl. Im Umkehrschluss ist bei einer tatsächlichen Kontrollierbarkeit von 90 % im Probandenkollektiv die Erfolgswahrscheinlichkeit für einen Nachweis der Kontrollierbarkeit bei diesen geringen Probandenzahlen unter 5 %.

Die so ermittelten Kontrollierbarkeitswerte sind dabei, zumindest theoretisch, nur für die jeweilige Situation gültig. Bei Änderung der Systemausprägung oder in anderen Situationskonstellationen sind die Versuche also gegebenenfalls zu wiederholen. Neben dem potenziell hohen Aufwand aufgrund einer Vielzahl notwendiger Test-Fälle für die Absicherung sind diese Test-Fälle zudem jeweils mit einer großen Anzahl von Probanden zu prüfen. Dabei ist die Erfolgswahrscheinlichkeit der Tests bei geringer Probandenanzahl gering, insbesondere wenn der Anteil der zu untersuchenden Eigenschaft, bspw. der Kontrollierbarkeit am Gesamtkollektiv gering ist.

5.2 Resultierende Anforderungen für Test, Bewertung und Absicherung von FAS

Für eine systematische objektive Auswahl von Prüfsituationen sind also sowohl die Eignung der Situation zur Prüfung der Eigenschaft (bspw. der Kontrollierbarkeit) als auch die statistische Relevanz für den späteren Einsatz des Fahrzeugs durch den Kunden zu bewerten. Dazu muss die statistische Relevanz, bezogen auf das zu erwartende Nutzungsprofil, berücksichtigt werden. Kann ein solcher Relevanzfaktor ermittelt werden, erlaubt dies die nachvollziehbare systematische Auswahl der minimal notwendigen Zahl von Test-Fällen für die Absicherung. Dieses ausgewählte Testsituationskollektiv deckt dann die hinsichtlich des Risikos kritischen Fälle ab. Die Bewertung muss eine hohe Übertragbarkeit zu ähnlichen Problemstellungen bieten, um den Analyseaufwand vertretbar zu halten.

Da zu Beginn der Betrachtungen keine Vollständigkeit der vorliegenden Daten zu erwarten ist, muss das Vorgehen die Abbildung von Unsicherheiten oder Abschätzungen zulassen. Zusätzlich ist eine schrittweise Erhöhung des Detaillierungsgrades der situationsbeschreibenden Parameter notwendig. Dann kann auf unterschiedlichen Detaillierungsstufen bewertet und dabei jeweils identifiziert werden, ob eine Erhöhung der Detaillierung der vorliegenden Daten sinnvoll ist.

Betrachtet werden dabei jeweils „globale“ Eigenschaften, also solche, die nur durch Untersuchungen oder Messungen am Gesamtsystem Fahrer-Fahrzeug in der jeweiligen Umgebung bewertet werden können. In WEITZEL et al. (2012) ist ein solches Beispiel für den Fall der Kontrollierbarkeitsbewertung aktiver Sicherheitssysteme beschrieben.

5.3 Detaillierung vs. Relevanz[200]

5.3.1 Detaillierungsproblematik

Für die Identifikation potenziell kritischer Situationen ist eine entsprechende Detaillierung der Situationsdefinition notwendig. Beispielsweise ist bei zu erwartenden negativen Einflüssen von Witterungsbedingungen, wie z. B. Regen, dessen Stärke u. U. bestimmend. Ebenso wird für die Darstellung in Versuchen ein geeignetes Szenario benötigt, in

---

199 PREVENT (2009)

200 Kapitel basierend auf WEITZEL (2013), S. 42 ff.

dem die Situationsparameter wie bspw. Umgebungsbedingungen, Fahrbahnzustand und Fahrereinfluss festgelegt werden müssen. Da dieses prinzipbedingt nur einen bestimmten Ausschnitt aus dem Gesamtsituationskollektiv darstellt, ist die Belastbarkeit einer daraus abgeleiteten Bewertung von der Belastbarkeit der Relevanzbewertung der betrachteten Situationen abhängig.

Wird diese für die Betrachtung spezifischer Situationen notwendige Detaillierung vorgenommen, kann sie zu einer „Granularisierung“ führen und damit zu einer sehr niedrigen Expositionswahrscheinlichkeit dieser spezifischen betrachteten Situation, wodurch die Relevanz dieser (Einzel-)Testergebnisse für die Gesamtbewertung der Eigenschaft sinkt.

In extremer Ausprägung kann beispielsweise die funktionale Sicherheit eines Fahrerassistenzsystems gemäß ISO 26262 theoretisch auf hohem Niveau abgesichert werden, indem das Gesamtkollektiv der Fahrsituationen in unendlich viele Einzelereignisse zerlegt wird. Deren Expositionswahrscheinlichkeiten sind dann so gering (entsprechend Exposure-Maß E1), dass sie unabhängig von ihrer Kontrollierbarkeitsstufe (C0-C4) nur auf der niedrigsten Absicherungsstufe liegen (und dadurch keine Einstufung höher als ASIL A, vgl. Tabelle 4).

5.3.2 Ansatz zur Relevanzquantifizierung

Für die Definition von Prüffällen sind im ersten Schritt die Fahrsituation hinreichend beschreibende Parameter zu definieren. Zahlreiche Arbeiten haben sich in der Vergangenheit mit der Identifikation geeigneter Fahrsituationsparameter auseinandergesetzt.[201] Dabei wird häufig die Unterteilung in Fahrer, Fahrzeug und Umwelt vorgenommen und diese dann weitergehend detailliert. Bild 12 stellt dies schematisch mit beispielhaften Detaillierungen dar.

Diese drei Bereiche werden in der Folge als Klassen bezeichnet, Detaillierungen innerhalb dieser Klassen als Subklassen.

Bezogen auf den Untersuchungsgegenstand (bspw. die Kontrollierbarkeit im Fall von nicht situationsgerechten Auslösungen) kann eine Auswahl von dafür notwendig zu betrachtenden Klassen bzw. Subklassen vorgenommen und dadurch die Parametervielfalt beschränkt werden. Wird beispielsweise nur ein spezifisches Fahrerassistenzsystem betrachtet, kann die Subklasse Fahrerassistenzsystem gestrichen werden. Innerhalb der Subklassen wird dann die Detaillierung in Parameterkategorien und Parameter vorgenommen. Durch Detaillierung wird dabei aus einem Parameter eine Parameterkategorie, die dann wiederum die detaillierteren Parameter enthält. Bild 13 zeigt das Schema des Klassifizierungsvorgehens.

Für die Definition, Klassifizierung und Auswahl von Klassen, Subklassen, Parameterkategorien und Parametern werden die folgenden Anforderungen definiert.

- Die Parameter-Subklassen müssen unabhängig voneinander sein Die Kategorien sind dann frei miteinander kombinierbar.
- Parameter bzw. Parameterkategorien müssen einander ausschließen, dadurch ergibt sich die

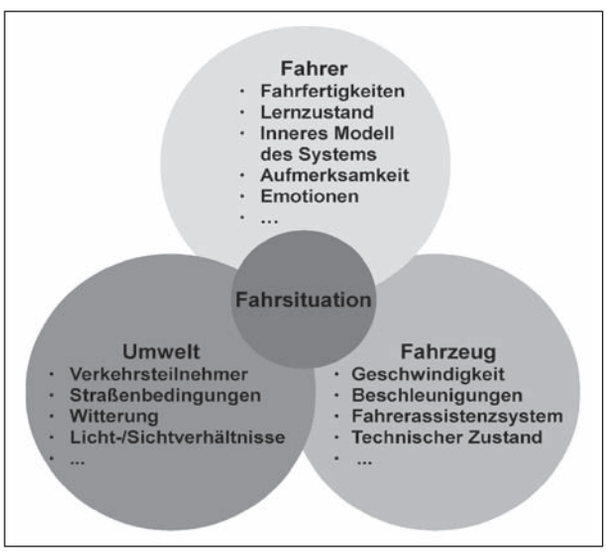

Bild 12: Beispiel für Parametereinteilung der Fahrsituation[202]

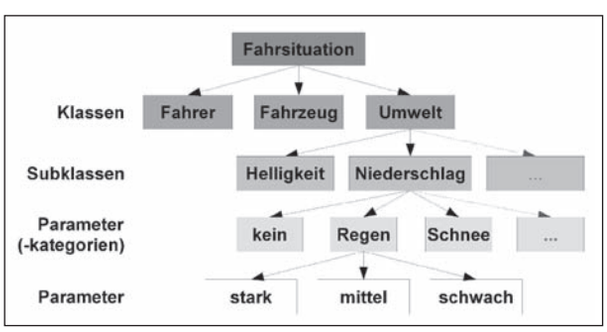

Bild 13: Schema der Aufteilung in Klassen, Subklassen und Parameter

[201] BENDA (1977), FASTENMEIER (1995), REICHART (2001), DOMSCH et al. (2008)

[202] DOMSCH et al. (2008)

Klassen	Subklassen	K	Beispiele für Einflüsse
Umwelt	Helligkeit	1	Wahrnehmungsdauer Fahrer
	Niederschlag	2	Wahrnehmungsdauer Fahrer, Reibwertmaximum
	Verkehrsdichte	3	Gefährdung, Komplexität der Verkehrssituation
	Straßenklasse	4	lateraler Ausweichraum, Sichtweite
Fahrer	Blickabwendung	5	Fahrerreaktionsverzögerungen
Fahrzeug	Längs- und Querbeschleunigung	6	verfügbares Längs- und Querkraftpotenzial

Tab. 8: Beispiel für Parameterklassen[203]

kumulierte Expositionswahrscheinlichkeit innerhalb der Kategorie zu 100 %.

Ein Beispiel für eine Parametereinteilung und daraus resultierende Einflüsse auf die Fahrsituation für die Bewertung von Kontrollierbarkeit zeigt Tabelle 8. Zur Identifikation sind die Subklassen mit der Indexvariablen K versehen.

In den Parameterkategorien ist dann der so genannte Basisanteil zu identifizieren.

Der Basisanteil ist eine Parameterausprägung, die die folgenden Anforderungen erfüllt:

- Er deckt einen hohen Expositionswahrscheinlichkeitsanteil der jeweiligen Parameterkategorie ab (möglichst den höchsten innerhalb der Kategorie),
- alle weiteren Parameteralternativen innerhalb derselben Kategorie führen zu Verschlechterungen der Situation hinsichtlich der zu messenden Eigenschaft.

Zusätzlich zum Basisanteil kann auch ein unbekannter „Rest“ innerhalb der Kategorie hinzugefügt werden. Dadurch können Unsicherheiten bezüglich der Vollständigkeit bzw. für unvorhersehbare Zustände/Ausprägungen adressiert werden.

Um die Veränderung der zu messenden Eigenschaft erfassen zu können, wird ein Bewertungsmaßstab benötigt, der als Gewichtungsfaktor dient. Der Bewertungsmaßstab muss eine relative Bewertung der jeweiligen Eigenschaft ermöglichen. Um einen wissenschaftlich belastbaren Nachweis mit vertretbarem Aufwand führen zu können, ist die Untersuchungshypothese zu dieser Eigenschaft so zu wählen, dass eine Falsifikation möglich ist und eindeutige Aussagen zulässt.[204] Entsprechend sollte in Fällen, in denen eine hohe Expositionswahrscheinlichkeit der Eigenschaft vermutet wird, die Gegenwahrscheinlichkeit herangezogen werden.

Für die Untersuchung von Kontrollierbarkeit beispielsweise wird entsprechend die Unkontrollierbarkeit als Bewertungskriterium herangezogen.[205] Dazu wird der Anteil von Fahrern ermittelt, für die die Situation unkontrollierbar ist.

Die Bewertung kann relativ zu einer Referenzgröße erfolgen. In Abhängigkeit vom Referenzniveau p_{Cx} ergibt sich mit der Bewertungsgröße p_U der Gewichtungsfaktor g dann gemäß Formel 10.

$$g = \frac{p_U}{p_{Cx}} \tag{10}$$

Dieser Gewichtungsfaktor wird dann in den Parameterausprägungen mit der Expositionswahrscheinlichkeit multipliziert. Anschließend werden diese innerhalb der (Sub-)Kategorien aufsummiert, wodurch sich der Gewichtungsfaktor auf der nächsthöheren Detaillierungsstufe ergibt. Auf der obersten Ebene errechnet sich dann aus den Expositionswahrscheinlichkeiten der Ausprägungen und den Gewichtungsfaktoren/Unkontrollierbarkeitswerten ein Anteil an Unkontrollierbarkeit in der gesamten Kategorie.

Für die mathematische Darstellung des Ansatzes wird folgende Namenskonvention eingeführt:

- Die Expositionswahrscheinlichkeit eines Parameters wird durch die Variable ρ beschrieben.
- Der Gewichtungsfaktor wird durch die Variable g beschrieben.

Die Indizes werden wie folgt zugewiesen:

- K bezeichnet die Subklasse,
- q ist der Index der ersten Parameterebene,

---

203 Vgl. FACH et al. (2010), S. 4

204 POPPER (2005), S. 14 ff.

205 Vgl. FACH et al. (2010), S. 4

- wird ein Parameter zu einer Parameterkategorie erweitert und dann weiter detailliert, wird jeweils ein Index *r, s, t, …* fortlaufend hinzugefügt.

Die Anzahl der Indizes gibt damit auch Aufschluss über die Detaillierungstiefe.

Daraus ergibt sich in der jeweiligen Parameterkategorie auf der jeweiligen Detaillierungsebene der Wahrscheinlichkeitsvektor $W_{K,q}$ (s. Formel 11).

$$\overline{W_{K,q}} = \begin{pmatrix} \rho_{K,q,1} \\ \rho_{K,q,2} \\ \rho_{K,q,3} \\ . \\ . \\ \rho_{K,q,n} \end{pmatrix} \quad (11)$$

Der entsprechende Gewichtungsfaktorvektor $\overline{G_{K,q}}$ wird analog gebildet (s. Formel 12).

$$\overline{G_{K,q}} = \begin{pmatrix} g_{K,q,1} \\ g_{K,q,2} \\ g_{K,q,3} \\ . \\ . \\ g_{K,q,n} \end{pmatrix} \quad (12)$$

Das Skalarprodukt dieses Vektors gemäß Formel 13 ergibt den Bewertungsanteil der als Gewichtungsfaktor auf der nächsthöheren Ebene verwendet wird.

$$g_{K,q} = \overline{W_{K,q}} \cdot \overline{G_{K,q}} \quad (13)$$

Auf der höchsten Ebene ist in den Vektoren $\overline{W_{K,q}}$ und $\overline{G_{K,q}}$ jeweils auch der Basisanteil enthalten.

Da sich innerhalb einer Klasse die detaillierteren Faktoren gegenseitig ausschließen, gilt innerhalb einer Parameterkategorie Formel 14.

$$\sum_{r=1}^{n} \rho_{K,q,r} = 1 \quad (14)$$

In Bild 14 ist die schematische Umsetzung des Ansatzes mit Formulierung eines „Rest-Anteils“ dargestellt.

Um den Aufwand der Detaillierung zu reduzieren, kann eine Vorauswahl von Detaillierungsfaktoren durch den Vergleich innerhalb einer Klasse auf der jeweiligen Detaillierungsebene getroffen werden. Dazu wird eine Relevanzschwelle benötigt. Dies wird hier am Beispiel der Kontrollierbarkeitsbewertung erklärt. Liegt das Produkt aus Expositionswahrscheinlichkeit und Unkontrollierbarkeitsänderung eines Parameters im Vergleich zum größten Produkt eines anderen Parameters unterhalb dieser Relevanzschwelle, so ist eine Detaillierung nicht sinnvoll, weil die Auswirkungen auf den Gewichtungsfaktor gering sind.

Diese Relevanzschwelle ist von der erwarteten Schätzungenauigkeit des Bewertungs-Gewichtungsfaktors *g* abhängig. Diese Schätzungenauigkeit ist die erwartete Abweichung zwischen dem beispielsweise für die einleitende „Hazard Classification“ geschätzten Bewertungsanteil $g_{K,q,schätz}$ gegenüber dem tatsächlichen Kontrollierbarkeitsanteil im Nutzerkollektiv $g_{K,q,schätz,real}$ (s. Formel 15).

$$s_{K,q} = \frac{g_{K,q,schätz}}{g_{K,q,schätz,real}} \quad (15)$$

Die Zusammenhänge werden an folgendem Beispiel gezeigt. Es wird eine Kontrollierbarkeitsbewertung durchgeführt, bei der eine Gesamtkontrollierbarkeit von p_K > 90 % erwartet wird. Als Gewichtungsfaktor dient der daraus resultierende maximal zulässige Unkontrollierbarkeitsanteil nach Formel 16 und 17.

$$g_{gesamt} \leq 1 - p_k \quad (16)$$

$$g_{gesamt} \leq 1\ \% \quad (17)$$

Die Subklasse setzt sich dabei aus *n* Parametern zusammen. Die Schätzungenauigkeit von $g_{K,q}$ wird nach Formel 18 mit angenommen.

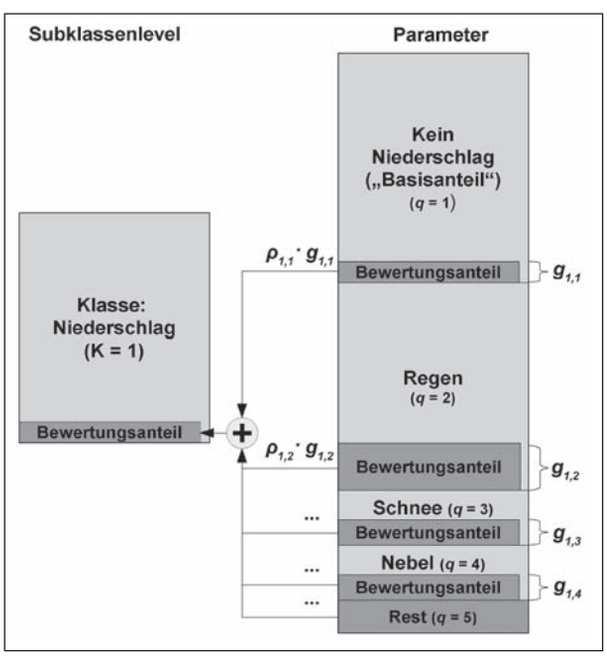

Bild 14: Schema Verrechnung Bewertungsanteile über die Detaillierungsebenen

$$s_{g,K,q} \leq 100\ \% \quad (18)$$

Die Relevanzschwelle (*RS*) legt fest, welcher Fehleranteil als tolerierbar angesehen wird. Diese wird für das folgende Beispiel auf ein Zehntel des angestrebten Unkontrollierbarkeitsanteil festgelegt:

$$RS \leq 10\ \% \quad (19)$$

Der maximal erlaubte relative Fehler ist dadurch mindestens um eine Potenz kleiner als die zu ermittelnde Größe.

$$f_{max} = RS \cdot g_{gesamt} \leq 1\ \% \quad (20)$$

Mit der Schätzungenauigkeit $u_{g,K,q}$ ergibt sich der resultierende Fehler von g_{gesamt} zu:

$$g_{gesamt} = f_{max} \cdot s_{g,K,q} \leq 1\ \% \quad (21)$$

Dabei handelt es sich um eine Betrachtung der Extremwerte. Abgesehen von der relativ hoch gewählten Schätzungenauigkeit wird in den meisten Fällen die Zahl *n* der Unterteilungen mindestens zwei oder größer sein. Ebenso ist eine gleichmäßigere Verteilung der Gewichtungsfaktoren zu erwarten.

Das abzusichernde Niveau p_K (im Beispiel p_K = 90 %) ist dabei implizit enthalten, weil es den Erwartungswert definiert und damit die zulässige Relevanzschwelle im Abstand von einer Potenz.

Gemäß den Formeln 15 bis 21 ist die Relevanzschwelle dabei direkt abhängig von der gewählten Absicherungsstufe.

Für die Priorisierung der Detaillierung der Situationsfaktoren wird dann das Abbruchkriterium für die weitere Detaillierung eines beliebigen Parameters ($q = i$) nach Formel 22 herangezogen.

$$\rho_{K,i} g_{K,i} \cdot \frac{1}{RS} < \max\left(\rho_{K,q} g_{K,q}\right) \quad (22)$$

mit

$$q = \{1, \ldots, n \mid q \neq i\}$$

Ist dieses Kriterium erfüllt, sind aus der Erhöhung des Detaillierungsgrades für diesen Faktor Änderungen für die Kontrollierbarkeit nur unterhalb der Relevanzschwelle zu erwarten. Diese Faktoren müssen dann nicht weiter detailliert werden.

5.3.3 Diskussion der Korrelationen

Bereits im Kapitel 5.3.1 wurde die Problematik der theoretisch unendlichen Abhängigkeitsbeziehungen zwischen Situationsparametern und die Auswirkungen auf die Expositionswahrscheinlichkeit und die Relevanzbewertung angesprochen.

Dem Lösungsansatz folgend sind die jeweiligen Subklassen miteinander frei kombinierbar. Daraus folgt auch, dass die Kombination von Situationen aus ungünstigen Parametern jeweils insgesamt eine geringere Expositionswahrscheinlichkeit und damit niedrigere Auswirkungen auf die Gesamtbewertung haben. Korrelieren Faktoren miteinander, ist diese Multiplikation der Einzelwahrscheinlichkeiten nicht mehr zulässig. Kritisch ist die Korrelation, wenn sie in eine Situation resultiert, die die zu bewertende Eigenschaft deutlich über- oder unterschätzt, weil die Kombination neue Effekte hervorruft. Bei der Einbeziehung aller denkbaren Situationsausprägungen sind Korrelationen nicht vermeidbar, gleichzeitig ist aber der eindeutige Nachweis aufgrund der Vielzahl potenzieller Wechselwirkungen oft kaum zu führen.

Um diese Problematik zu adressieren, muss bei vermuteter Korrelation (diese muss nicht linear sein) zwischen Situationsparametern unterschiedlicher Klassen eine gesonderte Expositionswahrscheinlichkeit der Kombination ermittelt und diese mit der kombinierten Wahrscheinlichkeit der Parameter verglichen werden.

$$r_{Abhängig} = \frac{\rho_{K1,q,r,\ldots\ K2,q,r,\ldots}}{\rho_{K1} \cdot \rho_{K2}} \quad (23)$$

Ist $r_{Abhängig} > 1$, dann besteht eine erhöhte Expositionswahrscheinlichkeit der Kombination. Die Korrelationssituation muss dann gesondert betrachtet werden. Da diese dann eine eigenständige Situation darstellt, muss sie auch dem Gesamtsituationskollektiv zugerechnet werden und damit auf höchster Detaillierungsebene, den Subklassen gleichgestellt, berücksichtigt werden.

Dadurch ergibt sich auf dieser Ebene die Notwendigkeit für die Einführung einer Subklasse „Sondersituationen“. Dort werden aus Korrelationen resultierende ungünstige Situationskonstellationen zusammengefasst, dort können auch die in Kapitel 5.1.2 diskutierten „pathologischen Situationen“ eingebracht werden.

Da für diese Klasse kein Basisanteil gebildet werden kann, werden diese in der Summation als fester Anteil betrachtet. Damit können sie Teil eines allgemeinen „Restes“ der Situationen sein, die die Bewertung im Allgemeinen beeinflussen, weil sie ein fester Anteil am Absicherungsniveau sind.

Die Menge nachweisbarer Korrelationen hat dadurch große Auswirkungen auf den Nutzen des hier beschriebenen Ansatzes zur Identifikation von Testsituationen. Sind davon sehr viele identifizierbar oder notwendig, ist ein großer Anteil der Situationen fest definiert und der Nutzen der Aufteilung in Klassen wird geringer.

Ausgehend von der Annahme, dass die Faktoren rückwirkungsfrei sind und Korrelationen daher Sonderfälle darstellen sollten, wird diese Vorgehensweise als effizient angesehen. Legt man jedoch die umgekehrte Annahme zugrunde, dass alle Faktoren stets miteinander korrelieren und eine Unabhängigkeit nicht nachzuweisen ist, so ergibt sich eine Vielzahl notwendiger Testsituationen, zu denen jeweils einzeln Expositionswahrscheinlichkeit und Bewertungsanteil zu ermitteln sind. Dies führt zurück zur Ausgangslage, die zur Entwicklung des beschriebenen Ansatzes geführt hat.

Allerdings ist dies kein Widerspruch, sondern eine logische Konsequenz des Ansatzes. Wird die Betrachtung der beliebigen Kombination von Einzelfaktoren und deren Expositionswahrscheinlichkeit als nicht praktikabel bewertet, da der Aufwand hierfür als sehr/zu hoch eingeschätzt wird, müssen Vereinfachungen getroffen werden. Durch diese Vereinfachungen kann keine absolute Vollständigkeit mehr erreicht werden, weil die unzähligen theoretisch möglichen Wechselwirkungen und Detailausprägungen der Einzelparameter nicht betrachtet werden. Dabei wird über Strukturierung und anhand von Vorwissen über das Gesamtsystem (Fahrer-Fahrzeug-Umwelt) angestrebt, eine hohe Abdeckung des im realen Betrieb zu erwartenden Gesamtsituationskollektivs hinsichtlich einer bestimmten Systemeigenschaft zu erhalten. Kritisch kann dies hinsichtlich der absoluten Quantifizierung sein, da systembedingt die jeweiligen Anteile über- bzw. unterschätzt werden können.

5.3.4 Einfluss der Wahl des Situationskollektivs

Das gewählte Situationskollektiv beeinflusst maßgeblich die Expositionswahrscheinlichkeiten und damit die Kontrollierbarkeitsbewertung. Für eine belastbare Bewertung ist daher auch die systematische objektive Bestimmung geeigneter Kollektive notwendig. Dieses muss dabei das Nutzungsprofil des Fahrzeugs hinreichend abbilden. Damit muss analysiert und bewertet werden, was als hinreichend gelten kann. Sollen Umgebungsbedingungen abgebildet werden, kommt zudem der regionale bzw. nationale Einfluss hinzu. Ein Situationskollektiv müsste entsprechend alle europäischen Einsatzgebiete potenziell abdecken, dabei aber hinsichtlich der Expositionswahrscheinlichkeiten einen Schwerpunkt auf dem Zielland haben. Extreme Situationen, beispielsweise mit starkem und häufigem Schneefall oder bei großer Hitze, treten aber ziellandspezifisch auf. Ein für Europa gültiges Kollektiv müsste dies abbilden, ohne bestimmte Bedingungen zu übervorteilen und damit potenziell negative Konsequenzen auf Länder mit spezifischen klimatischen Bedingungen zu konzentrieren. Ein solcher Ansatz wird sicherlich keine gesellschaftliche Akzeptanz finden. Allerdings ergibt sich daraus ein Zielkonflikt bei der Generierung von relevanten Situationskollektiven.

5.3.5 Erkenntnisse zu Detaillierung und Relevanzbetrachtungen

Die allgemeine Ermittlung des notwendigen Testaufwands für die Absicherung von umfelderfassenden Systemen mit konventionellen Methoden zeigt, dass der hierfür notwendige Aufwand sehr hoch ist. Anwendbare Beschleunigungsmechanismen, die den Umfang der Testkilometer reduzieren können, sind aktuell nicht bekannt. Zusätzlich zu dieser Situationsfülle muss bei der Darstellung in Testsituationen der Argumentation der ISO 26262 folgend unter Umständen eine große Anzahl von Tests absolviert werden, um belastbare Erkenntnisse ableiten zu können.

Die Betrachtung der möglichen Detaillierung von beeinflussenden Faktoren einer Fahrsituation zeigt, dass diese theoretisch beliebig detaillierbar sind und zudem auch hinsichtlich ihrer Expositionswahrscheinlichkeiten untereinander in beliebiger Wechselwirkung stehen können.

Um diesen Problematiken zu begegnen, wurde ein Ansatz entwickelt, der die Umweltbedingungen, die in der Fahrsituation auftreten können, in Klassen strukturiert und dann darin in voneinander unabhängige Subklassen unterteilt. In den Subklassen können beliebige Detaillierungen vorgenommen werden. Anhand eines Gewichtungsfaktors, der sich am zu untersuchenden Merkmal des Systems orientiert, wird jeder Faktor quantifiziert. Das Vorgehen erlaubt eine Betrachtung verschiedenster Situationsfaktoren auf unterschiedlichen Detaillierungsebenen und deren vergleichende Relevanzbewertung. Ebenso sind Unsicherheiten in der

Abbildung aller Parameter einer Subklasse durch einen „Restanteil“ darstellbar.

Damit wurde ein vereinfachender Ansatz geschaffen, der eine gezielte Identifikation relevanter Situationen ermöglicht. Dieser kann schrittweise entwickelt und weiter detailliert werden. Eine beispielhafte Anwendung findet sich in WEITZEL et al. (2013). Voraussetzung für eine belastbare Betrachtung ist, dass ein repräsentatives Situationskollektiv zugrunde gelegt werden kann, welches das Nutzungs- und Nutzerprofil hinreichend abbildet. Dabei ist der Ansatz auf eine einheitliche Auswahl von Situationsparametern angewiesen, um übertragbare Ergebnisse liefern zu können. Basierend darauf kann dann eine Prüfung auf Anwendbarkeit auf weitere Fahrerassistenzsysteme durchgeführt werden, um die Übertragbarkeit zu untersuchen. Im Gegensatz zu statistisch getriebenen Methoden ergibt sich die Möglichkeit, die Datenlage schrittweise und bedarfsgerecht zu verbessern.

Noch nicht abschließend geklärt werden konnte, inwiefern die getroffenen Annahmen und Überlegungen zu Wechselwirkungen von Situationsfaktoren bei der Anwendung des Ansatzes tatsächlich nur geringe Fehler bei der Relevanzbewertung erzeugen. Ergänzend können hierzu Situationslisten verwendet werden, in denen besonders kritische Situationen gesammelt werden können. Die vollständige Abbildung aller denkbaren Wechselwirkungen ist aber aufgrund des hohen resultierenden notwendigen Spezifizierungsgrades der Einzelsituationen und der damit verbundenen Relevanzreduktion aus Sicht der Autoren wenig zielführend.

6 Zusammenfassung und Identifikation des Forschungsbedarfs

Die Analyse bestehender Absicherungsansätze auch im Vergleich zu anderen Verkehrsträgern zeigt, dass Konzepte und Methoden der funktionalen Sicherheit auch in anderen Zusammenhängen umgesetzt worden sind. Der öffentliche Straßenverkehr weist dabei gegenüber größtenteils „professionell“ betriebenen Verkehrssystemen Besonderheiten auf. Dadurch sind nicht alle Kontrollmethoden übertragbar. Allerdings ergeben sich aus den Besonderheiten andere Kontrollmechanismen der funktionalen Sicherheit von Fahrerassistenzsystemen mit Umfeldwahrnehmung. Es konnten keine Indizien gefunden werden, dass diese nicht ausreichend sind bzw. diese nicht funktionieren. Eine Ergänzung der Erfassung von Unfällen, die während des Einsatzes von FAS auftreten, wurde als Erweiterungsmöglichkeit der bestehenden Methoden diskutiert. Inwiefern jedoch der zu erwartende Mehrnutzen angesichts vermutlich niedriger Fallzahlen gerechtfertigt ist, kann nicht abschließend geklärt werden. Hierfür ist eine detaillierte Betrachtung von Nutzenkonzepten und Aufwand notwendig.

Die für die Absicherung von Fahrerassistenzsystemen notwendigen Schritte zur Identifikation von Prüfsituationen wurden dargelegt und der mit konventionellen Methoden resultierende Aufwand ermittelt. Werden die Systeme auf immer größere Einsatzbereiche erweitert, stoßen bestehende Verfahren nach Ansicht der Autoren an ihre Grenzen. Insbesondere die belastbare Auswahl der für die Absicherung als hinreichend zu betrachtenden Test-Fälle stellt hier hohe Anforderungen.

Basierend auf diesen Erkenntnissen wurde ein Ansatz zur Relevanzquantifizierung entwickelt, der diese Problemstellungen adressiert. Damit ist eine schrittweise Verbesserung der statistischen Datenlage und der darin erfolgten Bewertungen von Systemeigenschaften, hier wurde als Beispiel die Kontrollierbarkeit herangezogen, möglich. Der Ansatz ermöglicht, bereits vorher abzuschätzen, in welchen Bereichen eine weitere Detaillierung der Situationsfaktoren oder der Probanden- bzw. Feldtests sinnvoll und lohnenswert sein kann.

Für die Umsetzung in die Praxis sind dabei verschiedene Herausforderungen zu bewältigen. Einerseits wird ein Fahrstreckenkollektiv benötigt, das repräsentativ für den jeweiligen späteren Einsatzzweck des Systems/Fahrzeugs ist. Mit der schnellen Entwicklung von Fahrerassistenzsystemen ist auch eine stetig wachsende Vernetzung zu erwarten. Ebenso werden sicherlich immer mehr Fahrsituationen durch die Systeme abgedeckt, unterstützt oder teilweise ausgeführt werden. Das notwendige Fahrstreckenkollektiv, das zur Bewertung herangezogen wird, und der darin abgebildete Detaillierungsgrad müssten daher beständig zunehmen, bis diese letztendlich für die Stufe von vollautomatisierten Systemen geeignet sind. Da dabei immer mehr Einzelparameter berücksichtigt werden müssen, ist der entstehende Aufwand für die Ermittlung repräsentativer Fahrsituationskollektive aus Realfahrstrecken vermutlich progressiv

steigend. Mit der aktuell gängigen Praxis, dass einzelne Anbieter von Systemen, Fahrzeughersteller wie Systemzulieferer, entsprechende Situationskollektive für ihre Produkte gestalten, ist diese Aufgabe in der Zukunft vermutlich kaum noch zu bewältigen. Zudem ist die Zusammensetzung dieser Kollektive von den Fragen abhängig, was die Systeme mindestens leisten und in welchen Situationen sie sich mindestens „bewähren“ müssen, um für den Straßenverkehr als geeignet zu gelten.[206]

Darin unterscheiden sich die Anforderungen an die Systeme und den Fahrer nicht. Auch bei den Fahrern wird die Erfüllung bestimmter Mindestanforderungen im Rahmen der Fahrausbildung mit abschließender Prüfung gefordert und überprüft.[207, 208] Dadurch wird implizit das gesellschaftlich akzeptierte Grenzrisiko abgebildet. Die darin enthaltene Risikotoleranz und daraus resultierende Anforderungen bei automatisierten Fahrzeugen müssten daher auch öffentlich diskutiert werden.

Ähnliche Ansätze müssten in der Vergangenheit bereits für Anforderungsdefinition an die passive Sicherheit von Fahrzeugen (bspw. NCAP[209]) oder dem Verbrauchszyklus (NEFZ und andere[210]) verwendet worden sein. Auch hier wurden Vereinfachungen vorgenommen, die zwar hinsichtlich der getroffenen Annahmen diskutiert werden können, die aber zumindest allgemein zugänglich sind, sodass die öffentliche Diskussion möglich ist. Für Fahrerassistenzsysteme mit Umfeldwahrnehmung steht dieser Prozess noch am Anfang. Aus Sicht der Autoren ist es aber gerade hier unbedingt notwendig, diese Diskussion baldmöglich anzustoßen, um nicht unfallvermeidende Systeme aufgrund von rechtlichen und gesellschaftlichen Unklarheiten in ihrer Funktion beschränken zu müssen und dadurch nicht das volle Unfallvermeidungspotenzial zu nutzen.

Dafür ist eine Methodik zur belastbaren objektiven Identifikation und Definition relevanter Absicherungsfälle notwendig. Um dabei hohe Übertragbarkeit zu erreichen, sind für ein breites Feld von Fahrerassistenzfunktionen Fahrsituationsparameter festzulegen, die Fahrsituationen ausreichend beschreiben und für eine generische Situationsdefinition geeignet sind. Diese müssen eine Verknüpfung mit statistischen Daten ermöglichen, sodass eine Relevanzbewertung erfolgen kann. Wie in Kapitel 5.3 gezeigt, existieren bereits zahlreiche Ansätze, die auf die Anwendbarkeit für die Testfall-Problematik zu prüfen sind. Inwiefern diese für die Beschreibung von Fahrsituationskollektiven zur Prüffallgenerierung geeignet sind, ist zu untersuchen.

Im nächsten Schritt können statistische Daten erhoben werden, die die Expositionswahrscheinlichkeiten definieren. Diese können bei Bedarf schrittweise weiter detailliert werden.

Parallel dazu sind Beschleunigungsmechanismen auf die Übertragbarkeit für die identifizierte Problemstellung zu prüfen. In Kapitel 5.1.3 wurden bereits Beispiele genannt, diese stellen jedoch nur einen Ausschnitt des Standes der Technik dar.

Basierend auf diesen Erkenntnissen kann die Entwicklung von relevanten Expositions-Lastkollektiven vorangetrieben werden.

Die für die Untersuchung von Systemeigenschaften für diese Expositionskollektive durchgeführten Versuche, beispielsweise in Form von Probandenversuchen, können dann entsprechend hinsichtlich ihrer Relevanz eingeordnet werden. Zudem ist ein Vergleich von Ergebnissen möglich, wenn die Situationsparameter einheitlich dokumentiert und quantifiziert sind.

In enger Verknüpfung zu dieser Verbreiterung und Vertiefung der statistischen Datenlage zu Fahrsituationen sind auch die Bedingungen für die Intensivierung von modellbasierten Testmethoden zu identifizieren. Dazu sind bezüglich der Sensoren Ansätze zur Diskretisierung von Umfeldkenngrößen zu klären, die danach durch Sensormodelle in Messgrößen transferiert werden können. Wie im Kapitel 4.4.6 dargestellt, lassen sich dabei auch Unsicherheiten der Sensoren im Wahrnehmungsprozess abbilden.

Ebenso sind Methoden zur Modellierung von Unsicherheiten in der Entwicklungsprozesskette notwendig. Dabei handelt es sich einerseits um die situativen Unsicherheiten, nicht nur hinsichtlich der statischen Gegebenheiten, also wo sich Objekte befinden, sondern auch der dynamischen Unsicherheiten, wie sich diese Objekte in näherer Zu-

---

206 Vgl. hierzu auch WINNER et al. (2012)

207 Vgl. hierzu BAHR et al. (2013)

208 Wobei eine starke „Lernfähigkeit“ des Fahrers auch nach der Führerscheinprüfung vorausgesetzt wird, die seine Fähigkeiten weiter verbessert.

209 HOBBS et al. (1998)

210 SIMANAITIS (1977)

kunft verhalten werden. Diese Fragestellungen führen vermutlich zu der Frage, welche Anforderungen eine Simulationsumgebung erfüllen muss, die für eine Vielzahl von Beteiligten nutzbar ist und X-in-the-Loop-Ansätze zulässt.

Anhand einer Simulationsumgebung lassen sich dann verschiedene Module situations- oder funktionsspezifisch schrittweise detaillieren und validieren und dadurch die modellgestützte Absicherung von Fahrerassistenzsystemen mit Umfeldwahrnehmung erweitern. Beispielsweise können auf dieser Basis Fahrermodelle entwickelt, geprüft und validiert werden, die den Testaufwand reduzieren können. Um Akzeptanz und Relevanz auch für die Produkthaftung zu erlangen, muss diese Vorgehensweise jedoch von möglichst vielen Beteiligten unterschiedlicher Interessen unterstützt werden. Solange die allgemeinen Eingangs- sowie die zu verwendenden Situationsparameter stark abhängig vom jeweiligen Anwendungszweck sind und zudem die möglichen Einflussparameter als unzählig gelten, kann keine Übersicht geschaffen werden, die jedoch für eine Übertragbarkeit und Einordnung von Erkenntnissen notwendig ist.

7 Literatur

BÄKER, B.: 25 Jahre Elektronik-Systeme im Kraftfahrzeug, Expert Verlag, Renningen, 2005

BAHR, M., STURZBECHER, D.: Bewertungsgrundlagen zur Beurteilung der Fahrbefähigung bei der praktischen Fahrerlaubnisprüfung, 6. Darmstädter Kolloquium Mensch + Fahrzeug, 06.-07.03.2013, Darmstadt, 2013

BENDA, H. v.: Die Häufigkeit von Verkehrssituationen; FP 7320 im Auftrag der Bundesanstalt für Straßenwesen, Technische Universität München, Lehrstuhl für Psychologie, 1977

BENZ, S.: Eine Entwicklungsmethodik für sicherheitsrelevante Elektroniksysteme im Automobil; Universität Karlsruhe, 2004

Bertrandt Ingenieurbüro GmbH: b.rabbit – Das Bertrandt Targetsystem, verfügbar unter: http://www.bertrandt.de/Sicherheit.html, Abruf am 12.12.2008

BGH VI ZR 107/08; Urteil vom 16.06.2009 – VI ZR 107/08; OLG Jena, Verfügbar unter: lexetius.com/2009,1744, Abruf am 05.12.2012

BÖRCSÖK, J.: Funktionale Sicherheit, 3. Auflage, VDE-Verlag, Berlin, Offenbach, 2011

BORGEEST, K.: Elektronik in der Fahrzeugtechnik, 2. Auflage, Vieweg+Teubner, Wiesbaden, 2010

BORTZ, J.: Statistik für Human- und Sozialwissenschaftler, 6. Auflage, Springer Medizin Verlag, Heidelberg, 2005

BRABAND, J.: Funktionale Sicherheit. In: FENDRICH, L.: Handbuch Eisenbahninfrastruktur, Springer, Berlin, 2007, S. 649-699

BREUER, B., SEIBERT, W., ENGEL, H. G.: Der Tankzugunfall Herborn, VDI-Fortschritt-Berichte Reihe 12, Nr. 152, Düsseldorf, 1991

BREUER, J.: Bewertungsverfahren von Fahrerassistenzsystemen. In: WINNER, H., HAKULI, S., WOLF, G.: Handbuch Fahrerassistenzsysteme, 2. Auflage. Vieweg+Teubner Verlag, Wiesbaden, 2012, S. 55-68

Bundesministerium für Verkehr: Bekanntmachung der Bestimmungen über die Lizenzierung von Piloten (Flugzeug) (JAR-FCL 1 deutsch), 2009

DARMS, M.: Eine Basis-Systemarchitektur zur Sensordatenfusion von Umfeldsensoren für Fahrerassistenzsysteme, Dissertation, TU Darmstadt, 2007

Deutsche Bahn: verfügbar unter: http://www.deutschebahn.com/site/dbtraining/de/seminarfinder/fahrzeugfuehrer/Tf3022.html?p=3, Abruf 28.11.2012

DFS: verfügbar unter: http://www.dfs.de/dfs/internet_2008/module/grundkurs_flugsicherung/deutsch/grundkurs_flugsicherung/system_flugsicherung/luftrauminfo_struktur/index.html, Abruf am 26.11.12

DIEBOLD, J.: Das APIA-Projekt – Der Weg zum unfall- und verletzungsvermeidenden Fahrzeug. In: System Partners 2003. Innovationen der Zulieferindustrie. Sonderausgabe der ATZ und MTZ, Nr. 105 (Sonderheft), 2003, S. 28-32

DIN EN 50126: Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS), 1999

DIN EN 50128: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverar-

beitungssysteme – Software für Eisenbahnsteuerungs- und Überwachungssysteme, 2011

DIN EN 50129: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik, 2003

DIN EN 50159: Bahnanwendungen – Sicherheitsrelevante Kommunikation in geschlossenen/offenen Übertragungssystemen, 2003

DOMSCH, C., NEGELE, H.: Einsatz von Referenzfahrsituationen bei der Entwicklung von Fahrerassistenzsystemen. In: 3. Tagung Aktive Sicherheit durch Fahrerassistenz, 07.-08.04.2008, Garching bei München, 2008

EASA: 2012 AMC and GM to Part 21 Issue 2, verfügbar unter: http://www.easa.europa.eu/rulemak-ing/faq/acceptable-means-of-compliance AMC.php, Abruf am 28.11.2012

EC 347/2012: EC 347/2012 Annex II und III, verfügbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32012R0347:EN:NOT, Abruf am 06.12.12

EBEL, S., WILHELM, U., GRIMM, A., SAILER, U.: Ganzheitliche Absicherung von Fahrerassistenzsystemen in Anlehnung an ISO 26262. In: Integrierte Sicherheit und Fahrerassistenzsysteme 26. VDI/VW-Gemeinschaftstagung, 06.-07.10.2010, Wolfsburg, 2010, S. 393-405

EG 611/2009: Verordnung (EG) Nr. 661/2009 des Europäischen Parlaments und des Rates vom 13. Juli 2009 über die Typgenehmigung von Kraftfahrzeugen, Kraftfahrzeuganhängern und von Systemen, Bauteilen und selbstständigen technischen Einheiten für diese Fahrzeuge hinsichtlich ihrer allgemeinen Sicherheit, verfügbar unter: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:200:0001:0024:DE:PDF, Abruf am 03.05.2011

Eisenbahn-Bundesamt: Allgemeinverfügung über das Melden gefährlicher Ereignisse im Eisenbahnbetrieb, Verfügbar unter: http://www.eisenbahn-unfallunterschung.de/cln_031/nn_317006/SharedDocs/Publikationen/EUB/DE/sonstige__Downloads/60__allgvfg__Unfallmeldung,templateId=raw,property=publicationFile.pdf/60_allgvfg_Unfallmeldung.pdf, 2009, Abruf am 07.02.2013

Eisenbahn-Bundesamt: Sicherheitsrichtlinie Fahrzeug (SIRF) 100, Allgemeiner Teil, 2012

Eisenbahn-Bundesamt: Sicherheitsrichtlinie Fahrzeug (SIRF) 400, Ausführungsbestimmungen, 2012

Eisenbahn-Bau- und Betriebsordnung (EBO) vom, 25. Juli 2012 (BGBl. I S. 1703), verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/ebo/gesamt.pdf, Abruf am 10.04.2013

European Aviation Safety Agency (EASA): Certification Specifications for Large Aeroplanes C-25; 2007

Euro NCAP: Die Bewertungen, verfügbar unter: http://de.euroncap.com/Content-Web-Page/b8102c33-2d19-4b1d-93a9-285f109b703c/die-bewertungen.aspx, Abruf am 10.07.2013

EUV: Eisenbahn-Unfalluntersuchungsverordnung vom 5. Juli 2007 (BGBl. I S. 1305, 1319), verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/euv/gesamt.pdf, Abruf am 10.04.2013

FAA: AC 25-1309-1A, verfügbar unter: http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2025.1309-1A.pdf, Ausgabe 1988, Abruf am 12.06.2012

FACH, M., BAUMANN, F., BREUER, J., MAY, A.: Bewertung der Beherrschbarkeit von Aktiven Sicherheits- und Fahrerassistenzsystemen an den Funktionsgrenzen. In: Integrierte Sicherheit und Fahrerassistenzsysteme 26. VDI/VW-Gemeinschaftstagung, 06.-07.10.2010, Wolfsburg, 2010, S. 425-435

FASTENMEIER, W.: Die Verkehrssituation als Analyseeinheit im Verkehrssystem. In: FASTENMEIER, W.: Autofahrer und Verkehrssituation – Neue Wege zur Bewertung von Sicherheit und Zuverlässigkeit moderner Straßenverkehrssysteme, Verlag TÜV Rheinland, Köln, Deutscher Psychologen Verlag, Bonn, 1995, S. 27-78

FORKENBROCK, G.: A Test Track Protocol for Assessing Forward Collision Warning Driver-Vehicle Interface Effectiveness, NHTSA Report DOT HS 811 501, 2011

FZV: Fahrzeug-Zulassungsverordnung, vom 25. Juni 2013 (BGBl. I S. 1849), verfügbar unter:

http://www.gesetze-im-internet.de/bundesrecht/fzv_2011/gesamt.pdf, Abruf am 18.07.2013

GASSER, T. M., ARZT, C., AYOUBI, M., BARTELS, A., BÜRKLE, L., EIER, J., FLEMISCH, F., HÄCKER, D., HESSE, T., HUBER, W., LOTZ, S., MAURER, M., RUTH-SCHUMACHER, S., SCHWARZ, J., VOGT, W.: Rechtsfolgen zunehmender Fahrzeugautomatisierung, Forschungsbericht Nr. F83 der Bundesanstalt für Straßenwesen, Bereich Fahrzeugtechnik, Köln, 2012

GEORGI, A., BRUNNER, H., SCHEUNERT, D.: GIDAS – German In-Depth Accident Study. In: FISITA 2004 World Automotive Congress, 23.-27.05.2006, Barcelona, Spanien, 2006

GEYER, S., BALTZER, M., FRANZ, B., HAKULI, S., KAUER, M., KIENLE, M., MEIER, S., WEIßGERBER, T., BENGLER, K., BRUDER, R., FLEMISCH, F. O., WINNER, H.: Concept and Development of a Unified Ontology for Generating Test and Use Case Catalogues for Assisted and Automated Vehicle Guidance. In: IET Intelligent Transport Systems, zur Veröffentlichung angenommen, 2013

GIDAS: Verfügbar unter: http://www.gidas.org/de/home; Abruf am 10.04.2013

GRIEBEL, S.: Sicherheitsnormen im Umbruch – Revision der EN 5012X-Suite. In: 5. Workshop zu Fragen von Risiko und Sicherheit im Verkehr SiT-Safety in Transportation, 13.-14.11.2012, Braunschweig, 2012

HABENICHT, S.: Entwicklung und Evaluation eines manöverbasierten Fahrstreifenwechselassistenten, Dissertation, TU Darmstadt, 2012

Hella: 2003 Technische Information, Elektronik – Kontaktlose Sensoren für X-By-Wire-Systeme, verfügbar unter: http://www.hella.com/produktion/HellaAT/WebSite/MiscContent/Download/AutoIndustrie/Elektronik/ELO_X_By_Wire.pdf, Abruf am: 06.10.2012

HOBBS, C. A., McDONOUGH, P. J.: Development of the European New Car Assessment Programme (Euro NCAP), Transport Research Laboratory 1998

HOFFMANN, D.: Software-Qualität, 2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York, 2013

HOFFMANN, J.: Das Darmstädter Verfahren (EVITA) zum Testen und Bewerten von Frontalkollisionsgegenmaßnahmen, Dissertation, TU Darmstadt, 2008

HOHM, A.: Umfeldklassifikation und Identifikation von Überholzielen für ein Überholassistenzsystem, Dissertation, TU Darmstadt, 2010

HOLZMANN, H.: Anwendungsorientierte Übersicht kommerzieller Fahrzeug-Simulations-Systeme, Fahrdynamik-Regelung – Modellbildung, Fahrerassistenzsysteme, Mechatronik, 1. Auflage, Friedrich Vieweg und Sohn Verlag, Wiesbaden, 2006

HOMANN, K.: Wirtschaft und gesellschaftliche Akzeptanz: Fahrerassistenzsysteme auf dem Prüfstand. In: STILLER, C., MAURER, M.: Fahrerassistenzsysteme mit maschineller Wahrnehmung, Springer-Verlag, Berlin, Heidelberg, New York, 2005, S. 239-244

HUMMEL, T., KÜHN, M., BENDE, J. et al.: Advanced Driver Assistance Systems, An investigation of their potential safety benefits based on an analysis of insurance claims in Germany, Unfallforschung der Versicherer (UdV), Research Report FS 03, 2011

IEC DIN EN 61508 – Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, 2010

IEEE-SA Standards Board: 829-2008 – IEEE Standard for Software and System Test Documentation. The Institute of Electrical and Electronic Engineers Inc., 1998

ISERMANN, R.: Fault-Diagnosis Systems, Springer-Verlag, Berlin, Heidelberg, New York, 2006

ISERMANN, R.: Mechatronische Systeme, 2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York, 2008

ISO 26262-1: Road vehicles – Functional safety – Part 1: Vocabulary, 2009a

ISO 26262-3: Road vehicles – Functional safety – Part 3: Concept Phase, 2009b

KBA: Kodex zur Ausführung des Produktsicherheitsgesetzes (ProdSG) bei Straßenfahrzeugen, verfügbar unter: http://www.kba.de/cln_030/nn_

125104/DE/Fahrzeugtechnik/Produktsicherheit__Rueckrufe/Kodex/kodex__pdf,templateId=raw,property=publicationFile.pdf/kodex_pdf.pdf, Abruf am 26.02.2013

KEMMANN, S., TRAPP, M.: SAHARA – A Systematic Approach for Hazard Analysis and Risk Assessment. In: SAE 2011 World Congress & Exhibition, 12.-14.04.2011, Detroit, USA, 2011

KIRCHHOFF, S., PETERMAN, D.: Unintended Acceleration in Passenger Vehicles, Congressional Research Service, 2010

KLUßMANN, N., MALIK, A.: Lexikon der Luftfahrt, Springer-Verlag, Berlin, Heidelberg, New York, 2004

KOBIELA, F.: Fahrerintentionserkennung für autonome Notbremssysteme, 1. Auflage, VS-Verlag für Sozialwissenschaften, Wiesbaden, 2011

KÜHN, M., HUMMEL, T., BENDE, J.: Benefit Estimation Of Advanced Driver Assistance Systems For Cars Derived From Real-Life Accidents. In: 21st International Technical Conference on the Enhanced Safety of Vehicles, 15.-18. Juni, Stuttgart, 2009

KUNERT, U., RADKE, S.: Personenverkehr in Deutschland – mobil bei hohen Kosten, DIW-Wochenbericht, Band 79, Ausgabe 24, 2012, S. 3-12

LUDLOFF, A.: Praxiswissen Radar und Radarsignalverarbeitung, 3. Auflage, Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig, Wiesbaden, 2002

LuftBO: Betriebsordnung für Luftfahrtgerät vom 4. März 1970 (BGBl. I S. 262), 15. Februar 2013 (BGBl. I S. 293), verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/luftbo/gesamt.pdf, Abruf am 03.04.2013

LuftVG: Luftverkehrsgesetz vom 1. August 1922 (RGBl. 1922 I S. 681), 6. Juni 2013 (BGBl. I S. 1809)verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/luftvg/gesamt.pdf, Abruf am 03.04.2013

LOSANO, M.: Turbulenzen im Rechtssystem der modernen Gesellschaft: Pyramide, Stufenbau und Netzwerkcharakter der Rechtsordnung als ordnungsstiftende Modelle. In: Rechtstheorie, Band 38, Ausgabe 1, 2007, S. 9-32

”Manufacturing the Audi Scare“, http://www.manhattan-institute.org/html/cjm_18.htm und http://www.thetruthaboutcars.com/2010/03/the-best-of-ttac-the-audi-5000-intended-unintended-acceleration-debacle/, Abruf am 13.01.2013

MARX, B: Bewertungsverfahren für Radareigenschaften von Personenkraftwagenkarosserien, Dissertation, Technische Universität Darmstadt, 2013

MAURER, M.: Entwurf und Test von Fahrerassistenzsystemen. In: WINNER, H., HAKULI, S., WOLF, G.: Handbuch Fahrerassistenzsysteme, 2. Auflage, 2012, S. 43-54

MEYNA, A., PAULI, B.: Taschenbuch der Zuverlässigkeits- und Sicherheitstechnik, 1. Auflage, Carl Hanser Fachbuchverlag, 2003

Motor Industry Software Reliability Association: Development Guidelines for Vehicle Based Software, 2. Auflage, RS Print Ltd, Leicester, United Kingdom, 1995

MUTTART, J. W.: Factors that Influence Driver´s Response Choice Decisions in Video Recorded Crashes. In: 2005 SAE World Congress & Exhibition, 11.-14.04.2005, Warrendale, USA, 2005

NHTSA: U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety, NHTSA 46-10, Friday December 7, 2012, verfügbar unter: http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety, Abruf am 03.04.2013

NITZ, G.: Entwicklung eines Systems zur aktiven Bremsung eines Fahrzeugs in Gefahrensituationen, Shaker-Verlag, Aachen, 2010

OMASREITER, H., METZKER, E.: A Context-Driven Use Case Creation Process for Specifying Automotive Driver Assistance Systems. In: 12th IEEE International Requirements Engineering Conference, 06.-10.09.2004, Kyoto, Japan 2004

PACHL, J.: Systemtechnik des Schienenverkehrs, 6. Auflage, Vieweg+Teubner Verlag, Wiesbaden, 2011

POPPER, K. R.: Logik der Forschung, Mohr Siebeck Verlag, Tübingen, 2005

PREVENT: Code of Practice for the Design and Evaluation of ADAS, 13.08.2009, 2009

ProdHaftG: Gesetz über die Haftung für fehlerhafte Produkte, Ausfertigungsdatum: 15.12.1989, zuletzt geändert 19.07.2002, verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/prodhaftg/gesamt.pdf, Abruf am 03.01.2013

Radio Technical Commission for Aeronautics (RTCA): DO-178B: Software Considerations in Airborne Systems and Equipment Certification, 1992

REICHART, G.: Sichere Elektronik im Kraftfahrzeug. In: Automatisierungstechnik, Band 46, Nummer. 2, 1998, S. 78-83

REICHART, G.: Menschliche Zuverlässigkeit beim Führen von Kraftfahrzeugen, VDI-Verlag, Düsseldorf, 2001

REICHART, G., BIELEFELD, J.: Einflüsse von Fahrerassistenzsystemen auf die Systemarchitektur im Kraftfahrzeug. In: WINNER, H., HAKULI, S., WOLF, G.: Handbuch Fahrerassistenzsysteme, 2. Auflage. Vieweg+Teubner Verlag, Wiesbaden, 2012, S. 84-92

REIF, K., NOREIKAT, K. E., BORGEEST, K.: Kraftfahrzeug-Hybridantriebe, Springer-Verlag, Wiesbaden, 2012

ROEHDER, M., HUMPHREY, S., GIESLER, B., BERNS, K.: Improving Pedestrian Safety in Urban Scenarios Through Autonomous Collision Avoidance. In: Advanced Microsystems for Automotive Applications 2010 – Smart Systems for Green Cars and Safe Mobility, Springer-Verlag Berlin, Heidelberg, New York, 2010

SAUST, F.: Entwicklungsbegleitendes Simulations- und Testkonzept für autonome Fahrzeuge in städtischen Umgebungen. In: AAET 2009, 11.-2.02.2009, Braunschweig, 2009

SCHÄUFFELE, J., ZURAWKA, T.: Automotive Software Engineering, Springer Fachmedien, Wiesbaden, 2010

SCHAFFNER, J.: Gefahrenanalyse und Sicherheitskonzept nach ISO 26262 für Fahrerassistenzsysteme. In: ATZelektronik, Band 6, Ausgabe 1, 2011, S. 34-39

SCHICK, B., HENNING, J., WURSTER, U., KLEIN-RIDDER, B.: Simulationsmethoden zur Evaluierung und Verifizierung von Funktion, Güte und Sicherheit von Fahrerassistenzsystemen im durchgängigen MIL-, SIL- und HIL-Prozess. In: 3. Tagung Aktive Sicherheit durch Fahrerassistenz, 07.-08.04.2008, Garching bei München, 2008

SCHMIDT, F.: Funktionale Absicherung kamerabasierter Aktiver Fahrerassistenzsysteme durch Hardware-in-the-Loop-Tests, Dissertation, Universität Kaiserslautern, Fakultät Informatik, 2012

SCHULTE, M.: Ko-KOMP – Realitätsnahe Testmethoden für kooperative Sensorsysteme, 2011

SEINIGER, P., BARTELS, O., LANGNER, T., WISCH, M.: Development of a Target Propulsion System for ASSESS, 23rd International Technical Conference on the Enhanced Safety of Vehicles, 27.-30.05.2013, Seoul, Korea, 2013

SHESKIN, D. J.: Handbook of Prametric and Nonparametric Statistical Procedures, 3. Auflage, CRC Press LLC, Florida, 2004

SIMANAITIS, D. J.: Emission test cycles around the world. In: Automotive Engineering, Band 85, Ausgabe 8, 1977, S. 34-43

STÄNDER, T.: Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262, Dissertation, Technische Universität Carolo-Wilhelmina zu Braunschweig, 2011

STÄNDER, T., BECKER, U., SCHNIEDER, E.: Branchenspezifische Normen und Standards – Aufwand, Nutzen und Herausforderungen. In: Tagung Automatisierungs-, Assistenzsysteme und eingebettete Systeme für Transportmittel, 13.-14. Februar 2008, Braunschweig, 2008

Statistisches Bundesamt: Verkehrsunfälle 2011, Wiesbaden, 2012

STILLER, C., MAURER, M.: Fahrerassistenzsysteme – Fahrerassistenzsysteme mit maschineller Wahrnehmung, Springer-Verlag, Berlin, Heidelberg, New York, 2005

STRASSER, B., SIEGEL, A., SIEDERSBERGER, K.-H., BUBB, H., MAURER, M.: Vernetzung von Test- und Simulationsmethoden für die Entwicklung von Fahrerassistenzsystemen. In: 4. Tagung Aktive Sicherheit durch Fahrerassistenz, 15.-16.04.2010, Garching bei München, 2010

StVO: Straßenverkehrs-Ordnung vom 6. März 2013 (BGBl. I S. 367), in Kraft getreten am 1.4.2013, verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/stvo_2013/gesamt.pdf, Abruf am 12.04.2013

StVZO: Straßenverkehrs-Zulassungs-Ordnung vom 26. April 2012 (BGBl. I S. 679), verfügbar unter: http://www.gesetze-im-internet.de/bundesrecht/stvzo_2012/gesamt.pdf, Abruf am 12.04.2013

TSS: ASTA, Active Safety Test Area, verfügbar unter: http://www.testsitesweden.com/safety, Abruf am 12.04.2013

VERSMOLD, H., GLEISSNER, T.: Einfluss des Technologiewandels auf die zukünftige Gestaltung von Fahrzeugelektronik und Systemarchitekturen. In: 13. Aachener Kolloquium, 04.-06.10.2004, Aachen, 2004

WAAGMEESTER, K.: Assess Target Object Development, verfügbar unter: http://www.humaneticsatd.com/about-us/industry-news/assess-target-object-development, Abruf am 12.12.2010

WEITZEL, A.: Objektive Bewertung der Kontrollierbarkeit nicht situationsgerechter Reaktionen umfeldsensorbasierter Fahrerassistenzsysteme, Dissertation, TU Darmstadt, in Druck, 2013

WEITZEL, A., WINNER, H.: Ansatz zur Kontrollierbarkeitsbewertung von Fahrerassistenzsystemen vor dem Hintergrund der ISO 26262. In: 8. Workshop Fahrerassistenzsysteme 26.-28. September 2012, Walting im Altmühltal, 2012, S. 15-25

WESTERKAMP, R.: Prozessgestaltung für Bahnanwendungen nach CENELEC – ideal und real. In: Braunschweiger Verkehrskolloqium des ZVB, 01.04.2004, Braunschweig, 2004

WINNER, H.: Einrichtung zum Bereitstellen von Signalen in einem Kraftfahrzeug, Patent, 2001

WINNER, H.: Radarsensorik. In: WINNER, H., HAKULI, S., WOLF, G.: Handbuch Fahrerassistenzsysteme, 2. Auflage, Vieweg+Teubner Verlag, Wiesbaden, 2012b, S. 123-71

WINNER, H., GEYER, S., SEFATI, M.: Maße für den Sicherheitsgewinn von Fahrerassistenzsystemen, 6. Darmstädter Kolloquium Mensch + Fahrzeug, Maßstäbe des sicheren Fahrens, 06.-07.03.2013, Darmstadt, 2013

WINNER, H., HAKULI, S., BRUDER, R., KONIGORSKI, U., SCHIELE, B.: Conduct-by-Wire – ein neues Paradigma für die Weiterentwicklung der Fahrerassistenz. In: 4. Workshop Fahrerassistenzsysteme, 4.-6.10.2006, Löwenstein/Hößlinsülz, 2006

WINNER, H., HEUSS, O.: X-by-Wire-Betätigungselemente – Überblick und Ausblick. In: 3. Darmstädter Kolloquium Mensch + Fahrzeug, Cockpits für Straßenfahrzeuge der Zukunft, 08.-09.03.2005, Darmstadt, 2005, S. 79-115

WINNER, H., WEITZEL, A.: Quo vadis, FAS? In: WINNER, H., HAKULI, S., WOLF, G.: Handbuch Fahrerassistenzsysteme, 2. Auflage, Vieweg+Teubner Verlag, Wiesbaden, 2012, S. 658-667

Schriftenreihe

Berichte der Bundesanstalt für Straßenwesen

Unterreihe „Fahrzeugtechnik“

2002

F 39: **Optimierung des rückwärtigen Signalbildes zur Reduzierung von Auffahrunfällen bei Gefahrenbremsung**
Gail, Lorig, Gelau, Heuzeroth, Sievert € 19,50

F 40: **Entwicklung eines Prüfverfahrens für Spritzschutzsysteme an Kraftfahrzeugen**
Domsch, Sandkühler, Wallentowitz € 16,50

2003

F 41: **Abgasuntersuchung: Dieselfahrzeuge**
Afflerbach, Hassel, Mäurer, Schmidt, Weber € 14,00

F 42: **Schwachstellenanalyse zur Optimierung des Notausstiegsystems bei Reisebussen**
Krieg, Rüter, Weißgerber € 15,00

F 43: **Testverfahren zur Bewertung und Verbesserung von Kinderschutzsystemen beim Pkw-Seitenaufprall**
Nett € 16,50

F 44: **Aktive und passive Sicherheit gebrauchter Leichtkraftfahrzeuge**
Gail, Pastor, Spiering, Sander, Lorig € 12,00

2004

F 45: **Untersuchungen zur Abgasemission von Motorrädern im Rahmen der WMTC-Aktivitäten**
Steven € 12,50

F 46: **Anforderungen an zukünftige Kraftrad-Bremssysteme zur Steigerung der Fahrsicherheit**
Funke, Winner € 12,00

F 47: **Kompetenzerwerb im Umgang mit Fahrerinformations-systemen**
Jahn, Oehme, Rösler, Krems € 13,50

F 48: **Standgeräuschmessung an Motorrädern im Verkehr und bei der Hauptuntersuchung nach § 29 StVZO**
Pullwitt, Redmann € 13,50

F 49: **Prüfverfahren für die passive Sicherheit motorisierter Zweiräder**
Berg, Rücker, Bürkle, Mattern, Kallieris € 18,00

F 50: **Seitenairbag und Kinderrückhaltesysteme**
Gehre, Kramer, Schindler € 14,50

F 51: **Brandverhalten der Innenausstattung von Reisebussen**
Egelhaaf, Berg, Staubach, Lange € 16,50

F 52: **Intelligente Rückhaltesysteme**
Schindler, Kühn, Siegler € 16,00

F 53: **Unfallverletzungen in Fahrzeugen mit Airbag**
Klanner, Ambos, Paulus, Hummel, Langwieder, Köster € 15,00

F 54: **Gefährdung von Fußgängern und Radfahrern an Kreuzungen durch rechts abbiegende Lkw**
Niewöhner, Berg € 16,50

2005

F 55: **1st International Conference on ESAR „Expert Symposium on Accident Research“ – Reports on the ESAR-Conference on 3rd/4th September 2004 at Hannover Medical School** € 29,00

2006

F 56: **Untersuchung von Verkehrssicherheitsaspekten durch die Verwendung asphärischer Außenspiegel**
Bach, Rüter, Carstengerdes, Wender, Otte € 17,00

F 57: **Untersuchung von Reifen mit Notlaufeigenschaften**
Gail, Pullwitt, Sander, Lorig, Bartels € 15,00

F 58: **Bestimmung von Nutzfahrzeugemissionsfaktoren**
Steven, Kleinebrahm € 15,50

F 59: **Hochrechnung von Daten aus Erhebungen am Unfallort**
Hautzinger, Pfeiffer, Schmidt € 15,50

F 60: **Ableitung von Anforderungen an Fahrerassistenzsysteme aus Sicht der Verkehrssicherheit**
Vollrath, Briest, Schießl, Drewes, Becker € 16,50

2007

F 61: **2nd International Conference on ESAR „Expert Symposium on Accident Research“ – Reports on the ESAR-Conference on 1st/2nd September 2006 at Hannover Medical School** € 30,00

F 62: **Einfluss des Versicherungs-Einstufungstests auf die Belange der passiven Sicherheit**
Rüter, Zoppke, Bach, Carstengerdes € 16,50

F 63: **Nutzerseitiger Fehlgebrauch von Fahrerassistenzsystemen**
Marberger € 14,50

F 64: **Anforderungen an Helme für Motorradfahrer zur Motorradsicherheit**
Dieser Bericht liegt nur in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden.
Schüler, Adoplh, Steinmann, Ionescu € 22,00

F 65: **Entwicklung von Kriterien zur Bewertung der Fahrzeugbeleuchtung im Hinblick auf ein NCAP für aktive Fahrzeugsicherheit**
Manz, Kooß, Klinger, Schellinger € 17,50

2008

F 66: **Optimierung der Beleuchtung von Personenwagen und Nutzfahrzeugen**
Jebas, Schellinger, Klinger, Manz, Kooß € 15,50

F 67: **Optimierung von Kinderschutzsystemen im Pkw**
Weber € 20,00

F 68: **Cost-benefit analysis for ABS of motorcycles**
Baum, Westerkamp, Geißler € 20,00

F 69: **Fahrzeuggestützte Notrufsysteme (eCall) für die Verkehrssicherheit in Deutschland**
Auerbach, Issing, Karrer, Steffens € 18,00

F 70: **Einfluss verbesserter Fahrzeugsicherheit bei Pkw auf die Entwicklung von Landstraßenunfällen**
Gail, Pöppel-Decker, Lorig, Eggers, Lerner, Ellmers € 13,50

2009

F 71: **Erkennbarkeit von Motorrädern am Tag – Untersuchungen zum vorderen Signalbild**
Bartels, Sander € 13,50

F 72: **3rd International Conference on ESAR „Expert Symposium on Accident Research“ – Reports on the ESAR-Conference on 5th / 6th September 2008 at Hannover Medical School** € 29,50

F 73: **Objektive Erkennung kritischer Fahrsituationen von Motorrädern**
Seiniger, Winner € 16,50

2010

F 74: **Auswirkungen des Fahrens mit Tempomat und ACC auf das Fahrerverhalten**
Vollrath, Briest, Oeltze € 15,50

F 75: **Fehlgebrauch der Airbagabschaltung bei der Beförderung von Kindern in Kinderschutzsystemen**
Müller, Johannsen, Fastenmaier € 15,50

2011

F 76: **Schutz von Fußgängern beim Scheibenanprall II**
Dieser Bericht liegt nur in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden.
Bovenkerk, Gies, Urban € 19,50

F 77: **4th International Conference on ESAR „Expert Symposium on Accident Research"**
Dieser Bericht liegt nur in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden. € 29,50

F 78: **Elektronische Manipulation von Fahrzeug- und Infrastruktursystemen**
Dittmann, Hoppe, Kiltz, Tuchscheerer € 17,50

F 79: **Internationale und nationale Telematik-Leitbilder und IST-Architekturen im Straßenverkehr**
Boltze, Krüger, Reusswig, Hillebrand € 22,00

F 80: **Untersuchungskonzepte für die Evaluation von Systemen zur Erkennung des Fahrerzustands**
Eichinger € 15,00

F 81: **Potential aktiver Fahrwerke für die Fahrsicherheit von Motorrädern**
Wunram, Eckstein, Rettweiler € 15,50

F 82: **Qualität von on-trip Verkehrsinformationen im Straßenverkehr – Quality of on-trip road traffic information – BASt-Kolloquium 23. & 24.03.2011**
Lotz, Luks € 17,50
Dieser Bericht liegt nur in digitaler Form vor und kann kostenpflichtig unter www.nw-verlag.de heruntergeladen werden.

2012

F 83: **Rechtsfolgen zunehmender Fahrzeugautomatisierung – Gemeinsamer Schlussbericht der Projektgruppe**
Gasser, Arzt, Ayoubi, Bartels, Bürkle, Eier, Flemisch,
Häcker, Hesse, Huber, Lotz, Maurer, Ruth-Schumacher,
Schwarz, Vogt € 19,50

F 84: **Sicherheitswirkungen von Verkehrsinformationen – Entwicklung und Evaluation verschiedener Warnkonzepte für Stauendewarnungen**
Bogenberger, Dinkel, Totzke, Naujoks, Mühlbacher € 17,00

F 85: **Cooperative Systems Stakeholder Analysis**
Schindhelm, Calderaro, Udin, Larsson, Kernstock,
Jandrisits, Ricci, Geißler, Herb, Vierkötter € 15,50

2013

F 86: **Experimentelle Untersuchung zur Unterstützung der Entwicklung von Fahrerassistenzsystemen für ältere Kraftfahrer**
Hoffmann, Wipking, Blanke, Falkenstein € 16,50

F 87: **5th International Conference on ESAR „Expert Symposium on Accident Research"**
Dieser Bericht liegt nur in digitaler Form vor und kann unter http://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 88: **Comparative tests with laminated safety glass panes and polycarbonate panes**
Gehring, Zander € 14,00

F 89: **Erfassung der Fahrermüdigkeit**
Platho, Pietrek, Kolrep € 16,50

F 90: **Aktive Systeme der passiven Fahrzeugsicherheit**
Nuß, Eckstein, Berger € 17,90

F 91: **Standardisierungsprozess für offene Systeme der Straßenverkehrstelematik**
Kroen € 17,00

F 92: **Elektrofahrzeuge – Auswirkungen auf die periodisch technische Überwachung**
Beyer, Blumenschein, Bönninger, Grohmann, Lehmann, Meißner,
Paulan, Richter, Stiller, Calker € 17,00

2014

F 93: **Entwicklung eines Verfahrens zur Erfassung der Fahrerbeanspruchung beim Motorradfahren**
Buld, Will, Kaussner, Krüger € 17,50

F 94: **Biokraftstoffe – Fahrzeugtechnische Voraussetzungen und Emissionen**
Pellmann, Schmidt, Eckhardt, Wagner € 19,50

F 95: **Taxonomie von Fehlhandlungen bei der Fahrzeugführung**
Oehme, Kolrep, Person, Byl € 16,50

F 96: **Auswirkungen alternativer Antriebskonzepte auf die Fahrdynamik von Pkw**
Schönemann, Henze € 15,50

F 97: **Matrix von Lösungsvarianten Intelligenter Verkehrssysteme (IVS) im Straßenverkehr**
Matrix of alternative implementation approaches of Intelligent Transport Systems (ITS) in road traffic
Lotz, Herb, Schindhelm, Vierkötter
Dieser Bericht liegt nur in digitaler Form vor und kann unter http://bast.opus.hbz-nrw.de/ heruntergeladen werden.

F 98: **Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung**
Weitzel, Winner, Peng, Geyer, Lotz, Sefati € 16,50

Alle Berichte sind zu beziehen im:

Carl Schünemann Verlag GmbH
Zweite Schlachtpforte 7
28195 Bremen
Tel. (0421) 3 69 03-53
Fax (0421) 3 69 03-48
www.schuenemann-verlag.de

Dort ist auch ein Komplettverzeichnis erhältlich.