TECHNISCHE UNIVERSITÄT MÜNCHEN
Institut für Maschinen- und Fahrzeugtechnik
Lehrstuhl für Fahrzeugtechnik

Sicherheitskonzept für hochautomatisierte Fahrerassistenzsysteme

Markus A. Hörwick

Vollständiger Abdruck der von der Fakultät für Maschinenwesen der Technischen Universität München zur Erlangung des akademischen Grades eines

Doktor-Ingenieurs
genehmigten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. H. Baier

Prüfer der Dissertation:
1. Univ.-Prof. Dr.-Ing. M. Lienkamp
2. Univ.-Prof. Dr.-Ing. H.-J. Wünsche (Universität der Bundeswehr München)

Die Dissertation wurde am 08.02.2011 bei der Technischen Universität München eingereicht und durch die Fakultät für Maschinenwesen am 07.10.2011 angenommen.

Vorwort

Diese Arbeit entstand im Rahmen meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Fahrzeugtechnik der Technischen Universität München in enger Zusammenarbeit mit der Abteilung Entwicklung Fahrerassistenzsysteme der Audi AG (I/EF-56).

Mein ganz besonderer Dank gilt meinen Doktorvätern Prof. Dr.-Ing. B. Heißing und Prof. Dr.-Ing. M. Lienkamp, die durch die Schaffung exzellenter Arbeitsbedingungen sowie ihre faire, positive und vertrauensvolle Art gegenüber mir und allen anderen Institutsmitarbeitern wesentlich zum Gelingen dieser Arbeit beigetragen haben. Für die Übernahme des Koreferats bedanke ich mich bei Prof. Dr.-Ing. H.-J. Wünsche, für den Prüfungsvorsitz bei Prof. Dr.-Ing. H. Baier.

Weiter möchte ich mich bei Dr.-Ing. U. Koser und Dr.-Ing. A. Meyer bedanken, die die Durchführung dieses Forschungsvorhabens im Rahmen des Kooperationsprojekts INI.TUM ermöglichten.

Ein ganz herzliches Dankeschön geht an meinen Betreuer bei der Audi AG Dr.-Ing. K.-H. Siedersberger, der den Anstoß zu dieser Arbeit gab und dessen fachliche Anregungen sowie Blick fürs Wesentliche für mich besonders wichtig und wertvoll waren. Für die gute Zusammenarbeit möchte ich mich auch bei allen anderen Kollegen in der Audi-Abteilung I/EF-56, namentlich bei Dr. rer. nat. R. Dubitzky, Dr.-Ing. U. Hofmann, M.-E. Bouzouraa, M. Bär, M. Reichel, M. Siebeneicher, J. Storz und J. Winhuysen bedanken. Ein besonderer Dank geht außerdem an M. Wimmer.

Speziell hervorgehoben sei die kollegiale Atmosphäre am Lehrstuhl für Fahrzeugtechnik, wo ich mich immer sehr wohl gefühlt habe. Ein besonderer Dank hierfür an alle Kollegen, speziell an S. Schramm und W. Schmid, sowie an T. Pesce, C. Schimmel und S. Kraus, die kreative Keimzellen für mich waren.

Ein besonderes Dankeswort gilt auch F. Kohlhuber, T. Prosser, S. Schickram, N. Ostgathe, H. Gunsell und S. Herbort, die durch ihr großes Engagement im Rahmen von Praktika bzw. Diplom- und Semesterarbeiten maßgeblich zum Erfolg der Arbeit beigetragen haben.

Nicht zuletzt gilt mein Dank P. Denkscherz und M. Hlavacek für ihre mentale Unterstützung, sowie meinen Eltern für die mir ermöglichte individuelle und berufliche Freiheit.

Slip inside the eye of your mind

Don't you know you might find

A better place to play?

[Oasis 1996]

Inhaltsverzeichnis

Abkürzungsverzeichnis

ABS	Anti Blockier System
ACC	Adaptive Cruise Control
ACC S&G	Adaptive Cruise Control Stop and Go
ADTF	Automotive Data and Time triggered Framework
A FAS	Autonomes Fahrerassistenzsystem
ANB	Automatische Notbremse
APU	Aktionsplan-Umsetzer
ASIL	Automotive Safety Integrity Level
AWA	Ausweichanalyse
CPU	Central Processing Unit
EFzg	Ego-Fahrzeug
ESP	Elektronisches Stabilitätsprogramm
FAS	Fahrerassistenzsystem
FS	Fail-Safe
FSM	Funktionales Softwaremodul
FÜA	Fahrerübernahmeaufforderung
GLÜ	Globaler Überwacher
GPS	Global Positioning System
H FAS	Hochautomatisiertes Fahrerassistenzsystem
HMI	Human Machine Interface
LKS	Lane Keeping Support System
LMÜ	Lokaler Modul-Überwacher
ROI	Region of Interest
SA FAS	Semiautomatisches Fahrerassistenzsystem
STA	Stauassistent
SW	Software
VA FAS	Vollautomatisches Fahrerassistenzsystem
WBA	Warnblinkanlage

1 Einführung in die Problemstellung

Durch das ständig wachsende Bedürfnis nach uneingeschränkter Mobilität im Personenkraftverkehr und die damit stetig zunehmende Fahrzeugdichte im Straßennetz erhöht sich die Gefahr von Unfällen durch Überforderung und Unachtsamkeit der Fahrer ebenso wie die physische und psychische Beanspruchung der Insassen während der Fahrt. Dies macht es notwendig, die Sicherheit und den Komfort moderner Kraftfahrzeuge ständig zu verbessern.

Einen wesentlichen Beitrag hierzu leisten Fahrerassistenzsysteme (FAS), von denen einige in der Lage sind, die Fahrzeuglängs- oder Fahrzeugquerführungsaufgabe zu übernehmen und den Fahrer somit gezielt zu unterstützen. Die bekanntesten Vertreter sind hierbei Adaptive Cruise Control Stop and Go (ACC S&G), ein Komfortsystem, das eine automatische, kontinuierliche Längsführung über den kompletten Geschwindigkeitsbereich realisiert, und Lane Keeping Support Systeme (LKS, oft auch als Heading Control Systeme bezeichnet), die den Fahrer in der Querführung durch gezielte Lenkeingriffe unterstützen.

Die Auswirkungen der Nutzung der beiden genannten FAS auf das menschliche Fahrverhalten können, infolge frei gewordener Kapazität, eine Neigung zur Beschäftigung mit Nebenaufgaben sein, die in einer Reduktion der Aufmerksamkeit und einem verringerten Situationsbewusstsein resultieren (vgl. [Buld & Krüger 2004]). Nachdem der Fahrer aber selbst bei gleichzeitiger Nutzung von ACC S&G und LKS notwendigerweise noch die Hände am Lenkrad halten muss, da LKS die Querführung nur unterstützen, nicht aber übernehmen, bleibt er direkt an der Fahrzeugführung beteiligt. Aus diesem Grund kann bislang immer noch davon ausgegangen werden, dass der Fahrer jederzeit sämtliche Aktionen des Fahrzeugs überwacht, unabhängig ob diese von ihm selbst oder dem FAS initiiert sind und dass er folglich bei Auftreten eines Systemfehlers korrigierend in die Längs- und/oder Querführung eingreift.

Im Rahmen der stetig voranschreitenden Automatisierung werden zukünftige FAS zusätzlich zur automatischen Längsführung die Querführung nicht mehr nur unterstützen, sondern ebenfalls komplett übernehmen. Der Fahrer wird dadurch in eine reine Überwachungsaufgabe gedrängt und muss das Lenkrad und die Pedalerie nur noch dann bedienen, wenn das FAS dazu nicht mehr in der Lage ist. Dies stellt ein erhebliches Problem dar, da Menschen für die Überwachung vollständig automatischer Systeme nicht besonders gut geeignet sind (vgl. [Bainbridge 1983]). Dies liegt daran, dass es bei solchen Systemen generell sehr weniger korrigierender Eingriffe bedarf, die aber zumeist in sehr kritischen Situationen notwendig sind. Für den Bediener ist es dann extrem schwer, rechtzeitig und adäquat zu reagieren, zumal er wahrscheinlicherweise abgelenkt und sich des Systemzustandes nicht mehr vollständig bewusst ist (vgl. Bild 1.1). Die Gefahr eines menschlichen Fehlers ist daher sehr hoch, vor allem wenn es sich um eine untrainierte Person handelt. Übertragen auf FAS, die die komplette Fahrzeugführungsaufgabe übernehmen, bedeutet dies, dass das Verhalten des Fahrzeugs für den durchschnittlichen Fahrer schwer kontrollierbar ist, wenn eine Grenze der Fahrerassistenzfunktion erreicht oder überschritten wird und dass in Konsequenz eine Gefahr in Form von Verkehrsbehinderungen oder gar Kollisionen besteht. Die dargelegten negativen

Folgen der Automation werden auch als „Out-of-the-loop Performance Problem“ bezeichnet (vgl. [Endsley & Kiris 1995]).

Bild 1.1: Mögliches Beispiel für Fahrerablenkung bei vollständiger Automatisierung der Fahrzeugführung (vgl. [Vehicle Vibes 2009])

Die vorliegende Arbeit zeigt ein integrales, funktionales Konzept zur Lösung des beschriebenen Problems und damit einen Weg zur Erlangung funktionaler Sicherheit bei derartigen Systemen auf. Dazu wird jeweils eine entsprechende Lösungsstrategie für vollautomatische Fahrzeugführungsfunktionen der nahen und der ferneren Zukunft vorgestellt. Zur Abgrenzung der Unterschiede solcher FAS mit unterschiedlichem Zeithorizont werden in Kapitel 1.1 die Begriffe vollautomatisches und autonomes FAS eingeführt und charakterisiert, woraufhin in Kapitel 1.2 die Funktion Stauassistent vorgestellt wird, die in dieser Arbeit in entsprechend unterschiedlicher Ausprägung als Anwendungsbeispiel für beide Strategien dienen soll. Dies ist sinnvoll, da einige der erarbeiteten Aspekte des Konzepts funktionsspezifischer Natur sind und somit für jede Funktion eine Einzelbetrachtung durchgeführt werden muss. Kapitel 1.3 definiert die Zielsetzung der Arbeit, indem die Hauptaufgaben des zu konzipierenden Sicherheitskonzepts in abstrakter Weise beschrieben werden. Einen vorgreifenden Überblick über die Struktur der gesamten Arbeit liefert abschließend Kapitel 1.4.

1.1 Hochautomatisierte Fahrerassistenzsysteme

Der Begriff hochautomatisierte Fahrerassistenzsysteme (H FAS) adressiert grundsätzlich FAS für Pkws im zivilen Straßenverkehr, die direkt in die Längs- und/oder Querführung eingreifen, um den Komfort und die Sicherheit der Fahrzeuginsassen zu erhöhen. Ausgeschlossen sind damit sämtliche Systeme die gemäß [Naab & Reichart 1998] in die Kategorie der informierenden Systeme und Servosysteme fallen, den Fahrer also lediglich vor potentiellen Gefahren warnen oder ihm „vorgegebene Betätigungsaktionen erleichtern“ ohne dabei die Fahrzeugführung intelligent zu beeinflussen. Die heute im Markt befindlichen H FAS lassen sich in die folgenden drei Klassen einteilen:

- Automatisch intervenierende FAS: Derartige Sicherheitssysteme greifen nur in sehr kritischen Situationen kurzfristig in die Fahrzeugführung ein, wenn es dem Fahrer nicht mehr möglich ist, das Fahrzeug zu stabilisieren oder Kollisionen zu vermeiden. Typische Beispiele hierfür sind das Anti Blockier System (ABS) und das elektronische Stabilitätsprogramm (ESP) (vgl. [Van Zanten & Kost 2009]), sowie die automatische

Notbremse (ANB) (vgl. [Kopischke 2000]), die, je nach Auslegung, zur Verhinderung oder Schadensfolgenminderung einer Kollision vor dem Aufprall automatisch eine Vollverzögerung einleitet.

- Automatisch unterstützende FAS: Die momentan einzigen im Markt befindlichen Systeme dieser Kategorie sind LKS. [Gayko 2009] charakterisiert LKS auf folgende Weise: „Ziel dieser Funktion ist, je nach Auslegung, eine Erhöhung der Sicherheit, eine Erhöhung des Fahrkomforts oder eine Kombination beider Ziele.“ Besonders kennzeichnend ist, dass diese Funktion „keine den Fahrer ersetzende Assistenz darstellt. Die motorische Ausführung der Lenkung des Fahrzeugs erfolgt somit durch den Fahrer und das LKS-System zugleich.“ Ersetzt man in diesem Zitat das Wort „Lenkung“ durch „Längs- und/oder Querführung“, erhält man eine allgemeine Definition für automatisch unterstützende FAS.
- Semiautomatische FAS (SA FAS): Im Unterschied zu automatisch unterstützenden FAS übernimmt das FAS hier entweder vollständig die Längs- oder die Querführung. Vertreter dieser Komfortsysteme im Serieneinsatz sind hinsichtlich der Übernahme der Längsführung Adaptive Cruise Control (ACC) bzw. ACC S&G (vgl. [Winner et al. 2009]) und hinsichtlich der Querführung Parklenkassistenten (vgl. [Schöning et al. 2006]).

Nachdem heute bereits weite Teile der Fahrzeugführung automatisiert werden können, ist es das Ziel aktueller Forschungs- und Entwicklungsbemühungen, Systeme zu konzipieren, die dem Fahrer die komplette Fahrzeugführung abnehmen können. Es soll an dieser Stelle geklärt werden, inwiefern derartige FAS kategorisiert werden können bzw. ab wann eine Funktion als autonom bezeichnet werden kann.

Der Begriff „Autonomie“ wird häufig mit dem Begriff „Selbstständigkeit“ gleichgesetzt. Im Allgemeinen spricht man von Selbstständigkeit wenn „sich ein Individuum eigene Ziele setzen, Mittel zu ihrer Erreichung auswählen, die Bewertung der eingesetzten Mittel und anvisierten Ziele weitgehend unabhängig von außen vornehmen und das Ausmaß der Zielerreichung realitätsangemessen beurteilen kann“. (vgl. [Brunner & Zeltner 1980])

Auf Basis dieser Definition lassen sich Komfortsysteme zur vollständigen Fahrzeugführung in die folgenden zwei Klassen einteilen, wobei der Unterschied darin besteht, welche Rolle der Fahrer im System einnimmt. Die funktionalen Umfänge der Systeme während des Normalbetriebs sind dagegen identisch.

- Vollautomatische FAS (VA FAS): VA FAS sind in der Lage „eigene Ziele“ festzulegen, „Mittel zu ihrer Erreichung“ auszuwählen und damit innerhalb definierter Grenzen ein vollautomatisches Fahren ohne Zutun des Fahrers zu realisieren. Allerdings ist es ihnen nicht möglich, eigenständig eine vollständige „Bewertung der eingesetzten Mittel und anvisierten Ziele“ vorzunehmen und auf diese Weise, „das Ausmaß der Zielerreichung realitätsangemessen“ zu beurteilen. Das hat zur Folge, dass der Fahrer jederzeit sämtliche Aktionen, die das FAS ausführt oder unterlässt, überwachen muss. Falls er ein Fehlverhalten erkennt oder ihn das System zur Übernahme auffordert, muss der Fahrer sofort in der Lage sein, korrigierend einzugreifen und die Fahraufgabe wieder vollständig zu übernehmen. Daher ist es ihm

nicht gestattet, stärker als im manuellen Fahrbetrieb abgelenkt zu sein und sich mit Nebenaufgaben zu beschäftigen. Der Fahrer muss also im Loop bleiben.

- Autonome FAS (A FAS): Im Gegensatz dazu erfüllt ein A FAS sämtliche Anforderungen hinsichtlich der Definition von Selbstständigkeit. So ist es derartigen Systemen möglich, jegliche Art von Fehlern bzw. verletzte Einschaltbedingungen selbstständig zu erkennen und zudem entsprechend zu reagieren, falls ein Eingreifen des Fahrers nach Ausgabe einer Fahrerübernahmeaufforderung ausbleibt. Dem Fahrer ist es daher erlaubt, stärker als bei manueller Fahrt abgelenkt zu sein und Nebentätigkeiten, wie Fernsehen oder Lesen, nachzugehen.

Es ist davon auszugehen, dass bereits in naher Zukunft erste VA FAS Serienreife erlangen werden, ehe einige Zeit später A FAS folgen werden. Aus den beiden Definitionen ergeben sich für die Systemauslegung derartiger Systeme schwerwiegende Konsequenzen, die in zwei grundsätzlich unterschiedlichen Strategien zur Erlangung funktionaler Sicherheit vollständig automatisierter Fahrfunktionen resultieren. Nachdem automatisch intervenierende FAS, automatisch unterstützende FAS und SA FAS bereits Stand der Technik sind, fokussiert diese Arbeit ausschließlich VA FAS und A FAS.

1.2 Anwendungsbeispiel Stauassistent

Wie sich im Verlauf der Arbeit zeigen wird, sind einige Aspekte des Sicherheitskonzepts von der genauen Funktionsspezifikation des jeweiligen betrachteten Systems abhängig. Daher ist die beispielhafte Anwendung der erarbeiteten Methoden auf eine konkrete Fahrerassistenzfunktion sinnvoll. Als Anwendungsbeispiel ist der Stauassistent (STA) besonders geeignet, da abzusehen ist, dass er sowohl in vollautomatischer als auch in autonomer Ausprägung eines der ersten FAS seiner Klasse sein wird.

Stauassistenten übernehmen im Stau vollständig die Fahrzeuglängs- und Querführung und ersetzen den Fahrer damit gezielt in einer monotonen und als störend empfundenen Fahrsituation. Der Einsatzbereich ist üblicherweise auf Geschwindigkeiten zwischen Null und maximal 60km/h begrenzt. Eine automatische Längsregelung reguliert dabei, analog ACC S&G, die Einhaltung eines geschwindigkeitsabhängigen Sicherheitsabstands zum Vorderfahrzeug. Der STA ist dabei ebenfalls in der Lage, bis in den Stillstand zu bremsen und danach wieder selbstständig anzufahren. Eine automatische Querregelung hält das Fahrzeug ab dem Zeitpunkt der Aktivierung innerhalb einer Fahrspur und realisiert zudem einen gewissen lateralen Mindestabstand zu bewegten und unbewegten Hindernissen. Ein automatischer Fahrspurwechsel ist nicht vorgesehen, was vor allem an der hohen Komplexität dieses Manövers liegt, das neben einer hohen Wahrnehmungsleistung auch kooperatives Verhalten aller beteiligten Verkehrsteilnehmer erfordert. Da die Realisierung eines adäquaten Verhaltens eines computergesteuerten Fahrzeugs in komplexen Fahrsituationen, beispielsweise an Ampeln, Kreuzungen oder Fußgängerüberwegen, oftmals nicht, oder nur mit sehr großem Aufwand möglich ist, wird das Einsatzgebiet des STA zudem auf Autobahnen und große Ringstrassen beschränkt.

Um das Fahrzeugumfeld wahrzunehmen, besitzen STA Sensoren zur Erfassung der Eigenbewegung, dynamischer und ortsfester Objekte sowie der Fahrspur. Die erfassten Daten werden einer Recheneinheit zur Verfügung gestellt, die daraufhin Stellgrößen berechnet, mit denen eine Motorsteuerung, eine aktive Bremse und eine aktive Lenkung angesteuert werden (vgl. Bild 1.2).

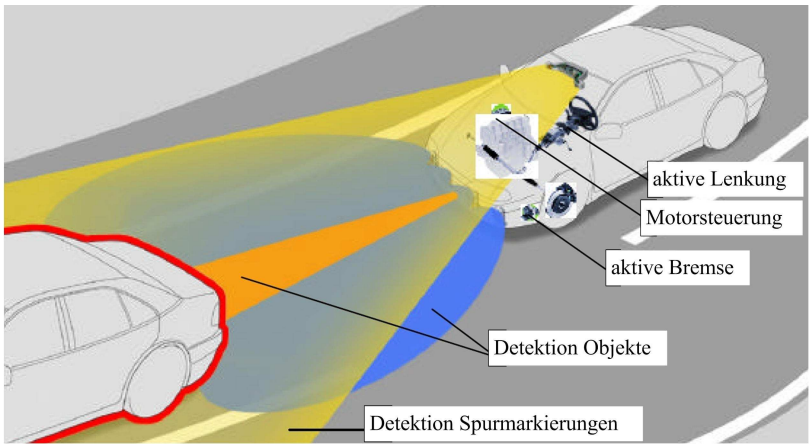

Bild 1.2: Aufbau und Komponenten eines Stauassistenten nach [Weilkes et al. 2002]

Erstmalig wurde eine derartige Funktion im Rahmen der Forschungsinitiative INVENT prototypisch umgesetzt (vgl. [Weilkes et al. 2002]). Neben Audi arbeiten auch andere führende Premium-Automobilhersteller wie BMW (vgl. [Schaller 2009]) und Daimler (vgl. [Schröder 2010]) an vergleichbaren Assistenzfunktionen. Bislang fallen sämtliche in der Literatur erwähnten Stauassistenz-Systeme in die Kategorie VA FAS, da immer davon ausgegangen wird, dass sich der Fahrer noch im Loop befindet.

1.3 Zielsetzung der Arbeit

Die bisher im Bereich der automatischen Fahrzeugführung bzw. Stauassistenz erzielten Forschungsergebnisse betreffen im Wesentlichen Themen der Aktorik und Sensorik, der Signalverarbeitung von Sensordaten, der darauf aufbauenden Situationsanalyse und Verhaltensentscheidung sowie regelungstechnischen Ansätzen zur Ansteuerung der Aktorik (vgl. beispielsweise [Hofmann 2004], [Siedersberger 2003], [Pellkofer 2003], [Maurer 2000] und [Schaller 2009]). Die zu Beginn von Kapitel 1 dargelegten resultierenden Probleme einer reduzierten bzw. fehlenden Fahreraufmerksamkeit infolge einer vollständigen Automatisierung der Fahrzeugführung sind bislang ungelöst. Eine umfassende sicherheitstechnische Betrachtung VA FAS und A FAS existiert somit nicht. Die genannten FAS befinden sich somit zum aktuellen Zeitpunkt noch in der Konzeptentwicklungsphase.

Im Jahr 2006 wurde mit dem Normentwurf ISO WD 26262 erstmals ein einheitlicher Sicherheitsstandard für Elektronik- und Softwaresysteme in der Automobilindustrie spezifiziert, der ab Mitte 2011 unter der Bezeichnung IS 26262 verbindlich für alle Automobilhersteller gültig ist. Der erste und bislang einzige frei verfügbare Stand trägt die Bezeichnung [ISO DIS 26262: 2009]. Hierin ist unter anderem für die Konzeptentwicklungsphase ein Vorgehen definiert, das im Wesentlichen aus drei aufeinander folgenden Schritten besteht:

- Gegenstandsdefinition und Einführung eines Sicherheits-Lebenszyklus: Hierbei werden die Funktion, Schnittstellen und potentielle Risiken des zu entwickelnden Systems definiert und das Management sicherheitsbezogener Aktivitäten und Prozesse geplant.
- Gefährdungsanalyse und Risikoeinstufung: Hierbei wird das von Fehlfunktionen des betrachteten Systems ausgehende Risiko in verschiedenen Fahrsituationen analysiert und einer Gefährdungsklasse, einem sogenannten ASIL (Automotive Safety Integrity Level), zugeordnet. Das ASIL des Risikos (Wertebereich QM-D) ergibt sich dabei gemäß Tabelle 1.1. Dabei ist S die Schadensschwere (engl. severity, Wertebereich S0-S3), E die Aufenthaltswahrscheinlichkeit in der Ausgangssituation (engl. exposition, Wertebereich E1-E4) und C die Kontrollierbarkeit des Fahrzeugs durch den Fahrer im Fehlerfall (engl. controllability, Wertebereich C0-C3). QM-Einstufungen (engl. Quality Management) bedürfen, im Gegensatz zu allen anderen ASIL-Stufen, keiner speziellen sicherheitsgerichteten Maßnahmen im Sinne der Norm. Aus der Summe der höheren Einstufungen müssen dagegen entsprechende Sicherheitsziele abgeleitet werden.
- Definition eines funktionalen Sicherheitskonzepts: Hierbei werden Sicherheitsanforderungen aus den zuvor erarbeiteten Sicherheitszielen abgeleitet, die grundlegende Sicherheitsmechanismen und Sicherheitsmaßnahmen beschreiben. Die Sicherheitsmechanismen betreffen dabei im Wesentlichen die Fehlererkennung, Übergänge in einen sicheren Zustand bzw. entsprechende Fehlertoleranzmechanismen, Fahrerwarnungen und die Entscheidungslogik zur Auswahl der am besten geeigneten Steuergröße aus unterschiedlichen Teilfunktionen. Außerdem muss eine Sicherheitsarchitektur entwickelt werden, die die Einbettung der Sicherheitsmechanismen und Sicherheitsmaßnahmen in die geplante Funktionsarchitektur realisiert. Dies beinhaltet auch die Beschreibung von Redundanzanforderungen. Das funktionale Sicherheitskonzept ist von einem technischen Sicherheitskonzept, das Anforderungen an die technische Implementierung definiert, zu unterscheiden. Letzteres ist erst im Rahmen der Serienentwicklung zu erarbeiten.

		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

S: Schadensschwere
E: Aufenthaltswahrscheinlichkeit in der Ausgangssituation
C: Kontrollierbarkeit durch Fahrer
A-D: ASIL-Stufe A-D
QM: Qualitätsmanagement

Tabelle 1.1: Bestimmung des Automotive Safety Integrity Level (ASIL) nach [ISO DIS 26262: 2009]

Das übergeordnete Ziel dieser Arbeit ist es, in Anlehnung an die [ISO DIS 26262: 2009], ein funktionales Sicherheitskonzept für zukünftige vollautomatische Fahrzeugführungsfunktionen (VA FAS und A FAS) zu entwickeln, welches es ermöglicht, jegliche denkbare Systemgrenzenüberschreitung zu detektieren, die die Aufrechterhaltung des Normalbetriebs verbietet, und welches es sodann erlaubt, einen sicheren Zustand wiederherzustellen bzw. beizubehalten. Es sollen somit Anforderungen und Funktionsweisen zur Erlangung funktionaler Sicherheit für vollautomatische Fahrzeugführungsfunktionen spezifiziert und auf diese Weise eine Basis für deren zukünftige Serienentwicklung erarbeitet werden.

Besonders herausfordernd ist in diesem Zusammenhang die Tatsache, dass die Kontrollierbarkeit des Fahrzeugs für den Fahrer eines VA FAS oder A FAS im Falle einer Systemgrenzenüberschreitung ohne weitere Maßnahmen nahezu unmöglich ist, da wie Eingangs erläutert, von einer stark reduzierten Aufmerksamkeit des Fahrers auszugehen ist (vgl. Bild 1.1). Die sich im Rahmen einer Risikoeinstufung daraus ergebenden, tendenziell hohen ASIL-Bewertungen (vgl. Spalte C3 in Tabelle 1.1) machen eine vom Einzelfall unabhängige grundlegende konzeptuelle Lösung dieses Problems notwendig.

Konkret soll zur Erlangung der oben genannten Ziele ein Konzept entwickelt werden, das definiert, welche sicherheitsgerichteten Komponenten auf welche Weise in die funktionale Architektur bestehender H FAS integriert werden müssen. Die angesprochenen Sicherheitskomponenten haben dabei im Wesentlichen die folgenden zwei Hauptaufgaben (vgl. Bild 1.3):

- Dauerhafte Überwachung aller relevanten Systemgrenzen während des Normalbetriebs
- Vorhaltung von Aktionsplänen, die das Fahrzeug beim Verlassen des Normalbetriebs des FAS infolge einer Systemgrenzenüberschreitung in einen sicheren Notaus-Zustand, eine sogenannte Rückfallebene, überführen, den Fahrer warnen und gleichzeitig das FAS deaktivieren

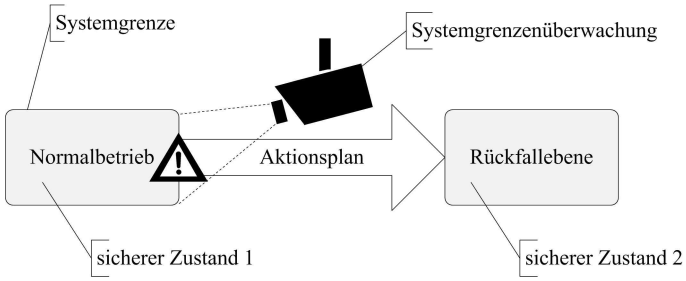

Bild 1.3: Hauptaufgaben des Sicherheitskonzepts

Wie bereits oben angedeutet, ist es das Ziel, jeweils eine Lösungsstrategie für vollautomatische sowie für autonome FAS zu erarbeiten. Funktionsspezifische Aspekte sollen exemplarisch am Beispiel der Funktion STA dargestellt werden.

Nachdem der Fokus der Arbeit auf A FAS liegt, sollen sämtliche entsprechend erarbeiteten Aspekte des Konzepts in einem realen STA-Versuchsträger implementiert bzw. validiert und somit ein hoher Reifegrad des Konzepts erreicht werden. Es sei an dieser Stelle explizit darauf hingewiesen, dass die eigentliche Innovation der Arbeit aber nicht die prototypischen Implementierungen darstellen sollen. Die Hauptinnovation soll stattdessen in der

konzeptuellen Beschreibung einer vollständigen und ganzheitlichen Lösungsstrategie zur Erlangung funktionaler Sicherheit bei vollautomatischen und autonomen FAS bzw. STA-Systemen liegen. Dies ist darin begründet, dass die Validität bzw. die Anwendbarkeit eines Sicherheitskonzepts, anders als in der konventionellen Funktionsentwicklung, bereits vor der Implementierungs- und Optimierungsphase offensichtlich sein muss. Es sind daher im Rahmen dieser Arbeit keine Versuchsreihen vorgesehen.

1.4 Struktur der Arbeit

Der strukturelle Aufbau dieser Arbeit wird in Bild 1.4 zusammengefasst.

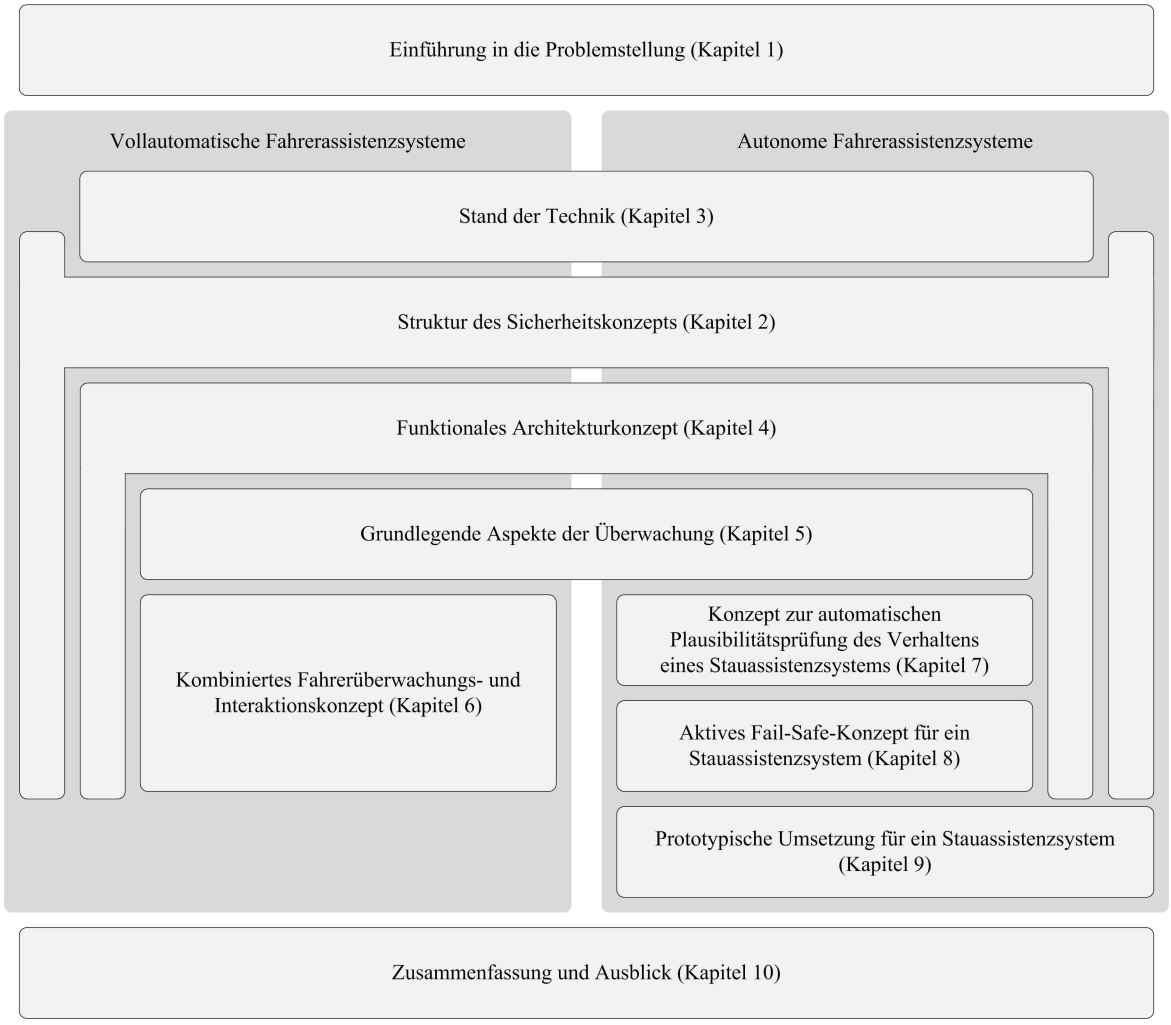

Bild 1.4: Struktureller Aufbau der Arbeit

Da bisher nur einzelne, spezielle Aspekte der Eingangs erläuterten Problemstellung bearbeitet wurden und keine Vorarbeiten für ein umfassendes funktionales Sicherheitskonzept, das sämtliche in Kapitel 1.3 definierten Ziele abdeckt, bestehen, wird im folgenden Kapitel 2 die grundlegende Struktur des erarbeiteten Sicherheitskonzepts erläutert. Dazu werden die zwei angesprochenen übergeordnete Lösungsstrategien zur Erlangung funktionaler Sicherheit bei VA FAS und A FAS vorgestellt und daraus die Kerngebiete der Arbeit abgeleitet und abgegrenzt. Bei letzteren handelt es sich hierbei um die Überwachung verschiedener Systemgrenzen, Fail-Safe-Mechanismen (FS) sowie ein funktionales Architekturkonzept. Auf

diese Kerngebiete wird im Hauptteil der Arbeit in den Kapiteln 4 bis 8 detailliert eingegangen.

Kapitel 3 liefert einen Überblick über den Stand der Technik bezüglich der verschiedenen zuvor definierten Kerngebiete und setzt daher auf Kapitel 2 auf.

Die Einbettung der unterlagerten Überwachungs- und FS-Komponenten (Kapitel 5 bis 8) des Sicherheitskonzepts in die Systemarchitektur von H FAS und deren Zusammenspiel ist Basis für das Verständnis der Funktionsweise des Sicherheitskonzepts. Daher wird in Kapitel 4 eine allgemein anwendbare, funktionale Architektur zur Überwachung automatischer Fahrzeugführungsfunktionen und zur Ansteuerung und Abarbeitung von Aktionsplänen infolge verletzter Einschaltbedingungen vorgestellt. Dabei wird besonders hervorgehoben, welche Redundanzen notwendig sind, um funktionale Sicherheit bei derartigen Systemen zu gewährleisten.

Kapitel 5 beschreibt Konzepte zur Überwachung thematisch verschiedener Systemgrenzen, die grundsätzlich bei allen vollautomatischen Fahrfunktionen, also VA FAS und A FAS, angewendet werden müssen. Es handelt sich hierbei um die Überwachung von Hardware- und Softwaremodulen, von externen Einflüssen sowie von Funktionsgrenzen. Im Unterschied zu den ersten beiden Aspekten ist die Funktionsgrenzenüberwachung von Funktion zu Funktion unterschiedlich und wird daher exemplarisch am Beispiel des STA erläutert.

In den beiden folgenden Kapiteln werden mit den Themen „Fahrerüberwachung“ (Kapitel 6) und „automatische Plausibilitätsüberwachung“ (Kapitel 7) spezielle Aspekte der Systemgrenzenüberwachung behandelt, die jeweils nur bei VA FAS bzw. bei A FAS umgesetzt werden müssen. So wird zum einen ein kombiniertes Überwachungs- und Interaktionskonzept vorgestellt, mit dem es auch bei VA FAS, die nur ein einzelnes Manöver automatisieren, möglich ist zu bestimmen, ob der Fahrer noch im Loop ist. Dies ist notwendig, da bei derartigen Systemen gewährleistet sein muss, dass der Fahrer nicht stärker als im manuellen Fahrbetrieb abgelenkt ist (vgl. Kapitel 1.1). Da der Fahrer als letzte Überwachungsinstanz bei A FAS nicht mehr zur Verfügung steht, wird mit der „automatischen Plausibilitätsüberwachung“ zum anderen ein Konzept vorgestellt, das genau jene Aspekte überwacht, für die beim VA FAS noch der Fahrer zuständig war. Da diese Aspekte genau wie die Funktionsgrenzenüberwachung funktionsspezifisch sind, wird die Plausibilitätsüberwachung am Beispiel des autonomen Stauassistenten beschrieben.

Nachdem sich die Kapitel 5, 6 und 7 mit der Systemgrenzenüberwachung bzw. der Überprüfung von Einschaltbedingungen beschäftigen, wird im darauffolgenden Kapitel 8 exemplarisch am Beispiel eines autonomen STA auf aktive Fail-Safe-Mechanismen eingegangen, die das Fahrzeug im Fehlerfall wieder in einen sicheren Zustand überführen. Hierbei wird zunächst der anzustrebende sichere Notaus-Zustand eines STA definiert, woraufhin Aktionspläne vorgestellt werden, die das Fahrzeug durch gezielte Längs- und Querführungseingriffe in diesen Notaus-Zustand manövrieren.

Im Rahmen dieser Arbeit wurden prototypische Implementierungen zu sämtlichen Kerngebieten des Sicherheitskonzepts für einen autonomen STA durchgeführt. Kapitel 9 zeigt die Ergebnisse einiger realer Fahrversuche.

Eine Zusammenfassung im letzten Kapitel 10 hebt die Schlüsselaspekte des Sicherheitskonzepts nochmals hervor und zeigt auf, inwiefern die erarbeiteten FS-Mechanismen eines autonomen STA für komplexere Assistenzfunktionen erweitert werden müssten.

2 Struktur des Sicherheitskonzepts

Da bisher kein umfassendes funktionales Sicherheitskonzept für vollautomatische und autonome Fahrerassistenzsysteme (FAS) existiert, werden in diesem Kapitel zunächst die erarbeiteten Strategien und Kernaspekte des Sicherheitskonzepts vorgestellt, bevor im Anschluss ein Überblick über den Stand der Technik relevanter Teilbereiche des Konzepts gegeben wird. Die Strategien basieren auf den Hauptaufgaben des Sicherheitskonzepts (vgl. Bild 1.3) und definieren zwei unterschiedliche Wege zur Absicherung vollautomatischer Fahrfunktionen, wobei die eine speziell auf vollautomatische FAS (VA FAS) und die andere auf autonome FAS (A FAS) abzielt. Aus ihnen werden direkt die relevanten, zu bearbeitenden Kernaspekte abgeleitet, die sich in den einzelnen Kapiteln dieser Arbeit widerspiegeln. Die folgenden Ausführungen sind somit für das Verständnis des erarbeiteten Sicherheitskonzepts fundamental und ziehen sich wie ein roter Faden durch diese Arbeit.

2.1 Übergeordnete Strategien

Die beiden Hauptaufgaben des Sicherheitskonzepts, Systemgrenzenüberwachung und Vorhaltung von Aktionsplänen, müssen sowohl im Falle vollautomatischer als auch autonomer Fahrerassistenz ausgeführt werden. Ziel ist immer eine Deaktivierung der Assistenzfunktion. Es ist hierbei jedoch zu unterscheiden, welche der Aufgaben der menschliche Fahrer und welche das FAS wahrnimmt bzw. wahrnehmen muss.

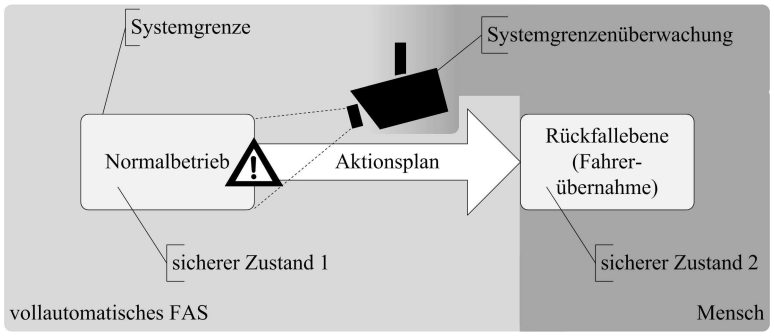

Bild 2.1: Strategie des Sicherheitskonzepts bei vollautomatischen Fahrerassistenzsystemen

Im Falle eines VA FAS erfolgt die Systemgrenzenüberwachung in weiten Teilen durch das FAS. Wird eine Systemgrenzenüberschreitung festgestellt, so wird ein Aktionsplan angesteuert, der zunächst eine Fahrerübernahmeaufforderung (FÜA) auslöst und danach die automatische Längs- und Querführung durch das FAS deaktiviert. Das System verlässt sich in diesem Fall auf den Fahrer als Rückfallebene. Der einzige sichere Rückfallebenenzustand stellt somit, wie auch bei semiautomatischen FAS (SA FAS), die Übernahme der kompletten Fahrzeugführung durch den menschlichen Fahrer dar (vgl. Bild 2.1).

Zudem muss ein Fehlverhalten des Systems im Normalbetrieb, das nicht durch das VA FAS detektiert wird, vom Fahrer erkannt und korrigiert werden. Entsprechende Beispiele für derartige Fehler sind bereits im Bereich SA FAS bekannt. So kann etwa beim ACC eine falsche Zielobjektauswahl zu einem Fehlverhalten, einer sogenannten Nebenspurstörung, führen (vgl. [Luh 2006]). Wie auch bei SA FAS muss der Nutzer eines VA FAS die

Systemüberwachung daher weiterhin unterstützen bzw. ständig plausibilisieren, ob das automatisch generierte Fahrverhalten sinnvoll ist. Stellt der Fahrer ein fehlerhaftes Verhalten fest, muss er korrigierend eingreifen.

Da der Fahrer also einerseits als Überwachungsinstanz und andererseits als Rückfallebene zwingend zur Verfügung stehen muss, ist neben einer systembezogenen Überwachung ebenfalls eine Fahrerüberwachungseinheit notwendig, die laufend überprüft, ob sich der Fahrer noch im Loop befindet. Wird erkannt, dass sich der Fahrer zu stark von seiner Überwachungsaufgabe zurückgezogen hat bzw. sich in einem Zustand befindet, der ihn nicht mehr schnell genug reagieren lässt, muss das VA FAS ebenfalls durch einen Aktionsplan deaktiviert werden.

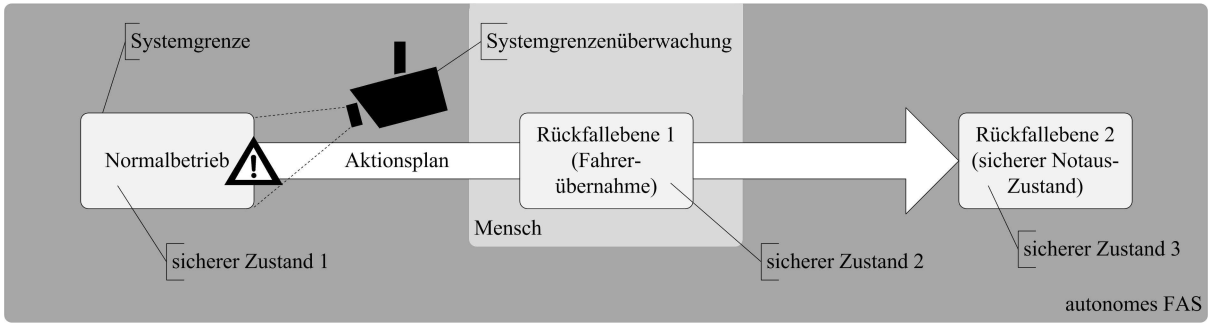

Bild 2.2: Strategie des Sicherheitskonzepts bei autonomen Fahrerassistenzsystemen

Da im Falle eines A FAS davon ausgegangen werden muss, dass der Fahrer Nebentätigkeiten nachgeht und er sich daher nicht mehr im Loop befindet, obliegt die Systemgrenzenüberwachung hier einzig und allein dem autonomen System. Das bedeutet, dass sämtliche Fehler, die eine nicht tolerierbare Beeinträchtigung des FAS-Verhaltens bzw. der Fahrzeuginsassen und des umliegenden Verkehrs zur Folge haben, vom System erkannt werden müssen. Dies gilt ebenfalls für die abschließende Plausibilisierung des automatisch generierten Fahrverhaltens, für die bei VA FAS noch der Fahrer zuständig ist. Die Anforderungen an die systembezogene Überwachung sind somit bei A FAS deutlich höher, wohingegen aber keine separate Fahrerüberwachung mehr notwendig ist.

Wurde vom System ein Fehler erkannt, so wird ein Aktionsplan angesteuert, der zunächst, wie im Falle eines VA FAS, eine FÜA auslöst. Falls der Fahrer jedoch nicht (rechtzeitig) eingreift bzw. eingreifen kann, sieht der Aktionsplan eine Übernahme der Längs- und optional der Querführung durch eine unterlagerte Komponente des Sicherheitskonzepts vor, die das Fahrzeug selbstständig in einen sicheren Notaus-Zustand überführt (vgl. Bild 2.2). Ein Fahrereingriff ist somit in letzter Konsequenz nicht mehr notwendig, um einen dauerhaft sicheren Zustand zu erreichen. Der anzustrebende Zustand dieser zweiten, systemeigenen Rückfallebene muss für jede autonome Assistenzfunktion eigens neu definiert werden. Das Fahrzeug verlässt diese Rückfallebene erst infolge einer expliziten Deaktivierung des A FAS, also einer Übernahme der Fahrzeugführung durch den Fahrer.

Es bedarf bei A FAS also einerseits Überwachungskomponenten, die in der Lage sind, ausnahmslos alle denkbaren Systemgrenzenüberschreitungen zu detektieren und andererseits Aktionsplänen, die das Fahrzeug in jedem dieser Fälle ohne Zutun des Fahrers in einen

sicheren, systemeigenen Notaus-Zustand überführen können. Derartige FAS sind somit die einzigen, die als eigensicher bezeichnet werden können.

2.2 Kerngebiete

Im Folgenden werden die Kerngebiete des Sicherheitskonzepts in Anlehnung an die [ISO DIS 26262: 2009] (vgl. Kapitel 1.3) aus den eben beschriebenen Strategien abgeleitet. Es handelt sich hierbei um verschiedene Aspekte der Systemgrenzenüberwachung, um Aktionspläne zur Erlangung eines sicheren Zustands und um architekturelle Aspekte des Sicherheitskonzepts. In diesem Zuge werden auch die Schwerpunkte dieser Arbeit definiert und die Relevanz der verschiedenen Themenbereiche für vollautomatische bzw. autonome FAS hervorgehoben.

2.2.1 Systemgrenzenüberwachung

Das folgende Bild 2.3 gibt eine Übersicht über die verschiedenen Kategorien von Systemgrenzen und die zugehörigen Detektionsmechanismen, die zur Überwachung vollautomatischer bzw. autonomer FAS entwickelt und implementiert werden müssen.

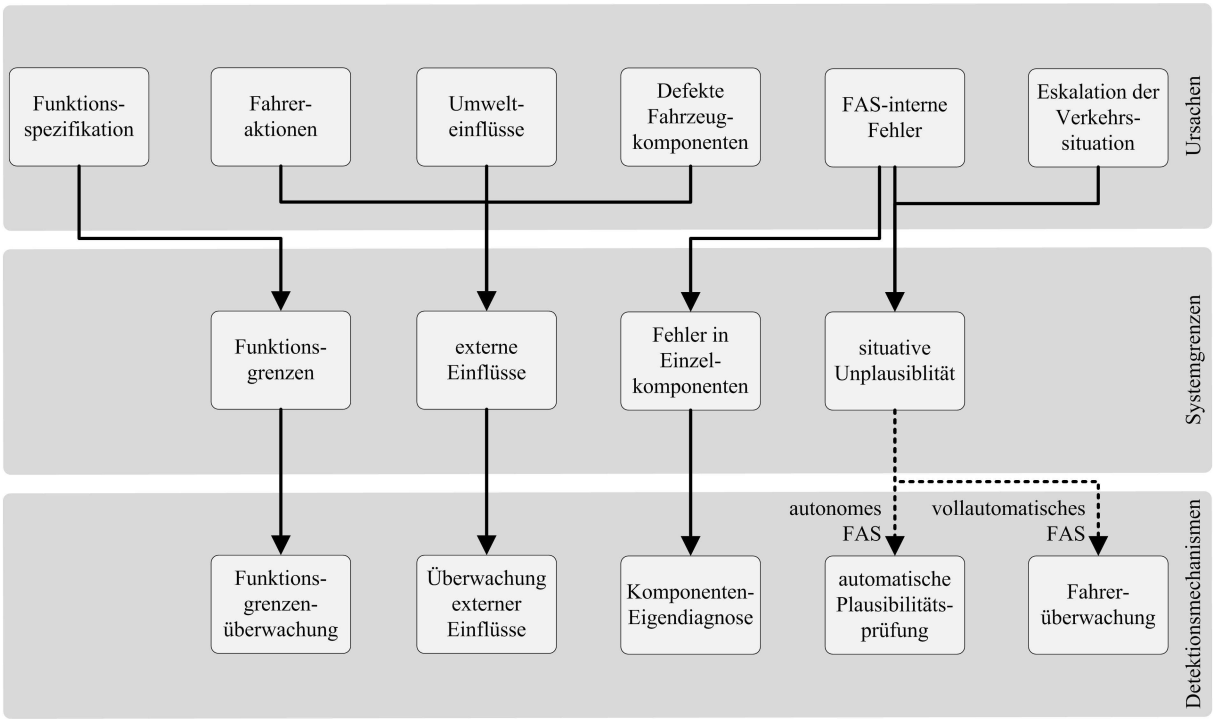

Bild 2.3: Systemgrenzen und zugehörige Detektionsmechanismen

Funktionsgrenzen können aus der Spezifikation und dem Einsatzbereich des jeweiligen FAS abgeleitet werden. Im Falle eines Stauassistenten (STA) muss hier im Wesentlichen überprüft werden, ob sich das STA-Fahrzeug im Stau auf einer Autobahn befindet (vgl. Kapitel 1.2) und ob die gewählte Fahrspur frei befahrbar ist und nicht durch stehende Hindernisse, wie beispielsweise ein Baustellenfahrzeug, blockiert wird oder endet. Im letzten Fall spricht man von einer sogenannten Systemblockade (engl. deadlock), die nur durch eine Fahrerübernahme aufgelöst werden kann, da der STA per Definition selbstständig keine Spurwechsel durchführen kann.

Externe Einflüsse ergeben sich durch untolerierbare Fahrer-Aktionen, beispielsweise dem Verlassen des Fahrzeugs im Stillstand bei aktiviertem FAS, durch negative Umwelteinflüsse wie beispielsweise Eisglätte und durch Defekte von Fahrzeugkomponenten, die nicht direkt mit dem FAS zusammenhängen, beispielsweise eine defekte Ölpumpe.

FAS-interne Fehler beruhen entweder auf Fehlfunktionen von Hardwarekomponenten des FAS oder auf der begrenzten Funktionalität von Softwarekomponenten. Beispiele hierfür sind Defekte in der Umfeld-Sensorik bzw. die Verletzung der Modellannahmen signalverarbeitender Softwarekomponenten. Letzteres tritt beispielsweise in einem Fahrstreifendetektor bei einem Wegfall der Spurmarkierungen auf. Theoretisch ist eine sehr große Zahl derartiger, unterschiedliche Fehler möglich, welche sich im Einzelnen nicht in einer standardisierten Weise überwachen lassen. Aus diesem Grund müssen diese Fehler von jeder Komponente einzeln, im Rahmen einer umfassenden Eigendiagnose, festgestellt werden. Ein Kernaspekt dieser Arbeit ist es, ein erweitertes Watchdog-Konzept zu entwickeln, das es Einzelkomponenten in einem verteilten FAS, bestehend aus mehreren Recheneinheiten, außerdem ermöglicht, intern festgestellte Fehler standardisiert zu melden und deren Auswirkung auf der Basis von a priori Wissen zu prädizieren.

Die Überwachung FAS-interner Fehler sollte im Rahmen eines Sicherheitskonzepts nicht ausschließlich auf der Eigendiagnose einzelner funktionaler Komponenten basieren, da derartige Module primär darauf ausgelegt sind, eine gewisse Funktion zu erfüllen und die Fähigkeit zur Eigendiagnose eine von vielen Anforderungen an das jeweilige Modul darstellt, der nicht immer mit letzter Konsequenz nachgekommen wird. Man sollte sich daher, falls möglich, nicht darauf verlassen, dass wirklich ausnahmslos alle internen Fehler über eine Komponenten-Eigendiagnose detektiert werden. Aus diesem Grund ist es sinnvoll, eine Art letzte, unterlagerte Kontrollinstanz vorzuhalten, die lediglich die Auswirkungen systeminterner Fehler auf das funktionale Gesamtverhalten des Fahrzeugs überschlagsmäßig überwacht und sogenannte situative Unplausibilitäten feststellt. Situative Unplausibilitäten sind in diesem Kontext kritische Fahrsituationen, die objektiv betrachtet gar nicht hätten zustande kommen dürfen. Im Falle des STA, der per Definition eine Querregelung bezüglich der Spurmitte realisiert, ist dies zum Beispiel ein Überfahren der eigenen Fahrstreifenmarkierung. Neben internen Fehlern, die im Rahmen der Eigendiagnose der Einzelkomponenten nicht erkannt wurden, kann auch eine plötzliche, dramatische Eskalation der Verkehrssituation im unmittelbaren Umfeld des eigenen Fahrzeugs zu derartigen Unplausibilitäten führen. Ein entsprechendes Beispiel ist das Herabfallen von Ladung vom Vorderfahrzeug des STA.

Wie bereits in Kapitel 2.1 angedeutet, soll die Überwachung und die Reaktion auf funktionale Unplausibilitäten bei VA FAS weiterhin durch den Fahrer geschehen. Um sicherzustellen, dass der Fahrer dieser Forderung nachkommt, ist eine Überwachungsinstanz notwendig, die kontinuierlich überprüft, ob sich der Fahrer der aktuellen Verkehrssituation noch bewusst ist und in einem Zustand befindet, der es ihm jederzeit umgehend ermöglicht, in adäquater Weise die komplette Fahrzeugführung zu übernehmen. Wird festgestellt, dass sich der Fahrer nicht mehr im Loop befindet, stellt dies ebenfalls eine Verletzung der Einschaltbedingungen dar, die eine Systemdeaktivierung zu Folge haben muss. Da der Fahrer bei einem VA FAS somit die letzte, absichernde Kontrollinstanz darstellt, sind die Anforderungen an die Güte der

Fahrerüberwachung sehr hoch. Einer der wichtigsten Kernaspekte dieser Arbeit stellt die Konzeptionierung eines umfassenden Fahrerüberwachungskonzepts für VA FAS dar, die, wie beispielsweise der vollautomatische STA, nur ein einziges Manöver automatisieren.

Da der Fahrer bei A FAS nicht mehr als Überwachungsinstanz zur Verfügung steht, muss die Erkennung funktionaler Unplausibilitäten hier durch das FAS selbst übernommen werden. Konkret muss in diesem Zusammenhang ein plausibilisierender Abgleich der Eigenbewegung des Fahrzeugs, die mittels Inertial-Sensorik erfasst wird, mit der Situation bzw. der Szene im unmittelbaren Umfeld des Fahrzeug, die durch Umfeld-Sensorik beobachtet wird, erfolgen. Wie bereits oben angedeutet, ist eine solche Überwachung von der Funktionsspezifikation des jeweiligen FAS abhängig. An dieser Stelle sei ausdrücklich darauf hingewiesen, dass eine automatische Plausibilitätsprüfung zwingend valide sensorische Umfelddaten erfordert und somit durch die Leistungsfähigkeit der sensorischen Wahrnehmung begrenzt ist. FAS-interne Fehler im Bereich der sensorischen Wahrnehmung müssen dagegen ausschließlich durch Komponenten-Eigendiagnose detektiert werden. Die automatische Plausibilitätsüberwachung für einen autonomen STA stellt einen der wichtigsten Kernaspekte dieser Arbeit dar.

Externe Einflüsse, Funktionsgrenzen und Fehler in Einzelkomponenten müssen im Prinzip in gleicher Weise bei VA FAS und A FAS überwacht werden. Allerdings sind die Anforderungen an die Qualität und die Vollständigkeit der Überwachung bei A FAS, insbesondere hinsichtlich der Eigendiagnose von Fehlern in Einzelkomponenten, beträchtlich höher, da eine automatische Plausibilitätsprüfung, anders als der Mensch, nicht über separate Sensorik und ein Situationsverständnis auf dem Niveau eines Menschen verfügt. Generell muss es das Ziel sein, alle relevanten Fehlermuster detektieren und entsprechend behandeln zu können. Man spricht in diesem Zusammenhang von der Forderung, dass im System ausschließlich sogenannte sichere Fehler (engl. safe faults) auftreten können dürfen (vgl. [ISO DIS 26262: 2009]).

Da im Kontext dieser Arbeit jedes einzelne Fehlermuster immer eine Deaktivierung des FAS zur Folge haben soll (vgl. Kapitel 2.1) werden keine Betriebsstörungen betrachtet, die sich infolge einer Kombination mehrerer, zeitlich versetzt auftretender Fehler ergeben können. Außerdem werden keine Komfortgrenzen überwacht, die nicht unmittelbar sicherheitskritische Auswirkungen haben.

2.2.2 Aktionspläne zur Erlangung eines sicheren Zustands

Aktionspläne zur Erlangung eines sicheren Zustands werden ausgeführt, wenn der sichere Normalbetriebszustand eines hochautomatisierten FAS (H FAS) infolge einer Systemgrenzenüberschreitung verlassen wurde. Sie definieren eine Abfolge verschiedener Aktionen, die das System „Fahrer-Fahrzeug-umliegender Verkehr“ wieder in einen sicheren Zustand überführen und gleichzeitig das FAS deaktivieren.

Im Falle eines VA FAS definiert der Aktionsplan einen Fahrerübergabeprozess, dessen wesentlicher Bestandteil eine FÜA ist, in deren Folge davon ausgegangen wird, dass der Fahrer die Fahrzeugführung wieder übernimmt und somit wieder einen sicheren Zustand herstellt. Greift der Fahrer nicht ein, so sieht der Aktionsplan nach einiger Zeit eine

vollständige Deaktivierung des FAS bzw. der entsprechenden Fahrzeugführungsfunktion vor. Dieses Vorgehen ist zulässig, da davon ausgegangen werden darf, dass sich der Fahrer zu jeder Zeit im Loop befindet. Wird von einer gesonderten Überwachungsinstanz das Gegenteil festgestellt, so wird der Fahrer aufgefordert die ausgeführte Nebentätigkeit einzustellen. Kommt er dieser Aufforderung nicht nach, so wird, auch wenn sich das FAS in einem sonst voll funktionsfähigen Zustand befindet, ebenfalls ein FÜA angestoßen und das FAS deaktiviert.

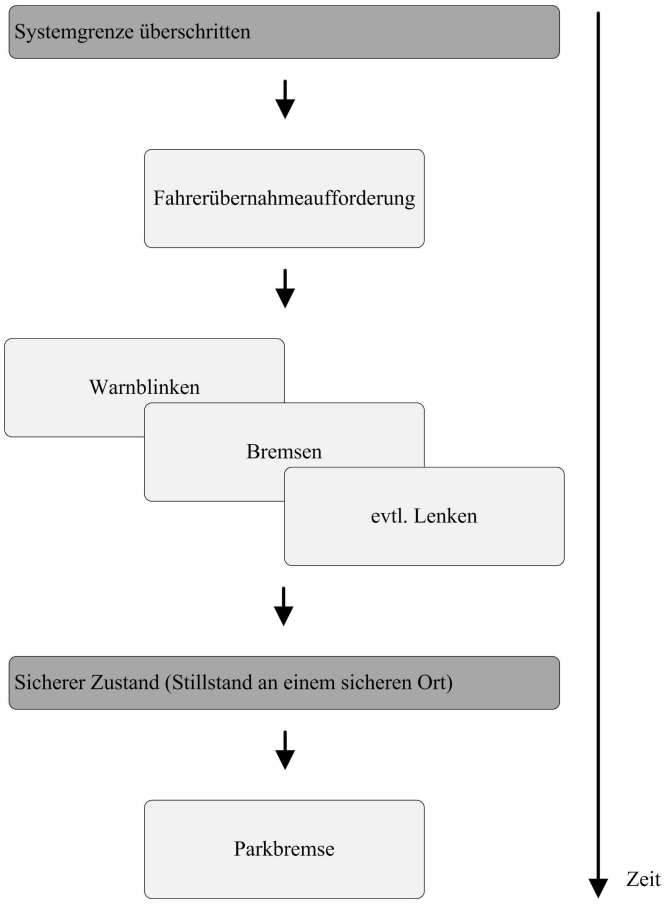

Bild 2.4: Aufbau von Aktionsplänen für autonome Fahrerassistenzsysteme

Die Aktionspläne für A FAS (vgl. Bild 2.4) unterscheiden sich grundsätzlich von jenen für VA FAS, wobei auch hier nach Überschreitung einer Systemgrenze zunächst immer erst eine FÜA ausgelöst wird[1]. Falls der Fahrer eingreift, wird wie im vollautomatischen Fall, die automatische Fahrzeugführung deaktiviert und in den manuellen Fahrbetriebsmodus übergegangen. Da der Fahrer bzw. Nutzer eines A FAS per Definition in umfangreicher Weise Nebentätigkeiten nachgehen kann und eine Fahrerübernahme somit nicht immer rechtzeitig möglich ist, sehen Aktionspläne für A FAS nach einer gewissen Zeit, in der kein Fahrereingriff erfolgt ist, einen kontinuierlichen Eingriff in die Fahrzeugführung vor, durch den das Fahrzeug automatisch in einen definierten, sicheren Zustand manövriert wird. Gleichzeitig wird auch der umliegende Verkehr durch die Betätigung der Warnblinkanlage

[1] Im Rahmen dieser Arbeit wird davon ausgegangen, dass die Auslösung einer FÜA in vollautomatischen oder autonomen FAS nur durch Aktionspläne des Sicherheitskonzepts erfolgen kann.

gewarnt. Man bezeichnet ein derartiges Vorgehen als aktives Fail-Safe (FS). Sämtliche durch den Aktionsplan angesteuerten Aktionen werden deaktiviert, sobald der Fahrer in die Fahrzeugführung eingreift. Der anzustrebende sichere FS-Zustand ist abhängig von der Funktionsspezifikation. Einer der wichtigsten Kernaspekte dieser Arbeit stellt die Konzeptionierung von Aktionsplänen für einen autonomen STA dar. Wie später noch genau erörtert wird, ist der sichere Zustand dieses FAS der Stillstand innerhalb der eigenen Fahrspur (vgl. Kapitel 8.1). Um genau diesen Zustand zu erreichen, ist neben einer Übersteuerung der Längsführungsstellgrößen der Normalfunktion[2] mit einem definierten Verzögerungswert (überlagerte Bremsung) in einigen Fällen auch eine Übersteuerung der Querführungsstellgrößen der Normalfunktion (überlagertes Lenken) notwendig. Generell muss es das Ziel sein, mit möglichst wenigen Aktionsplänen bei entsprechender Parametrierung auf alle möglichen Systemgrenzenüberschreitungen reagieren zu können. Neben aktivem FS existieren auch andere Strategien, um auf Fehler zu reagieren, die eine Aufrechterhaltung des Betriebs zum Ziel haben. Auf diese Strategien soll aber in dieser Arbeit nicht eingegangen werden.

2.2.3 Funktionale Architektur

Für die Realisierung der beiden Hauptaufgaben des Sicherheitskonzepts (Systemgrenzenüberwachung und Vorhaltung von Aktionsplänen zur Erlangung eines sicheren Zustands) ist ein entsprechendes funktionales Architekturkonzept notwendig, das auf der funktionalen Architektur existierender H FAS, bestehend aus Sensoren, Aktoren und funktionalen Software-Komponenten, aufbaut. Ein wichtiger Kernaspekt dieser Arbeit ist daher die Definition relevanter überwachender bzw. Aktionen ansteuernder Software-Komponenten sowie deren Einbettung und Interaktion in bestehenden Architekturschemata (vgl. Bild 2.5). Die angesprochene Interaktion erfolgt über definierte Schnittstellen und betrifft dabei sowohl das Zusammenspiel der Komponenten des Sicherheitskonzepts untereinander, als auch deren Zusammenspiel mit den Komponenten der Normalfunktion. Bei A FAS ist in diesem Zusammenhang unter anderem eine spezielle Entscheidungslogik zu konzipieren, die definiert, wie bei einer Längs- und Querführungs-Anforderung durch einen Aktionsplan eine Übersteuerung der Fahrzeugregelgrößen der Normalfunktion erfolgt.

[2] Mit dem Begriff Normalfunktion werden alle Komponenten eines FAS bezeichnet, die für die Realisierung einer kundenwerten Funktion notwendig, jedoch nicht Bestandteil des Sicherheitskonzepts sind (vgl. Bild 4.1).

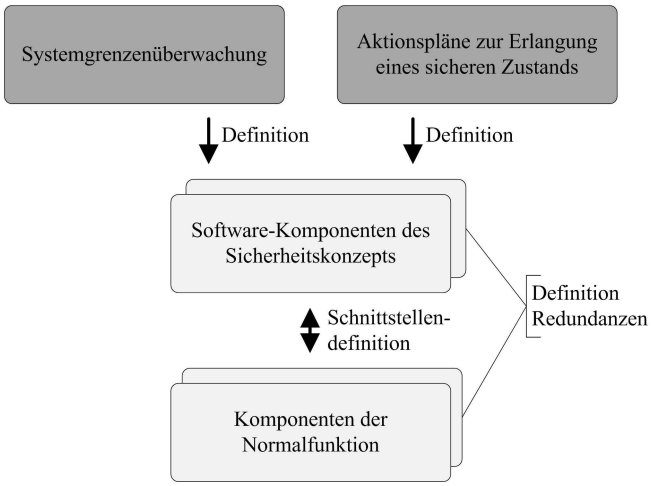

Bild 2.5: Inhalte des funktionalen Architekturkonzepts

Um sicherzustellen, dass alle Systemgrenzenüberschreitungen in die Kategorie der sicheren Fehler fallen (vgl. Kapitel 2.2.1), sind neben einer umfangreichen Systemgrenzenüberwachung und dem Vorhalten entsprechender Aktionspläne auch Redundanzen notwendig. Unter Redundanz wird prinzipiell das mehrfache Vorhandensein gleicher oder ähnlicher Komponenten verstanden. Die Beschreibung von Redundanzanforderungen ist ein weiterer Kernaspekt dieser Arbeit. Prinzipiell erscheinen Redundanzen aus den folgenden drei Gründen notwendig:

- Fehleridentifikation: Die Identifikation unplausibler Sensordaten ist ausschließlich durch den Vergleich dieser Daten mit den Daten eines redundanten Sensors möglich. Redundante Sensoren sind besonders bei A FAS notwendig, da die automatische Plausibilitätsprüfung derartige Fehler nicht abfangen kann (vgl. Kapitel 2.2.1).
- Fehlerbehebung: Um sicherzustellen, dass bei A FAS, auch im Falle eines Ausfalls eines elektronisch ansteuerbaren Aktors zur Fahrzeugführung, immer automatisch ein sicherer FS-Zustand erreicht werden kann, sind derartige Aktoren redundant vorzusehen.
- Aufrechterhaltung eines funktionsfähigen Zustands des Sicherheitskonzepts: Da die Software-Komponenten des Sicherheitskonzepts durch einen Absturz der Recheneinheit, auf der sie implementiert sind, ausfallen können, müssen auch diese Komponenten redundant auf verschiedenen Recheneinheiten vorhanden sein. Auf diese Weise wird sichergestellt, dass auch Ausfälle von Komponenten des Sicherheitskonzepts erkannt werden können und eine sicherheitsgerichtete Ausfallreaktion möglich ist.

Konkretere Redundanz-Anforderungen müssen erst im Rahmen der Serienentwicklungsphase definiert werden, da erst hier die konkrete Hardware-Architektur festgelegt wird (vgl. [ISO DIS 26262: 2009]).

2.3 Übergeordnete Prinzipien

In den vorangegangenen Kapiteln wurden bereits einige grundlegende, übergeordnete Prinzipien angedeutet, die bei der Entwicklung des Sicherheitskonzepts beachtet werden müssen. Sie werden an dieser Stelle vervollständigt und gebündelt aufgelistet.

- Einfachheit und Prädizierbarkeit: Je geringer die Komplexität der Mechanismen des Sicherheitskonzepts ist, desto fehlerunanfälliger sind die Mechanismen. Zudem werden die Ausfallreaktionen des Gesamtsystems auf diese Weise für sämtliche Fehlerfälle vorhersehbar und nachweisbar, was eine methodische Bewertung der Systemsicherheit ermöglicht.
- Vollständige Fehlererkennung: Das Sicherheitssystem muss alle Systemgrenzenüberschreitungen detektieren können.
- Garantie eines sicheren Zustands: Für jede detektierbare Systemgrenzenüberschreitung muss ein Aktionsplan existieren, der das Fahrzeug wieder in einen sicheren Zustand überführen kann. Wird auch das Prinzip der vollständigen Fehlererkennung eingehalten, so existieren für das System nur sichere Fehler.
- Prävention: Je früher und schneller Fehler erkannt werden, umso früher lassen sich deeskalierende Aktionen einleiten. Auf diese Weise wird vermieden, dass sich die Auswirkungen von Fehlern fortpflanzen, die Situation weiter eskaliert und dadurch heftigere Aktionen notwendig werden, um einen sicheren Zustand zu erreichen.
- Echtzeitfähigkeit: Zur Einhaltung des Prinzips der Prävention ist die Forderung nach Echtzeitfähigkeit aller Komponenten des Sicherheitskonzepts Voraussetzung. So muss nach der Detektion einer Systemgrenzenüberschreitung schnellstmöglich wieder ein sicherer Zustand des Fahrzeugs hergestellt werden. Daher sollte vor allem der Eingriff in die Fahrzeugführung im Falle eines A FAS möglichst direkt ohne Umwege erfolgen.
- Trennung vom Gesamtsystem: Im Rahmen der Auslegung der funktionalen Systemarchitektur muss auf eine klare Trennung zwischen den Komponenten der Normalfunktion und den Komponenten des Sicherheitskonzepts geachtet werden. Die notwendigen Schnittstellen zwischen diesen beiden Bereichen sollten wohl definiert und auf ein Minimum begrenzt sein. Auf diese Weise werden Abhängigkeiten reduziert und die systeminterne Kommunikation transparent, was wiederum die Einfachheit und Prädizierbarkeit verbessert (vgl. erster Punkt).
- Modularität und Adaptierbarkeit: Das Sicherheitskonzept sollte modularen Charakter haben und sich an spezielle Funktionsspezifika und Systemarchitekturen anpassen lassen können. Vor allem Letzteres ist notwendig, da die Definition der finalen Systemarchitektur mit der Konzeptentwicklungsphase noch nicht abgeschlossen ist.

2.4 Abgrenzung

Das in dieser Arbeit vorgestellte funktionale Sicherheitskonzept umfasst alle Inhalte, die im Rahmen der Konzeptphase zu entwickeln sind. Wie bereits angedeutet, ist es von einem technischen Sicherheitskonzept zu unterscheiden, das erst im Rahmen des Serienentwicklungsprozesses zu entwickeln ist. Es werden daher keine konkreten Anforderungen erarbeitet und vorgestellt, die beschreiben, wie die einzelnen funktionalen Aspekte im Detail zu implementieren sind und welchen Hardware- und Software-Komponenten sie endgültig zuzuordnen sind. Außerdem werden keine Forderungen hinsichtlich der Produktion, des Gebrauchs, der Wartung und Außerbetriebnahme von H FAS formuliert. (vgl. [ISO DIS 26262: 2009])

Folgende Aspekte stehen ebenfalls nicht im Fokus dieser Arbeit:

- Fehlerdetektion und Fehlerdiagnose: Es existieren verschiedene Mechanismen zur Erkennung und Klassifikation von Fehlern, die im Rahmen der Eigendiagnose von Einzelkomponenten angewendet werden müssen. Sie werden im Stand der Technik im nächsten Kapitel kurz vorgestellt. Die Anwendung auf konkrete Problemstellungen ist Teil der Entwicklung der verschiedenen speziellen Einzelkomponenten.
- Strategien zur Aufrechterhaltung des Betriebs infolge eines Fehlers: Die vorliegende Arbeit beschäftigt sich in erster Linie mit Mechanismen zur kontrollierten Deaktivierung von vollautomatischen und autonomen FAS. Im Fehlerfall wird daher immer ein definierter Notaus-Zustand angestrebt. Überdies existieren andere Ausfallreaktionen, wie beispielsweise die Selbstheilung des Systems durch den Neustart von Systemkomponenten oder die Degradierung des Systems in einen anderen Betriebsmodus, der nur noch eine eingeschränkte Funktionalität zur Verfügung stellt. Derartige Mechanismen werden der Vollständigkeit halber ebenfalls im Stand der Technik kurz vorgestellt.
- Absicherung durch Testen: Im Rahmen der Entwicklung eines H FAS ist die Absicherung der entwickelten Fahrerassistenzfunktion durch systematische Tests in Simulation und Realität zwingend erforderlich. Allerdings spielen derartige Untersuchungen in der Konzeptentwicklungsphase eine untergeordnete Rolle, da die Systeme noch nicht detailliert genug spezifiziert sind und die Entwicklungsreife der Funktionen noch nicht hoch genug sind.
- Mensch-Maschine-Schnittstelle: Im Falle von Systemgrenzenüberschreitungen sind FÜA notwendig, die visueller, akustischer und haptischer Natur sein können. Um den Fahrer schnellst- und bestmöglich reagieren zu lassen, sind daher über diese Arbeit hinaus Konzepte zu entwickeln, die vor allem ergonomische und psychologische Aspekte berücksichtigen und durch aufwendige Benutzerstudien abgesichert sind.

3 Stand der Technik

Da, wie bereits erläutert, kein umfassendes funktionales Sicherheitskonzept für vollautomatische und autonome Fahrerassistenzsysteme (FAS) existiert, wird in diesem Kapitel der Stand der Technik relevanter Aspekte bezüglich der in Kapitel 2 erarbeiteten Kerngebiete erörtert. Zunächst soll einleitend ein Überblick über die grundsätzliche Vorgehensweise bei der Überwachung und Behebung von Fehlern in technischen Systemen gegeben werden (Kapitel 3.1). Danach wird auf die für vollautomatische FAS (VA FAS) und autonome FAS (A FAS) wichtigen Aspekte der Systemgrenzenüberwachung genauer eingegangen (Kapitel 3.2). Im Anschluss werden die, vor allem als Voraussetzung für eine spätere Fehlerbehandlung notwendigen, grundlegenden Redundanzmechanismen vorgestellt (Kapitel 3.3). Da, wie in Kapitel 2.1 ausgeführt wurde, bei dem hier vorgeschlagenen Sicherheitskonzept im Fehlerfall immer eine Deaktivierung des FAS angestrebt wird, gibt Kapitel 3.4 einen Überblick über die Deaktivierungsprozesse automatischer, bewegter Systeme. Eine Betrachtung des Deaktivierungsprozesses eines Kernkraftwerks, als hochgradig sicherheitskritisches System, rundet diesen Abschnitt ab (Kapitel 3.5).

3.1 Der Überwachungs- und Fehlerbehandlungsprozess

Im Folgenden soll ein kurzer Überblick über den allgemeinen Prozess zur Erkennung und Behandlung in technischen Systemen intern auftretender Fehler gegeben werden. Dazu wird das folgende Bild 3.1 betrachtet:

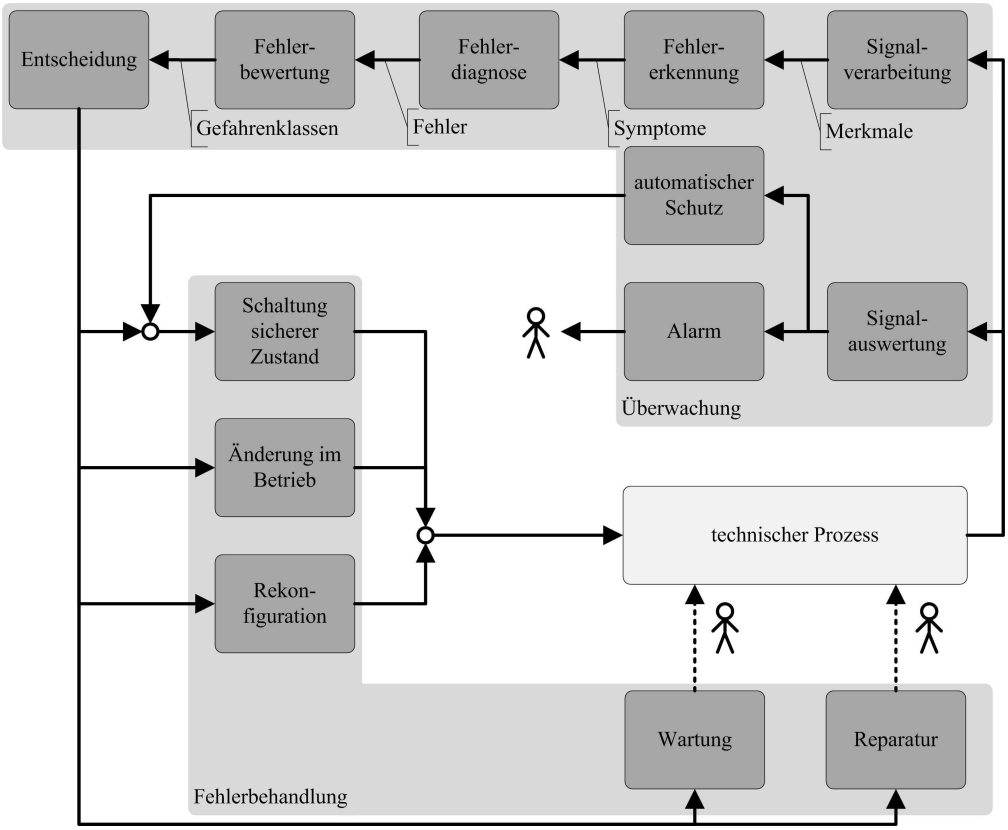

Bild 3.1: Übersicht über den Überwachungs- und Fehlerbehandlungsprozess nach [Isermann 2010]

Ausgangspunkt ist ein allgemeiner, technischer Prozess bzw. ein System (vgl. Mitte des Bildes). Fehler im System können durch die Messung von Abweichungen der Ausgangsgrößen erkannt werden. Im einfachsten Fall erfolgt die Fehlererkennung durch eine Grenzwertüberwachung, bei der überprüft wird, ob die Messwerte innerhalb einer festgelegten Toleranzzone liegen. Wird durch diese Signalauswertung eine unzulässige Abweichung festgestellt, so wird an den Bediener eine Alarmmeldung ausgegeben, der daraufhin entsprechende Gegenmaßnahmen einleiten muss. Für gefährliche Fehlerfälle, die der Mensch nicht schnell genug oder adäquat beheben kann, ist eine automatische Schutzvorrichtung vorzusehen, die das System automatisch in einen sicheren Zustand überführt. Da eine reine Grenzwertüberwachung nur ein oberflächliches Verfahren zur Erkennung großer Schwankungen darstellt und daher in vielen Fällen eine rechtzeitige, gezielte Einleitung von Gegenmaßnahmen unmöglich ist, ist es notwendig, zusätzliche Informationen über den Prozess- bzw. den Systemzustand zu generieren. Dazu wird oftmals zusätzliche Sensorik verbaut und der dadurch erweiterte Satz an Messgrößen als Eingang für mathematische Prozessmodelle verwendet, die das Systemverhalten beschreiben und dadurch eine rechtzeitige, gezielte Fehlerbestimmung ermöglichen. Das Vorgehen gliedert sich hierbei in mehrere Stufen. In einem ersten Schritt werden die sensorisch erfassten Daten in einem Signalverarbeitungsschritt zu Prozess beschreibenden Merkmalen und Kenngrößen aufbereitet. Aus der Beobachtung der Wertänderungen der Merkmale leitet die eigentliche Fehlererkennung dann Fehler beschreibende Symptome ab, die bereits frühzeitig auf einen Fehler hinweisen. Die nachfolgende Fehlerdiagnose bestimmt auf Basis der festgestellten Symptome unter Verwendung von digitalisiertem Prozesswissen den Fehler bzw. die eigentliche Fehlerursache. Für die Fehlererkennung und die Fehlerdiagnose existieren

vielfältige Methoden, die ausführlich in [Isermann 2010] beschrieben sind. Abschließend ordnet ein Fehlerbewertungsschritt den Fehlern Gefahrenklassen zu, die als Basis für die Entscheidung für eine den Fehler behebende Aktion dienen. (vgl. [Isermann 2010])

Diese prinzipielle Vorgehensweise der modellbasierten Fehlererkennung wird auch bei Steuerungs- und Regelungsfunktionen im Automobilbereich angewendet, wobei hier neben der Regelstrecke auch die Aktoren und die Sensoren gesondert modelliert werden und die Fehlerbehandlung meist direkt auf den erkannten Symptomen aufsetzt (vgl. Bild 3.2):

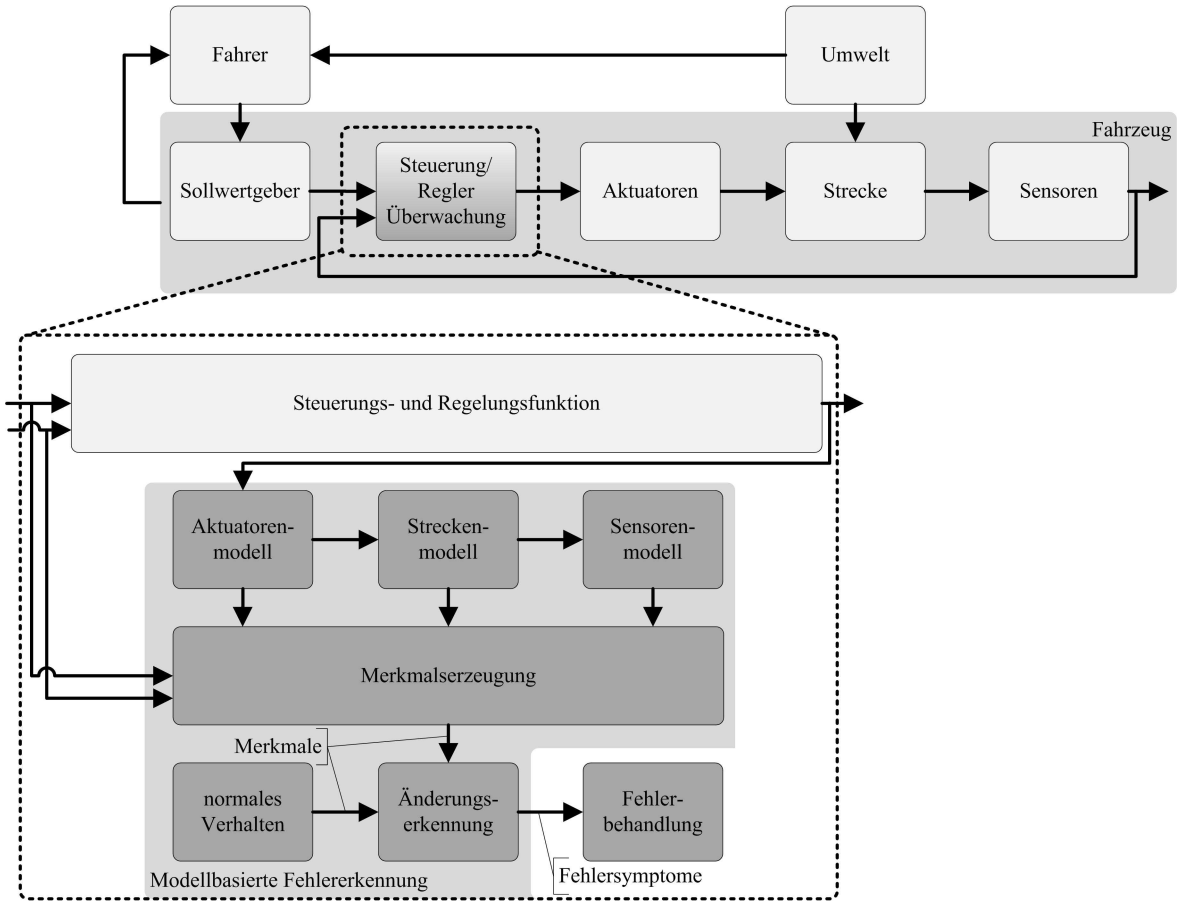

Bild 3.2: Modelbasierte Fehlererkennung im Automobilbereich nach [Schäuffele & Zurawka 2006]

Neben der internen Überwachung von Steuerungs- und Regelungsfunktionen auf einem Steuergerät (vgl. Kapitel 3.2.2.1) werden im Automobilbereich auch die Programmausführung mittles Watchdogmechanismen (vgl. Kapitel 3.2.2.2) und die Kommunikation zwischen Steuergeräten überwacht (vgl. [Schäuffele & Zurawka 2006]).

Die Aufgabe der Fehlerbehandlung, oft auch als Fehlermanagement bezeichnet, ist die Absicherung der potentiell in einem System auftretenden Fehler und damit der Erhalt der Betriebszuverlässigkeit. Eine hohe Betriebszuverlässigkeit kann hierbei entweder durch den Ansatz der Perfektion oder der Fehlertoleranz erreicht werden. Die Perfektion hat das Ziel, Fehler durch methodisches Vorgehen im Produktentwicklungsprozess und durch laufende Instandhaltung des Systems während des Betriebs generell zu vermeiden. Dem entgegen steht der Ansatz der Fehlertoleranz, der das Ziel hat, Fehler unter der Verwendung von Redundanzen (vgl. Kapitel 3.3) zu kompensieren bzw. zu beheben. Die Aktionen, die im Rahmen einer Fehlertoleranzstrategie eingesetzt werden, können während des laufenden

Betriebs oder danach erfolgen. Nach dem Betrieb lassen sich, oftmals auf der Basis von gespeicherten Fehlerdaten, gezielt Wartungs- und Reparaturarbeiten zur Instandhaltung des Systems durchführen. In vielen Fällen ist jedoch noch vor Beendigung des Betriebs eine Reaktion auf den aufgetretenen Fehler notwendig. Das System kann beispielsweise in einen sicheren Zustand geschaltet, rekonfiguriert oder der Betriebsmodus geändert werden (vgl. Bild 3.1). (vgl. [Isermann 2010])

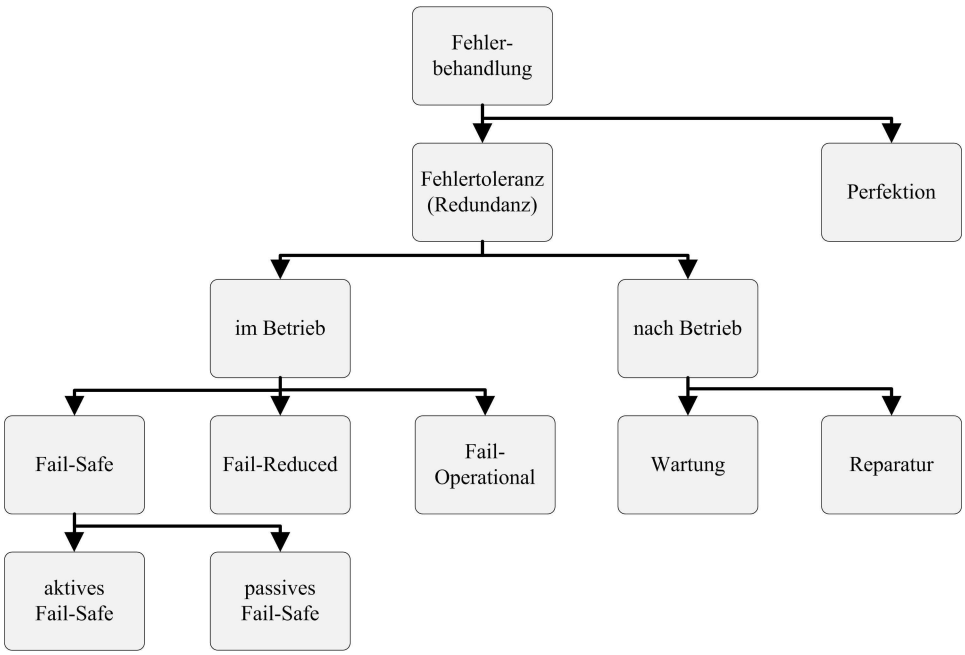

Bild 3.3: Alternative Fehlerbehandlungsmechanismen

Für diese Arbeit sollen die Fehlerbehandlungsmaßnahmen zur Laufzeit, etwas anders als bei [Isermann 2010], unter besonderer Beachtung des sicheren Zustands des Systems, klassifiziert werden (vgl. Bild 3.3).

Ist ein sicherer Zustand technisch nicht möglich, muss auf ein „Ersatzsystem als Rückfallebene umgeschaltet werden“. Man bezeichnet ein System mit einer solchen Sicherheitsreaktion als Fail-Operational-System. Kann dagegen ein sicherer Zustand eingenommen werden, oftmals ist dies der Not-Aus-Zustand, „kann eine Sicherheitsreaktion aus der Einleitung dieses Zustands bestehen“. Man spricht dann von Fail-Safe (FS) bzw. FS-Verhalten. Der sichere Zustand muss dabei dauerhaft sein und darf nur kontrolliert wieder verlassen werden können. „Folgt aus der Einnahme eines sicheren Zustands eine Betriebshemmung, so spricht man von einem Fail-Reduced-System. Dabei ist eine weitere, wenn auch reduzierte oder eingeschränkte Funktionsfähigkeit des Systems gegeben, wie zum Beispiel im Notlauf“. (vgl. [Schäuffele & Zurawka 2006])

Im Bereich der Eisenbahnanwendungen wird der Begriff FS auch in einer Norm definiert. Er wird hierbei beschrieben, als das „Konzept, das in den Entwurf eines Produktes so einfließt, dass bei Eintreten einer Fehlfunktion ein sicherer Zustand eingenommen oder beibehalten wird“, wobei dies durch eine „sicherheitsgerichtete Ausfallreaktion“ erreicht wird (vgl. [DIN EN 50129: 2003]).

Weiterhin unterscheidet man unter anderem in der Bahnsicherungstechnik zwischen dem passiven (auch echten) und aktiven FS-Konzept (auch Quasi-FS). Bei ersterem wird

automatisch, ohne weiteres Zutun, nach dem Auftreten einer Fehlfunktion ein sicherer Zustand eingenommen. Im Unterschied dazu muss beim Quasi-FS-Prinzip durch äußere oder systeminterne Handlungen der neue sichere Zustand gezielt angesteuert werden, bevor er schlussendlich erreicht wird. Dies verlangt im Vergleich zum passiven FS zusätzlich überwachende Elemente, die das Fehlverhalten der Komponenten zunächst registrieren. Je nach System kann es auch mehrere sichere Zustände geben, die hierarchisch geordnet sind und bei mehreren aufeinander folgenden Ausfällen nacheinander eingenommen werden können. Man spricht in diesem Zusammenhang von Rückfallebenen. Es sei an dieser Stelle darauf hingewiesen, dass auch der Normalbetrieb bei „fehler- und ausfallfreier Funktion“ einen sicheren Zustand darstellt, nämlich den „sicheren Ausgangszustand“. (vgl. [Fenner et al. 2003])

Die ausgeführten Begrifflichkeiten und Konzepte aus der Bahntechnik werden in dieser Arbeit auf VA FAS sowie A FAS übertragen und wurden bereits in Kapitel 2.1 verwendet.

3.2 Systemgrenzenüberwachung

Der Stand der Technik bezüglich der in Bild 2.3 dargelegten Systemgrenzen automatischer Fahrfunktionen bzw. der entsprechenden Detektionsmechanismen ist Inhalt dieses Unterkapitels. Es wird dabei auf die Überwachung externer Einflüsse im Rahmen des Stillstandsmanagements moderner Assistenzfunktionen, auf die Überwachung bzw. Eigendiagnose systeminterner Fehler im Automotive-Bereich und auf verschiedene Ansätze zur Fahrerüberwachung eingegangen. Die Funktionsgrenzenüberwachung kann nicht verallgemeinernd betrachtet werden, da sie für jede FAS-Funktion speziell ausgelegt werden muss (vgl. Betrachtung zum Stauassistenten in Kapitel 5.3). Sie ist deshalb nicht Inhalt dieses Abschnitts. Mit hochautomatisierten FAS (H FAS) vergleichbare Systeme, bei denen eine automatische Plausibilitätsprüfung des funktionalen Gesamtverhalten des Fahrzeugs durchgeführt wird, sind trotz intensiver Recherche nicht bekannt und aus diesem Grund ebenfalls nicht Inhalt dieses Unterkapitels.

3.2.1 Überwachung externer Einflüsse im Rahmen des Stillstandsmanagements

Im Rahmen des Stillstandsmanagements moderner Fahrzeuge werden verschiedene Aspekte überwacht, die sich in die Gruppe der externen Einflüsse einordnen lassen.

Das Stillstandsmanagement betrifft alle „Assistenzsysteme, die das Fahrzeug lang anhaltend autark über die Einrichtung der Betriebsbremse im Stillstand halten können“ (vgl. [Wohland 2007]). Ein entsprechendes Beispiel ist ACC S&G. Das Stillstandsmanagement formuliert und überprüft sowohl Einschaltvoraussetzungen für derartige Funktionen als auch Voraussetzungen für das automatisch angesteuerte Lösen der Parkbremse durch diese Funktionen. Bei Daimler wird unter anderem kontrolliert, ob der Motor läuft, die Motorhaube und der Kofferraumdeckel geschlossen ist und der Fahrer im Fahrzeug anwesend ist.

Letzteres geschieht durch die Überprüfung des Gurtschloss- und des Türkontaktsensors. (vgl. [Wohland 2007])

BMW führt ebenfalls ein Stillstandsmanagement durch und überwacht hierbei ebenfalls die Fahreranwesenheit durch Tür- und Gurtkontrolle, sowie durch einen zusätzlichen Sitzbelegungssensor (vgl. [Esch & Kern 2007]). Außerdem findet eine Überprüfung der Temperatur von Bremse und Bremsventilen statt. (vgl. [Pfeiffer et al. 2007])

Auch Audi überprüft im Rahmen seines Stillstandsmanagements unter anderem Türkontakte und die Aktivität des Motors (vgl. [Breu & Maurer 2007]).

3.2.2 Überwachung systeminterner Fehler

Zur Überwachung systeminterner Fehler werden in elektronischen Fahrzeug-Steuergeräten heute umfangreiche Überwachungs- und Diagnosesysteme für Steuergeräte-Hardware und die darauf implementierte Software verwendet. Sie werden im folgenden Abschnitt kurz beschrieben. In einem eigenen Abschnitt wird zudem genauer auf die darin implementierten Watchdogmechanismen eingegangen.

3.2.2.1 Überwachung von Automotive-Steuergeräten

Bild 3.4 gibt einen schematischen Überblick über das Überwachungs- und Diagnosesystem eines Steuergeräts:

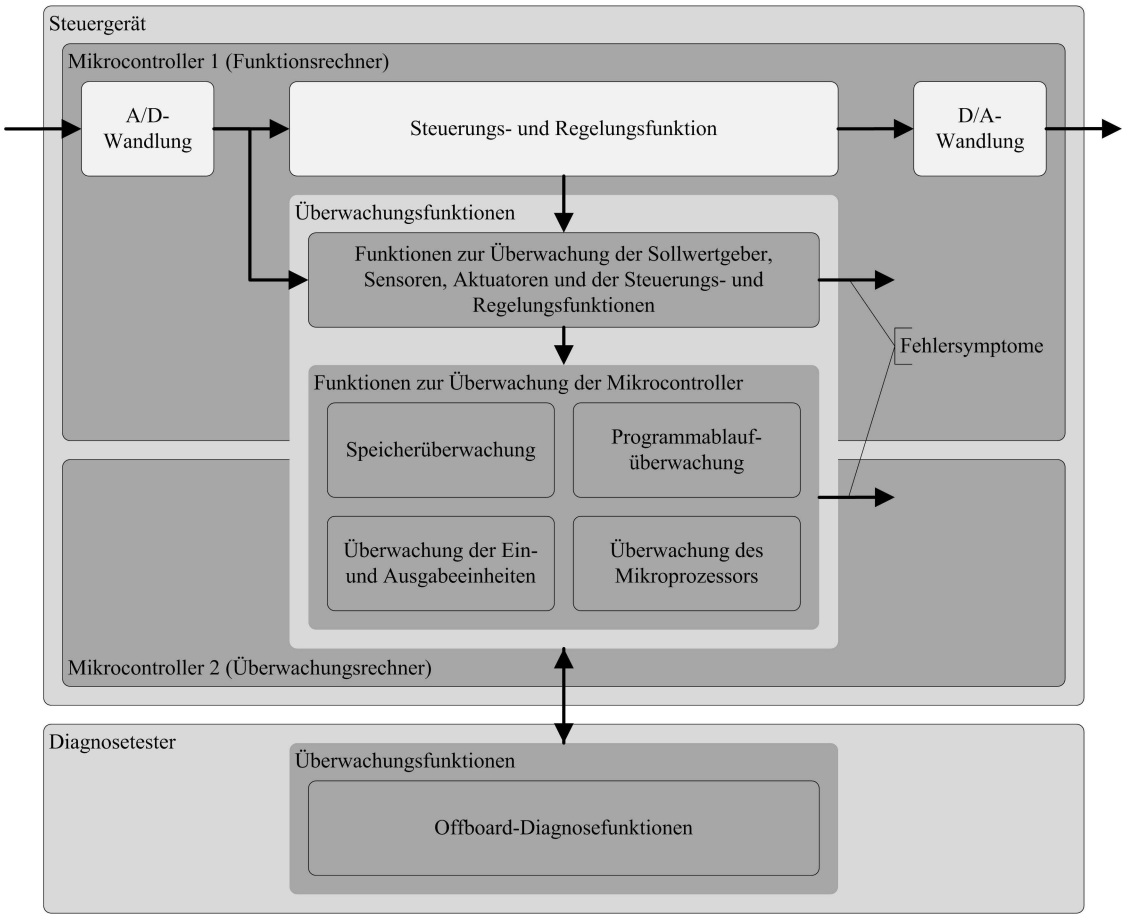

Bild 3.4: Überwachung von Automotive-Steuergeräten (vgl. [Schäuffele & Zurawka 2006])

Im Bild sind zwei Überwachungsebenen des Steuergeräts dargestellt. Die untere übernimmt die Überwachung der Hardware, also des Mikrocontrollers auf dem die Steuerungs- und Regelungsfunktion implementiert ist, wohingegen die obere die Überwachung der SW-Funktion (engl. software) selbst, sowie der zugehörigen Sollwertgeber, Sensoren und Aktuatoren übernimmt. „Für die Überwachung eines Mikrocontrollers ist in der Regel ein zweiter sogenannter Überwachungsrechner notwendig“, wobei „die Software-Funktionen zur Überwachung der Mikrocontroller (…) auf Funktions- und Überwachungsrechner verteilt“ sind und sich beide Rechner gegenseitig überwachen. Die Funktionen zur Überwachung des Mikrocontrollers überprüfen hauptsächlich während der Initialisierung und im Nachlauf, nach Abstellen des Fahrzeugs, die Funktionsfähigkeit des Prozessors sowie der zugehörigen Speicher- und Ein-/Ausgabeeinheiten. Während der Laufzeit findet außerdem eine Programmablaufüberwachung statt, die in der Regel auf Watchdog-Schaltungen basiert (vgl. Kapitel 3.2.2.2). (vgl. [Schäuffele & Zurawka 2006])

Zudem kann der Überwachungsrechner im laufenden Betrieb Referenzinformationen, die er in der Initialisierungsphase vom Funktionsrechner erhält, mit Statusinformationen, die er zur Laufzeit erhält, oder mit selbst generierten Informationen vergleichen und so untolerierbare Abweichungen feststellen (vgl. [Michel 1992]).

Die Überwachung der Steuerungs- und Regelungsfunktion selbst (vgl. Bild 3.2), geschieht auf Basis ihrer berechneten Ausgangswerte. Diese werden „häufig anhand der Ausgangswerte einer vereinfachten Überwachungsfunktion auf Plausibilität überprüft“. Sollwertgeber und

Sensoren werden ebenfalls einer Plausibilitätskontrolle unterzogen, die meist durch das „Ausnützen bekannter physikalischer Zusammenhänge zwischen verschiedenen Sollwertgeber- und Sensorsignalen“ oder durch eine einfache Überprüfung auf Grenzwertüberschreitungen erfolgt. Zudem werden die Versorgungsspannungen zum Betrieb dieser Komponenten und die Intaktheit der Verbindungsleitungen überwacht. Bei den Aktuatoren werden ebenso die Verbindungsleitungen kontrolliert und die während der Ansteuerung aufgenommenen Stromwerte mit definierten Grenzwerten verglichen. Erkennt eine der beschriebenen Überwachungsfunktionen einen Fehler, so erfolgt ein Eintrag in einen Fehlerspeicher. Beim Service kann an das Steuergerät zur Fehlerdiagnose ein Diagnosetester angeschlossen werden, mit dem die Fehlerspeichereinträge ausgelesen werden können. Zudem können im Diagnosebetrieb steuergerätinterne Größen sowie Eingangssignale von Sensoren und Sollwertgebern an den Diagnosetester übertragen und für eine Analyse durch den Werker online dargestellt werden. Der Diagnosemodus ermöglicht ebenso eine „gezielte Aktivierung einzelner Aktuatoren des Steuergeräts, um damit die Funktionsfähigkeit zu prüfen“. (vgl. [Schäuffele & Zurawka 2006])

3.2.2.2 Watchdogmechanismen

Watchdogs dienen der Überwachung des Programmablaufs auf Mikrocontrollern und damit der Verbesserung der Funktionssicherheit von Steuergeräten (vgl. [Krüger 2008]). Der prinzipielle Mechanismus einer Watchdog-Schaltung ist im folgenden Bild 3.5 dargestellt:

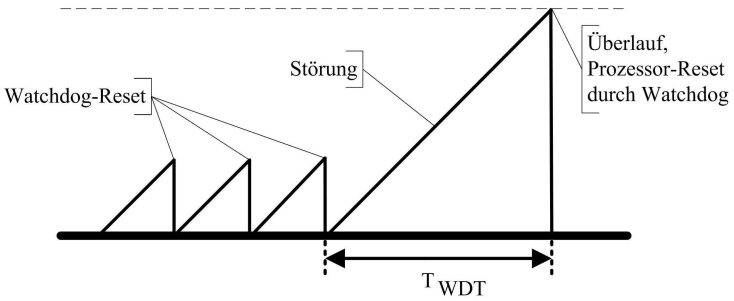

Bild 3.5: Watchdogmechanismus (vgl. [Wüst 2009])

Jede Software benötigt für die Verarbeitung bestimmter Funktionen eine gewisse Zeit. Watchdogmechanismen basieren darauf, dass an einer bestimmten Stelle in einem Programm, ein sogenannter Watchdog-Reset durchgeführt wird, der als Herzschlag des Systems interpretiert werden kann. Bei einer Hardware-Watchdog-Schaltung, auch externer Watchdog genannt, wird der Watchdog-Reset in Form eines Flankenwechsels an einem definierten Ausgangs-Port-Pin des Mikrocontrollers realisiert. Der Flankenwechsel wird von einer an den Pin angeschlossenen externen Hardware (in Kapitel 3.2.2.1 Überwachungsrechner genannt) erkannt, die daraufhin „entscheidet, ob die Frequenz dieses Kontrollsignals noch innerhalb eines gültigen Bereichs liegt“. Wird eine zu große Periodendauer T_{WDT} festgestellt, löst der überwachende Mikrocontroller, der üblicherweise in den Spannungsregler-Baustein integriert ist, eine Rekonfiguration des Funktionsrechners bzw. einen Programmneustart aus. Der Flankenwechsel ist notwendig, um zu verhindern, dass ein dauerhaftes Setzen des Pins auf einen Wert infolge eines Fehlers ein Ausbleiben der Rekonfiguration bewirkt. Heutzutage ist bei vielen Mikrocontrollern eine kleine Oszillatorschaltung eingebaut, durch die im

Mikrocontroller intern eine Rekonfiguration ausgelöst werden kann. Dadurch wird der Watchdogmechanismus hardwaremäßig vereinfacht. Man spricht dann von einem Software-Watchdog bzw. einem internen Watchdog. Statt einer Invertierung des Watchdog-Ports müssen beim Software-Watchdog zyklisch spezielle Mikrocontroller-Befehle aufgerufen werden. Hardware-Watchdogs lassen sich verbessern, indem der Watchdog-Port nicht pauschal invertiert wird, sondern von einer Funktionsgruppe immer statisch auf „high“ und von einer zweiten Funktionsgruppe, die abwechselnd mit der ersten Funktionsgruppen aufgerufenen wird, immer statisch auf „low“ gesetzt wird. Auf diese Weise ist es möglich, statt einem zwei wichtige Punkte im Programm zu überwachen. (vgl. [Krüger 2008])

Einen guten Überblick über Watchdog-Konzepte liefern ebenfalls [Brinkschulte & Ungerer 2007] und [Xi et al. 2007]. Bezüglich der Implementierung von Watchdogs sei auf [Schmitt 2000] verwiesen.

3.2.3 Fahrerüberwachung

Wie bereits in Kapitel 2.2.1 erläutert wurde, ist bei einem VA FAS eine Überwachungsinstanz notwendig, die kontinuierlich überprüft, ob sich der Fahrer noch im Loop befindet. Im Loop bedeutet im Kontext dieser Arbeit, dass sich der Nutzer eines VA FAS dauerhaft in einem Zustand befindet, in dem er sich der aktuellen Verkehrssituation noch bewusst ist und der es ihm jederzeit umgehend ermöglicht, in adäquater Weise die komplette Fahrzeugführung zu übernehmen. Ist dies nicht der Fall, ist eine Deaktivierung des VA FAS notwendig. Es existieren einige Arbeiten, die sich mit der Erfassung des Situationsbewusstseins des Fahrers beschäftigen. Einen guten Überblick liefert beispielsweise [Rauch 2009]. Allerdings gibt es momentan keine Arbeiten, die beschreiben, was einen Fahrer, der im Loop ist, auszeichnet bzw. wie er sich verhält oder verhalten soll. Dennoch existieren einige Ansätze und auch prototypische Umsetzungen, die sich mit der Überwachung des Fahrerzustands beschäftigen. Sie sollen in diesem Abschnitt vorgestellt werden.

Grundsätzlich ist zwischen zwei verschiedenen Herangehensweisen zu unterscheiden. Zum einen gibt es Ansätze, die das Fahrerverhalten mittels entsprechender Messtechnik beobachten und so eine Aussage über den Fahrerzustand treffen. Zum anderen existieren Bedienkonzepte, die den Fahrer zu einer zusätzlichen Bedienhandlung mit einer Mensch-Maschine-Schnittstelle zwingen. Gibt der Fahrer nicht in der geforderten Regelmäßigkeit Rückmeldung an das System[3], so wird geschlussfolgert, dass er sich nicht mehr im Loop befindet. Beide Herangehensweisen lassen sich gemäß des folgenden Bildes 3.6 weiter unterteilen und werden in den nächsten zwei Unterkapiteln ausführlich beschrieben.

[3] Eine derartige Rückmeldung wird auch als Trigger bezeichnet.

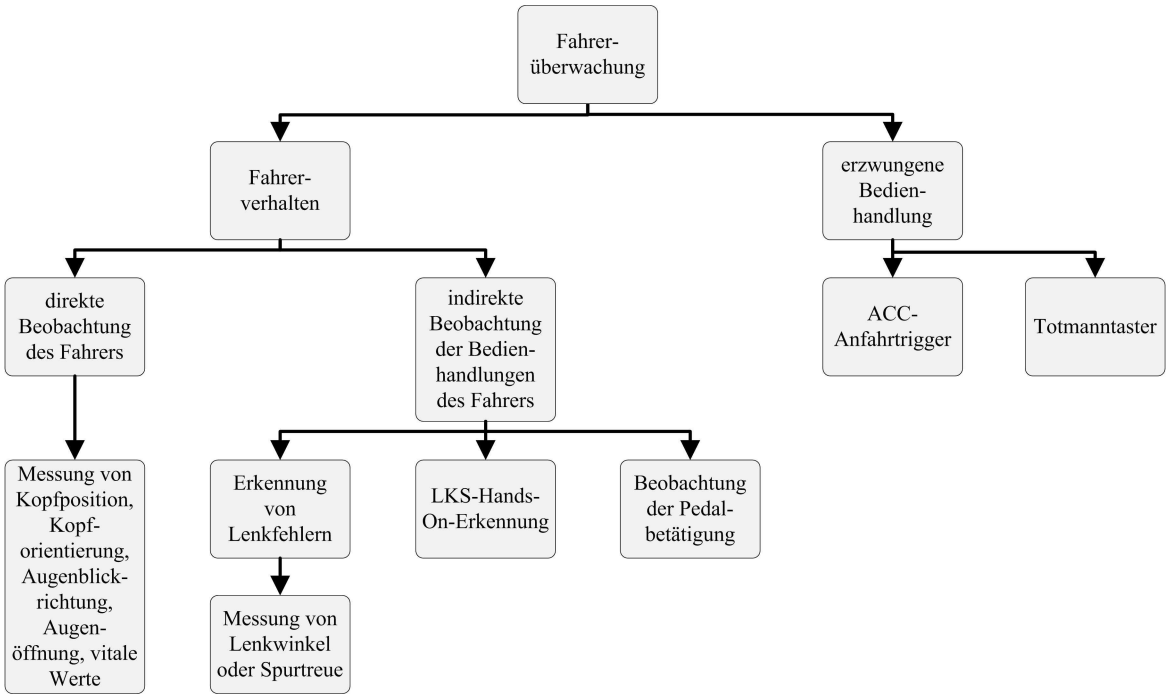

Bild 3.6: Ansätze zur Fahrerüberwachung

Neben den im Bild aufgezeigten Ansätzen zur Fahrerüberwachung werden in einem weiteren Unterkapitel außerdem drei Bedienkonzepte für automatisierte Fahrfunktionen vorgestellt, die das Ziel haben, den Fahrer aktiv in die Fahraufgabe einzubinden und ihn dabei möglichst transparent und durchgehend zu unterstützen. Durch die Bedienung des Systems und entsprechende Rückkopplungen soll hierbei realisiert werden, dass der Fahrer im Loop bleibt. Es lassen sich daraus weitere wichtige Anforderungen für die Konzeptionierung des Fahrerüberwachungsmoduls eines VA FAS ableiten.

Abschließend wird noch kurz auf die Überwachung von Piloten in der Luftfahrt eingegangen.

3.2.3.1 Überwachung des Fahrerverhaltens

Die Fahrerverhaltensüberwachung lässt sich in zwei Bereiche unterteilen. Zum einen kann der Fahrerzustand durch eine direkte Beobachtung des Kopfs, der Augen oder vitaler Werte bestimmt werden. Zum anderem besteht die Möglichkeit, die Bedienhandlungen des Fahrers bzw. deren Auswirkung zu beobachten und somit indirekt eine Aussage über sein Verhalten bzw. seinen Zustand zu treffen. (vgl. [Altmüller 2007])

Im Rahmen einer direkten Fahrerbeobachtung können entweder mittels einer Kamera der Kopf und die Augen des Fahrers beobachtet oder den Fahrer beschreibende vitale Zustandsgrößen, wie beispielsweise die Gehirnaktivität, der Herzschlag, die Atemfrequenz, der Blutdruck, die Hauttemperatur oder die Hautleitfähigkeit erfasst werden (vgl. [Altmüller 2007]). Für den mittel- und nahfristigen Serieneinsatz kommt bislang ausschließlich die videobasierte Erfassung des Fahrers in Frage. Grundlegendes Messinstrument ist hierbei entweder ein Mono- oder Stereokamerasystem, welches sich entweder im Kombiinstrument vor dem Fahrer oder in der A-Säule des Fahrzeugs befindet (vgl. [Jan et al. 2005] und Bild 3.7). Zusätzlich kann eine Infrarot-Beleuchtungseinheit verwendet werden, um dafür zu

sorgen, dass das Kamerasystem auch bei ungünstigen Lichtbedingungen betrieben werden kann (vgl. [Smart Eye AB 2010]).

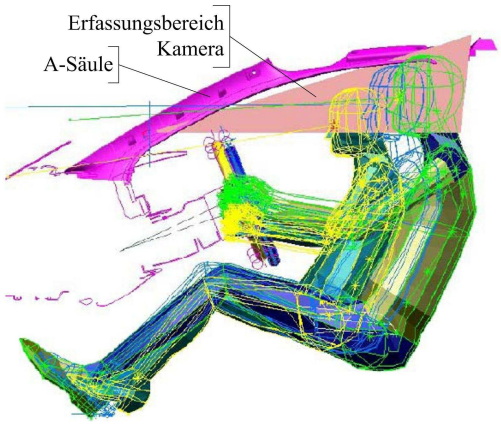

Bild 3.7: Erfassungsbereich einer Kamera in der A-Säule (vgl. [Jan et al. 2005])

Der von der Kamera generierte Bilddatenstrom wird von einem Auswertungsalgorithmus dazu verwendet, verschiedene Zustandsgrößen zu bestimmen. Bislang können folgende Größen detektiert werden:

- Existenz des Fahrerkopfs
- Kopfposition des Fahrers in vertikaler und horizontaler Richtung
- Kopforientierung des Fahrers um die Gier-, Nick- und Rollachse
- Augenöffnungswinkel der Fahrers
- Lidschlussfrequenz des Fahrers
- Blickrichtung der Augen des Fahrers

Es existieren mit „Seeing Machines“ und „Smart Eye“ zwei Unternehmen, die bereits heute entsprechende Kamerasysteme mit dazugehöriger Software vertreiben. „Seeing Machines“ bietet mit den Paketen „Driver State Sensor“ ein Mono- und mit „Face Lab“ ein Stereosystem an, deren Funktionsweise in zahlreichen Quellen ausführlich beschrieben wird (vgl. [Altmüller 2007], [Seeing Machines 2008], [Seeing Machines 2010] und [Trefflich 2009]). Das von „Smart Eye“ vertriebene Monokamerasystem trägt den Namen „Antisleep“ (vgl. [Smart Eye AB 2010]). Daneben existieren auch Prototypen im universitären Umfeld. Erwähnenswert sind hierbei vor allem die Ansätze der University of California (vgl. [Murphy-Chutorian et al. 2007]) und der University of Central Florida (vgl. [Smith et al. 2003]). Beide Forschungsinstitute verwenden eine Monokamera. Die folgende Tabelle 3.1 gibt eine vergleichende Übersicht, welche Systeme welche der oben aufgelisteten Zustandsgrößen bestimmen können:

		Seeing Machines		University of California	University of Central Florida	Smart Eye
		DSS	Face Lab			
Kopf	Kopferkennung	x	x	x	x	x
	Position vertikal	x	x		x	x
	Position horizontal	x	x		x	x
	Rollwinkel	x	x		x	x
	Nickwinkel	x	x	x	x	x
	Gierwinkel	x	x	x	x	x
Augen	Augenöffnungsgrad	x	x			x
	Lidschlag	x	x		x	x
	Blickrichtung Auge		x		x	

Tabelle 3.1: Vergleich kamerabasierte Fahrerüberwachungssysteme

Durch Auswertung der Kopfposition, der Kopforientierung und der Augenblickrichtung bzw. der entsprechenden Änderungen im zeitlichen Verlauf kann nun auf die Aufmerksamkeit des Fahrers geschlossen werden. Es wird dazu davon ausgegangen, dass ein aufmerksamer Fahrer mit einer gewissen Regelmäßigkeit durch einen definierten Bereich in der Windschutzscheibe (engl. Region of Interest, ROI) blicken muss, um das Verkehrsgeschehen angemessen verfolgen zu können (vgl. Bild 3.8). (vgl. [Mottok et al. 2008] und [Trefflich 2009])

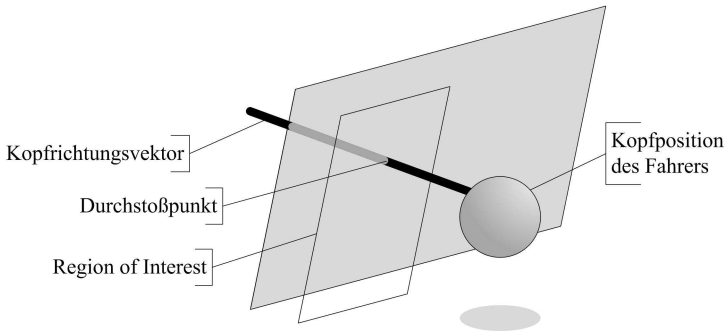

Bild 3.8: Blick eines aufmerksamen Fahrers durch die Windschutzscheibe (vgl. [Mottok et al. 2008])

Die Kopfposition, die Kopforientierung, die Lidschlagfrequenz und der Augenöffnungswinkel geben Aufschluss darüber, ob der Fahrer müde oder gar eingeschlafen ist. Mittels dieser Zustandsgrößen können müdigkeitsinitiierte Symptome, wie ein nach vorne Nicken des Kopfes, eine charakteristische Lidschlaghäufung und ein längerfristiges, vollständiges Schließen der Augen erkannt werden. (vgl. [Trefflich 2009])

Als einziger Automobilhersteller bietet bisher Lexus in seiner Baureihe LS ein videobasiertes Fahrerüberwachungssystem unter dem Namen „Driver Monitoring System“ in Serie an. Im Rahmen der Funktion „Advanced Pre-Crash Safety“ wird hierbei durch eine sich direkt über dem Lenkrad im Kombi befindliche Monokamera unter Zuhilfenahme dazu gehörender Infrarotbeleuchter die Kopforientierung des Fahrers bestimmt. Erkennt das System eine Gefahrensituation, beispielsweise ein Hindernis unmittelbar vor dem Fahrzeug, und wendet der Fahrer zeitgleich seinen Blick zu lange von der Fahrbahn vor ihm ab, wird eine optische und akustische Warnung ausgegeben. Wendet der Fahrer seinen Kopf daraufhin nicht sofort der Fahrbahn zu, so wird überdies ein Bremsruck zur Fahrerwarnung ausgelöst. (vgl. [Trefflich 2009] und [Lexus 2010])

Es sei an dieser Stelle darauf hingewiesen, dass sich die Zustandsgrößen des Kopfes deutlich robuster bestimmen lassen als die der Augen, weshalb im System von Lexus auch ausschließlich erstere berechnet und verwendet werden. Eine rein videobasierte Müdigkeitsüberwachung, wie oben beschrieben, ist noch nicht serienreif. Generell existieren etliche Störgrößen, die die Messung teilweise stark beeinflussen. Ein Beispiel hierfür sind Probleme bei der Erfassung von Brillenträgern.

Der indirekten Fahrerbeobachtung liegt die Idee zugrunde, die Bedienhandlungen des Fahrers zu überwachen und so auf seinen Zustand zu schließen. Es existieren mit der Lenkfehler-Erkennung, der Hands-On-Erkennung und der Beobachtung der Betätigung der Pedalerie drei Gruppen von Systemen, bei denen dieses Überwachungsprinzip bereits in Serie Anwendung findet. Sie zielen primär auf die Überwachung von Bedienhandlungen der primären Fahraufgabe ab. Die primäre Fahraufgabe umfasst dabei alle Aufgaben, die mit dem Halten des Fahrzeugs auf der Straße zu tun haben (Lenken, Gas geben und Bremsen), wohingegen sich die sekundäre Fahraufgabe aus den Verkehrsregeln bzw. Verkehrs- und Umweltbedingungen ergibt und sich die tertiäre Fahraufgabe auf Handlungen zur Befriedigung von Komfort- und Informationsbedürfnissen bezieht (vgl. [Wolf et al. 2006]). Es sei an dieser Stelle darauf hingewiesen, dass bereits erste Überlegungen existieren, auch die Bedienhandlungen der sekundären und tertiären Fahraufgabe zu überwachen, da festgestellt wurde, dass vor allem die intensive Nutzung neuartiger interaktiver Dienste im Fahrzeug eine Reduzierung der Fahrleistung zur Folge haben kann (vgl. [Urbas et al. 2008]).

Der Lenkfehler-Erkennung liegt die Annahme zugrunde, dass ein müder und unaufmerksamer Fahrer während manueller Fahrt kleine Lenkfehler macht, die er auf eine charakteristische Weise korrigiert bzw. ausgleicht (vgl. [Daimler AG 2008]). Altmüller liefert einen guten Überblick über die zwei unterschiedlichen Mechanismen zur Erfassung von Lenkfehlern. Sie basieren entweder auf einer Beobachtung von Lenkradbewegungsverläufen oder auf einer Beobachtung von Querablageverläufen des Fahrzeugs bezüglich des Fahrstreifens (vgl. [Altmüller 2007]). Gemäß dieser Klassifikation lassen sich auch die zwei momentan im Markt befindlichen Systeme von Daimler und Volvo unterscheiden.

Das System „Attention Assist“ in der Daimler E-Klasse basiert auf der Messung des Lenkwinkelverlaufs und fordert den Fahrer, sobald dieser beginnt müde zu werden, optisch und akustisch dazu auf, eine Pause zu machen. In die Berechnung des Warnzeitpunkts fließen neben dem Lenkwinkel noch etliche weitere Parameter ein. Sie beschreiben die Fahrweise des Fahrers bzw. die Fahrerbedienhandlungen der primären (Geschwindigkeit, Fahrtdauer, Längs- und Querbeschleunigung) und der sekundären Fahraufgabe (Blinker- und Pedalbetätigung). Überdies werden auch noch auf den Fahrer einwirkende Einflüsse, etwa die Tageszeit, die aktuelle Verkehrslage, der momentan wirkende Seitenwind und der Fahrbahnzustand berücksichtigt. (vgl. [Bähnisch 2007], [Daimler AG 2008] und [Deppe 2010])

Im Gegensatz zu Daimler, wird bei dem System „Driver Alert Control“ von Volvo im V70, XC70 und S80 der Verlauf der Querablage des Fahrzeugs von der Fahrstreifenmitte unter Verwendung einer auf die Fahrstreifenmarkierungen gerichteten Kamera und Inertial-Sensorik registriert. Auf diese Weise wird bei Geschwindigkeiten über 60km/h die zurückgelegte Fahrtrajektorie des Fahrzeugs rekonstruiert und beurteilt, ob diese kontrolliert innerhalb des Fahrstreifens verläuft. Bemerkenswerter Weise gibt das System mittels fünf

Balken in der Kombianzeige kontinuierlich Auskunft über den daraus abgeleiteten, aktuellen Konzentrationsgrad des Fahrers. Ist nur noch ein Balken vorhanden, empfiehlt das System eine Erholungspause. (vgl. [Ritter 2007] und [Lamb & McHugh 2008])

Im Rahmen der Hands-On-Erkennung wird bei Lane Keeping Support Systemen (LKS), wie beispielsweise dem „Lane Assist“ von Volkswagen oder dem „Lane Keeping Assist“ System von Honda, beobachtet, ob der Fahrer mit seinen Händen das Lenkrad bedient bzw. berührt. Ziel ist es hierbei, zu überprüfen, ob sich der Fahrer noch in der von ihm geforderten Intensität an der Querführungsaufgabe beteiligt. Dazu erfassen Sensoren im Lenkrad das aktuell vom Fahrer aufgebrachte Lenkmoment. Erkennt das LKS keine eigenständige Lenkbewegung des Fahrers mehr, deaktiviert es sich nach einer gewissen Toleranzzeit, die üblicherweise im einstelligen Sekundenbereich liegt, automatisch. (vgl. [Gayko 2009], [Honda AG 2010] und [Volkswagen AG 2010])

Der Vollständigkeit halber sei darauf hingewiesen, dass sich auch durch die Beobachtung der auf die Pedalerie wirkenden Kräfte Rückschlüsse auf die Aufmerksamkeit des Fahrers ziehen lassen (vgl. [Dong et al. 2009]).

3.2.3.2 Erzwingung von Bedienhandlungen

Fahrerüberwachungssysteme, die auf durch das System erzwungenen, zusätzlichen Bedienhandlungen basieren, sind derzeit im Bereich der semiautomatischen FAS (SA FAS) bei ACC S&G und der Eisenbahn bereits im Serieneinsatz. Die Grundidee ist hierbei, die Aufmerksamkeit des Fahrers bzw. des Bedieners regelmäßig oder in speziellen Situationen abzufragen und durch eine aktive Bedienhandlung, einen sogenannten Trigger, bestätigen zu lassen. Bleibt der Trigger aus, so kann davon ausgegangen werden, dass sich der Bediener nicht mehr im Loop befindet.

Bei ACC S&G Systemen besteht ab dem Erreichen des Stillstands die Gefahr, dass der Fahrer dazu verleitet wird, Nebentätigkeiten nachzugehen, da er dann der Querführungsaufgabe nicht mehr nachgehen muss und somit vollständig von der Fahraufgabe entbunden ist. Würde das Fahrzeug anfahren, ohne dass dies der Fahrer bemerkt, könnte es von der Fahrbahn abkommen und im schlimmsten Fall kollidieren. Um dies zu vermeiden, wurde ein Mechanismus eingeführt, der den Fahrer bei Standzeiten über einer bestimmten Dauer (meist etwa 3s) zu einem sogenannten Anfahrtrigger auffordert, damit das Fahrzeug wieder selbstständig anfährt (vgl. [Winner et al. 2009]). Bei BMW und Daimler muss beispielsweise entweder das Gaspedal kurz angetippt oder der BMW-ACC-Bedientaster gedrückt bzw. der Daimler-Tempomathebel gezogen werden (vgl. [BMW AG 2010] und [Wohland 2007]).

Der Totmanntaster ist Hauptbestandteil der sogenannten Sicherheitsfahrschaltung, die bei Triebfahrzeugen im Schienenverkehr zur Anwendung kommt und durch die Norm [DIN VDE 0119-207-5: 2004] geregelt ist. Idee hierbei ist es, den Triebwagenführer in gewissen zeitlichen Abständen durch ein optisches Signal dazu aufzufordern, eine aktive Bedienhandlung durchzuführen und damit seine Wachsamkeit aufrechtzuerhalten. In deutschen Zügen muss aus diesem Grund alle 30s ein Fußpedal losgelassen und wieder gedrückt werden. Kommt der Zugführer dieser Forderung nicht nach, erfolgt zunächst ein akustisches Signal und nach einer weiteren Zeitspanne die Einleitung einer Zwangsbremsung

(vgl. Kapitel 3.4.3.2). Die Bremsung wird aufgehoben sobald das Pedal wieder betätigt wird. (vgl. [DIN VDE 0119-207-5: 2004], [Anders 2008] und [Geyer & Prostrednik 2006])

3.2.3.3 Bedienkonzepte zur kooperativen Automation von Fahrfunktionen

Die nun vorgestellten Bedienkonzepte manöverbasiertes Fahren, Conduct-by-Wire und H-Metapher haben das Ziel, den Fahrer eines Fahrzeugs mit hohem Automationsgrad durch intensive, kooperative Interaktion mit einer Mensch-Maschine-Schnittstelle aktiv in die Fahraufgabe einzubinden und ihn dadurch im Loop zu halten. Der Begriff der kooperativen Automation wurde als gemeinsamer Kern dieser Ansätze identifiziert (vgl. [Hakuli et al. 2009]).

Dem Konzept des manöverbasierten Fahrens liegt die sogenannte Playbook™-Metapher zugrunde, die ihr Vorbild im amerikanischen Football hat. Hier sind in den Spielbüchern der Trainer hinter prägnanten Begriffen bestimmte, komplexe Spielzüge abgelegt. Im Kontext vollautomatisch fahrender Fahrzeuge delegiert der Fahrer durch die Auswahl eines Fahrmanövers Aufgaben der Fahrzeugführung an das FAS. Für die Auswahl eines für die Situation geeigneten Manövers muss der Fahrer aufmerksam sein und bleibt dadurch, so die Idee, im Loop. Das Anfahren aus dem Stillstand oder das Überholen des vorausfahrenden Fahrzeugs sind Beispiele für Manöver, die automatisiert durch das Fahrzeug übernommen werden. Der Vollständigkeit halber sei darauf hingewiesen, dass es auch Manöver mit niedrigeren Automationsgraden gibt, bei denen der Fahrer beispielsweise in Baustellen selbst die Querführung übernimmt. In Fahrversuchen mit einem prototypisch umgesetzten VA FAS zeigte sich, dass sich die Kontrollierbarkeit des Fahrzeugs durch die Probanden bei einem Systemausfall verbesserte, wenn eine Manöversteuerung in der beschriebenen Form in das Bedienkonzept integriert wurde. (vgl. [Miller et al. 2005] und [Petermann & Niemann 2010])

Das Forschungsprojekt Conduct-by-Wire hat eine Reduzierung der Bedienkomplexität der zukünftig in modernen Fahrzeugen gleichzeitig verfügbaren (teil-)automatisierten Fahrfunktionen zum Ziel, die mit dem Ansatz der seriell-sequenziellen Assistenz erreicht werden soll. Dies soll dazu führen, dass der Fahrer durch die zunehmende Aufgabenfülle nicht überfordert und dadurch zusätzlich abgelenkt wird. Der Fahrer wirkt hierbei ausschließlich durch das Assistenzsystem auf die Führung des Fahrzeugs ein, das seine nacheinander erfolgenden Eingaben sequenziell umsetzt. Ein direkter Zugriff auf das Fahrzeug unter Umgehung der Assistenz ist nicht möglich. Ähnlich wie beim Manöverbasierten Fahren, sollen also auch hier Teile der Fahraufgabe an das FAS delegiert werden können. (vgl. [Winner et al. 2006] und [Hakuli et al. 2009])

Die H-Metapher beschreibt ein Prinzip zum kooperativen Zusammenwirken von Fahrer und Maschine zur Lösung des „Out-of-the-loop“-Problems. Hierbei dient das Pferd (engl. horse) als Vorbild für das harmonische und intuitive Zusammenspiel von Mensch und einem intelligentem Fahr- bzw. Flugzeug. Dies betrifft zum einen die Autonomie des Pferds, das in der Lage ist, Hindernisse selbstständig zu erkennen und ihnen auszuweichen. In Anlehnung daran wird davon ausgegangen, dass auch ein VA FAS bestimmte komplexe Handlungen eigenständig vollziehen kann. Zum Anderen steht das H in der H-Metapher aber auch für eine andauernde haptische Rückkopplung. Genau wie ein Pferd dem Reiter über den Sattel und die

Zügel seine momentane Aktion, Intention und sein Befinden mitteilt, sollte auch der Fahrer eines VA FAS, beispielsweise durch den Druck oder die Vibration eines aktiven Bedienteils, laufend spüren können, wie sich das intelligente Fahrzeug bewegt und ob eine Gefahr besteht. Die Steuerung des Fahrzeugs soll, ebenfalls wie beim Pferd, kontinuierlich über den haptischen Kanal erfolgen. Diese Bidirektionalität soll dazu führen, den Fahrer davon abzuhalten, Nebenbeschäftigungen nachzugehen, die dazu führen, dass er nicht mehr im Loop ist. (vgl. [Flemisch 2003], [Flemisch & Dittrich 2008] und [Hakuli et al. 2009])

3.2.3.4 Überwachung von Flugzeugpiloten

Wenn in einem Flugzeug der Autopilot aktiv ist, findet keine Überwachung der Piloten statt. Dies liegt daran, dass davon ausgegangen werden kann, dass sich das Flugzeug bei aktiviertem Autopiloten andauernd in einem sicheren Zustand befindet, da die komplette Flugtrajektorie vorgeplant wird und allen anderen Flugzeugen bekannt ist. Aus diesem Grund ist ein kurzfristiges, korrigierendes Eingreifen des Piloten zu keiner Zeit notwendig. Zudem sind Piloten Profis, die speziell für alle potentiell auftretenden Ereignisse trainiert sind.[4]

Durch die fehlende Überwachung ist es schon vorgekommen, dass ein Flugzeug 240km über sein eigentliches Ziel hinausgeflogen ist, weil sich die Piloten in ein hitziges Gespräch vertieft hatten (vgl. [SZ 2009]).

3.3 Architekturelle Redundanzkonzepte

Wie in Kapitel 2.2.3 bereits beschrieben wurde, sind Redundanzen für die Fehleridentifikation und Fehlerbehebung notwendig. Diese Feststellung wird durch [Schäuffele & Zurawka 2006] bestätigt. Im Folgenden werden die wichtigsten Redundanzmechanismen vorgestellt (vgl. Bild 3.9).

[4] Diese Informationen stammen aus einem persönlichen Gespräch mit Prof. Dr.-Ing. Florian Holzapfel vom Lehrstuhl für Flugsystemdynamik der TU München.

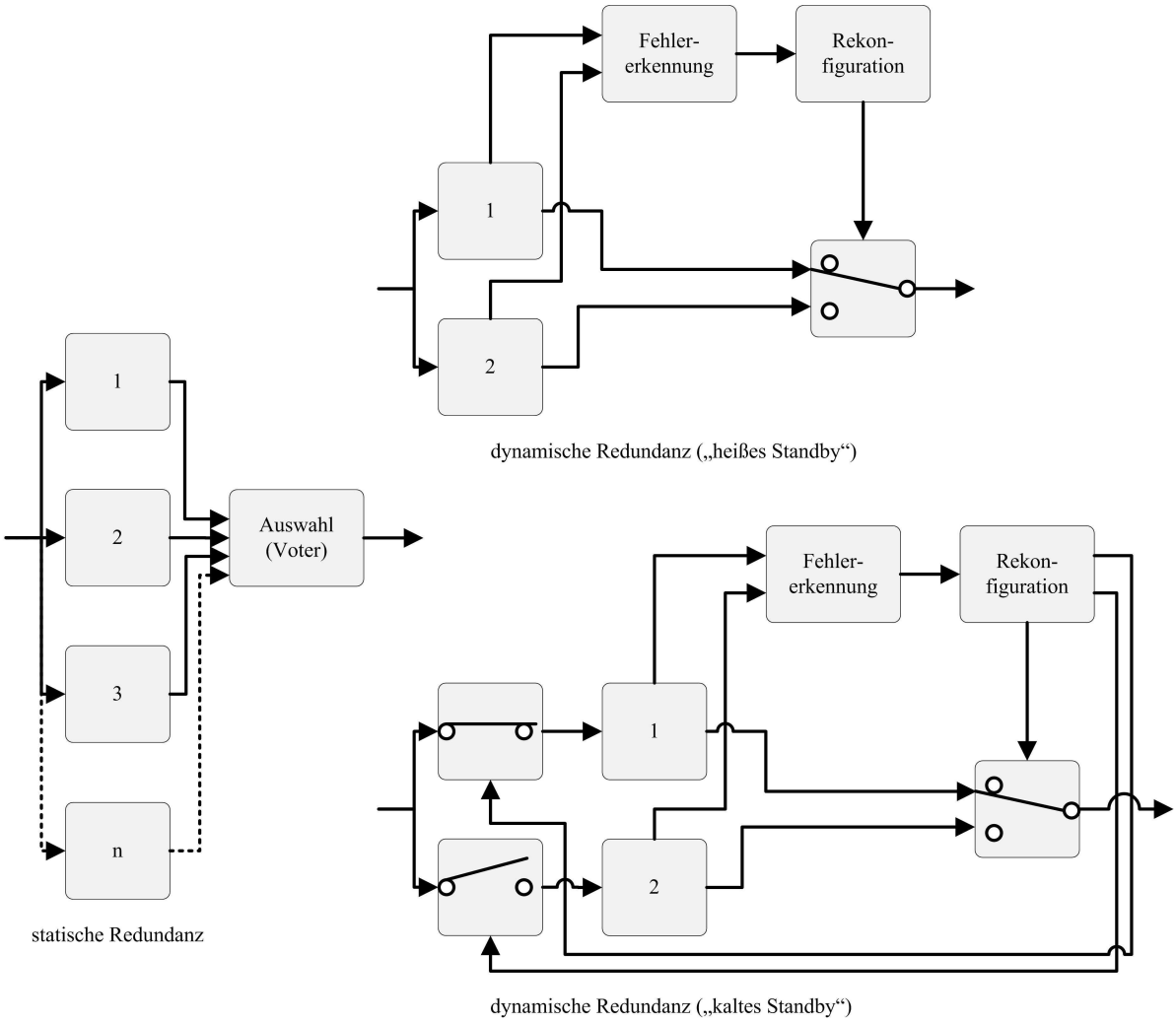

Bild 3.9: Redundanzmechanismen nach [Isermann 2010]

Grundsätzlich ist zwischen statischer und dynamischer Redundanz zu unterscheiden, wobei dynamische Redundanzmechanismen wiederum in das sogenannte „heiße“ und „kalte Standby“ gegliedert werden können. Besonders einfach umzusetzen ist das statische Redundanzprinzip. Hierbei sind drei oder mehr gleichartige, parallel geschaltete Hardware- oder Software-Komponenten, die alle die selbe Eingangsinformation erhalten und zu jeder Zeit aktiv arbeiten, mit einem sogenannten Voter verbunden. Der Voter überprüft, ob die Ausgangsinformationen der Komponenten gleich sind und entscheidet dann per Mehrheitsbetrachtung, welche Informationen valide und welche fehlerhaft sind. Am Ausgang des Voters wird daraufhin nur der valide Wert weitergeleitet. Allgemein lässt sich die tolerierbare Anzahl fehlerhafter Komponenten k in Abhängigkeit der Anzahl redundanter Module n berechnen, wobei n ungerade sein muss:

$$k = \frac{n-1}{2} \tag{3.1}$$

Die Nachteile statischer Redundanz sind im Falle redundanter Hardware-Komponenten hohe Kosten, hoher Energieverbrauch, sowie hohes Gewicht und im Falle redundanter Software-Komponenten eine erhöhte Rechenzeit, was sich wiederum in erhöhten Kosten niederschlägt, falls zusätzliche Prozessoren notwendig werden. Außerdem können durch den einfachen

Vergleichsmechanismus keine systematischen Fehler, die gleichzeitig in allen Komponenten auftreten, erkannt werden. Bei der dynamischen Redundanz müssen mindestens zwei gleichartige Komponenten vorhanden sein. Eine Komponente ist hierbei immer aktiv in Betrieb. Fällt sie aus, erfolgt eine Übernahme durch die Reservekomponente. Zur Fehlererkennung ist eine Überwachungskomponente notwendig, die in der Lage ist, einen Ausfall der aktiven Komponente zu erkennen und im Fehlerfall einen Rekonfigurationsschritt anzustoßen, durch den die fehlerhafte Komponente inaktiv und die Reservekomponente aktiv geschaltet wird. Im Falle redundanter Software wird zur Rekonfiguration ein speziell dafür vorgesehener Code-Abschnitt aufgerufen. Auch bei dynamischer Redundanz ist k von n abhängig, wobei n sowohl gerade, als auch ungerade sein darf:

$$k = n - 1 \tag{3.2}$$

Der prinzipielle Vorteil dynamischer Redundanz liegt somit vor allem in einer Reduzierung redundanter Komponenten und der Möglichkeit einer umfassenderen Fehlererkennung, da beliebige, intelligente Fehlererkennungsalgorithmen implementiert werden können. Auf der anderen Seite stellt die Entwicklung der Fehlererkennungs- und Rekonfigurationseinheiten einen erheblichen Aufwand dar. Je nachdem, ob die Reservekomponente auch im Normalbetrieb kontinuierlich arbeitet oder erst infolge eines erkannten Fehlers zu arbeiten beginnt, liegt entweder das sogenannte „heiße“ oder das „kalte Standby“ vor. Der Vorteil des „kalten Standbys“ ist, dass Hardware-Komponenten nicht unnötig verschlissen werden. Allerdings sind zur Aktivierung zwei zusätzliche Schalter am Eingang der Komponenten notwendig und es ist, bedingt durch die Anlaufphase, von einer höheren Transferzeit bei der Umschaltung auf die Reservekomponente auszugehen. (vgl. [Isermann 2010])

Betrachtet man die Unterschiede zwischen redundanter Hardware und redundanter Software, so lässt sich überdies folgendes feststellen (vgl. [Isermann 2010]):

- Da Softwarefehler grundsätzlich systematisch sind und nicht zufällig auftreten, ist eine Duplizierung derselben Software nicht sinnvoll. Aus diesem Grund muss redundante Software immer diversitär gestaltet werden. Dies kann durch die Entwicklung in unterschiedlichen Programmierteams sowie die Verwendung anderer Computersprachen und Compiler erreicht werden.
- Bei rein mechanischen, statisch redundanten Komponenten bzw. Systemen ist kein Voter in Form von Software oder einer elektronischen Schaltung verfügbar. Fällt eine Komponente aus, so übernehmen in diesem Fall die anderen Komponenten deren Aufgabe. Dies geschieht gemäß der physikalischen Prinzipien der Kompatibilität oder Kontinuität. Sofern die Güte der Fehlererkennung ausreicht, ist statische Redundanz bei derartigen Systemen sinnvoll, da nicht eigens eine Recheneinheit in das Gesamtsystem integriert werden muss.
- Bei mechatronischen Systemen ist die Anwendung von „kaltem Standby“ besonders naheliegend, da Informationen für die Fehlererkennung oftmals bereits vorliegen und die notwendigen Recheneinheiten bereits vorhanden sind. „Hot Standby“ oder gar statische Redundanz machen nur Sinn, falls eine besonders niedrige Transferzeit bei der Umschaltung angestrebt oder ganz vermieden werden muss.

Einen allgemeinen Überblick zum Thema Redundanzen liefern auch [Blischke & Murthy 2000] und aus Sicht der Informatik [Bode & Hellwagner 2006].

3.4 Deaktivierungsprozesse hochautomatisierter, bewegter Systeme

In diesem Abschnitt wird zunächst ein Überblick über die Deaktivierungsprozesse heutiger SA FAS gegeben. Danach wird beschrieben, wie der sichere Zustand von Landfahrzeugen, der im Rahmen einer aktiven FS-Strategie anzustreben ist, in der Literatur definiert wird. Abschließend werden konkrete Umsetzungen der aktiven FS-Strategie im Automobilumfeld, in der Zugtechnik, bei mobilen Robotern und bei unbemannten U-Booten vorgestellt.

3.4.1 Semiautomatische Fahrerassistenzsysteme

Tritt bei einem heute im Markt befindlichen ACC- oder ACC S&G-System ein Fehler in Motor, Bremssystem, Steuergerät oder einem Umfeldsensor auf, so muss das System, gemäß der Norm [ISO 15622: 2010], generell deaktiviert und der Fahrer darüber sofort informiert werden. Die Fehleranzeige darf erst erlöschen, wenn das ACC-System ausgeschaltet wurde. Falls ein Sensorfehler vorliegt und sich das System im Verzögerungsregelmodus befindet, muss mit der letzten gültigen Verzögerung weiter verzögert werden. Eine Reaktivierung des Systems ist erst nach einem erfolgreich durchgeführten Selbsttest zulässig. (vgl. [ISO 15622: 2010])

Für die Deaktivierung von Parklenkassistenten werden durch eine ECE-Regelung (engl. für Economic Commission For Europe) entsprechende Vorgaben gemacht: Die Steuerung durch die automatische Lenkfunktion „muss automatisch ausgeschaltet werden, wenn die Fahrzeuggeschwindigkeit den eingestellten Grenzwert von 10 km/h um mehr als 20 % überschreitet oder die auszuwertenden Signale nicht mehr empfangen werden. Bei Beendigung der Steuerung muss der Fahrzeugführer jedes Mal durch ein kurzes, aber charakteristisches optisches Signal und entweder ein akustisches oder ein fühlbares Signal an der Betätigungseinrichtung der Lenkanlage gewarnt werden“. (vgl. [ECE R 79 2006])

Es wird daraus ersichtlich, dass die Ausfallsreaktionen heutiger SA FAS immer eine Systemdeaktivierung zum Ziel haben, die mit einer Fahrerübernahmeaufforderung (FÜA) einher geht. Ein sicherer Zustand kann nur durch die Übernahme der kompletten Fahrzeugführung durch den Fahrer wieder hergestellt werden.

3.4.2 Der sichere Zustand von Landfahrzeugen

Der in dieser Arbeit für A FAS im Fehlerfall angestrebte FS-Mechanismus (vgl. Kapitel 2) basiert, wie in Kapitel 3.1 bereits beschrieben, darauf, dass „bei Eintreten einer Fehlfunktion ein sicherer Zustand eingenommen oder beibehalten wird“ (vgl. [DIN EN 50129: 2003]). Es soll nun erörtert werden, wie der Begriff „sicherer Zustand“ in der Literatur definiert wird bzw. was er darstellt.

Grundsätzlich haben viele der Begriffe und Definitionen zum Thema Sicherheit bei Fahrzeugen ihren Ursprung in der Eisenbahntechnik, da der Zug das älteste maschinengetriebene Fortbewegungsmittel ist. Entsprechend definiert die Norm [DIN EN 50129: 2003], die aus dem Bereich der Bahnanwendungen stammt, einen „Zustand, der die Sicherheit weiterhin bewahrt“ als einen sicheren Zustand. Solange ein System fehlerfrei betrieben wird und keinen Ausfall aufweist, muss es sich also in einem sicheren Zustand befinden. (vgl. [Fenner et al. 2003])

Es muss nun noch geklärt werden, was einen sicheren Zustand nach Auftritt eines Fehlers eigentlich darstellen kann. Nach [Halang & Konakovsky 1999], die sich sicherheitsgerichteten Echtzeitsystemen widmen, sind „typische Beispiele für sichere Zustände (…) der Haltezustand von Verkehrssystemen und der Abschaltzustand von Produktionsanlagen“. Verschiedene Quellen führen deutlich aus, dass bei Schienenfahrzeugen der Stillstand der sicheren Zustand ist (vgl. [Anders 2008] und [Fenner et al. 2003]). [Geyer & Prostrednik 2006], die ebenfalls im Bereich der Schienenfahrzeuge tätig sind, konkretisieren diese Definition, indem sie ebenfalls zu dem Schluss kommen, dass „bei einem Fahrzeug (…) zumeist der Stillstand des Fahrzeugs als sicherer Zustand definiert“ ist, der Stillstand aber außerhalb eines Tunnels eingenommen werden soll, da es sich hierbei um einen „gefahrenträchtigen Bereich“ handelt. Der Zustand Stillstand wird hier also um eine Ortsangabe erweitert. Dieser Gedanke wird von [Isermann 2010] verallgemeinert und auf Automobile übertragen: „For automobiles, (usually) a safe state is stand still (or low speed) at a nonhazardous place.“

Es sei an dieser Stelle zusammenfassend nochmals auf die Tatsache hingewiesen, dass aufgrund der Komplexität eines A FAS, dessen Funktionalität zu einem Großteil von elektronischen Steuergeräten und der darauf laufenden Software abhängt, ein allgemein gültiges FS-Verhalten nur ein aktives sein kann. Es müssen daher softwareseitig Pläne vorgehalten werden, die das Fahrzeug in die Rückfallebene „Stillstand an einem sicheren Ort“ überführen. Dies stellt auch [Isermann 2010] fest: „However, if no mechanical back-up exists after failure of electronics, only an action by other electronics (switch to a still operating module) can bring the vehicle (in motion) to a safe state, i.e. to reach a stop through active fail-safe.”

3.4.3 Systeme mit aktivem Fail-Safe-Verhalten

Da bislang kein Seriensystem in einem Straßenfahrzeug existiert, welches eigenständig in der Lage ist, einen Übergang in die Rückfallebene „Stillstand an einem sicheren Ort“ (vgl. Kapitel 3.4.2) herbeizuführen und daher relativ wenige Erfahrungswerte mit derartigen Systemen vorliegen, werden im Folgenden auch andere, artverwandte Wissenschaftsbereiche betrachtet, in denen bereits ähnliche Konzepte umgesetzt wurden.

3.4.3.1 Automobile

Im Rahmen von drei Forschungsprojekten und zwei Patentmeldungen wurden fünf, teilweise ähnliche, Lösungsansätze formuliert, bei denen jeweils der Stillstand als Rückfallebene in einem Fehlerfall angestrebt wird.

Die aktuellste Forschungsbemühung unternimmt derzeit die BMW Forschung und Technik GmbH, die in Zusammenarbeit mit dem Bundesministerium für Bildung und Forschung das Projekt „Intelligente Dienste und Dienstleistungen für Senioren - SmartSenior“ ins Leben gerufen hat, in dem unter anderem ein sogenannter Nothalteassistent entwickelt werden soll. Dieses System soll bei einem medizinischen Notfall des Fahrzeuglenkers die Kontrolle über das Automobil übernehmen, den umgebenden Verkehr per Warnblinkanlage warnen und vollkommen selbstständig im umgebenden Straßenverkehr den rechten Fahrbahnrand anfahren, um dort stehenzubleiben. Danach soll ein Notruf mit Informationen über den Aufenthaltsort des Fahrzeugs und den Gesundheitszustand des Fahrers abgesetzt werden. Als Basis für dieses neue FAS sollen vor allem ACC und ein System zur Warnung des Fahrers vor Ausführung riskanter Spurwechsel dienen. Wegen der Komplexität innerstädtischer Verkehrssituationen soll der Einsatz des Prototyps zunächst auf Autobahnen und autobahnähnliche Straßen beschränkt werden. (vgl. [Kämpchen et al. 2010] und [Schröder 2009])

Ein dem BMW Nothalteassistenten ähnliches System wurde bereits in den Jahren 1996 bis 1998 im Rahmen des Projekts SAVE (System for Effective Assessment of Driver State and Vehicle Control in Emergency Situations) angedacht. Auch hier war die Idee, den Aufmerksamkeitszustand des Fahrers zu überwachen, ihn frühzeitig zu warnen, und das Fahrzeug, falls der Fahrer seiner Führungsaufgabe nicht mehr nachkommen kann, automatisiert am Fahrbahnrand zu parken. Das System wurde in Form von drei Komponenten umgesetzt. Eine sogenannte Integrated Monitoring Unit überwacht, ob der Fahrer durch Müdigkeit, Alkoholeinfluss oder Ohnmacht nicht mehr in der Lage ist, sein Fahrzeug sicher zu steuern. Wird eine Fahruntüchtigkeit festgestellt, so tritt das sogenannte SAVE Warning System in Aktion. Diese Komponente warnt sowohl den Fahrer in optischer und akustischer Form, als auch, je nach Ausmaß der Gefahr, durch Blinken der Brems- und Blinklichter, sowie durch ein spezielles, leuchtendes Warndreieck im Heckfenster den umliegenden Verkehr. Greift der Fahrer daraufhin nicht korrigierend ein, wird das sogenannte Automatic Control Device aktiviert, welches automatisch, sowohl in die longitudinale, als auch die laterale Fahrzeugführung eingreift und das Fahrzeug, durch mehrere kontrollierte Abbrems- und Spurwechselvorgänge, am rechten Fahrbahnrand zum Stehen bringt (vgl. Bild 3.10). Als erstes kommerzielles Einsatzszenario wurde ebenfalls eine Autobahn mit mehreren Fahrstreifen angenommen. (vgl. [Bekiaris 1999], [Bekiaris & Peters 1999] und [Brookhuis et al. 1998])

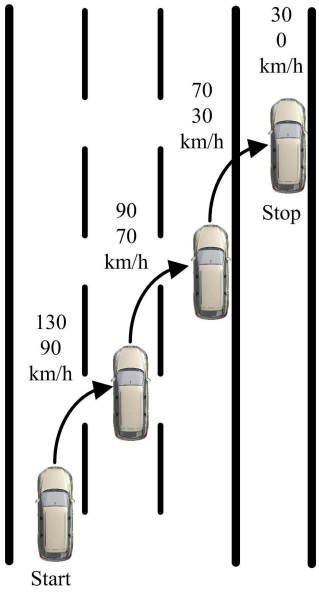

Bild 3.10: Nothaltemanöver im SAVE-Projekt (vgl. [Bekiaris 1999])

Eine weitere, den beiden zuvor genannten Konzepten ähnliche Idee ist in einem deutschen Patent angemeldet worden. Es wird hierbei ein Verfahren zur Überprüfung des Aufmerksamkeitsniveaus des Fahrers vorgeschlagen, welches den Fahrer im Falle verminderter Aufmerksamkeit, zunächst versucht wach zu rütteln und das Fahrzeug danach, falls das Aufmerksamkeitsniveau nicht gestiegen ist, in den Stillstand abbremst. Die Fahrerwarnung erfolgt vor allem in haptischer Form, indem durch das wiederholte Ansteuern der Bremse, eine Vibration der Karosserie erzeugt wird. Zusätzlich werden eine optische und eine akustische Warnung ausgegeben. Hat das System entschieden, in den Haltezustand überzugehen, wird der Hydraulikdruck in der Bremsvorrichtung allmählich erhöht und das Fahrzeug bei aktivierter Warnblinkanlage langsam verzögert. Ist der Stillstand erreicht, wird die Parkbremse eingelegt. Anders als bei den zwei zuvor beschriebenen Ansätzen ist in diesem Fall kein Eingriff in die Querführung des Fahrzeugs angedacht. (vgl. [Aizawa et al. 2004])

Eine durch Ansteuerung der Parkbremse automatisch auslösbare Vollverzögerung wird als FS-Verhalten für ein automatisch betriebenes Fahrzeug im Rahmen eines amerikanischen Patents vorgeschlagen. Das Patent beschreibt grundsätzlich einen Mechanismus, ein Fahrzeug automatisch entlang einer zuvor manuell abgefahrenen und in Form von GPS (Global Positioning System)-Koordinaten-Punkten gespeicherten Strecke zu führen. Jede Komponente des Gesamtsystems kann bei Auftreten eines Fehlers ein Abschalten des Gesamtsystems bewirken, also das beschriebene FS-Verhalten anstoßen. Für die Ansteuerung der Parkbremse existiert eine eigene unterlagerte Komponente, die die Energiezufuhr zu denjenigen Aktuatoren unterbrechen kann, die im Regelbetrieb die Parkbremse lösen. Da die Parkbremse so konstruiert ist, dass sie sich stromlos im eingelegten Zustand befindet, handelt es sich um ein passives FS-Verhalten. (vgl. [Gudat et al. 1999])

Im Rahmen des Teilprojekts „Automated Highway Systems“ des amerikanischen Forschungsprogramms „Partners for Advanced Transit and Highways“, das sich mit der automatisierten Führung mehrerer, in einer Kolonne befindlicher Fahrzeuge beschäftigt hat, wurden ebenfalls FS-Mechanismen spezifiziert, die im Fehlerfall den Nothalt einzelner

Kolonnen-Fahrzeuge herbeiführen. Für den Fall, dass die Bremsanlage des fehlerhaften Fahrzeugs noch funktionstüchtig ist, wird je nach Kritikalität des Fehlers, entweder das FS-Manöver „Gentle Stop“ oder „Crash Stop“ ausgeführt, also entweder eine Bremsung mit definierter Verzögerung oder ein Vollverzögerung. Da die Fahrzeuge per Car-2-Car-Technologie miteinander kommunizieren können, kann das rückwärtige Fahrzeug über die Bremsung des Vordermanns informiert und ein Auffahrunfall vermieden werden. Sollte das fehlerhafte Fahrzeug nicht mehr mit eigenen Mitteln anhalten können, so kann das FS-Manöver „Aided Stop“ angesteuert werden. Dabei wird das in der Kolonne vorausfahrende Fahrzeug per Car-2-Car-Kommunikation dazu aufgefordert, sich langsam zurückfallen zu lassen, bis es mit dem fehlerbehafteten Fahrzeug sanft kollidiert. Danach bremst das vordere Fahrzeug beide Fahrzeuge langsam bis in den Stillstand ab. (vgl. [Lygeros et al. 1995])

3.4.3.2 Züge

Um Züge im Schienenverkehr kontinuierlich zu überwachen und in einem sicheren Zustand zu halten, gibt es heutzutage die sogenannte Zugbeeinflussung. Die Hauptaufgabe der Zugbeeinflussung besteht darin, die Geschwindigkeit des Zuges mit der erlaubten Höchstgeschwindigkeit zu vergleichen und bei einer Überschreitung eine sogenannte Zwangsbremsung einzuleiten, um die Geschwindigkeit entsprechend anzupassen oder den Zug, bei einer geforderten Sollgeschwindigkeit von 0km/h, auch vollständig zum Stehen zu bringen. Neben einer Geschwindigkeits-Begrenzung für einen Streckenabschnitt kann beispielsweise auch die technisch maximal zulässige Geschwindigkeit des Zuges eine Geschwindigkeitsobergrenze darstellen. Eine Zwangsbremsung in den Stillstand wird ebenfalls eingeleitet, wenn der Zugführer innerhalb eines definierten Zeitintervalls nicht auf die Wachsamkeitskontrolle reagiert und rechtzeitig die Totmannvorrichtung (vgl. Kapitel 3.2.3.2) betätigt. (vgl. [Schnieder 2007] und [Fenner et al. 2003])

Weitere Gründe für das Auslösen einer Zwangsbremsung in den Stillstand sind offensichtlich auch Defekte im Zugsystem, beispielsweise ein Defekt der Anhängekupplung zur Verbindung von zwei Wagons (vgl. [Hutter 2007]).

Um zu verhindern, dass ein Zug auf einen vor ihm befindlichen (stehenden) Zug auffährt, existiert der sogenannte Blocksicherungsmechanismus, der auch im Falle einer Zwangsbremsung zum Tragen kommt. Fährt ein Zug in einen bestimmten Abschnitt ein, wird dieses Streckenstück für nachfolgende Züge solange durch ein Signal automatisch als blockiert und damit als nicht befahrbar gekennzeichnet, bis sämtliche Achsen des Zuges den Abschnitt wieder verlassen haben. Auf diese Weise kann der Stillstand eines Zuges infolge einer Zwangsbremsung abgesichert werden. (vgl. [Schnieder 2007])

3.4.3.3 Mobile Roboter

Im Rahmen eines amerikanischen Patents wird ein FS-Mechanismus für mobile Roboter beschrieben. Derartige Roboter kommen beispielsweise in großen Fabrikanlagen zum Einsatz und werden durch Navigationssysteme gesteuert, die der mobilen Einheit Geschwindigkeits- und Richtungsanweisungen vorgeben. Die Idee des FS-Mechanismus ist, im Falle eines Leistungsverlusts des Roboters, eines Abrisses der Kommunikationsverbindung zum

Navigationssystems oder eines anderen triftigen Grunds, den Roboter automatisch in den Stillstand abzubremsen. Dies soll sowohl durch einen Eingriff des Bremssystems, als auch der Radaktuatoren erreicht werden. Dazu werden die Räder des Roboters entgegen der aktuellen Bewegungsrichtung ausgerichtet und auf diese Weise eine zusätzliche Bremskraft erzeugt. Die zur Ansteuerung der Bremse notwendige Energie wird in einer eigenen Speichereinheit vorgehalten. (vgl. [Doth 1989])

3.4.3.4 Unbemannte U-Boote

Der kontrollierte Missionsabbruch stellt einen der wichtigsten Umplanungsbefehle für unbemannte U-Boote dar, die meist in großer Tiefe eigenständig Arbeiten, wie beispielsweise das Verlegen von Datenleitungen, durchführen. Gründe für einen Missionsabbruch können zum Beispiel der Ausfall eines Umfeldsensors oder eines Aktors sein. Mittels eines Notauftauchsystems wird bei derartigen Ereignissen ein sofortiges Erreichen der Wasseroberfläche angestrebt. Dies kann durch die Mitnahme von Ballast erreicht werden, der in Notsituationen abgeworfen wird und dadurch den notwendigen Auftrieb erzeugt. (vgl. [Wernstedt et al. 2004])

Der Auftrieb kann auch durch das Füllen von Luft-Ballast-Tanks erzeugt werden. Der sichere Zustand ist dann eingetreten, wenn das U-Boot unbewegt und mit aufgeblasenen Lufttanks an der Wasseroberfläche treibt. (vgl. [Ferguson 2003])

3.5 Der Deaktivierungsprozess eines Atomkraftwerks

Das Austreten von Radioaktivität aus einem Kernkraftwerk infolge einer Explosion nach einer Kernschmelze stellt eine große Gefahr für Mensch und Umwelt dar und muss daher unter allen Umständen vermieden werden. Da Atomreaktoren, verglichen mit allen anderen technischen Systemen, den allerhöchsten Sicherheitsstandards gerecht werden müssen, soll der Stand der Technik dieser Arbeit mit einer Betrachtung der in diesem Kontext gängigen FS-Konzepte abgerundet werden.

Ein Atomreaktor benutzt im Normalbetrieb zur Steuerung und Regelung seiner technischen Anlagen, wie etwa der Reaktorkühlung, die Energie, die er selbst produziert. Bei einem Systemfehler kann es vorkommen, dass diese Energie nicht mehr zur Verfügung steht. Um in diesem Fall die Kühlung sowie andere wichtige Prozesse aufrechtzuerhalten und ein aktives FS-Verhalten zu ermöglichen, stehen gesonderte Dieselgeneratoren zur Verfügung, die die Energieversorgung für eine längere Zeit übernehmen können. Da die in einem Fehlerfall notwendigen Notmaßnahmen von einem Anlagenbediener nicht schnell und verlässlich genug ausgeführt werden können, wird bei einer untolerierbaren Überschreitung eines wichtigen Operationsparameters, wie etwa der Temperatur oder dem Druck, automatisch ein Abschaltevorgang eingeleitet, bei dem die Brennstäbe vollständig in ein Wasserbad versenkt werden[5]. Auf diese Weise wird die Anzahl der Kernspaltungsprozesse reduziert und die unkontrollierte Energieerzeugung nahezu eingestellt. Dennoch ist es notwendig, das

[5] Ein derartiger Abschaltvorgang kann auch manuell vom Anlagenbediener eingeleitet werden.

Kraftwerk nach der Abschaltung dauerhaft aktiv zu kühlen, da auch im abgeschalteten Zustand noch Energie produziert wird, die, bei mangelhafter Kühlung, zu einer Kernschmelze führen kann. (vgl. [Glasstone & Sesonske 1994])

Diese letztgenannte Tatsache unterscheidet das FS-Verhalten eines Atomreaktors von vielen anderen technischen Systemen, bei denen nach der Notabschaltung keine weiteren Aktionen zur Aufrechterhaltung eines sicheren Zustands mehr notwendig sind.

4 Funktionales Architekturkonzept

In diesem Kapitel wird, aufbauend auf der verallgemeinerten Funktionsarchitektur hochautomatisierter Fahrerassistenzsysteme (H FAS) die Einbettung zusätzlicher funktionaler Komponenten zur Systemgrenzenüberwachung (vgl. Kapitel 2.2.1) und Ausführung von Aktionsplänen (vgl. Kapitel 2.2.2) beschrieben. Überdies wird auf die Notwendigkeit verschiedenartiger Redundanzen im Falle eines Stauassistenten (STA) hingewiesen. Das hier vorgestellte Architekturschema hat dabei den Anspruch allgemeingültig und damit auf beliebige vollautomatische bzw. autonome FAS anwendbar zu sein.

4.1 Funktionale Architektur hochautomatisierter Fahrerassistenzsysteme

Nach [Maurer 2000] sind automatisch gesteuerte Fahrzeuge im Kern aus funktionalen Modulen aufgebaut, die sich entlang der Informationsverarbeitungskette im Wesentlichen in fünf Bereiche einordnen lassen und somit eine für den Menschen erlebbare Fahrfunktion implementieren. Diese Strukturierung lässt sich auf H FAS übertragen und ist im folgenden Bild 4.1 skizziert. Die Gesamtheit der angesprochenen Module wird im Folgenden als Normalfunktion bezeichnet.

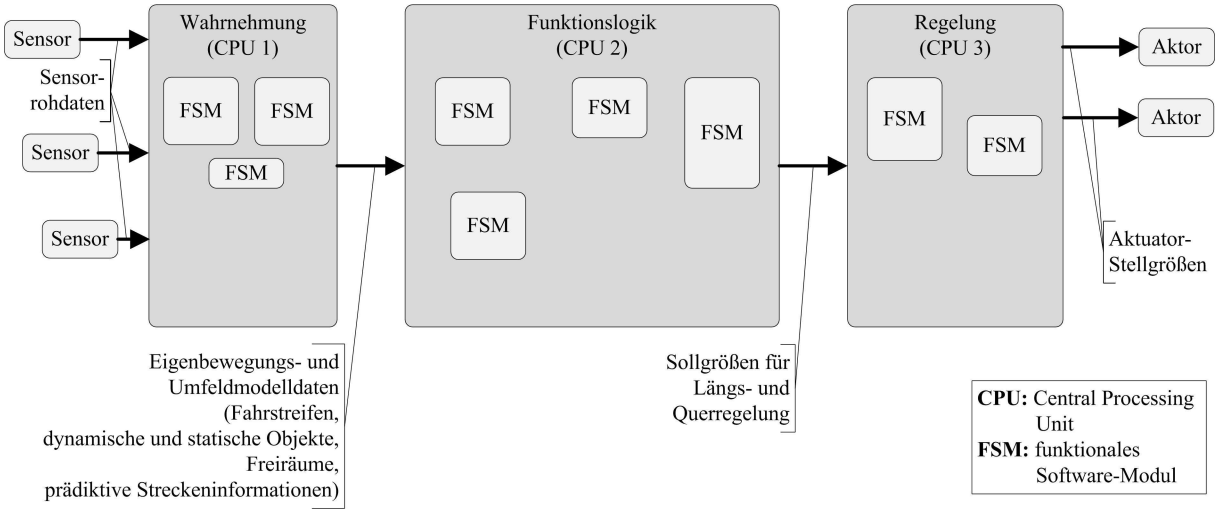

Bild 4.1: Funktionale Architektur der Normalfunktion eines hochautomatisierten Fahrerassistenzsystems in Anlehnung an [Maurer 2000]

Sensoren sind Hardware-Komponenten, die mittels verschiedener Messprinzipien Rohdaten generieren, die die Eigenbewegung des eigenen Fahrzeugs und das Umfeld, in dem sich das Fahrzeug bewegt, beschreiben. Umfelderfassungssensoren, die im Bereich der FAS Einsatz finden, sind unter anderem GPS (Global Positioning System)-, Ultraschall-, Kamera-, Radar- und Lasersysteme.

Die hiermit erfassten Sensorrohdaten werden durch funktionale Softwaremodule (FSM) der sensorischen Wahrnehmung zu Eigenbewegungs- und Umfeldmodelldaten verarbeitet. Eigenbewegungsdaten sind beispielsweise die aktuelle Geschwindigkeit oder die Gierrate des

eigenen Fahrzeugs. Das Umfeldmodell ist ein uninterpretiertes Abbild der aktuellen Verkehrsszene, das in einer für den Menschen verständlichen Repräsentationsform, beispielsweise einer Objektliste, vorliegt. Es enthält Informationen über folgende Aspekte:

- Fahrstreifen (Verlauf der Markierungen auf der Straße[6])
- Bewegte bzw. dynamische Objekte wie beispielsweise andere Fahrzeuge oder Fußgänger (Position, Ausdehnung, Geschwindigkeit und Beschleunigung)
- Unbewegte bzw. statische Objekte wie beispielsweise Leitplanken oder Pannenfahrzeuge (Position, Ausdehnung)
- Freiräume ohne statische oder dynamische Hindernisse, die von der Wahrnehmung explizit als befahrbar klassifiziert wurden (Position, Ausdehnung)
- Unbekannte Gebiete, die von den Sensoren, aufgrund von Verdeckungen durch statische oder dynamische Hindernisse, nicht einsehbar sind (Position, Ausdehnung)
- Prädiktive Streckeninformationen, auch prädiktive Streckendaten genannt, die beispielsweise mittels des GPS aus einer Navigationskarte extrahiert werden oder durch eine Schildererkennung wahrgenommen werden (beispielsweise der aktuell befahrene Straßentyp)

Die im Anschluss an die Wahrnehmung gelagerte Funktionslogik interpretiert diese Szenenbeschreibung in einem ersten Schritt und reichert sie um weitere Informationen an. Man spricht hierbei von Situationsanalyse. Ein entsprechendes Beispiel ist etwa die Klassifikation eines dynamischen Objekts als Fahrzeug, das in die eigene Fahrspur einschert. In einem zweiten Schritt, der sogenannten Verhaltensentscheidung, werden alle nun vorhandenen Informationen von der Funktionslogik dazu verwendet, für die Fahrzeugführung entsprechende Soll-Größen für die Längs- und Querregelung zu berechnen, die festlegen, wie sich das Fahrzeug bewegen soll.

Diese Regelgrößen dienen einer Kaskade nachgelagerter Regler als Eingangs-Soll-Größen. Entsprechend werden daraus zyklisch Aktuator-Stellgrößen zur Ansteuerung der nachgelagerten Aktorik berechnet. Hierbei handelt es sich im Wesentlichen um Eingriffe in Gas, Bremse und Lenkung.

Die in Bild 4.1 dargestellte Verteilung der FSM auf verschiedene zentrale Recheneinheiten (engl. central processing unit, CPU) ist lediglich als Beispiel für eine mögliche Systemauslegung zu betrachten und muss nicht zwingender Weise in derartiger Form erfolgen.

[6] Im Gegensatz zum Begriff Fahrstreifen beschreibt der Begriff Fahrspur den Verlauf des vor dem eigenen Fahrzeug ohne Spurwechsel befahrbaren Korridors inklusive einer definierten Vorausschau. Die Fahrspur bzw. der Fahrspurkorridor wird durch den Verlauf von Fahrstreifenmarkierungen am Boden, also des Fahrstreifens, oder durch Randbebauungen, beispielsweise Leitplanken oder durch in Kolonne vorausfahrende Fahrzeuge bzw. Fahrzeugkolonnen in den Nebenspuren oder durch eine Kombination der genannten Aspekte festgelegt.

4.2 Einbettung von Komponenten des Sicherheitskonzepts

Um die beiden Hauptaufgaben des Sicherheitskonzepts (Systemgrenzenüberwachung und Vorhaltung von Aktionsplänen zur Erlangung eines sicheren Notaus-Zustands, vgl. Kapitel 1.3) zu erfüllen, ist die Einbettung zusätzlicher FSM in die im vorangegangenen Kapitel vorgestellte Funktionsarchitektur notwendig. Dabei wird auf der, im Stand der Technik in Bild 3.1 aufgezeigten, architekturellen Trennung in Überwachungs- und Fehler behebende Aktionseinheiten aufgebaut.

Zur Überwachung der in Kapitel 2.2.1 detailliert erläuterten Systemgrenzen sind die in Bild 2.3 zusammengefassten Detektionsmechanismen notwendig. Entsprechend müssen in jedem vollautomatischen und autonomen FAS folgende Überwachungskomponenten in das FAS integriert werden (vgl. auch Bild 4.2):

- Überwacher externer Einflussgrößen
- Funktionsgrenzen-Überwacher
- Lokale Modul-Überwacher (LMÜ)

Für jede CPU ist ein eigener LMÜ notwendig, der es den FSM, die auf der CPU laufen ermöglicht, ihre per Eigendiagnose intern festgestellten Fehler zu melden. LMÜ müssen ebenfalls für Sensoren und Aktoren vorgehalten werden[7]. Je nachdem, ob das geplante FAS vollautomatisch oder autonom ausgelegt werden soll, muss zusätzlich eine der beiden folgenden Überwachungskomponenten in das System integriert werden:

- Fahrer-Überwacher im Falle eines vollautomatischen FAS (VA FAS)
- Plausibilitätsüberwacher im Falle eines autonomen FAS (A FAS)

Bild 4.2 baut auf Bild 4.1 auf und verdeutlicht, welche der eben erläuterten Überwachungs-Komponenten welche Eingangsdaten benötigen[8]. Bezüglich der Eingangsdaten, die die Überwachungs-Komponenten verwenden, sei auf die entsprechenden Kapitel zur Systemgrenzenüberwachung verwiesen (5, 6 und 7).

[7] LMÜ für Sensoren und Aktoren sind aus Gründen der Übersichtlichkeit nicht in Bild 4.2 eingezeichnet.

[8] Die in diesem Kapitel vorgestellten architekturellen Zusammenhänge wurden bereits vorveröffentlicht (vgl. [Hörwick & Siedersberger 2010b]).

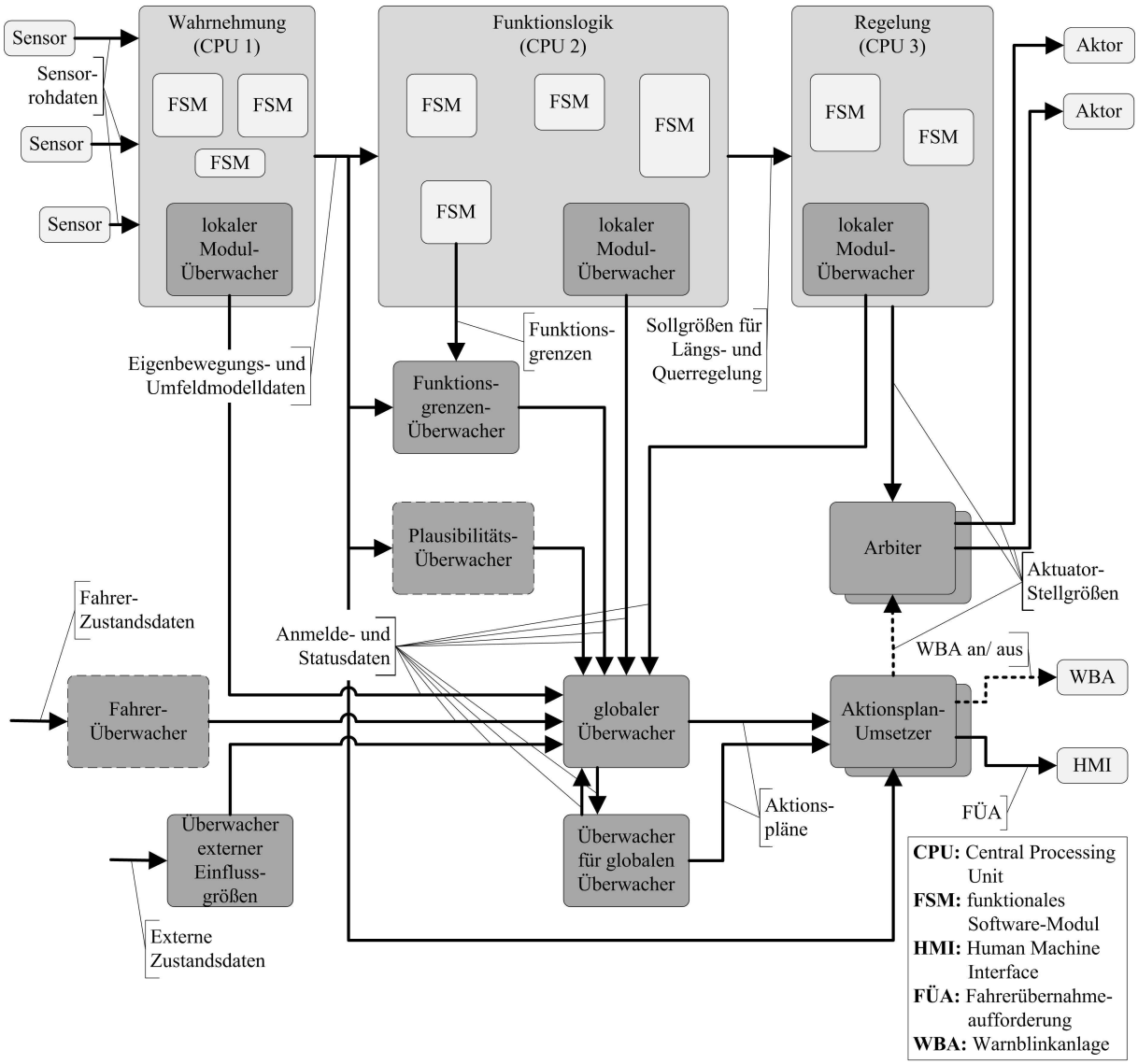

Bild 4.2: Funktionale Architektur des Sicherheitskonzepts für vollautomatische und autonome Fahrerassistenzsysteme (Komponenten des Sicherheitskonzepts in dunkelgrau)

Wie Bild 4.2 zeigt, senden alle genannten Überwachungskomponenten ihren aktuellen Status zyklisch an einen zentralen globalen Überwacher (GLÜ). Die Statusdaten informieren den GLÜ über alle aktuell überschrittenen Systemgrenzen. Der GLÜ hat dadurch den kompletten Überblick über den Zustand des FAS. Aus diesem Grund ist er die zentrale Instanz zur Ansteuerung von Aktionsplänen zur Erlangung eines sicheren Zustands. Um im Falle einer Systemgrenzenüberschreitung die richtigen Aktionspläne anzusteuern, werden dem GLÜ in der Systeminitialisierungsphase Anmeldedaten von den LMÜ und allen anderen Überwachungskomponenten geschickt. In den Anmeldedaten ist jeder Systemgrenzenüberschreitung[9] ein Aktionsplan zugeordnet. Überdies ist der GLÜ in der Lage, die Auswirkungen der in den FSM intern festgestellten und an die LMÜ gemeldeten Fehler zu prädizieren. Die Anmeldedaten der LMÜ informieren deshalb auch, wie die FSM zum Datenaustausch miteinander verkettet sind. Auf Basis dieser Information wird die

[9] Eine Systemgrenzenüberschreitung kann in diesem Kontext auch ein Ausfall der Überwachungskomponente selbst sein.

Prädiktion von Fehlerauswirkungen möglich (vgl. auch Kapitel 5.1). Um einen Ausfall des GLÜ infolge eines Ausfalls der CPU auf der er läuft abfangen zu können, existiert ein gesonderter Überwacher für den GLÜ, der ebenfalls in der Lage ist, Aktionspläne anzusteuern. Beide Komponenten müssen sich bei der jeweils anderen anmelden und zur Ausfallsüberprüfung zyklisch ihren Status melden. Fällt der Überwacher für den GLÜ, aus muss das FAS ebenfalls deaktiviert werden.

Für die Erfüllung der zweiten Hauptaufgabe des Sicherheitskonzepts, der Ausführung von Aktionsplänen zur Erlangung eines sicheren Zustands, ist die Komponente Aktionsplan-Umsetzer (APU) zuständig. Sie wird vom GLÜ oder dem Überwacher für den GLÜ angesteuert. Neben der Anforderung einer Fahrerübernahmeaufforderung (FÜA) bei der Mensch-Maschine-Schnittstelle (engl. Human Machine Interface, HMI) kann der APU im Falle einer autonomen Systemausprägung (gestrichelte Pfeile in Bild 4.2) zudem die Warnblinkanlage (WBA) aktivieren und Aktuator-Stellgrößen zum Eingriff in die Bremse und die Lenkung generieren. Es handelt sich hierbei qualitativ um dieselben Aktuator-Stellgrößen, die auch von der Regelung des A FAS generiert werden. Im Folgenden wird kurz erläutert, wie die Komponente Arbiter (engl. für Schiedsrichter) diese beiden Stellgrößen-Forderungen miteinander abgleicht und an die Aktoren weiterleitet (vgl. Bild 4.3).

Während des Normalbetriebs der autonomen Assistenzfunktion ist der APU inaktiv und generiert keinerlei Forderungen. Daher werden die Stellgrößen der Regelung vom Arbiter direkt an die Aktoren durchgestellt. Fordert der APU dagegen eine Verzögerung, so wird diese vom Arbiter mit der aktuell von der Regelung gestellten Verzögerung verglichen und der größere Wert, also die stärkere Verzögerung, ausgewählt und an die Bremse gestellt. Durch diese kombinierte Längregelung wird ein maximal sicheres Verhalten des Fahrzeugs realisiert. Die Querregelung erfolgt in diesem Fall weiterhin durch die Normalfunktion.

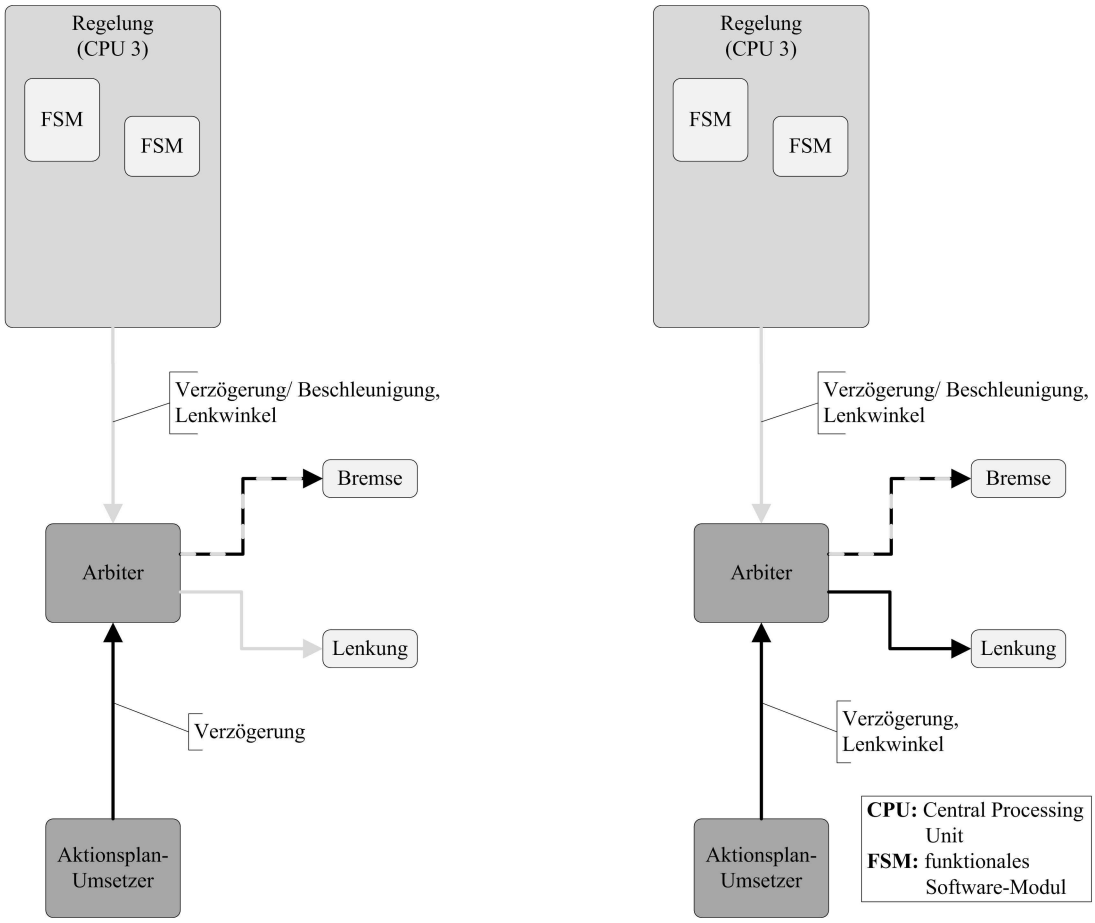

Bild 4.3: Aktuatoransteuerung bei überlagerter Verzögerungsanforderung (links) sowie bei zusätzlicher Lenkwinkelanforderung (rechts)

Wird durch den APU zusätzlich zu einer Verzögerung auch ein Lenkwinkel angefordert, so stellt der Arbiter diese Forderung direkt an die Lenkung durch. Dies liegt daran, dass aus Sicht der Systemsicherheit, anders als im Falle einer Verzögerung, keine pauschale Einschätzung möglich ist, welcher Lenkwinkel der sicherere ist. Die Querregelung erfolgt somit, anders als die Längsregelung, nicht kombiniert.

An dieser Stelle sei abschließend darauf hingewiesen, dass alle Komponenten des Sicherheitskonzepts, die Umfeldinformationen benötigen, ausschließlich Daten des Umfeldmodells verwenden. Ein Eingriff in die Fahrzeugführung erfolgt bei A FAS ausschließlich über den Arbiter. Somit wird, wie in Kapitel 2.3 gefordert, eine strikte Trennung des Sicherheitskonzepts von der Normalfunktion realisiert. Weiterhin wird durch das direkte Generieren von Aktuator-Stellgrößen durch den APU ein sehr direkter, schneller Eingriff in die Fahrzeugsführung realisiert und somit dem übergeordneten Prinzip der Echtzeitfähigkeit Rechnung getragen.

4.3 Redundanzanforderungen an das System Stauassistent

Im Rahmen der architekturellen Auslegung vollständig automatisierter Fahrfunktionen müssen vor allem im Falle einer autonomen Systemausprägung, aus den in Kapitel 2.2.3 genannten Gründen, einige Hardware- und Softwarekomponenten redundant vorgesehen

werden. Im Folgenden werden Redundanzanforderungen, die sich in der Konzeptphase auf funktionaler Ebene für einen STA ergeben, erläutert. Ein konkreteres, auf die finale FAS-Architektur ausgelegtes Redundanzkonzept kann erst im Rahmen der Serienentwicklung definiert werden (vgl. [ISO DIS 26262: 2009]). Grundsätzlich lässt sich aber, nach Recherche des Stands der Technik (vgl. Kapitel 3.3), feststellen, dass für FAS, als typische Vertreter der mechatronischen Systeme, dynamische Redundanzmechanismen angewendet werden müssen, da auf diese Weise die Kosten für Sensorik, Aktorik und Steuergeräte niedrig gehalten werden und die notwendige, komplexe Systemgrenzenüberwachung überhaupt erst möglich wird. Da in H FAS und speziell bei A FAS zur Erkennung fehlerhafter Sensordaten selbige Daten redundant von unterschiedlichen Sensoren verfügbar sind bzw. sein müssen (vgl. Kapitel 2.2.1), muss hier das sogenannte „heiße Standby“ angewendet werden. Aktoren können dagegen dynamisch redundant im „kalten Standby“ vorgehalten und dadurch vor unnötigem Verschleiß geschützt werden. Die im Folgenden aufgelisteten Hardware-Komponenten müssen, falls nicht ausdrücklich darauf hingewiesen wird, ausschließlich im Falle einer autonomen Systemausprägung redundant ausgelegt werden.

- Elektronisch ansteuerbare Bremse: Da, wie in Kapitel 8.1 noch genau hergeleitet wird, der sichere Notaus-Zustand eines autonomen STA der Stillstand innerhalb der eigenen Fahrspur ist, muss auch bei einem Ausfall der konventionellen elektronisch ansteuerbaren Bremse die Ausführung eines Bremsmanövers möglichen sein. Dazu muss eine redundante elektronisch ansteuerbare Bremse, beispielsweise die Parkbremse, vorhanden sein.
- Elektronisch ansteuerbare Lenkung: Um den STA bei einem Ausfall der konventionellen, elektronisch ansteuerbaren Lenkung während des Bremsvorgangs zur Erlangung des sicheren Notaus-Zustands innerhalb der eigenen Fahrspur zu halten, muss ein redundanter Pfad zum Eingriff in die Querführung existieren. Denkbar wäre dabei die Erzeugung eines Giermoments durch die Ansteuerung einzelner Radbremsen durch das elektronische Stabilitätsprogramm (ESP), wie es beim „aktiven Totwinkel-Assistenten“ von Daimler bereits in Serie praktiziert wird (vgl. [Howland 2010]). Die Ausführung eines derartigen Notlenkmanövers ist, wie im Folgenden dargelegt wird, vor allem bei höheren Geschwindigkeiten und damit verbundenen größeren Bremswegen zwingend notwendig. Bild 4.4 zeigt, dass die Querablage geometrisch vom Bremsweg und dem Sinus des Gierwinkels[10] des Fahrzeugs gegenüber des Fahrstreifens abhängig ist. Geht man bei einer STA-Maximalgeschwindigkeit von 60km/h von einem Mindest-Bremsweg von etwa 15m aus, so erhält man bereits bei einem Gierwinkel von 7° eine Querablage von etwa 1,8m. Bei einer Fahrzeugbreite von etwa 2m und einer Fahrstreifenbreite von 3,75m auf deutschen Autobahnen (vgl. [RAS-Q 1996]) muss unter den genannten Umständen davon ausgegangen werden, dass das Fahrzeug auf jeden Fall die Spur verlässt. Aus diesem Grund ist die

[10] Genau genommen handelt es sich hierbei um den Kurswinkel, der sich als Summes des Gier- und des Schwimmwinkels berechnet. Bei STA-Systemen kann aufgrund der geringen Dynamik von einem Schwimmwinkel von Null ausgegangen werden. Daher wird der Begriff Gierwinkel in dieser Arbeit synonym zum Begriff Kurswinkel verwendet.

Vorhaltung einer redundanten Lenkung zur Durchführung eines Notlenkmanövers zwingend erforderlich.

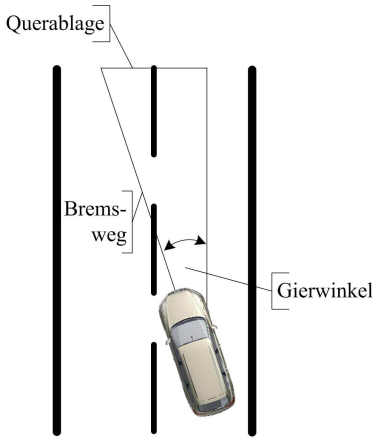

Bild 4.4: Begründung der Notwendigkeit einer redundanten, elektronisch ansteuerbaren Lenkung

- Inertial-Sensorik: Ein Ausfall der Inertial-Sensorik bzw. der von ihr generierten Eigenbewegungsdaten hat den Ausfall sämtlicher Umfeldmodelldaten zur Folge, da die FSM der Umfeld-Wahrnehmung zur Durchführung einer Eigenbewegungs-Kompensation Eigenbewegungsdaten benötigen. Bei einem gleichzeitigen Ausfall der Eigenbewegungs- und Umfeldmodelldaten ist es nicht möglich, die Querführung aufrecht zu erhalten, was auch im Falle einer sofortigen Vollbremsung dazu führen kann, dass das Fahrzeug die Spur verlässt (vgl. Fußnote 36 auf Seite 107, sowie obiges Beispiel). Aus diesem Grund ist die Inertial-Sensorik redundant vorzusehen.
- Umfeld-Sensorik: Unplausible Sensorrohdaten, die zu einem unplausiblen Umfeldmodell führen, das wiederum zu einem unplausiblen Verhalten des eigenen Fahrzeugs bzw. situativen Unplausibilitäten führt, müssen bei A FAS, wie dem autonomen STA, im Rahmen der Eigendiagnose der Wahrnehmung erkannt werden (vgl. Kapitel 2.2.1). Dies ist ausschließlich durch den Vergleich redundanter Information von redundanten Umfeldsensoren möglich.
- Sensorik zur Fahreranwesenheitserkennung: Im Rahmen der Überwachung externer Einflüsse (vgl. Kapitel 2.2.1) ist unter anderem eine Überprüfung der Fahreranwesenheit notwendig, um zu verhindern, dass der Fahrer das Fahrzeug im Stillstand verlässt, sich vor das Fahrzeug bewegt und vom anfahrenden Fahrzeug erfasst wird. In der Gefährdungsanalyse und Risikoeinstufung ergibt sich für diese Fehlfunktion ein Automotive Safety Integrity Level (ASIL) im Bereich A bis B. Aus diesem Grund ist die entsprechende Sensorik redundant auszulegen. Denkbar sind beispielsweise eine Kombination aus Türkontakt- und Gurtschlosssensor. Diese Redundanzforderung gilt auch für den vollautomatischen STA bzw. VA FAS allgemein.
- Sensorik zur Domänenerkennung: Im Rahmen der Funktionsgrenzenüberwachung (vgl. Kapitel 2.2.1) ist unter anderem eine Überprüfung notwendig, ob sich der STA innerhalb der Domäne Autobahn bewegt. Es ergibt sich in der Gefährdungsanalyse und Risikoeinstufung für die Fehlfunktion „Verlassen der Autobahn“ ein ASIL von C.

Aus diesem Grund sind auch hier redundante Informationsquellen notwendig. Beispielsweise ließen sich prädiktive Streckeninformationen aus einer Navigationskarte und Daten aus einer auf Umfeld-Sensorik basierenden Schildererkennung verwenden. Diese Redundanzforderung gilt auch für den vollautomatischen STA.

Die bisher genannten Redundanzforderungen betreffen ausschließlich Hardware-Komponenten. Eine genaue Vorgabe, welche Software-Komponenten diversitär redundant ausgelegt werden müssen, ist in der Konzeptentwicklungsphase nicht sinnvoll, da die Software-Architektur hier noch nicht fertig definiert ist. Allerdings lässt sich bereits in dieser frühen Phase feststellen, dass einige Software-Komponenten des Sicherheitskonzepts redundant auf verschiedenen CPUs vorzuhalten sind, um im Falle eines Ausfalls einer dieser CPUs trotzdem noch einen Aktionsplan zur Erlangung eines sicheren Zustand ansteuern bzw. ausführen zu können:

- Arbiter: Der Arbiter ist nur bei A FAS bzw. einem autonomen STA notwendig, da nur hier ein unterlagerter Eingriff in die Fahrzeugführung vorzuhalten ist.
- GLÜ: Die Vorhaltung eines Überwachers für den GLÜ ist, wie bereits in Kapitel 4.2 beschrieben wurde, notwendig und stellt ebenfalls eine Art Redundanz dar. Diese Redundanzforderung gilt für VA FAS und A FAS bzw. die entsprechenden STA-Ausprägungen gleichermaßen.
- APU: Diese Redundanzforderung gilt für VA FAS und A FAS bzw. die entsprechenden STA-Ausprägungen gleichermaßen.

5 Grundlegende Aspekte der Überwachung vollautomatischer und autonomer Fahrerassistenzsysteme

In Kapitel 2.2.1 wurden die verschiedenen Aspekte, die bei automatischen Fahrfunktionen zu überwachen sind, vorgestellt. An dieser Stelle sollen nun auf die in Bild 2.3 aufgeführten Mechanismen zur Detektion der Systemgrenzen eingegangen werden, die in gleicher Form bei vollautomatischen und autonomen Fahrerassistenzsystemen (FAS) notwendig sind.

5.1 Überwachungskonzept zur Erkennung von Fehlern in Einzelkomponenten

Fehler in einzelnen Komponenten eines FAS, also im FAS intern auftretende Fehler, beruhen unter anderem auf Fehlfunktionen der Sensoren und Aktoren des FAS oder auf der begrenzten Funktionalität der funktionalen Softwaremodule (FSM), die die Steuerungs- und Regelungsfunktion des FAS implementieren (Bild 3.4)[11]. Im Stand der Technik wurde dargelegt, dass eine Erkennung und Diagnose dieser Fehler in der Regel durch eine modellbasierte Überwachung erfolgt (vgl. Bild 3.2). Die Implementierung derartiger Überwachungsfunktionen zur Komponenteneigendiagnose ist dabei von der in dem jeweiligen FSM implementierten Funktionalität abhängig und muss daher im jeweiligen Einzelfall durch den entsprechenden Entwickler erfolgen. Ein allgemeiner, auf unterschiedliche FSM anwendbarer Überwachungsmechanismus oder Algorithmus ist daher nicht realisierbar und deshalb auch nicht Ziel dieser Arbeit. Es sei aber an dieser Stelle darauf hingewiesen, dass gerade im Bereich der sensorischen Umfeldwahrnehmung Forschungsbedarf hinsichtlich der Eigendiagnosefähigkeit und der Generierung verlässlicher Gütemaße für Umfeldmodelldaten (vgl. Kapitel 4.1) besteht. Dies erscheint vor allem im Hinblick auf autonome FAS (A FAS) wichtig, da hier sämtliche Fehler im Bereich der sensorischen Wahrnehmung per Eigendiagnose detektiert werden müssen (vgl. Kapitel 2.2.1).

In diesem Kapitel soll ein Konzept vorgestellt werden, das es Einzelkomponenten in einem verteilten FAS, bestehend aus mehreren Recheneinheiten, ermöglicht, intern festgestellte Fehler standardisiert zu melden und deren Auswirkung auf der Basis von a priori Wissen zu prädizieren. Dazu soll der im Stand der Technik in Kapitel 3.2.2.2 vorgestellte Mechanismus der Programmablaufüberwachung auf einem Steuergerät mittels eines Watchdogs aufgegriffen, erweitert und auf die funktionalen Einzelkomponenten des FAS (Sensoren, FSM

[11] Die Überwachung der Hardware, auf der die Software implementiert ist, also die Funktionsfähigkeit des Prozessors und der zugehörigen Speicher- und Ein-/Ausgabeeinheiten sowie der Datenübertragung, ist von der konkreten Zielhardware abhängig. Die Erarbeitung entsprechender Überwachungsmechanismen ist deshalb nicht Aufgabe eines funktionalen Sicherheitskonzepts in der Konzeptphase (vgl. Kapitel 1.3).

und Aktoren) angewendet werden. Es wird dabei davon ausgegangen, dass all diese Komponenten mit einer gewissen Mindestfrequenz arbeiten. Diese ist in der Regel durch den Takt, in dem die Sensoren Daten liefern oder durch systeminterne Timer vorgegeben.

Die Grundidee des Konzepts besteht darin, dass jede funktionale Komponente regelmäßig, innerhalb vereinbarter Zykluszeiten, Watchdog-Resets ausführen muss. Mit der Abgabe der Watchdog-Resets soll das Modul zudem binäre Qualitätsangaben, entweder „OK“ oder „nicht OK“, über seinen aktuellen Status machen. Auf diese Weise wird einer jeden Komponente eine Schnittstelle geboten, per Eigendiagnose intern erkannte Fehler zu melden. Da die Überwachung intelligenter Funktionen meist auf Basis ihrer errechneten Ausgangswerte geschieht (vgl. Kapitel 3.2.2.1), ist es sinnvoll, die Qualitätsaussagen genauso wie die vereinbarten Zykluszeiten auf die Datenstrukturen an den verschiedenen Ausgabeschnittstellen einer Komponente, also deren Ausgängen, zu beziehen (vgl. Bild 5.1). Jede Einzelkomponente wird daher dazu verpflichtet, immer zeitgleich mit dem Versenden einer validen oder invaliden Datenstruktur einen Watchdog-Reset inklusive einer entsprechenden Qualitätsangabe abzusetzen[12]. Durch den Vergleich der verstrichenen Zeit seit dem letzten Sendezeitpunkt mit einem vereinbarten Maximalwert und die Auswertung der binären Zusatzinformation kann somit eine gleichzeitige Frequenz- und Qualitätskontrolle vollzogen werden. Genau wie bei der Qualitätskontrolle werden auch bei der Frequenzkontrolle nur die Zustände „OK“ und „nicht OK“ unterschieden. Daraus abgeleitet ergeben sich für eine Ausgabeschnittstelle vier mögliche Fehlerzustände. Aus Performancegründen ist es sinnvoll, auf jeder Central Processing Unit (CPU) einen lokalen Modul-Überwacher (LMÜ) als Watchdogeinheit einzurichten (vgl. Kapitel 4.2), die die Watchdog-Resets der darauf befindlichen FSM empfängt, die Prüfung der Sendefrequenz durchführt und somit die aktuellen Zustände an allen Ausgabeschnittstellen aller FSM seiner CPU kennt. Da die funktionalen Komponenten eines hochautomatisierten FAS (H FAS) entlang der Datenverarbeitungskette Sensorik - Wahrnehmung - Funktionslogik - Regelung - Aktorik in vordefinierter Weise über Schnittstellen Informationen weiterleiten, ist es möglich, im Falle eines Fehlers in einer funktionalen Komponente die Auswirkungen auf die nachfolgenden funktionalen Komponenten vorherzusagen und somit Zeit bei der Auswahl und Einleitung entsprechender Gegenmaßnahmen zu sparen. Somit wird dem Prinzip der „Prävention“ (vgl. Kapitel 2.3) Rechnung getragen. Diese sogenannte Fehlerpropagation kann allerdings nur durch eine Instanz im System erfolgen, die über ein komplettes Abbild der gesamten Systemarchitektur mit allen Sensoren, Aktoren, CPUs, darauf implementierten FSM und der zugehörigen verbindenden Schnittstellen verfügt. Dabei stellt insbesondere die Tatsache, dass H FAS im allgemeinen verteilte Systeme sind, eine Herausforderung dar, da auch die Propagation von Fehlern in FSM auf FSM anderer CPUs, also über Rechnergrenzen hinweg, angestrebt wird. Die dazu notwendige zentrale Speicherung des Systemabbildes wird im globalen Überwacher (GLÜ) umgesetzt (vgl. Kapitel 4.2). An dieses Modul leitet jeder

[12] Bei der softwaremäßigen Realisierung des vorgestellten Konzepts empfiehlt es sich, ähnlich wie von [Papp & Zoutendijk 2003] vorgeschlagen, eine auf beliebige FSM anwendbare Sicherheitshülle (engl. safety wrapper) zu implementieren, die die Funktionalität des Absetzens der Watchdog-Resets mit den zugehörigen Qualitäts-Informationen kapselt.

LMÜ die bei ihm gemeldeten Qualitäts-Fehler oder durch ihn erkannten Fehler in der Sendefrequenz zur Auswertung weiter. Der GLÜ kennt dadurch zu jedem Zeitpunkt alle gemeldeten Fehler im System und ist in der Lage, die Fehlerfortpflanzung auf Basis des Gesamtsystemabbildes zu prädizieren. Für jeden einzelnen prädizierten Fehlerfall in einer funktionalen Komponente sind in einer Nachschlagetabelle Identifikationsnummern für entsprechende Aktionspläne zur Fehlerbehandlung hinterlegt. Diese werden vom GLÜ nach Bestimmung und Propagation aller Fehler im System ausgelesen und an den APU (Aktionsplan-Umsetzer) zur Abarbeitung weitergeleitet. Durch zyklisches Absetzen eines Statusbits durch jeden einzelnen LMÜ ist mittels des GLÜ zudem die Überwachung der CPUs selbst möglich. Eine Übersicht über die beschriebenen, architekturellen Zusammenhänge wurde bereits in Bild 4.2 gegeben. Es sei an dieser Stelle darauf hingewiesen, dass das hier vorgeschlagene Konzept lediglich ein Verfahren zur Onboard-Diagnose darstellt. Ein Konzept zur Fehlerdiagnose nach Verlassen des Normalbetriebs, beispielsweise durch einen Diagnosetester in der Werkstatt, ist nicht Ziel dieser Arbeit (vgl. Kapitel 1.3).

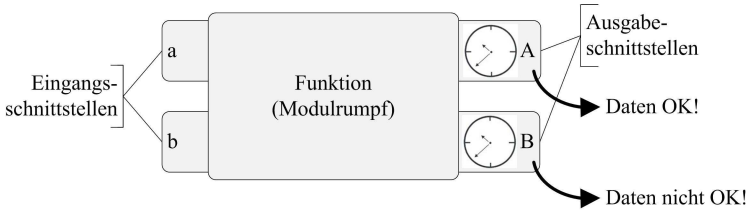

Bild 5.1: Funktionales Softwaremodul als Blackbox

In den folgenden Unterkapiteln wird das eben skizzierte Überwachungskonzept detailliert beschrieben, wobei zunächst ausschließlich auf FSM eingegangen wird und Sensoren und Aktoren vorerst ausgeklammert werden. Ein FSM ist in diesem Kontext als Blackbox mit einer beliebigen Zahl von Eingangs- und Ausgabeschnittstellen zu verstehen, über die das FSM mit anderen FSM verknüpft ist (vgl. Bild 5.1).

In Kapitel 5.1.1 werden zunächst die möglichen Fehlerzustände an der Ausgabeschnittstelle eines FSM definiert. Kapitel 5.1.2 zeigt, dass die Fehlerbehebungsmaßnahmen, die ein derartiger Fehler erfordert, von den FSM bestimmt wird, denen die Ausgabeschnittstelle als Datenquelle dient. Daraufhin wird in Kapitel 5.1.3 das Prinzip der Fehlerpropagation ausführlich beschrieben. Da durch die Fehlerpropagation für eine Datenschnittstelle, neben dem durch das FSM gemeldeten Fehlerzustand, ein davon verschiedenartiger Fehlerzustand prognostiziert werden kann, ist es notwendig, in Kapitel 5.1.4 eine Hierarchie der Fehlerzustände einzuführen. Die systeminterne Kommunikation zwischen FSM, LMÜ, GLÜ und APU während der Initialisierung und im Normalbetrieb wird in Kapitel 5.1.5 beschrieben. Abschließend wird dargelegt, wie das Konzept, das im Wesentlichen für FSM ausgelegt ist, auf Sensoren und Aktuatoren adaptiert werden kann (Kapitel 5.1.6).

5.1.1 Fehlerzustände an Modulausgängen

Das in diesem Abschnitt beschriebene Überwachungskonzept hat zum Ziel, die Ausgabeschnittstellen von FSM hinsichtlich Datengüte und Datensendefrequenz zu

überwachen, wobei die Datengüte einer jeden Ausgabeschnittstelle per Eigendiagnose vom FSM selbst beurteilt und in binärer Form an den LMÜ gemeldet wird. Die Einhaltung von minimalen Datensendefrequenzen an den verschiedenen Ausgabeschnittstellen wird dagegen direkt vom LMÜ geprüft. Abgeleitet daraus lassen sich vier Fehlerzustände für Modulausgänge definieren, die ein LMÜ feststellen kann. Sie sind in Tabelle 5.1 dargestellt.

		Datenfrequenz OK	Datengüte OK	Wechsel in anderen Zustand möglich
Status an Ausgabe-schnittstelle	OK	ja	ja	ja
	Frequenzfehler	nein	ja	ja
	temporärer Fehler	unerheblich	nein	ja
	Totalausfall	unerheblich	nein	nein

Tabelle 5.1: Fehlerzustände an der Ausgabeschnittstelle eines funktionalen Softwaremoduls

Werden beide Prüfkriterien eingehalten, so liegt der fehlerfreie Grundzustand „OK“ vor. Wird dagegen seitens des LMÜ festgestellt, dass die gelieferten Daten zwar in Ordnung sind, die vorgegebene maximale Sendezykluszeit aber überschritten wird, so liegt ein „Frequenzfehler“ vor. „Frequenzfehler“ können sich beispielsweise durch zu hohe Prozessorauslastungen ergeben. Meldet ein FSM, dass seine momentan versendeten Daten nicht in Ordnung sind, liegt ein sogenannter „temporärer Fehler“ vor. Es ist dabei unerheblich, ob die Datenpakete noch rechtzeitig versendet werden, da sie ja nicht zur Verarbeitung herangezogen werden können. Ein entsprechendes Beispiel ist etwa das Erblinden der Kamerasensorik aufgrund einer Verdeckung mit Schmutz oder Eis, was wiederum von einem Bildverarbeitungsalgorithmus festgestellt wird. Es ist möglich, aus den beiden zuletzt genannten Fehlerzuständen wieder in den Zustand „OK“ überzugehen, falls die entsprechenden Kriterien dazu wieder erfüllt sind. Ein FSM kann seine Fehlerbotschaft im Vergleich zu einem „temporären Fehler“ aber noch verstärken und stattdessen einen „Totalausfall“ melden. Es gibt damit an, dass das Befüllen der Schnittstelle mit validen Daten in absehbarer Zeit nicht mehr möglich sein wird und deshalb in Zukunft ein Wechsel in den Zustand „OK“ ausgeschlossen ist. Einen „Totalausfall“ stellt beispielsweise ein Defekt in einem Sensor infolge mechanischer Einwirkung dar.

5.1.2 Fehlerauswirkungsbeurteilung an Moduleingängen

Nachdem im vorangegangenen Kapitel erläutert wurde, wie im FAS intern auftretende Fehler erkannt und klassifiziert werden können, muss nun im nächsten Schritt festgelegt werden, welche Konsequenzen das Auftreten eines Schnittstellenfehlers hat. Dies muss logischerweise jeweils von denjenigen FSM festgelegt werden, die die betroffenen Daten nutzen. Es wird daher gefordert, dass alle FSM für jeden ihrer Eingänge festlegen, inwiefern sie Fehler tolerieren können und, falls möglich, wie schwerwiegend ein Fehler an einem Eingang für das Gesamtsystem ist und ob bzw. welcher Aktionsplan zum Übergang in einen sicheren Zustand dementsprechend ausgeführt werden soll.

Da „Frequenzfehler“ und „temporäre Fehler“ im Gegensatz zu endgültigen „Totalausfällen“ nur vorübergehende Zustände sind, muss es für ein FSM, das die entsprechende Schnittstelle als Datenquelle nutzt, möglich sein festzulegen, wie viele dieser Fehler es innerhalb eines

gewissen Zeitintervalls toleriert und ab wann sich der Fehlerzustand der Datenquelle damit gewissermaßen auf seinen Eingang überträgt. Dies hängt beispielsweise davon ab, ob die Eingangsdaten vom FSM gepuffert werden, wie oft der Algorithmus eine Aktualisierung der Eingangswerte verlangt und ob mittels Prädiktion noch eine gewisse Zeit valide Ausgangsdaten bestimmt werden können. Umgesetzt wird dieses Toleranzprinzip durch je eine sogenannte Fehlerrelevanztabelle pro FSM. Hierin sind für alle Eingänge des FSM, sowohl für den Zustand „Frequenzfehler“ als auch „temporärer Fehler“, jeweils eine tolerierte Fehlerzahl und der Betrachtungszeitraum hinterlegt, innerhalb dem diese Fehlerzahl auftreten darf, um das FSM gerade noch nicht zu beeinträchtigen und somit keinen Aktionsplan hervorzurufen.

Eingang	Fehlerzustand	tolerierte Fehlerzahl	Betrachtungs-zeitraum [s]
a	Frequenzfehler	2	3
	temporärer Fehler	1	4
b	Frequenzfehler	1	2
	temporärer Fehler	0	0

Tabelle 5.2: Beispielhafte Fehlerrelevanztabelle für ein funktionales Softwaremodul

Wie man im oben abgebildeten Beispiel (Tabelle 5.2) für das Modul aus Bild 5.1 sehen kann, überträgt sich ein „Frequenzfehler“ der Datenquelle auf den Eingang a, sobald dieser mehr als zweimal innerhalb von 3s auftritt. Für den Ausgang b ist dagegen ein „temporärer Fehler“ bereits beim ersten Auftreten nicht tolerierbar.

Grundsätzlich beeinflussen sich die beiden angesprochenen Fehlerarten nicht gegenseitig. Sie werden daher separat gezählt. Wird die Anzahl der zulässigen ausbleibenden oder fehlerhaften Datenpakete an der Datenquelle wieder unterschritten, wird auch der Fehlerzustand des Eingangs wieder auf „OK“ zurückgesetzt. Letzteres gilt nicht für den Zustand „Totalausfall“. Dieser überträgt sich direkt auf den Eingang und bleibt dort bis zur Systemdeaktivierung erhalten.

Nachdem nun für jeden Zeitpunkt geklärt ist, welche Fehlerzustände die Eingänge der FSM in Abhängigkeit ihrer Datenquellen bzw. ihrer Vorgängermodule aufweisen, wird nun definiert, welcher Aktionsplan abhängig vom Eingangszustands ausgelöst werden soll. Dazu wird die sogenannte Fehlerauswirkungstabelle eingeführt.

Fehlerkombination am Eingang	Aktionsplan	Propagierter Fehler an Ausgabeschnittstelle
Frequenzfehler(a)	---	temporärer Fehler(A)
temporärer Fehler(a)	---	Frequenzfehler(A)
Totalausfall(a)	---	Totalausfall(A) + Totalausfall(B)
Frequenzfehler(b)	---	Frequenzfehler(A)
temporärer Fehler(b)	---	temporärer Fehler(A)
Totalausfall(b)	---	Totalausfall(B)
Frequenzfehler(a) + Totalausfall(b)	„Bremsung (0s, -4m/s^2)“	Totalausfall(B)
temporärer Fehler(a) + Totalausfall(b)	---	Frequenzfehler(A) + Totalausfall(B)

Tabelle 5.3: Beispielhafter Ausschnitt aus einer Fehlerauswirkungstabelle für ein funktionales Softwaremodul

Die Fehlerauswirkungstabelle enthält in der ersten Spalte sowohl alle Fehlerzustände für einzelne Eingänge als auch Kombinationen von Fehlerzuständen mehrerer Eingänge und legt dazu in der zweiten Spalte jeweils den Aktionsplan in Form einer Typbezeichnung, einer Identifikationsnummer und einer Parameterliste fest, der bei Auftreten einer bestimmten Kombination aktiviert werden soll. Auf die Bedeutung der dritten Spalte wird in Kapitel 5.1.3 näher eingegangen. Tabelle 5.3 zeigt einen beispielhaften Ausschnitt aus einer Fehlerauswirkungstabelle für das Modul aus Bild 5.1, wobei nicht alle möglichen Fehlerzustandskombinationen für die Eingänge a und b dargestellt sind[13]. Ändert sich der Fehlerzustand eines oder mehrerer Eingänge eines FSM, so wird jedes Mal dessen Fehlerauswirkungstabelle nach dem aktuellen Fehlermuster durchsucht und der entsprechende Aktionsplan ausgewählt. Das folgende Bild 5.2 verdeutlicht diesen Mechanismus nochmals bezüglich des oben aufgeführten Beispiels:

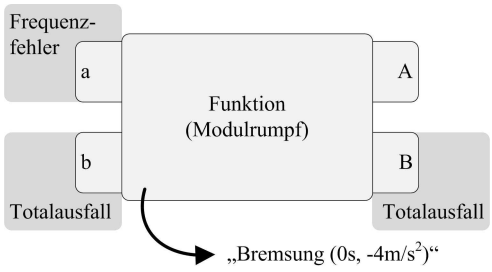

Bild 5.2: Aktionsplanauswahl und Fehlerpropagation

[13] Die Bezeichnung der Aktionspläne erfolgt hier gemäß den Definitionen in Kapitel 8.2 und 8.4. Es ist auch möglich, im Fehlerfall keinen Aktionsplan auszuführen. Dies ist durch „---“ gekennzeichnet.

5.1.3 Fehlerpropagation

In der Regel besteht zwischen den Fehlerzuständen an den Eingängen FSM und den sich dadurch ergebenden Fehlerzuständen an den Ausgängen kein unmittelbarer Zusammenhang. Fehlerhafte oder fehlende Eingangsdaten führen aber mittelbar mit einer gewissen Zeitverzögerung dazu, dass FSM ihre Ausgabeschnittstellen nicht mehr sinnvoll befüllen können und dies selbstständig durch die vorhandenen Eigendiagnosemechanismen feststellen bzw. dies extern durch einen LMÜ festgestellt wird. Es ergibt sich somit das Problem, dass sich bei der Fortpflanzung eines Fehlers durch das System an jedem FSM eine gewisse Latenz ergibt. Geht man allerdings davon aus, dass der Entwickler eines FSM im Voraus bereits absehen kann, welche Konsequenz fehlerbehaftete Datenquellen auf die Funktionsweise des FSM haben und welche Ausgabeschnittstellen dementsprechend nicht mehr bedient werden können, so lassen sich die entstehenden Folgefehler prädizieren. Dieses Verfahren wird Propagation genannt. Es hat den Vorteil, dass die entsprechenden Aktionspläne jedes einzelnen fehlerhaften Moduleingangs entlang der prognostizierten Fehlerkette bereits vor Ablauf der Latenzzeiten ausgelöst werden können und somit einer Eskalation der Fehlerfolgen vorgebeugt wird. Ein weiterer Vorteil besteht darin, dass lediglich für jene FSM Aktionspläne definiert werden müssen, bei denen die Konsequenzen von entsprechenden Fehlern an den Eingangsschnittstellen auf das Funktionieren des Gesamtsystems wirklich abschätzbar sind. Klassischerweise handelt es sich hierbei um weiter hinten in der Datenverarbeitungskette liegende FSM der Funktionslogik oder Regelung. In den Fehlerauswirkungstabellen der FSM der Wahrnehmung müssen somit keine Aktionspläne angegeben werden. Derartige Fehler lassen sich propagieren und lösen damit Aktionspläne von FSM aus, die das Fahrzeugverhalten generieren. Bild 5.3 zeigt eine beispielhafte Fehlerpropagationskette an deren Ende das Modul aus Bild 5.2 steht.

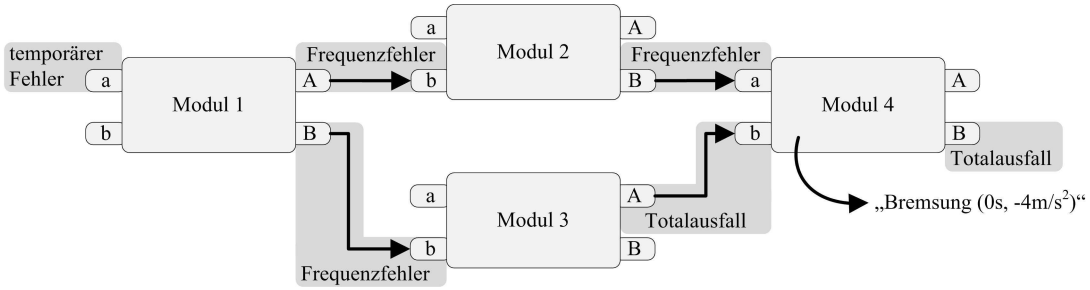

Bild 5.3: Beispiel für eine Fehlerpropagationskette

Umgesetzt wird die Fehlerpropagation ebenfalls mittels der bereits angesprochenen Fehlerauswirkungstabelle (vgl. Tabelle 5.3). Diese enthält für alle möglichen Fehlerzustände der einzelnen Eingänge eines FSM sowie für deren Kombinationen neben dem auszuführenden Aktionsplan auch eine kausale Kombination von Fehlerzuständen an den Ausgängen des FSM, die sich als Folge der Fehler am Eingang ergeben (vgl. Beispiel in Bild 5.2). Ein, in derartiger Weise, an einen Ausgang propagierter Fehler überträgt sich im Gegensatz zu einem vom FSM gemeldeten Fehler sofort auf die Eingänge der nachfolgenden FSM, die diesen Ausgang als Datenquelle verwenden. Auf diese Weise wird die Vermeidung der Latenzzeiten erreicht. An den letztgenannten Eingängen wird der Fehler dann wieder mit entsprechenden Fehlerauswirkungstabellen propagiert. Dieser Vorgang wird so lange wiederholt, bis das Ende der Datenverarbeitungskette erreicht ist.

5.1.4 Hierarchie der Fehlerzustände

Durch das Propagieren besteht an einer Ausgabeschnittstelle zusätzlich zu dem Fehlerzustand, der vom FSM gemeldet bzw. vom LMÜ festgestellt wird, ein weiterer Fehlerzustand. Wie bereits erwähnt, überträgt sich der erstgenannte Fehlerzustand in einigen Fällen erst nach einer gewissen Zeit auf die verbundenen Eingänge nachfolgender FSM, wohingegen sich jeglicher an einen Ausgang propagierter Fehlerzustand sofort auf die entsprechenden Eingänge überträgt. Somit bestehen also theoretisch auch an einem Moduleingang zwei Fehlerzustände, die unterschiedlich sein können. Um mit der Fehlerauswirkungstabelle eindeutig einen Aktionsplan bestimmen und die Fehlerpropagation durch das Gesamtsystem durchführen zu können, wird im Folgenden eine Fehlerhierarchie eingeführt, die bestimmt, welcher der beiden Fehlerzustände schwerwiegender ist und deshalb mit der Fehlerauswirkungstabelle ausgewertet werden soll. Im Gegensatz zu einem Ausgang darf der Eingang eines FSM somit per Definition nur einen einzigen Fehlerzustand einnehmen.

Der nach „OK“ am wenigsten schwerwiegende Fehlerzustand ist der „Frequenzfehler“, da die nachfolgenden FSM hierbei auf Basis der zwar zu selten versendeten, aber dennoch validen Daten, meist noch für einen verhältnismäßig langen Zeitraum ein Fortführen ihrer Funktionalität ermöglichen können. Wenn bei einem „temporären Fehler“ dagegen keine validen Daten mehr geliefert werden, können die nachfolgenden FSM aufgrund der fehlenden Eingangsdaten meist nur noch kurze Zeit weiter funktionieren. Dabei ist es unerheblich, ob die Daten noch regelmäßig versendet werden, da die nachfolgenden FSM üblicherweise vom Datenlieferanten über die mangelhafte Datenqualität informiert werden und sie deshalb nicht weiter verwenden. Der „temporäre Fehler“ ist somit schwerwiegender als der „Frequenzfehler“, lässt aber immerhin die Möglichkeit offen, dass wieder der Zustand „OK“ erreicht werden kann. Da dies bei einem „Totalausfall“ nicht mehr möglich ist, ist er der schwerstwiegende Fehlerzustand in der Fehlerhierarchie. Die Fehlerhierarchie ist, von oben nach unten betrachtet, auch aus Tabelle 5.1 ersichtlich.

5.1.5 Kommunikation während Initialisierung und Normalbetrieb

Den bisherigen Ausführungen ist zu entnehmen, dass für jeden Ausgang eines FSM ein direkt dort festgestellter Fehlerzustand und ein propagierter Fehlerzustand existiert, der sich im zeitlichen Verlauf jeweils beliebig ändern kann. Eine Ausnahme stellt der „Totalausfall“ dar, der nach Eintreten nicht mehr verlassen werden kann. Nach jeder Fehlerzustandsänderung an einem beliebigen Ausgang eines FSM und der eventuell zeitlich versetzten Übertragung dieses Zustands auf den Eingang eines nachfolgenden FSM werden ausgehend von diesem Eingang, der dort unter Beachtung der Fehlerhierarchie festgestellte Fehlerzustand durch das System propagiert und entsprechende Aktionspläne angestoßen. Das bedeutet, dass die Fehlerzustände der Ein- und Ausgänge sämtlicher in der Signalverarbeitungskette nachfolgender FSM mittels der jeweiligen Fehlerauswirkungstabellen und unter Beachtung der Fehlerhierarchie neu bestimmt werden und dabei die in den Fehlerauswirkungstabellen hinterlegten Aktionspläne angefordert werden.

Die Propagation von Fehlern über Rechnergrenzen und die damit einhergehende Auslösung von Aktionsplänen muss, wie Eingangs bereits erwähnt, durch eine zentrale Instanz, den

GLÜ, erfolgen, dem ein Abbild der Vernetzung der FSM über das gesamte System, losgelöst von Hardwaregrenzen, vorliegt. Das dazu notwendige a priori Wissen liegt dem GLÜ beim Systemstart nicht vor und muss ihm deshalb in einer Initialisierungsphase erst übermittelt werden, bevor er dann in der Normalbetriebsphase der oben beschriebenen Aufgabe nachgehen kann. Der Grundgedanke, auf Basis von in der Initialisierungsphase übermittelten Daten eine Systemgrenzenüberwachung durchzuführen, wurde bereits im Stand der Technik erwähnt (vgl. [Michel 1992] in Kapitel 3.2.2.1).

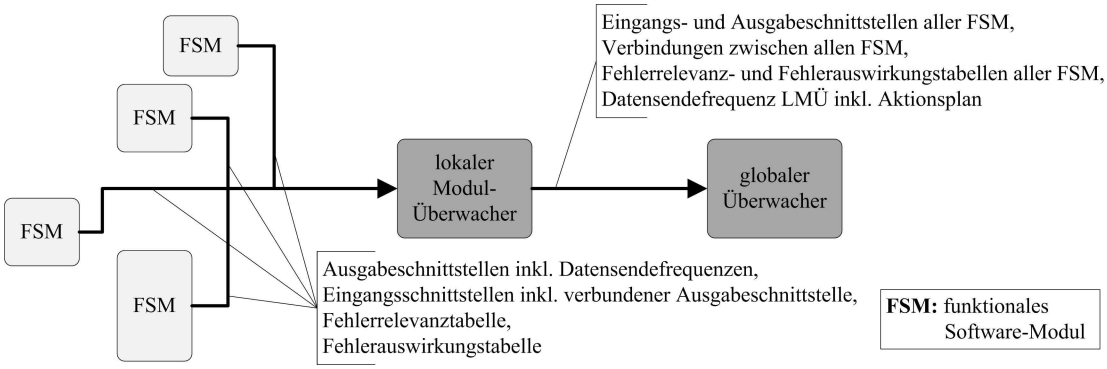

Bild 5.4: Kommunikation in der Initialisierungsphase

Zu Beginn der Initialisierungsphase liegen die moduleigenen Informationen, wie die Bezeichnung der bedienten Ausgabeschnittstellen, die zugehörigen vereinbarten Datensendefrequenzen, die Bezeichnung der Eingangsschnittstellen inklusive der Bezeichnung der entsprechend damit verbundenen Ausgabeschnittstelle des davor befindlichen Moduls, sowie die Fehlerauswirkungs- und die Fehlerrelevanztabellen bei den FSM selbst (vgl. Bild 5.4). Sie werden zunächst an den entsprechenden LMÜ übergeben, der sie dann, mit Ausnahme der Datensendefrequenz, an den GLÜ weiterleitet, so dass dieser daraus die komplette Systemarchitektur rekonstruieren kann. Der LMÜ übermittelt zudem analog zu den Ausgabeschnittstellen eines FSM eine Mindestfrequenz, mit der er sich verpflichtet, den GLÜ über seinen aktuellen Status, also implizit über das Funktionieren der CPU, auf der er implementiert ist, zu informieren. Zusätzlich liefert er dem GLÜ die Beschreibung eines zugehörigen Aktionsplans, der bei Nichteinhaltung der Mindestfrequenz ausgeführt werden soll.[14]

Nachdem die Initialisierungsphase abgeschlossen ist, sendet jeder LMÜ während der Statusphase zyklisch, immer nach Ablauf seiner minimalen Zykluszeit, ein Datenpaket an den GLÜ, das angibt, ob er selbst „OK“ oder „nicht OK“ ist, sowie ob, und falls ja, welche Fehlerzustandsänderungen an von ihm überwachten Modulausgängen aufgetreten sind. Durch das zyklische Versenden dieser Statusnachricht kann der GLÜ in jedem Zeitschritt überprüfen, ob ein LMÜ ausgefallen ist. Ist ein LMÜ ausgefallen oder ein Fehler in einem FSM gemeldet worden, wählt der GLÜ den oder die notwendigen Aktionspläne aus bzw. führt im zweiten Fall zuvor noch die Fehlerpropagation durch. Die Bezeichnungen und

[14] Dieses Prinzip der frequenzbasierten Überwachung von Überwachungskomponenten wird auch auf den Überwacher externer Einflussgrößen, den Funktionsgrenzen-Überwacher und den Fahrer-Überwacher bzw. den Plausibilitätsüberwacher angewendet.

Parameterlisten der Aktionspläne werden dann an den APU versendet, dem deren Verwaltung und koordinierte Abarbeitung obliegt.

5.1.6 Adaption auf Sensoren und Aktuatoren

Bislang wurde das Konzept zur Überwachung von Fehlern in Einzelkomponenten ausschließlich im Hinblick auf FSM betrachtet. Um auch die Sensoren und Aktuatoren eines FAS in den Überwachungsprozess einzubinden, ist pro Bauteil jeweils ein spezieller LMÜ notwendig, der über Softwareschnittstellen der Hardware Informationen über deren Funktionstüchtigkeit empfängt. Sensoren können dabei virtuell wie FSM, allerdings ohne Eingänge, betrachtet werden. Sie besitzen daher keine Fehlerrelevanz- und Fehlerauswirkungstabellen. An den Sensorausgängen können dieselben oben beschriebenen Fehlerzustände auftreten. Analog dazu können Aktuatoren virtuell als FSM mit nur einem Ausgang betrachtet werden. Für die Eingänge werden ebenso Fehlerauswirkungs- und Fehlerrelevanztabellen festgelegt. Als virtueller Ausgang des Aktors kann sein mechanisches Wirken in der Umwelt verstanden werden. Die Softwareschnittstellen des Aktors werden daher dazu verpflichtet, den LMÜ zyklisch mit einer vereinbarten Mindestfrequenz über das Funktionieren des Aktors zu informieren, wobei diese Statusmeldung auf den virtuellen Aktorausgang bezogen wird. Somit sind auch für den virtuellen Aktorausgang alle oben genannten Fehlerzustände möglich. Da der virtuelle Ausgang aber kein Nachfolgemodul zur Bewertung seiner Fehlerzustände besitzt, muss eine spezielle Aktuatorausfall-Auswirkungstabelle für jeden Aktor eingeführt werden, die jedem Fehlerzustand des Ausgangs einen entsprechenden Aktionsplan zuordnet. Im Falle eines „Frequenzfehlers“ bzw. eines „temporären Fehlers“ sind zudem, in Anlehnung an die Fehlerrelevanztabelle, eine tolerierte Fehlerzahl und ein entsprechender Betrachtungszeitraum anzugeben. Über diese beiden Größen wird definiert, mit welcher Latenz der zugehörige Aktionsplan ausgelöst werden soll.

5.2 Überwachung externer Einflüsse

Ebenso wie die Überwachung auf Fehler in Einzelkomponenten muss sowohl für vollautomatische FAS (VA FAS) als auch für A FAS prinzipiell eine Überwachung externer Einflüsse durch einen Überwacher externer Einflussgrößen erfolgen. Die dazu notwendigen Informationen sind meist über Fahrzeugbussysteme verfügbar und stammen von Diagnosesystemen anderer Fahrzeugsubsysteme oder eigens dafür vorgesehenen, fahrzeuginternen Sensoren. Unter die zu überwachenden Aspekte fallen all jene, die auch im Rahmen des Stillstandsmanagements moderner Fahrzeuge überwacht werden (vgl. Stand der Technik in Kapitel 3.2.1). Dabei ist auch für die eigensicheren A FAS eine Kontrolle der Fahreranwesenheit notwendig, da vermieden werden muss, dass der Fahrer aussteigt und sein Fahrzeug davon fährt[15].

[15] Im Falle VA FAS erfolgt die Überwachung der Fahreranwesenheit durch den Fahrer-Überwacher.

Im Vergleich zu FAS mit niedrigeren Automatisierungsgraden gibt es bei A FAS noch einige weitere Aspekte, die im Bereich der externen Einflüsse überwacht werden müssen. So muss das versehentliche Deaktivieren des Motors durch den Fahrer auch während der Fahrt überwacht werden, da nicht davon auszugehen ist, dass der Fahrer, der möglicherweise Nebenbeschäftigungen nachgeht, schnell genug in der Lage ist, den Motor wieder einzuschalten und adäquat die Kontrolle über das Fahrzeug zu übernehmen. Aus diesem Grund ergibt sich für A FAS auch die Forderung, dass die elektronische Ansteuerung der Bremse und Lenkung zum Erreichen eines sicheren Zustands auch nach Abschaltung des Motors noch für kurze Zeit möglich ist. Ein weiterer, insbesondere für A FAS wichtiger Aspekt ist die Überwachung von Defekten im Fahrzeug, die eine sofortige Deaktivierung des Gesamtfahrzeugs erfordern, beispielsweise ein Defekt der Ölpumpe, der zu einer Motorüberhitzung führen kann. Dies ist darin begründet, dass aufgrund der Ablenkung des Fahrers die Gefahr besteht, dass der Fahrer die in diesem Fall üblichen optischen und akustischen Warnungen nicht wahrnimmt und das Fahrzeug deswegen irreparabel geschädigt wird. Aus demselben Grund erscheint es bei A FAS außerdem notwendig, wichtige fahrzeugdynamische Grenzwerte zu überwachen, deren Überschreitung eine Verletzung der Grundannahmen der Funktionslogik bedeuten. Ein entsprechendes Beispiel ist der Reibwert zwischen Straße und Reifen, der einen direkten Einfluss auf den maximal realisierbaren Verzögerungswert hat[16]. Die Überschreitung derartiger Grenzwerte ist meist durch äußere Umwelteinflüsse, wie Eisglätte oder eine Ölspur, induziert.

5.3 Überwachung von Funktionsgrenzen eines Stauassistenzsystems

Funktionsgrenzen lassen sich aus der Spezifikation von FAS ableiten. Wie im Stand der Technik zu Beginn von Kapitel 3.2 bereits erwähnt wurde, kann daher kein verallgemeinerndes Funktionsgrenzenüberwachungs-Konzept entwickelt werden. Im Rahmen dieses Kapitels soll deshalb exemplarisch aufgezeigt werden, wie eine Funktionsgrenzenüberwachung bei einem Stauassistenten (STA) konzipiert werden muss. Die folgenden Ausführungen sind dabei in vollkommen identischer Weise auf eine vollautomatische bzw. autonome Systemausprägung eines STA anwendbar.

Grundsätzlich werden Funktionsgrenzen dann überschritten, wenn eine Verkehrssituation eintritt oder einzutreten droht, für die das FAS nicht ausgelegt ist oder die zu einer Systemblockade führt, die nur durch eine Aktion des Fahrers durchbrochen werden kann. Die Erkennung derartiger Funktionsgrenzen erfolgt durch FSM der Funktionslogik. Wie in Kapitel 4.1 beschrieben wurde, besteht die Aufgabe der Funktionslogik unter anderem darin, auf Basis der Umfeldmodelldaten der Wahrnehmung eine Situationsanalyse durchzuführen und die verschiedenartigen Objekte im Fahrzeugumfeld miteinander in Beziehung zu setzen.

[16] Eine Überprüfung des Reibwerts ist zudem besonders wichtig, da auch bezüglich der in Kapitel 8 vorgestellten Fail-Safe-Mechanismen davon ausgegangen wird, dass jederzeit jede beliebige Verzögerung größer -9,81m/s^2 realisiert werden kann.

Die Erkennung von Situationsaspekten, die Funktionsgrenzen beschreiben, erfolgt dabei meist in einem der ersten, von der Zielfunktion noch unabhängigen Schritte, das heißt durch relativ weit vorne in der Datenverarbeitungskette befindliche FSM. Derartige FSM, teilen dem Funktionsgrenzen-Überwacher laufend das aktuelle Ergebnis ihrer Analyse in Form einer boolschen Variable mit (vgl. Bild 4.2). Um zu bestimmen, ob die übermittelte Information valide ist, unterzieht der Funktionsgrenzen-Überwacher dieses Ergebnis daraufhin vor Auslösung eines entsprechenden Aktionsplans durch Meldung an den globalen Überwacher (vgl. Kapitel 4.2) einer rudimentären Plausibilisierung, wobei er dazu die Daten des Umfeldmodells verwendet. Dieser Plausibilisierungsschritt ist notwendig, um das Sicherheitssystem gegen Fehlinformationen der Normalfunktion abzusichern. Es lassen sich auf diese Weise sowohl Fehlauslösungen von Aktionsplänen, als auch eine unerlaubte Aktivierung des STA verhindern.

Bei einem aktivierten STA können folgende drei Situationen eintreten, die eine Funktionsgrenzenüberschreitung darstellen:

- Der Stau löst sich auf und das Fahrzeug befindet sich daraufhin nicht mehr im langsamen Kolonnenverkehr, für den der STA ausgelegt ist.
- Das Fahrzeug verlässt die Domäne Autobahn und befindet sich dadurch in einem Umfeld, in dem komplexere Verkehrs- und Verhaltensregeln gelten, für die der STA ebenfalls nicht ausgelegt ist.
- Das Fahrzeug gelangt an ein Spurende. Da der STA per Definition selbstständig keinen Spurwechsel durchführen kann, ist zur Lösung dieser Systemblockade eine Übernahme durch den Fahrer notwendig.

Die Stauerkennung wird von einem FSM der Funktionslogik durchgeführt und kann beispielsweise, wie von [Hörwick & Herbort 2009] vorgeschlagen, durch die Beobachtung des zeitlichen Verlaufs des Verkehrsflusses erfolgen, wobei hierbei für jede Fahrspur einzeln analysiert wird, ob ein Stau vorliegt. Ein positives Ergebnis wird dann geliefert, wenn die gemittelte Durchschnittsgeschwindigkeit aller dort befindlichen Fahrzeuge für eine gewisse Zeit unter einem definierten Schwellwert liegt[17]. Die Eingangs angesprochene Plausibilisierung der Daten des FSM durch den Funktionsgrenzen-Überwacher besteht hinsichtlich der Information „kein Stau“ darin, dass kontrolliert wird, ob die Geschwindigkeit des STA oder die seines Vorderfahrzeugs größer als ein vordefinierter Geschwindigkeitswert ist. Meldet ein FSM dagegen „Stau“, so erscheint dies plausibel, wenn die eigene Geschwindigkeit und die des Vorderfahrzeugs kleiner als ein vordefinierter Grenzwert sind. Wie später noch erläutert wird, ist es außerdem zwingend notwendig nachzuweisen bzw. abzuprüfen, dass sich hinter dem STA-Fahrzeug noch ein weiteres Fahrzeug befindet (vgl. Fußnote 30 auf Seite 100).

[17] Es sei angemerkt, dass aus dem ACC-Bereich bekannte Stauerkennungsmechanismen, wie beispielsweise von [Boecker & Hoetzer 2005] vorgeschlagen, in einem STA nicht direkt anwendbar sind, da eine spezielle Applikation des Algorithmus auf den Autobahnstau notwendig ist (vgl. [Hörwick & Herbort 2009]). Beispielsweise darf der STA aus Sicherheitsgründen nur dann betrieben werden, wenn sich die Fahrzeuge in allen Fahrstreifen der Autobahn stauen. Der zuerst genannte Mechanismus ist dazu nicht in der Lage.

Unter der Annahme, dass der zukünftige Fahrtweg eines STA-Systems durch den Verlauf der Spur, in der sich das Fahrzeug befindet, vorherbestimmt ist, kann durch die Auswertung der prädiktiven Streckeninformationen des Umfeldmodells in einem FSM der Funktionslogik prädiziert werden, wann das Fahrzeug die Autobahn verlassen wird. Es sei angemerkt, dass auch innerhalb der Domäne Autobahn kritische Routenpunkte existieren, die nicht überfahren werden dürfen. Dazu zählen beispielsweise Ländergrenzen, Mautstationen und eventuell auch Tunnels. Sie können ebenfalls durch die Auswertung der prädiktiven Streckendaten frühzeitig erkannt werden. Bezüglich des entsprechenden FSM leitet sich daraus die Forderung ab, dass bereits ausreichende Zeit vor Erreichen eines kritischen Routenpunkts der Wert der gemeldeten Statusvariable von „kein kritischer Routenpunkt“ auf „kritischer Routenpunkt“ wechselt. Die Plausibilisierung der Warnung vor einem kritischen Routenpunkt besteht darin, dass der Funktionsgrenzen-Überwacher überprüft, ob in einem vordefinierten Umkreis um das STA-Fahrzeug ein kritischer Routenpunkt existiert. Die Nachricht „kein kritischer Routenpunkt“ ist dagegen dann plausibel, wenn sich das Fahrzeug auf der Autobahn befindet und in einem vordefinierten Umkreis um das STA-Fahrzeug kein kritischer Routenpunkt existiert.

Eine Systemblockade durch ein Spurende kann explizit oder implizit erkannt werden. Eine explizite Detektion stellt beispielsweise die direkte Klassifikation von in der Fahrspur des STA befindlichen, statischen Objekten dar. Dabei kann es sich etwa um Baustellenfahrzeuge oder Trümmerteile handeln. In dieselbe Kategorie fiele auch die direkte Erkennung von Sperrflächen nach einem straßenbaulich definierten Spurwegfall. Eine implizite Spurendedetektion zielt dagegen darauf ab, den zeitlichen Verlauf des Verkehrsflusses in den verschiedenen Fahrspuren zu beobachten. Eine Systemblockade wird dann erkannt, wenn das STA-Fahrzeug längere Zeit steht und sich dabei aber der Verkehr in den Nebenfahrspuren bewegt. Die Meldung „Spurende erreicht“ plausibilisiert der Funktionsgrenzen-Überwacher, indem er überprüft, ob sich das eigene Fahrzeug bereits länger als eine definierte Mindestzeit im Stillstand befindet. Die Nachricht „kein Spurende erreicht “ ist dagegen solange plausibel, bis der Stillstand länger als eine definierte Maximalzeit andauert.

6 Kombiniertes Fahrerüberwachungs- und Interaktionskonzept für vollautomatische Fahrerassistenzsysteme

Das primäre Ziel des in diesem Kapitel vorgestellten Fahrerüberwachungskonzepts ist es, den Fahrer eines vollautomatischen Fahrerassistenzsystems (VA FAS) in einem Zustand zu halten, der es ihm erlaubt, die aktuelle Verkehrssituation zu beobachten, das Verhalten seines Fahrzeugs zu plausibilisieren und im Fehlerfall als operative Rückfallebene zur Verfügung zu stehen. Wird festgestellt, dass der Fahrer den genannten Zustand nicht mehr einnimmt, er sich also nicht mehr im Loop befindet, so stellt dies ebenfalls eine Systemgrenzenüberschreitung dar, die zu einer Systemdeaktivierung führen muss. Wie bereits in Kapitel 2.2.1 ausgeführt wurde, ist ein derartiges Konzept notwendig, da absehbar ist, dass ein Fahrer, der vollkommen von der Fahrzeugführungsaufgabe entbunden wurde, den beschriebenen Zustand nicht dauerhaft einnehmen und damit die an ihn gestellten Forderungen nicht erfüllen wird. „Vollkommene Entbindung von der Fahrzeugführungsaufgabe“ bedeutet in diesem Kontext nicht nur ein Fernbleiben der Füße von der Pedalerie, sondern explizit auch eine Fernbleiben der Hände des Fahrers vom Lenkrad. Es wird also davon ausgegangen, dass keinerlei kontinuierliche, physikalische Kopplung mehr zwischen dem Menschen und den Bedienteilen zur Fahrzeugführung besteht. VA FAS grenzen sich somit von FAS ab, bei denen semiautomatische Fahrzeuglängsführungsfunktionen, beispielsweise ACC, mit automatisch unterstützenden Fahrzeugquerführungsfunktionen, also Lane Keeping Support Systemen (LKS), kombiniert werden (vgl. Kapitel 1.1). Zusammenfassend lässt sich feststellen, dass ein Fahrerüberwachungskonzept essentiell für den dauerhaft sicheren Betrieb eines VA FAS ist, da es sicherstellt, dass der Fahrer als letzte Kontrollinstanz und zum Abfangen von Systemgrenzenüberschreitungen erhalten bleibt. Die Anforderungen an die Güte des Fahrerüberwachungsmechanismus sind daher sehr hoch.

Gleichsam mit dem oben beschriebenen Hauptziel werden bei der Entwicklung des Konzepts noch einige weitere Ziele verfolgt. Dazu zählen unter anderem die in Kapitel 2.3 aufgeführten übergeordneten Prinzipien und hier besonders das der „Einfachheit“ und der „vollständigen Fehlererkennung“. Letzteres bedeutet in diesem Zusammenhang, dass nachweislich jegliches nicht tolerierbares Fahrerverhalten erkannt werden muss. Neben diesen übergeordneten Prinzipien werden außerdem noch die folgenden Ziele angestrebt:

- Realisierbarkeit im Rahmen der aktuellen technischen Möglichkeiten bei überschaubaren Entwicklungs- und Hardwarekosten: Da VA FAS nur einen Zwischenschritt auf dem Weg zu autonomen FAS (A FAS) darstellen, bei denen eine Fahrerüberwachung aufgrund ihrer vollständigen Eigensicherheit nicht mehr notwendig sein wird, muss das Konzept in naher Zukunft, also vor Erlangung der Serienreife A FAS, vollständig realisierbar sein. Entsprechend müssen zu hohe Kosten vermieden werden, die durch die Entwicklung entstehen oder durch die Verwendung

von Sensoren hervorgerufen werden, die in absehbarer Zeit nicht in modernen Fahrzeugen verfügbar sein werden.

- Nutzengewinn aus Kundensicht: Die Definition VA FAS impliziert ein gravierendes Dilemma, das darin besteht, dass der Nutzengewinn durch die vollständige Automatisierung der Fahrzeugführung in einem gewissen Ausmaß dadurch kompensiert wird, dass der Fahrer weiterhin als Überwacher und Rückfallebene fungieren muss und seine Kapazität nicht beliebig frei nutzen kann. Das Fahrerüberwachungskonzept muss einen Ausweg aus diesem Dilemma finden. Dabei soll zudem, im Vergleich zu semiautomatischen FAS (SA FAS) und VA FAS, bei denen der Fahrer die Hände weiterhin am Lenkrad halten muss, eine spürbare Komforterhöhung feststellbar sein.
- Adaptierbarkeit auf beliebige VA FAS: Das Fahrerüberwachungskonzept soll neben dem Stauassistent (STA) prinzipiell auch auf andere VA FAS anwendbar sein. Ein entsprechendes Beispiel wäre etwa ein weiter entwickeltes STA-System, das die Fahrzeugführung auch bei höheren Geschwindigkeiten im Kolonnenverkehr automatisiert.

Bevor im Hauptteil der zur Lösung der aufgeführten Ziele entwickelte Mechanismus zur Überwachung des Fahrers sowie der Fahrerübergabeprozess infolge eines Fahrerfehlverhaltens vorgestellt wird (Kapitel 6.3)[18], soll zunächst erörtert werden, anhand welcher Indizien ein objektiver, externer Beobachter bestimmen kann, ob sich der Fahrer eines Fahrzeugs im Loop befindet (Kapitel 6.1). Darauf aufbauend wird dann begründet, warum bei VA FAS eine Kombination der im Stand der Technik vorgestellten Ansätze zur Fahrerüberwachung notwendig ist (Kapitel 6.2). Abschließend wird auf Anforderungen an eine Mensch-Maschine-Schnittstelle eingegangen, die aus dem entsprechenden, kombinierten Fahrerüberwachungs- und Interaktionskonzept resultieren (Kapitel 6.4).

6.1 Zustand „Fahrer im Loop“

Das von [Welford & Birren 1965] vorgeschlagene Handlungsmodell des Menschen beschreibt in einfacher Weise den Regelkreis der menschlichen Informationsverarbeitung (vgl. Bild 6.1)[19]. Demnach nimmt der Mensch Informationen und Reize aus seiner Umwelt wahr, auf deren Basis er sich dann für sein zukünftiges Handeln entscheidet. Danach werden die geplanten Aktionen ausgeführt und dadurch der Zustand der Umwelt verändert.

[18] Das kombinierte Fahrerüberwachungs- und Interaktionskonzept wurde bereits vorveröffentlicht (vgl. [Hörwick et al. 2009], [Hörwick et al. 2010b] und [Hörwick & Wimmer 2010]). Die Konzepterarbeitung erfolgte mit Hilfe der Unterstützung zweier Semestranden (vgl. [Schickram et al. 2009] und [Ostgathe et al. 2010]).

[19] Es existieren überdies weitere, komplexere Handlungsmodelle. Für die Betrachtungen im Rahmen dieser Arbeit ist das Modell nach [Welford & Birren 1965] jedoch vollkommen ausreichend.

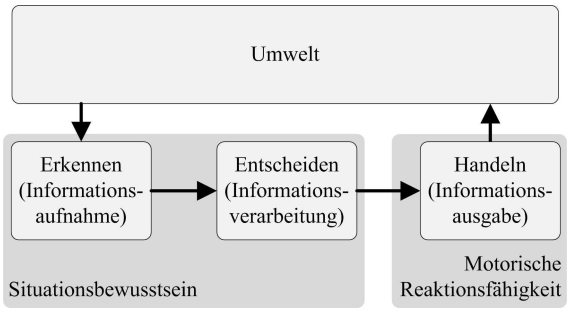

Bild 6.1: Handlungsmodell des Menschen nach [Welford & Birren 1965]

Aus der Modellvorstellung von Welford & Birren lassen sich zwei grundlegende Anforderungen an den Zustand eines verantwortungsvollen VA FAS-Fahrers ableiten. Es handelt sich dabei erstens um ein ausreichendes Situationsbewusstsein bezüglich der aktuellen Verkehrssituation und zweitens um die motorische Reaktionsfähigkeit im Hinblick auf eine eventuell notwendige unverzügliche Übernahme der Fahraufgabe. Nach [Endsley 1988] umfasst der Begriff Situationsbewusstsein die Wahrnehmung und Bedeutungserfassung von Elementen in einer dynamischen Umwelt sowie deren Zustandsprojektion in die nahe Zukunft. Übertragen auf die Fahrzeugführung ist darunter das aufmerksame Verfolgen der aktuellen Verkehrssituation zu verstehen. Streng genommen umfasst die Definition nach Endsley nur den Schritt des „Erkennens“ im Handlungsmodell nach Welford & Birren. Im Kontext dieser Arbeit wird diese Definition um den Aspekt der Informationsverarbeitung gemäß dem Modell von Welford & Birren aufgeweitet. Demnach soll der Begriff Situationsbewusstsein im Weiteren auch implizieren, dass der Mensch neben der reinen Informationsaufnahme ständig einen Handlungsplan für die nahe Zukunft entwirft. Diese Begriffsaufweitung ist sinnvoll, da der Fahrer eines VA FAS im Rahmen der von ihm geforderten Plausibilisierung des Verhaltens des Fahrzeugs als Referenzgröße genau einen derartigen Handlungsplan bzw. eine Vorstellung über das vom Fahrzeug gewünschte Verhalten generieren muss. Die kognitiven Aspekte des zu Beginn des Oberkapitels beschriebenen primären Ziels des Fahrerüberwachungskonzepts, nämlich den Fahrer in einem Zustand zu halten, der es ihm erlaubt, die aktuelle Verkehrssituation zu beobachten und das Verhalten seines Fahrzeugs zu plausibilisieren, lassen sich somit mit dem Begriff Situationsbewusstsein adressieren. Das Vorhalten eines Handlungsplans im Rahmen der Situationsplausibilisierung durch den Fahrer ist auch wichtig, um Latenzen bei der Übernahme der Fahraufgabe durch den Fahrer, im Falle einer erkannten Systemgrenzenüberschreitung, zu vermeiden und die Aktionen des gespeicherten Handlungsplans ohne Zeitverzug starten zu können. Die Fähigkeit, den Handlungsplan dann auch in die Tat umsetzen zu können, wird im Weiteren als motorische Reaktionsfähigkeit bezeichnet. Konkret bedeutet dies, dass der Fahrer jederzeit motorisch in der Lage sein muss, die Fahrzeugführung mittels eines adäquaten Eingriffs der Füße oder der Hände in die Pedalerie bzw. in das Lenkrad zu übernehmen.

Zusammenfassend lässt sich sagen, dass sich ein Fahrer genau dann im Loop befindet, wenn er sowohl ein ausreichendes Situationsbewusstsein, als auch eine ausreichende motorische Reaktionsfähigkeit aufweist. Im Rahmen dieses Unterkapitels soll nun noch erörtert werden, anhand welcher Indizien, vom Standpunkt eines objektiven menschlichen Beobachters aus, bestimmt werden kann, ob sich der Fahrer eines Fahrzeugs im Loop befindet. Diese Indizien

müssen dann durch die technischen Komponenten des Fahrerüberwachungskonzepts erfasst bzw. entsprechend abgedeckt werden. Die folgende Tabelle 6.1 liefert einen Überblick über die relevanten Indizien:

Situationsbewusstsein	motorische Reaktionsfähigkeit
freie Sicht	freies Lenkrad
Blick auf Straße	einsatzbereite Hände
Müdigkeit, Schlaf	freier Fußraum
geistige Ablenkung	einsatzbereite Füße
	Sitzeinstellung

Tabelle 6.1: Objektiv beobachtbare Indizien für einen Fahrer im Loop

Um zu beurteilen, ob sich der Fahrer der aktuellen Verkehrssituation bewusst ist, muss überprüft werden, ob er einerseits sein Umfeld visuell wahrnehmen kann und ob er andererseits ein ausreichendes geistiges Aktionspotential aufweist. Grundvoraussetzung für die visuelle Wahrnehmung der Verkehrssituation ist eine freie Sicht des Fahrers auf die Straße. Dies ist dann der Fall, wenn der Raum zwischen dem Kopf des Fahrers und der Windschutzscheibe nicht verdeckt ist, beispielsweise durch eine aufgeschlagene Zeitung. Zudem muss der Blick des Fahrers, abgesehen von vereinzelten Blickabwendungen, beispielsweise in den Rückspiegel oder auf Anzeigeelemente des Infotainmentsystems, kontinuierlich auf die vor ihm liegende Straße gerichtet sein. Das konkrete geistige Aktionspotential eines Fahrers ist nur schwer von einem externen Standpunkt aus beobachtbar. Allerdings ist es erkennbar, wenn ein Fahrer stark ermüdet und damit ein Mindestmaß an geistiger Aktivierung unterschritten ist. Einfacher feststellbar ist die Eskalation dieses Zustandes, der Schlaf. Müdigkeit und Schlaf äußern sich vor allem in den Kopfbewegungen und der Augenöffnung des Fahrers. Von außen dagegen kaum feststellbar ist jedoch, worauf ein wacher Fahrer seine geistige Kapazität richtet. Insbesondere infolge der vollständigen Entbindung des Fahrers eines VA FAS von der Fahrzeugführungsaufgabe ist es durchaus denkbar, dass dieser einer geistigen Nebenbeschäftigung nachgeht, die ihn vollkommen vereinnahmt, obwohl sein Blick eigentlich auf die Straße vor ihm gerichtet ist. Den einzigen beobachtbaren Zustand für eine rein geistige Abwendung der Konzentration vom Straßenverkehr stellt der sogenannte starre Blick dar, bei dem der Blick des Fahrers für eine gewisse Zeit auf einen festen Punkt fixiert ist (vgl. [Dong et al. 2009]). Eine geistige Abgelenktheit bedingt jedoch nicht automatisch einen starren Blick.

Eine ausreichende motorische Reaktionsfähigkeit des Fahrers ist dann gegeben, wenn eine sofortige, uneingeschränkte Nutzung des Lenkrades sowie der Pedalerie möglich ist. Dazu muss der Raum im Bereich des Lenkrads und der Pedalerie zu jeder Zeit frei zugänglich und nicht durch dort befindliche Gegenstände versperrt sein, beispielsweise durch einen Laptop auf dem Schoß des Fahrers oder einen ausgezogenen Schuh im Fußraum. Außerdem müssen sich die Hände und die Füße des Fahrers in einem einsatzbereiten Zustand befinden, um sofort das Lenkrad greifen bzw. auf die Pedale treten zu können. Dazu muss zumindest eine der beiden Hände frei sein und nicht zum Greifen von Gegenständen, wie Getränkedosen oder Essen, verwendet werden. Um die Pedale schnell bedienen zu können, müssen sich beide Füße im Fußraum vor den Pedalen befinden. Die Beine dürfen deshalb beispielsweise nicht überschlagen oder so angewinkelt werden, dass der Fuß auf dem Sitz ruht. Eine wichtige

Grundvoraussetzung für die Bedienung des Lenkrads und der Pedalerie sowie für eine gute Sicht auf die Straße ist eine richtige Sitzeinstellung. Sie wird verlassen, wenn der Sitz zu weit verschoben oder heruntergeklappt wird. Die im Bezug auf die motorische Reaktionsfähigkeit genannten Aspekte sind durch einen externen Beobachter generell gut feststellbar.

6.2 Begründung der Notwendigkeit eines kombinierten Ansatzes

Gemäß dem Prinzip der „vollständigen Fehlererkennung“ wird im Folgenden analysiert, inwiefern die im vorangegangenen Kapitel aufgeführten Indizien mithilfe der aus dem Stand der Technik bekannten Ansätzen zur Fahrerüberwachung erkannt bzw. abgedeckt werden können. Am Ende dieser Betrachtung wird dann geschlussfolgert, dass bei VA FAS nur durch eine Kombination aus einer vorwiegend direkten Fahrerüberwachung und einer regelmäßigen, erzwungenen Bedienhandlung abschätzbar ist, ob sich ein Fahrer im Loop befindet.

Vorweg sei erwähnt, dass sich die Bedienkonzepte zur kooperativen Automation von Fahrfunktionen (vgl. Kapitel 3.2.3.3) nicht auf die hier betrachteten VA FAS anwenden lassen. Dies liegt beim manöverbasierten Fahren daran, dass der Fahrer hier nur dann in die Fahraufgabe eingebunden wird, wenn das VA FAS auch in der Lage ist, verschiedene Manöver auszuführen und aufgrund der Verkehrssituation auch regelmäßig Manöverwechsel notwendig sind. Für längere Zeitabschnitte, in denen keine Manöverwechsel, notwendig sind bzw. für erste VA FAS, etwa STA-Systeme, die mit der einfachen Kolonnenfolgefahrt nur ein einziges Manöver automatisieren, ist das Konzept untauglich. Dies steht entgegen der Eingangs formulierten Forderung, dass eine allgemeine Lösung für alle VA FAS angestrebt wird. Auch die H-Metapher (vgl. Kapitel 3.2.3.3) ist für VA FAS unbrauchbar, da sie auf einer kontinuierlichen Rückkopplung zwischen Mensch und Fahrzeug beruht, was bei einem VA FAS, bei dem der Fahrer ja vollkommen von der Fahrzeugführungsaufgabe entbunden wird, aber explizit nicht möglich ist.

Noch vor der eigentlichen Analyse der in Tabelle 6.1 aufgeführten Indizien hinsichtlich der Ansätze des Stands der Technik wird zunächst festgestellt, dass drei Indizien nicht beachtet werden müssen. Dazu zählen, wie im Folgenden erörtert wird, die Überwachung der Füße, die Überwachung des Fußraums und die Überprüfung, ob das Lenkrad frei zugänglich ist.

VA FAS stellen bezüglich ACC-Systemen eine evolutorische Weiterentwicklung dar, bei der zusätzlich eine automatisierte Querführungsfunktion implementiert ist. Die Längsführungsfunktion ist dabei identisch derer von ACC-Systemen. Nachdem die heute bereits in Serie etablierten ACC-Systeme auf eine Überwachung des Fußraums und der Fußstellung zur Sicherstellung eines schnellen Eingriffs in die Längsführung verzichten, erscheint eine entsprechende gesonderte Überwachungseinheit auch bei VA FAS nicht notwendig.

Eine Überwachung, ob das Lenkrad frei zugänglich ist, muss nach Rücksprache mit Experten für funktionale Sicherheit der Audi AG ebenfalls nicht durchgeführt werden, da eine mutwillige Blockade des Bereichs vor dem Lenkrad durch Gegenstände einen groben Missbrauch des Fahrers darstellt, für die der Fahrer somit auch selbst verantwortlich ist.

Die verbleibenden Indizien lassen sich jeweils entweder mit dem Ansatz der direkten Fahrerüberwachung oder dem der erzwungenen Bedienhandlung abdecken (vgl. Tabelle 6.2). Aufgrund der vollständigen Entkopplung des Fahrers von der Fahrzeugführungsaufgabe, insbesondere der Hände von der Querführung, muss von einer Anwendung der in Bild 3.6 aufgeführten Mechanismen zur indirekten Fahrerüberwachung bei VA FAS abgesehen werden. Möglich ist lediglich die Überwachung der Bedienhandlungen der sekundären und tertiären Fahraufgabe (vgl. [Urbas et al. 2008]). Um eine zeitnahe, kostengünstige und einfache Umsetzbarkeit zu gewährleisten wird im Folgenden, neben der in modernen Fahrzeugen bereits vorhandenen Sensorik, lediglich von einer Kamera zur direkten Beobachtung des Fahrers ausgegangen.

Situationsbewusstsein	motorische Reaktionsfähigkeit
freie Sicht	
Blick auf Straße	einsatzbereite Hände
Müdigkeit, Schlaf	
geistige Ablenkung	
	Sitzeinstellung

direkte Fahrerbeobachtung
Erzwingung von Bedienhandlungen

Tabelle 6.2: Abdeckung der Indizien für einen Fahrer im Loop durch direkte Fahrerbeobachtung bzw. durch Erzwingung von Bedienhandlungen

Mit einer Kamera und bereits existierenden Bildverarbeitungsalgorithmen kann der Kopf eines Menschen robust erkannt werden (vgl. Tabelle 3.1). Ist die Kamera in günstiger Lage, beispielsweise in der A-Säule des Fahrzeugs (vgl. Bild 3.7) verbaut, so kann geschlussfolgert werden, dass der Fahrer genau dann eine freie Sicht hat, wenn auch sein Kopf erkannt wird. Da die Position und Orientierung des Kopfes durch Bildverarbeitungsalgorithmen ebenfalls robust bestimmbar ist, kann auch, wie von [Mottok et al. 2008] vorgeschlagen, einfach festgestellt werden, ob der Fahrer auf die Straße blickt. Es wird dazu geprüft, ob der Vektor der Fahrerkopforientierung eine definierte (Region of Interest) ROI in der Ebene der Windschutzscheibe schneidet (vgl. Bild 3.8). Veränderungen der Sitzeinstellung sind in modernen Fahrzeugen über im Sitz verbaute Sensoren mess- und somit direkt detektierbar. Die Indizien „freie Sicht“, „Blick auf Straße“ und „Sitzeinstellung“ sind also grundsätzlich mittels einer direkten Fahrerüberwachung bestimmbar, lassen sich aber nicht durch eine zusätzliche Bedienhandlung feststellen. Allerdings können durch einen entsprechenden Trigger die Indizien „Müdigkeit“, die rein videobasiert nur schwer messbar ist (vgl. Kapitel 3.2.3.1), sowie „geistige Ablenkung“ und „einsatzbereite Hände“, die mit einer Kamera und auch anderen berührungslosen Sensoren nicht erfassbar sind, abgedeckt werden. So kann davon ausgegangen werden, dass der Fahrer einer Aufforderung des System mit ihm zu interagieren (ähnlich wie bei einem ACC-Anfahrtrigger oder einem Totmanntaster; vgl. Kapitel 3.2.3.2) nur dann nachkommt, wenn er nicht müde oder stark geistig abgelenkt ist. Ist das Bedienteil zur Triggerung so ausgelegt, dass es mit der Hand bedient werden muss, so ist eine Betätigung nur mit mindestens einer einsatzbereiten Hand möglich. Zusammenfassend wird festgestellt, dass nur ein kombiniertes Fahrerüberwachungs- und Interaktionskonzept in der Lage sein kann, den Fahrer eines VA FAS „im Loop“ zu halten.

6.3 Überwachungsmechanismus und Fahrerübergabeprozess

Die Grundidee des Konzepts besteht darin, dass der Fahrer regelmäßig ein Bedienteil betätigen muss. Der Triggerungszeitpunkt ist dabei im Gegensatz zu einer Totmannschaltung nicht fix definiert, sondern primär von Zustandsgrößen der direkten, kamerabasierten Fahrerüberwachung abhängig. Man stelle sich in diesem Zusammenhang eine Wassersäule vor, die bei der Aktivierung des VA FAS vollständig gefüllt ist. In Abhängigkeit der Zustandsgrößen der Fahrerüberwachung wird dann zyklisch in jedem Zeitschritt eine Sinkgeschwindigkeit (im Folgenden v_{sink} genannt) der Wassersäule berechnet, welche dann mit der Periodendauer multipliziert und daraufhin der Füllstand der Wassersäule entsprechend verringert wird. Ist die Wassersäule leer, wird der Fahrer zu einer Bedienhandlung aufgefordert, durch die sich die Wassersäule wieder auffüllt und dann von neuem abzusinken beginnt. Kommt der Fahrer der Trigger-Aufforderung nicht innerhalb einer definierten Zeit nach, wird das VA FAS deaktiviert. Die vorgestellte Grundidee wird im Folgenden konkretisiert und um einige weitere Aspekte ergänzt, wobei der Begriff Wassersäule im Rahmen dieser Ausführungen auch als Potential und die Bedienhandlung als Potentialtrigger bezeichnet wird.

Die Indizien der direkten, kamerabasierten Fahrerüberwachung „freie Sicht“ und „Blick auf Straße“ werden im Folgenden zu der Zustandsgröße „Blick in freie ROI“ zusammengefasst. Dies ist sinnvoll, da die Detektion des Fahrerblicks auf der Bestimmung der Kopforientierung basiert, die wiederum nur möglich ist, wenn der Fahrerkopf erkannt und damit implizit auch eine freie Sicht festgestellt wurde. Konkret beschreibt die Zustandsgröße den prozentualen Anteil eines bis zum aktuellen Zeitpunkt reichenden Zeitintervalls definierter Länge, in dem der Fahrer seinen Blick durch die freie ROI richtet. Der Wertebereich liegt damit zwischen Null und Eins. Werte nahe Eins sollen ein langsames, Werte nahe Null dagegen ein schnelles Absinken des Potentials bewirken. Da die Sitzeinstellung, wie bereits erwähnt, eine Grundvoraussetzung für die Bedienung des Lenkrads und der Pedalerie, sowie für eine gute Sicht auf die Straße ist, soll eine signifikante Sitzverstellung direkt zu einer Deaktivierung des VA FAS führen. Entsprechend wird eine Zustandsgröße „signifikante Sitzverstellung“ als hartes Abwurfkriterium eingeführt, die entweder den Wert „wahr“ oder „falsch“ einnehmen kann. Basis für die Bestimmung des Werts ist die Position des Sitzes und die Stellung der Rückenlehne vor der Aktivierung des VA FAS, wobei jeweils ein gewisser Toleranzbereich definiert wird, in dem eine Verstellung auch während des Betriebs des VA FAS tolerierbar ist. Zusätzlich zur Zustandsgröße „Blick in freie ROI“ soll auch eine Fahreraufmerksamkeitskenngröße v_{sink} beeinflussen, die auf einer indirekten Überwachung der durch den Fahrer vollzogenen Bedienhandlungen der tertiären Fahraufgabe basiert. Sie wird in Form der Zustandsgröße „Infotainmentnutzung“ beschrieben. Diese definiert, wie viele Bedienaktionen des Infotainmentsystems innerhalb eines bis zum aktuellen Zeitpunkt reichenden Zeitintervalls definierter Länge erfolgen. Die Information, ob aktuell Bedienteile des Infotainment-Systems betätigt werden, ist in der Regel über die Fahrzeugdatenbusse verfügbar. Neben der Bestimmung des Fahrerzustands ist es sinnvoll, in einem Fahrerüberwachungskonzept auch die aktuelle Verkehrssituation zu berücksichtigen, da durch sie impliziert wird, wie aufmerksam der Fahrer sein muss. Da eine relativ hohe Fahrzeuggeschwindigkeit bei einem vergleichsweise niedrigen Abstand zum Vorderfahrzeug

das Risiko für eine Gefahrensituation erhöht, ist in derartigen Situationen eine erhöhte Fahreraufmerksamkeit notwendig. Es ergibt sich somit die Forderung, dass der Fahrer in derartigen Situationen stärker in die Fahraufgabe eingebunden werden und deshalb häufiger einen Potentialtrigger setzen muss. Entsprechend soll auch ein niedriger Wert der Zustandsgröße „Zeitlücke zum Vorderfahrzeug“, welche sich als Quotient des momentanen Abstands und der aktuellen Geschwindigkeit ergibt, zu einer Erhöhung von v_{sink} beitragen.

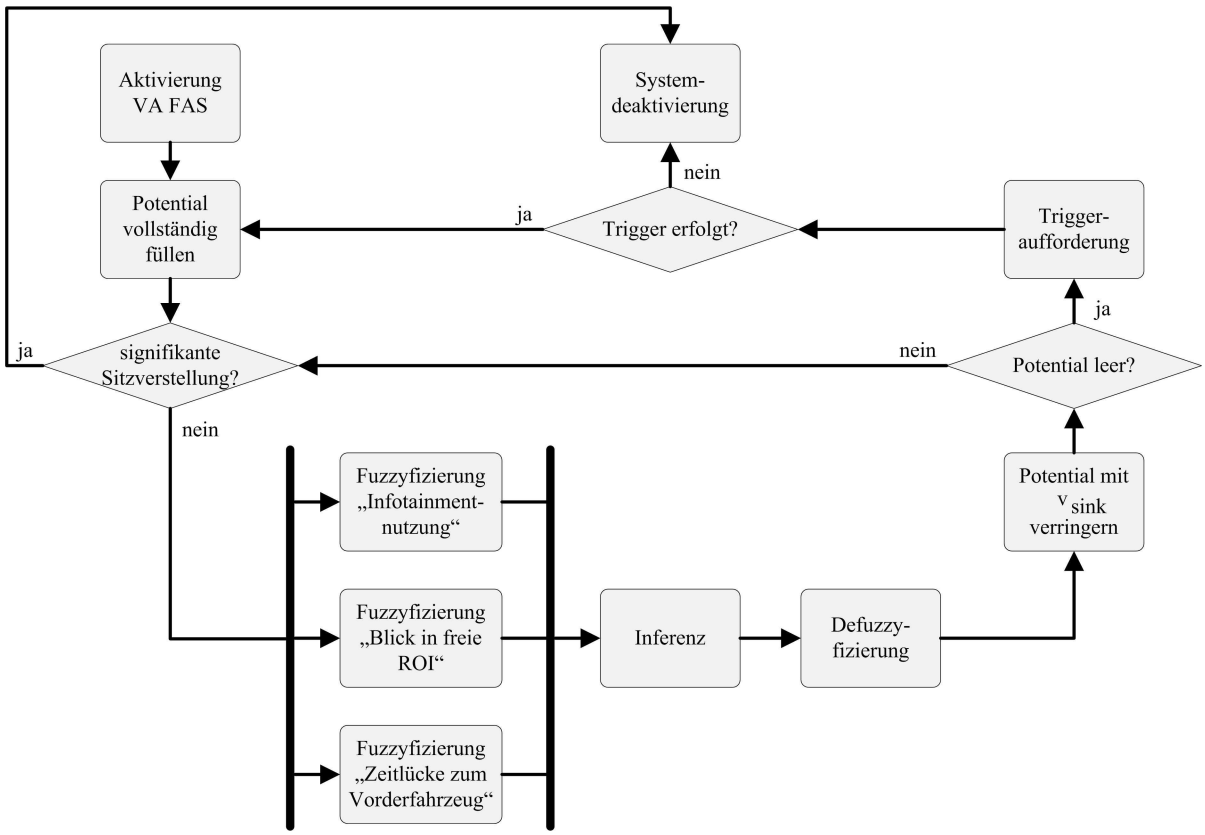

Bild 6.2: Flussdiagramm des kombinierten Fahrerüberwachungs- und Interaktionskonzepts

Im unteren Teil des Bildes 6.2, das die beschriebe Funktionslogik zusammenfasst, ist zu erkennen, dass die Berechnung von v_{sink} mittels einer Fuzzy-Logik erfolgt[20]. Die Verwendung einer Fuzzy-Logik ist dabei Mittel zum Zweck, um die Berechnung von v_{sink} möglichst

[20] Mit Hilfe der Fuzzy-Logik ist es möglich, qualitative Aussagen bezüglich beliebiger Zustandsgrößen zu modellieren und diese über Regeln zu verknüpfen, um Aussagen über beliebige Zielgrößen zu bestimmen. Die modellierte Zustandsgröße wird dabei als linguistische Variable und ihre Ausprägungen, etwa „klein“, „mittel“ und „groß“, als linguistische Terme bezeichnet. Die Berechnung der Ausgangswerte erfolgt in drei Schritten (vgl. Bild 6.2). In der Fuzzyfizierung wird aus den Zustandsgrößen durch jeweils zugehörige Fuzzy-Sets die quantifizierbare Zugehörigkeit zu ihren verschiedenen linguistischen Termen berechnet. In der Inferenz werden dann linguistische Terme unterschiedlicher Zustandsgrößen durch eine boolsche Logik miteinander verknüpft und daraus die Erfüllungsgrade der linguistischen Terme einer oder mehrerer Ergebnisvariablen ermittelt. In der Defuzzifizierung wird auf die Fuzzy-Sets der linguistischen Ergebnisvariablen jeweils ein Operator angewendet, durch den schließlich die physikalischen Ergebnisgrößen bestimmt werden. Für eine detailliertere Beschreibung der Mechanismen der Fuzzy-Logik sei auf [Kramer 2009] verwiesen.

anschaulich darzustellen. Bild 6.3 zeigt die Fuzzy-Sets der drei zuvor definierten, in die Fuzzy-Klassifikation eingehenden Zustandsgrößen sowie das der Ergebnisgröße, wobei nur die linguistischen Terme eingezeichnet sind, die später durch eine Inferenzregel verwendet werden. Die Verläufe der Kurven haben dabei lediglich einen qualitativen Charakter, da konkrete Werte erst noch im Rahmen von Probandenstudien bestimmt werden müssen[21]. Aus diesem Grund erfolgt auch keine Skalierung der Abszissen.

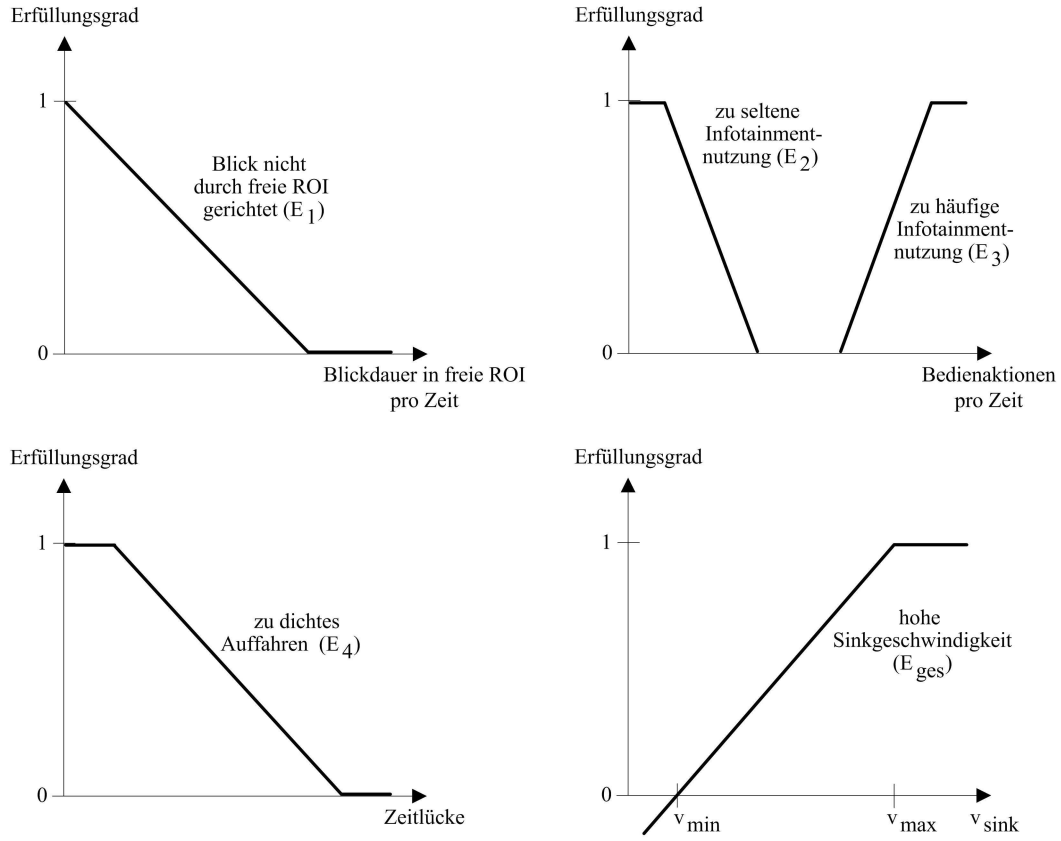

Bild 6.3: Fuzzy-Sets für Eingangs- und Ausgangsgrößen des kombinierten Fahrerüberwachungs- und Interaktionskonzepts

Nachdem die Erfüllungsgrade der linguistischen Terme der Eingangsgrößen „Blick auf Straße“, „Infotainmentnutzung“ und „Zeitlücke zum Vorderfahrzeug“ mittels der Fuzzy-Sets zeitgleich ermittelt wurden, findet die Inferenz statt (vgl. Bild 6.2). Hierbei werden die aus Bild 6.3 ersichtlichen, linguistischen Eingangsterme durch folgenden logischen Ausdruck zu einem die Sinkgeschwindigkeit beschreibenden linguistischen Ergebnisterm verknüpft:

[21] Die prototypische Realisierung des in diesem Kapitel vorgestellten kombinierten Fahrerüberwachungs- und Interaktionskonzepts erfolgt bei der Audi AG derzeit im Rahmen eines Dissertationsprojekts, das von Martin Wimmer bearbeitet wird. Letzteres hat unter anderem das Ziel, ein entsprechendes Bedienteil zu entwickeln sowie in Probandenstudien sinnvolle Werte für die freien Parameter festzulegen.

WENN [Blick nicht durch freie ROI gerichtet] ODER [zu seltene Infotainmentnutzung][22] ODER [zu häufige Infotainmentnutzung] ODER [zu dichtes Auffahren] DANN [hohe Sinkgeschwindigkeit]

Da der ODER-Operator aus mathematischer Sicht einer Addition entspricht, ergibt sich die folgende Gleichung, wobei hierin die in Bild 6.3 aufgeführten Abkürzungen für die Erfüllungsgrade der verschiedenen, linguistischen Terme verwendet werden:

$$E_{ges} = E_1 \cdot g_1 + (E_2 + E_3) \cdot g_2 + E_4 \cdot g_3 \tag{6.1}$$

Wie man erkennt, werden die Erfüllungsgrade der Eingangsgrößen noch jeweils mit einem Faktor g_i gewichtet, die per Definition in Summe Eins ergeben sollen. Somit lässt sich später im Rahmen einer Parameterabstimmung ein prozentual unterschiedlich großer Einfluss der Eingangsgrößen definieren. Nachdem nun E_{ges} berechnet wurde, lässt sich die Sinkgeschwindigkeit durch einfaches Ablesen im entsprechenden Fuzzy-Set bestimmen[23]. Man beachte, dass sich auch bei einem Gesamterfüllungsgrad $E_{ges} = 0$ eine minimale Sinkgeschwindigkeit größer Null ergibt. Dies ist notwendig, da einige der Indizien aus Tabelle 6.2 ausschließlich durch eine erzwungene Bedienhandlung abgedeckt werden können. Auf Basis von v_{min} kann entsprechend die Zeit t_{max} berechnet werden, die maximal zwischen zwei Potentialtriggern vergeht (x_{pot} ist dabei die Höhe des vollständig gefüllten Potentials):

$$t_{\max} = \frac{x_{pot}}{v_{\min}} \tag{6.2}$$

Wie bereits ausgeführt wurde, muss das VA FAS deaktiviert werden, wenn der Fahrer einer Triggeraufforderung infolge eines leeren Potentials nicht innerhalb einer definierten Zeit, im Folgenden $t_{Trigger}$ genannt, nachkommt. Nach Ablauf dieser Zeitspanne ist eine Systemdeaktivierung nicht mehr vermeidbar und es wird deshalb eine Fahrerübernahmeaufforderung (FÜA) ausgegeben. Das VA FAS wird dann nach der Übernahme durch den Fahrer bzw. nach Ablauf einer weiteren definierten Zeitschwelle $t_{Deaktivierung}$ abgeschaltet. Der beschriebene Fahrerübergabeprozess ist zusammenfassend in dem folgenden Bild 6.4 dargestellt:

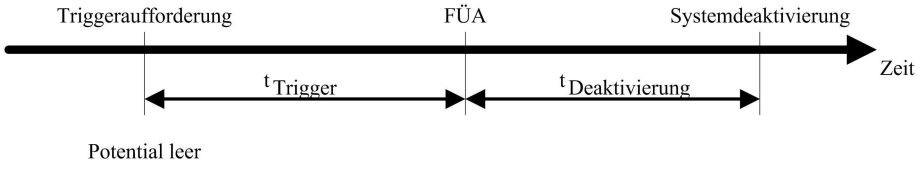

Bild 6.4: Fahrerübergabeprozess bei nicht erfolgtem Trigger

[22] Der Einbeziehung dieses linguistischen Terms liegt die Idee zugrunde, dass nicht nur, wie im Stand der Technik beschrieben, eine zu ausgiebige Infotainmentnutzung auf einen unaufmerksamen Fahrer schließen lässt. So ist anzunehmen, dass ein Fahrer, der geistig abwesend ist, das Infotainmentsystem für lange Zeit nicht bedient. Ob eine zu seltene Infotainmentnutzung aber auf eine Fahrerunaufmerksamkeit schließen lässt, muss aber noch mit einer Probandenstudie belegt werden (vgl. Fußnote 21).

[23] Im Sinne der Fuzzy-Logik entspricht dies einem Left-Max-Operator.

6.4 Resultierende Forderungen an eine Mensch-Maschine-Schnittstelle

Auch wenn die konkrete Definition eines Bedienteils zum Absetzen von Potentialtriggern prinzipiell nicht Inhalt eines Sicherheitskonzepts ist, müssen dennoch folgende Anforderungen gestellt werden, die bei der Entwicklung einer entsprechenden Mensch-Maschine-Schnittstelle zu berücksichtigen sind:

- Um den Aspekt „einsatzbereite Hände“ abzudecken, darf die Betätigung des Bedienteils, wie bereits erwähnt, nur mit der Hand möglich sein.
- Um zu verhindern, dass der Fahrer trotz Unaufmerksamkeit einen Trigger auslöst, der das VA FAS aktiv hält, ist eine erzwungene Bedienhandlung nur nach expliziter Aufforderung durch das VA FAS erlaubt. Das Absetzen eines Potentialtriggers ohne vorherige Aufforderung führt deshalb zu einer Systemdeaktivierung. Ohne diese Vorkehrung wäre es einem unaufmerksamen Fahrer möglich, das VA FAS durch ein andauerndes stupides Betätigen des Bedienteils aktiv zu halten.
- Die Triggeraufforderung darf lediglich optisch an einem für einen aufmerksamen Fahrer gut erkennbaren Ort erfolgen, beispielsweise in einem Head-Up-Display. Ein akustisches oder haptisches Signal könnte der Fahrer trotz Nebenbeschäftigung wahrnehmen. In diesem Fall soll er das VA FAS aber nicht aktiv halten können.
- Eine FÜA muss dagegen so erfolgen, dass sie auch ein unaufmerksamer Fahrer wahrnimmt. Daher ist hier neben einer optischen auch eine akustische oder haptische Warnung sinnvoll.

Abschließend wird festgestellt, dass es mit dem vorgeschlagenen Konzept möglich erscheint, Fahrer beliebiger VA FAS im Loop zu halten. Jedoch ist es zwingend notwendig, das Konzept durch Probandenstudien zu validieren und dabei Erfahrung im Hinblick auf eine sinnvolle Festlegung der freien Parameter zu sammeln. Erst dadurch kann die Tauglichkeit des Konzepts vollständig erwiesen werden (vgl. Fußnote 21 auf Seite 83). Im Zuge der Probandenstudien ist zudem kritisch zu überprüfen, ob ein derartiges Bedienkonzept von zukünftigen Kunden akzeptiert werden würde.

7 Konzept zur automatischen Plausibilitätsprüfung des funktionalen Verhaltens eines autonomen Stauassistenzsystems

Grundsätzlich sollte ein autonomes Fahrerassistenzsystem (A FAS) mittels der Komponenten der Normalfunktion (vgl. Bild 4.1) sowohl in der Lage sein, alle potentiell möglichen Fahrsituationen, die innerhalb des definierten Einsatzbereichs auftreten können, selbstständig zu meistern, als auch intern auftretende Fehler selbstständig per Eigendiagnose zu erkennen. Es ist daher davon auszugehen, dass es den Normalfunktionen zukünftiger A FAS erlaubt sein wird, ohne jede Beschränkung Längs- und Querführungsaktionen auszuführen[24]. In Kapitel 2.2.1 wurde bereits beschrieben, dass es allerdings aufgrund nicht erkannter, systeminterner Fehler oder aufgrund einer plötzlichen, dramatischen Eskalation der Verkehrssituation zu sogenannten situativen Unplausibilitäten kommen kann. Hiermit sind Fahrsituationen gemeint, die objektiv betrachtet gar nicht hätten eintreten dürfen und in denen daher eine sofortige Deaktivierung des A FAS zwingend erforderlich ist, um eine weitere Eskalation der Situation zu vermeiden (vgl. Prinzip der „Prävention“ in Kapitel 2.3). Ebenfalls wurde festgestellt, dass bei A FAS die dauernde, überschlagsmäßige Überprüfung des funktionalen Gesamtverhaltens des Fahrzeugs zur Erkennung derartiger Fahrsituationen durch eine technische Komponente erfolgen muss, da der Fahrer, anders als bei einem vollautomatischen FAS (VA FAS), nicht mehr als letzte Überwachungsinstanz zur Verfügung steht. Im Rahmen der Systemüberwachung ist es daher notwendig, dass A FAS selbstständig eine Plausibilisierung der Eigenbewegung des Fahrzeugs hinsichtlich der Situation im unmittelbaren Umfeld durchführen. Es sei an dieser Stelle nochmals ausdrücklich darauf hingewiesen, dass für diesen Überwachungsmechanismus zwingend valide, sensorische Umfelddaten erforderlich sind und es nicht möglich ist, mit diesem Mechanismus nicht erkannte interne Fehler im Bereich der sensorischen Wahrnehmung abzufangen. Derartige Fehler müssen vollständig im Rahmen der Komponenten-Eigendiagnose detektiert werden.

Da die Beurteilung der Plausibilität von Fahrzeugaktionen nur auf Basis einer genauen Funktionsdefinition des jeweiligen A FAS möglich ist, wird im Folgenden exemplarisch ein Konzept zur Plausibilitätsprüfung des funktionalen Verhaltens für ein autonomes Stauassistent-System (STA) beschrieben[25]. Dabei sollen keine situativen Unplausibilitäten, die ein unkomfortables Fahrzeugverhalten zur Folge haben, detektiert werden, etwa ein ungleichmäßiges Beschleunigen, sondern nur solche, die als sicherheitskritisch eingestuft werden. Da keine vergleichbaren Ansätze im Stand der Technik bestehen, musste das Konzept vollkommen neu entwickelt werden. Als Eingangsgrößen sollen valide Eigenbewegungsdaten, sowie valide Umfeldmodelldaten, die die Szene im unmittelbaren

[24] Im Unterschied dazu existieren beispielsweise für ACC-Systeme vorgeschriebene Betriebsgrenzen, die unter anderem eine Begrenzung der Maximalverzögerung auf -3m/s^2 festlegen (vgl. [ISO 15622: 2010]).

[25] Das Konzept wurde bereits vorveröffentlicht (vgl. [Hörwick et al. 2010a]).

Umfeld des autonomen STA beschreiben, dienen. Es wird explizit darauf verzichtet, interne Ergebnisgrößen der Funktionslogik, also die Soll-Größen für die nachgelagerte Regelung, zu plausibilisieren, wie es bei ACC-Systemen beispielsweise im Rahmen einer Hüllkurvenüberwachung geschieht. Dies liegt daran, dass im Rahmen der Plausibilisierung nicht nur Fehler abgefangen werden sollen, die in der Funktionslogik auftreten, sondern auch solche, die im Bereich der Regelung oder Aktorik entstehen. Die genannten Fehler spiegeln sich letztendlich allesamt in der Bewegung des Fahrzeugs wieder, die sich wiederum durch die Eigenbewegungsdaten beschrieben wird.

Im folgenden Unterkapitel 7.1 werden zunächst, gemäß dem Prinzip der „vollständigen Fehlererkennung“, systematisch sämtliche situative Unplausibilitäten erörtert, die im Rahmen der Plausibilitätsüberwachung eines autonomen STA notwendigerweise erkannt werden können müssen. Im Anschluss daran werden in Kapitel 7.2 alle erforderlichen Überwachungsmechanismen vorgestellt. Abschließend werden einige Forderungen formuliert, die sich an die Sensorik und die funktionalen Softwaremodule (FSM) der Wahrnehmung eines autonomen STA ergeben (Kapitel 7.3).

7.1 Situative Unplausibilitäten

Im Folgenden werden zunächst jene situativen Unplausibilitäten erörtert, die bei einem autonomen STA durch funktionales Fehlverhalten infolge eines internen Fehlers entstehen können und danach jene, die sich durch eine dramatische Eskalation der Verkehrssituation ergeben können.

Um die Gesamtheit aller möglichen Verhaltensfehler eines STA zu erfassen, muss zunächst genau definiert werden, welches Verhalten das STA-Fahrzeug hinsichtlich der relevanten Teilaspekte der gesamten Verkehrssituation, im Weiteren Situationsaspekte[26] genannt, erwartungsgemäß zeigen soll. Entspricht das Verhalten nicht in vollem Umfang den Erwartungen, stellt dies zwangsläufig eine situative Unplausibilität dar.

[26] Die Verwendung des Begriffs „Situationsaspekte“ erfolgt in Anlehnung an [Pellkofer 2003]. Dieser liefert folgende Definition: „Ein Situationsaspekt beschreibt einen Teilaspekt der Verkehrssituation; alle Situationsaspekte zusammen umschreiben die gesamte Situation.“

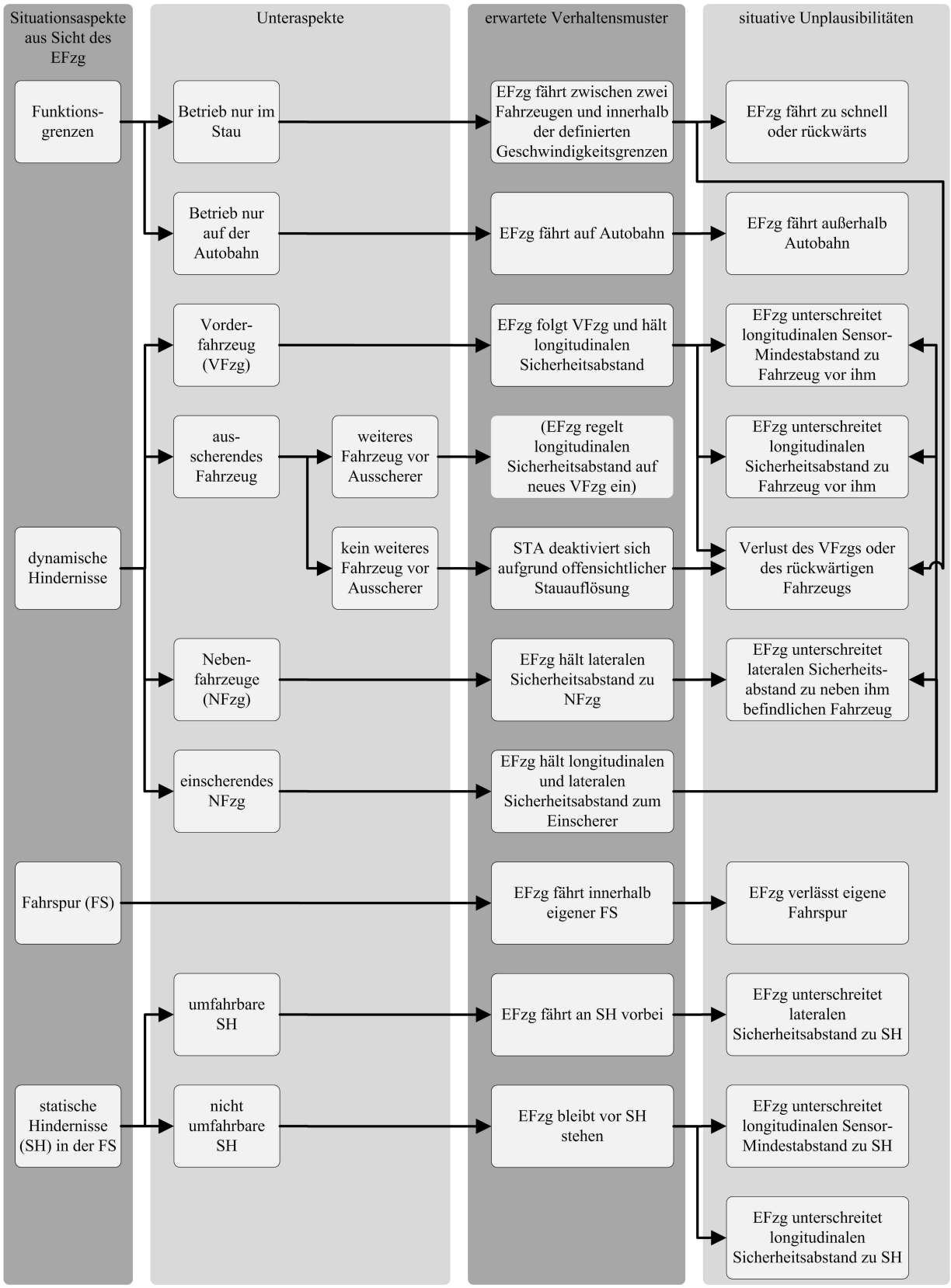

Bild 7.1: Situative Unplausibilitäten infolge eines systeminternen Fehlers

Im Folgenden sei Bild 7.1 betrachtet. Hierin sind in der ersten Spalte alle relevanten Situationsaspekte aus Sicht eines STA-Fahrzeugs, im Weiteren auch Ego-Fahrzeug (EFzg) genannt, aufgeführt. Die Situationsaspekte sind direkt aus dem Umfeldmodell abgeleitet (vgl. Kapitel 4.1). Es müssen an dieser Stelle auch die Funktionsgrenzen berücksichtigt werden.

Dies liegt daran, dass die Erkennung von Funktionsgrenzen durch FSM der Normalfunktion erfolgt und deren Einhaltung daher zusätzlich durch das Sicherheitskonzept abgesichert werden muss[27]. Die Situationsaspekte werden in der zweiten Spalte des Bildes, sofern notwendig, noch in weitere Unteraspekte aufgegliedert. Die unten im Bild aufgeführten statischen Hindernisse werden hierbei als umfahrbar eingestuft, wenn sie vom STA-Fahrzeug umfahren werden können, ohne dass ein Teil des Fahrzeugs die Fahrspur verlassen muss. Als „Vorderfahrzeug" wird jenes vorausfahrende, ebenfalls in dieser Fahrspur befindliche Fahrzeug bezeichnet, das dem EFzg am nächsten ist. „Neben-Fahrzeuge" sind alle Fahrzeuge, die sich in einer direkt an die eigene Fahrspur angrenzenden Fahrspur befinden und die das EFzg bei einem Spurwechsel touchieren würde. Den einzelnen Situationsaspekten wird in der dritten Spalte, gemäß der Funktionsdefinition des STA in Kapitel 1.2, jeweils eine Erwartungshaltung hinsichtlich des EFzg-Verhaltens zugeordnet. Aufbauend darauf, können nun in der vierten Spalte die potentiell auftretenden situativen Unplausibilitäten formuliert werden. Im Bild sind dabei nur die Unplausibilitäten aufgeführt, die als sicherheitskritisch einzustufen sind, da sie entweder bereits eine gefährliche Fahrsituation implizieren oder, wie beispielsweise im Falle des Verlassens der Autobahn, zu gefährlichen Situationen führen können. Lässt sich aus einem erwarteten Verhaltensmuster keine sicherheitskritische Unplausibilität ableiten, so ist dies im Bild durch eine Einklammerung gekennzeichnet. Es sei angemerkt, dass insbesondere auch der Verlust des Vorderfahrzeugs infolge eines Ausschervorgangs oder einer Geschwindigkeitserhöhung des Vorderfahrzeugs kritisch ist, da dies bedeutet, dass sich der STA nicht mehr in dem vorgesehenen Einsatzbereich, dem Stau, bewegt. Wie aus dem Bild zudem zu erkennen ist, muss neben einem situationsabhängigen, longitudinalen Sicherheitsabstand auch ein sogenannter Sensor-Mindestabstand zu bewegten oder unbewegten Objekten vor dem EFzg eingehalten werden, um ein fehlerfreies Arbeiten der Sensoren sowie der FSM der Wahrnehmung zu ermöglichen. Außerdem erkennt man, dass die Unplausibilitäten bezüglich der Reaktion auf einen Einscherer dieselben sind, wie die auf ein Vorderfahrzeug und Nebenfahrzeuge. Dies liegt daran, dass ein Einscherer zu Beginn des Einschervorgangs als Nebenfahrzeug und gegen Ende als neues Vorderfahrzeug betrachtet werden kann.

Um die Gesamtheit aller möglichen situativen Unplausibilitäten zu erfassen, die durch eine dramatische Eskalation der Verkehrssituation hervorgerufen werden, werden zunächst, wie in Bild 7.2 zu sehen ist, ausgehend von den für einen STA relevanten Situationsaspekten, alle im jeweiligen Zusammenhang denkbaren, kritischen Ereignisse formuliert. Nahezu alle Unplausibilitäten, die sich durch diese kritischen Ereignisse ergeben, lassen sich mit den bereits in Bild 7.1 aufgeführten Formulierungen beschreiben. Einzige Ausnahme stellt das Auftauchen von Fußgängern innerhalb der eigenen Fahrspur dar. Da sich Fußgänger in nur schwer prädizierbarer Art und Weise bewegen und Kollisionen mit Fußgängern im Rahmen einer Gefährdungsanalyse und Risikoeinstufung (vgl. Kapitel 1.3) außerdem zu hohen Automotive Safety Integrity Leveln (ASIL) im Bereich von C führen, sollten erste autonome

[27] Die Plausibilisierung der Funktionsgrenzen erfolgt streng genommen bereits im Rahmen der Funktionsgrenzenüberwachung (vgl. Kapitel 5.3), ist hier aber der Vollständigkeit halber mit aufgeführt.

STA-Systeme in diesem Fall deaktiviert werden. Das genannte Ereignis soll deshalb als situative Unplausibilität betrachtet werden.

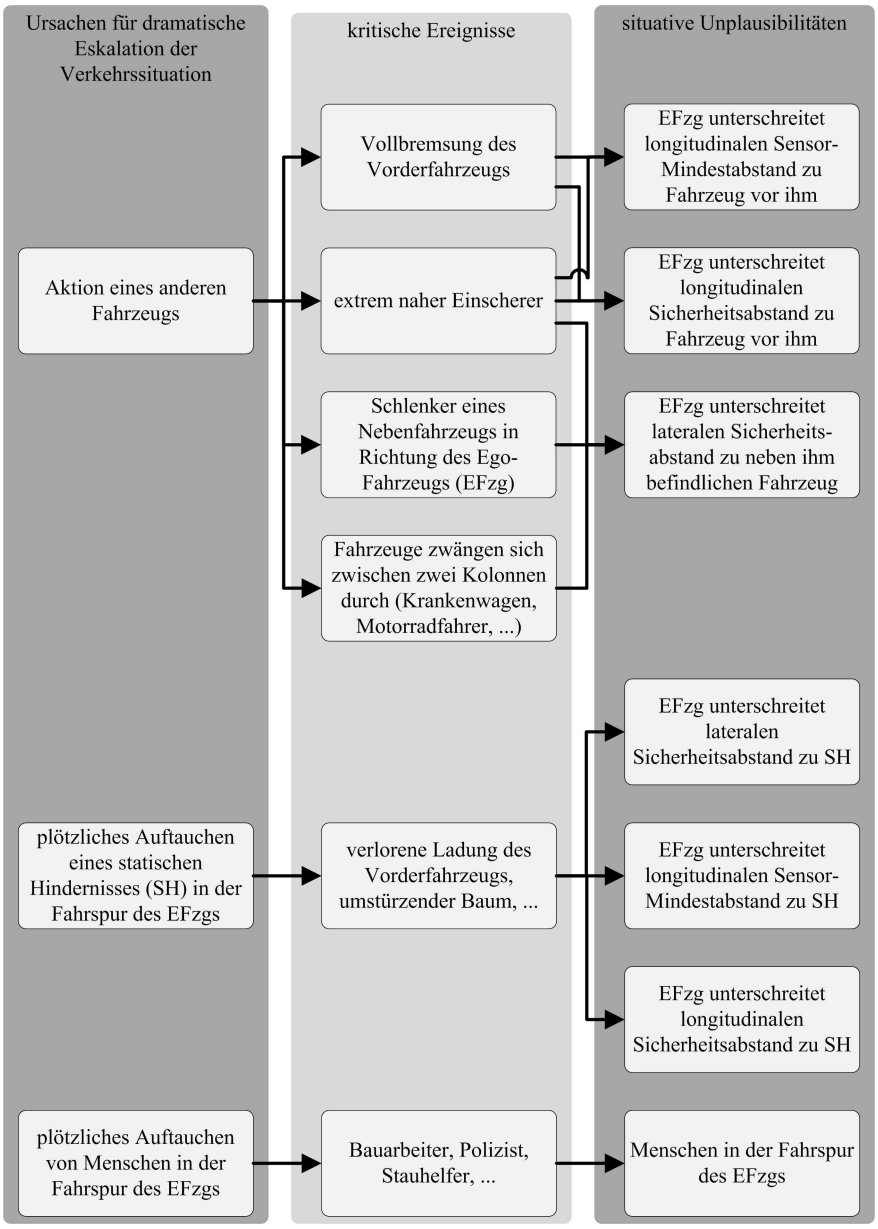

Bild 7.2: Situative Unplausibilitäten infolge einer dramatischen Eskalation der Verkehrssituation

7.2 Überwachungsmechanismen

Im Rahmen dieses Kapitels wird erläutert mithilfe welcher Überwachungsmechanismen die in Bild 7.1 und 7.2 aufgeführten situativen Unplausibilitäten erkannt werden können. Dabei liegt hinsichtlich der Überwachung der Einhaltung eines Sicherheitsabstandes zu statischen und dynamischen Objekten in longitudinaler Richtung die Idee nahe, einen expliziten Wert für diesen Sicherheitsabstand zu berechnen und genau dann auf eine situative Unplausibilität zu schließen, wenn der Abstand des EFzg zu einem Hindernis diesen Wert unterschreitet. Im Rahmen der automatischen Plausibilitätsprüfung gilt der longitudinale Sicherheitsabstand als unterschritten, sobald innerhalb der Grenzen der Fahrphysik kein kollisionsvermeidendes

Manöver mehr möglich ist. Die Berechnung des longitudinalen Sicherheitsabstands muss berücksichtigen, dass neben einer Vollbremsung auch ein Ausweichen das letzte kollisionsfrei Manöver für den STA sein kann. Diese Tatsache wird durch Bild 7.3 verdeutlicht.

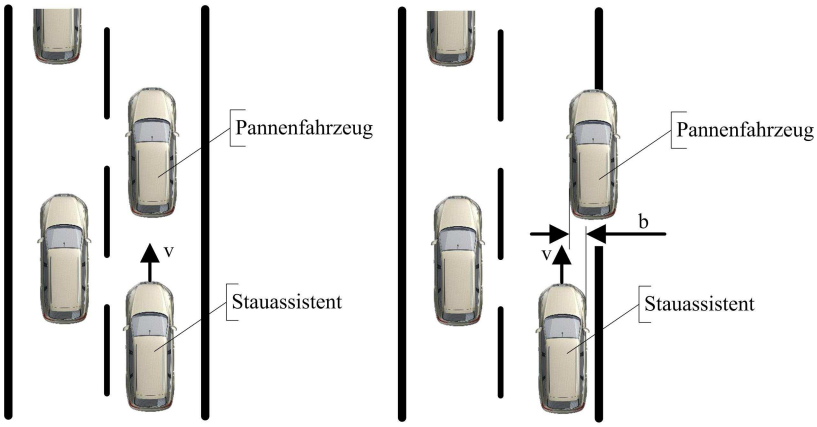

Bild 7.3: Vollbremsung (links) und Notausweichen (rechts) als letztmögliches kollisionsvermeidendes Fahrmanöver

Wie man sieht sind zwei Fahrsituationen abgebildet, in denen der STA, der aktuell eine Geschwindigkeit von v hat, jeweils auf ein stehendes Pannenfahrzeug reagieren muss. Im linken Beispiel ist es dem STA nicht möglich, dem Pannenfahrzeug ohne Verlassen des Fahrstreifens auszuweichen, weshalb sich der longitudinale Sicherheitsabstand hier auf Basis des Bremswegs x_{brems} des STA-Fahrzeugs bei einer Vollbremsung auf 0km/h berechnen lässt. x_{brems} hängt dabei gemäß nachfolgender Formel vom Ortsfaktor g, also der maximal möglichen Bremsverzögerung, und v ab.

$$x_{brems} = \frac{v^2}{2 \cdot g} \tag{7.1}$$

Befindet sich das Pannenfahrzeug, wie auf der rechten Seite in Bild 7.3 dargestellt, allerdings am Fahrbahnrand, so ist ein Ausweichen innerhalb des Fahrstreifens möglich. Der Weg $x_{ausweich}$ den das STA-Fahrzeug in longitudinaler Richtung zurücklegt, wenn es einem Hindernis der Breite b innerhalb des Fahrstreifens durch ein Notlenken mit einer maximalen Querbeschleunigung von g ausweicht, kann über die folgende Formel aus dem Bereich der Spurwechselvorgänge berechnet werden (vgl. [Weiss 1988]).

$$x_{ausweich} = 2{,}67 \cdot v \cdot \sqrt{\frac{b}{g}} \tag{7.2}$$

Geht man beispielhaft von einer Geschwindigkeit v = 40km/h aus, so lässt sich auf Basis der beiden Formeln zeigen, dass für b < 0,44m $x_{ausweich} < x_{brems}$ gilt. Somit wird ersichtlich, dass der Algorithmus zur Berechnung des longitudinalen Sicherheitsabstands sowohl alle fahrphysikalisch möglichen Brems- als auch Lenkmanöver bzw. entsprechende Kombinationen berücksichtigen muss. Konkret ist also ein Algorithmus notwendig, der unter Beachtung sämtlicher im Fahrzeugumfeld befindlicher Hindernisse in jedem Zeitschritt die absolute Länge x_{max} der längsten, im Rahmen der Grenzen der Fahrphysik frei befahrbaren Trajektorie bestimmt. Ist der Bremsweg x_{brems} bei einer Vollverzögerung kleiner als x_{max}, so

ist ein kombiniertes Lenk-Bremsmanöver zur Verhinderung einer Kollision noch möglich und der longitudinale Sicherheitsabstand somit noch nicht unterschritten.

Die beschriebene Problematik existiert ebenfalls bei ANB-Systemen (automatische Notbremse, vgl. Kapitel 1.1). Auch hier muss festgestellt werden, wie groß x_{max} ist, damit entschieden werden kann, ob eine Notbremsung ausgelöst werden soll oder nicht. Im Rahmen des Teilprojekts „automatische Gefahrenbremsung“ der Forschungsinitiative AKTIV wurde zur Lösung des Problems bereits eine sogenannte Ausweichanalyse (AWA) entwickelt. Diese verwendet als Eingangsinformationen Daten über die Eigenbewegung des Fahrzeugs sowie über beliebig strukturierte statische Objekte, Freiräume und unbekannte Gebiete. An ihrer Ausgabeschnittstelle liefert sie x_{max}. Zur Berechnung von x_{max} wird hierbei intern zunächst die Menge aller Punkte vor dem Fahrzeug berechnet, die im Rahmen der Fahrphysik und unter Berücksichtigung der Hindernisse in der Umgebung kollisionsfrei erreichbar ist. Dieses Gebiet wird als Erreichbarkeitsmenge bezeichnet. Auf Basis der Erreichbarkeitsmenge berechnet der AWA-Algorithmus dann den Weg x_{max}. Bild 7.4 zeigt auf der linken Seite aus der Vogelperspektive eine schematische Darstellung des fahrphysikalisch theoretisch erreichbaren Bereichs eines Fahrzeugs. Auf der rechten Seite befinden sich in diesem Bereich statische Hindernisse, die dazu führen, dass sich das Fahrzeug nur in dem hell dargestellten Gebiet bewegen kann. Nachdem die Menge aller kollisionsfrei erreichbaren Punkte in diesem Fall endlich ist, spricht man hier von einer abgeschlossenen Erreichbarkeitsmenge. (vgl. [Reichel et al. 2010])

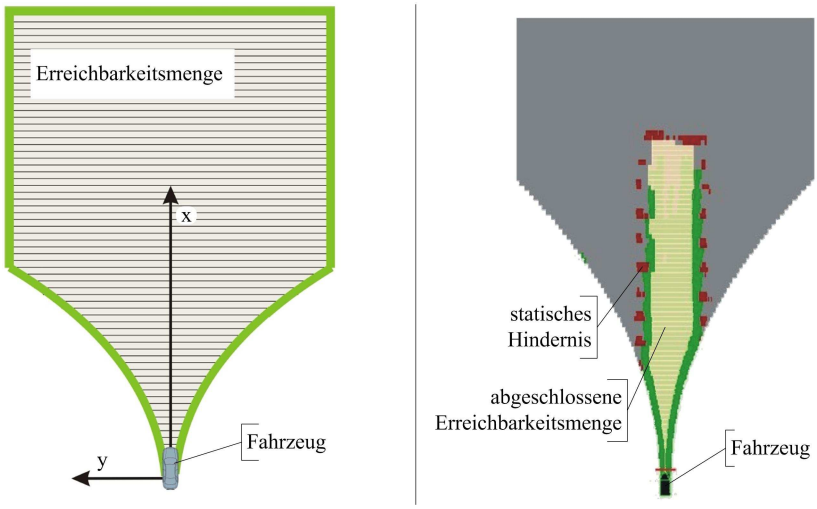

Bild 7.4: Erreichbarkeitsmenge ohne (links) und mit Hindernissen (rechts) nach [Reichel et al. 2010]

Um zu erkennen, ob das STA-Fahrzeug unplausibler Weise den longitudinalen Sicherheitsabstand zu einem statischen Hindernis unterschreitet, soll im Rahmen der hier vorgeschlagenen automatischen Plausibilitätsprüfung der AWA-Algorithmus nach [Reichel et al. 2010] verwendet werden. Der mindestens einzuhaltende Sicherheitsabstand in longitudinaler Richtung $x_{min,long}$ ergibt sich als Summe aus dem von der AWA berechneten Wert x_{max} und einem Pufferwert p. Ist $x_{min,long}$ kleiner als x_{brems}, so wird geschlussfolgert, dass eine situative Unplausibilität vorliegt.

In [Reichel et al. 2010] wird darauf hingewiesen, dass bei Sicherheitssystemen wie der ANB ein Eingriff in die Fahrzeugführung erst dann erfolgen darf, wenn zweifelsfrei feststeht, dass

eine Kollision unmittelbar bevorsteht, da eine Bevormundung des Fahrers unbedingt vermieden werden muss. Bei der Verwendung der AWA in einem ANB-System müssen deshalb die im Umfeldmodell als unbekannt klassifizierten Gebiete vom AWA-Algorithmus als frei interpretiert werden. Im Gegensatz dazu muss bei einem A FAS, bei der die letzte Überwachungsinstanz ja das System selbst ist, zu jedem Zeitpunkt zweifelsfrei sicher sein, dass keine Kollision droht. Dies hat zur Folge, dass bei einer Verwendung der AWA im Rahmen der automatischen Plausibilitätsprüfung des Verhaltens eines STA-Systems wirklich nur die Gebiete als frei interpretiert werden dürfen, die auch explizit so klassifiziert wurden. Die unbekannten Gebiete im Umfeldmodell müssen dagegen vor Eingang in die AWA in belegte Bereiche umgewandelt werden. Werden auch die freien Bereiche, die außerhalb der Fahrspur des STA-Fahrzeugs liegen, als belegt betrachtet, so liefert die AWA für den Fall, dass der STA die Fahrspur verlässt, einen Wert x_{max} von Null, wodurch somit auch diese situative Unplausibilität erkannt werden kann. Zudem wird durch diesen Vorverarbeitungsschritt der Eingangsdaten der Tatsache Rechnung getragen, dass die Normalfunktion das STA-Fahrzeug bei einem Ausweichmanöver nicht in Bereiche außerhalb der Fahrspur führen darf.

Bild 7.5 gibt einen Überblick, welche der in Bild 7.1 und 7.2 aufgeführten situativen Unplausibilitäten mit welchem Überwachungsmechanismus detektiert werden sollen. Wie man sieht, soll mittels der AWA, neben einer ausbleibenden Reaktion auf vor dem Fahrzeug befindliche statische Hindernisse und einem Spurverlassen, auch die Unterschreitung des longitudinalen Sicherheitsabstands zu vor dem STA befindlichen Fahrzeugen, also zu dynamischen Objekten, erkannt werden. In den Ausführungen von [Reichel et al. 2010] werden keine dynamische Objekte als Eingangsdaten für den AWA-Algorithmus berücksichtigt. Der Algortihmus wurde jedoch mittlerweile um die Einbeziehung dynamischer Objekte erweitert. Eine entsprechende Veröffentlichung ist von den oben genannten Entwicklern für das Jahr 2011 geplant. Der verbesserte Algorithmus soll zukünftig auch für die automatische Plausibilitätsprüfung verwendet werden.

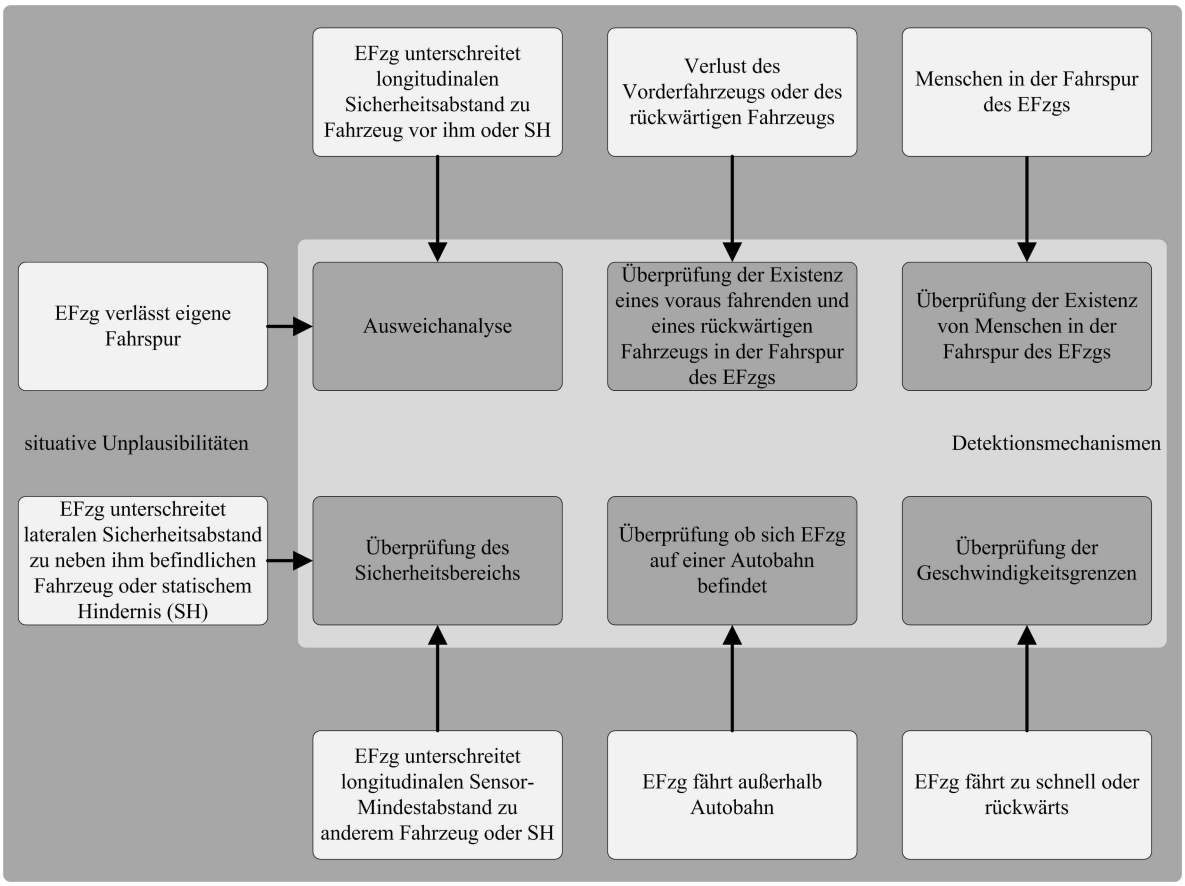

Bild 7.5: Zuordnung situativer Unplausibilitäten zu Überwachungsmechanismen

Im Gegensatz zum longitudinalen Sicherheitsabstand lässt sich die Einhaltung eines lateralen Sicherheitsabstands $x_{min,lat}$ zu dynamischen und statischen Objekten, wie dem obigen Bild zu entnehmen ist, mittels eines Sicherheitsbereichs um das EFzg, in dem sich zu keiner Zeit ein Hindernis befinden darf, realisieren. Es ist damit ebenfalls möglich, die Einhaltung des Sensor-Mindestabstands $x_{min,Sensor}$ zu überprüfen. Entsprechend wird der in Bild 7.6 dargestellte, bezüglich der STA-Geschwindigkeit unveränderliche, Sicherheitsbereich definiert. Taucht ein Hindernis in diesem Bereich auf, so wird auf eine situative Unplausibilität geschlossen. Aus den im Zusammenhang mit der AWA ausgeführten Gründen müssen die im Umfeldmodell als unbekannt klassifizierten Gebiete auch hier als belegt angenommen werden. Der Bereich außerhalb der Spur darf dagegen nicht als belegt angenommen werden.

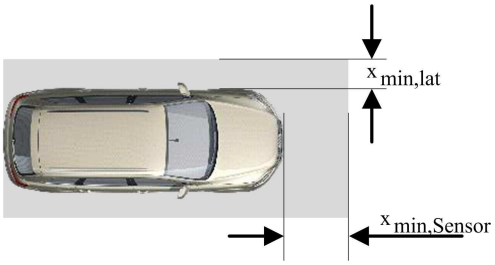

Bild 7.6: Sicherheitsbereich zur Überwachung des lateralen Sicherheitsabstands und des Sensor-Mindestabstands

Die Erkennung der verbleibenden situativen Unplausibilitäten erfolgt, wie Bild 7.5 ebenfalls zu entnehmen ist, durch das Abprüfen verschiedener Bedingungen bezüglich der

Umfeldmodelldaten. So ist dann ein unplausibler Zustand eingetreten, wenn sich innerhalb der Fahrspur vor bzw. hinter dem EFzg kein weiteres dynamisches Objekt befindet, wenn sich vor dem EFzg ein Mensch innerhalb der Fahrspur aufhält, wenn sich das EFzg nicht auf einer Autobahn befindet oder wenn die Geschwindigkeit des EFzgs die definierte, obere Geschwindigkeitsgrenze überschreitet oder kleiner als Null ist.

Stellt der für die automatische Plausibilitätsprüfung zuständige Plausibilitätsüberwacher einen Fehler fest, so teilt er dem globalen Überwacher (GLÜ) im Rahmen seiner Statusnachricht mit, mit welchem Detektionsmechanismus er dies festgestellt hat (vgl. Kapitel 4.2). Eine explizite Beschreibung, welche Unplausibilität genau aufgetreten ist, kann nicht erfolgen. Daher wird in den Anmeldedaten des Plausibilitätsüberwachers auch direkt jedem einzelnen Detektionsmechanismus ein Aktionsplan zugeordnet.

7.3 Resultierende Forderungen an die Wahrnehmung

Wie bereits mehrfach ausgeführt wurde, ist es für das Funktionieren der vorgestellten, automatischen Plausibilitätsprüfung zwingend erforderlich, dass sämtliche im Fahrzeugumfeld befindliche, nicht durch Hindernisse verdeckte, statische und dynamische Objekte fehlerfrei detektiert werden können. Dies gilt insbesondere auch für dynamische Objekte, die sich im Seitenbereich des Fahrzeugs befinden. Nur wenn diese Information vorhanden ist, kann der Einfluss solcher Objekte rechtzeitig in der AWA berücksichtigt werden und eine Überprüfung des lateralen Sicherheitsbereichs (vgl. Bild 7.6) erfolgen. Zudem ist eine Klassifizierung notwendig, die explizit Menschen von anderen dynamischen Objekten unterscheidet. Zusammenfassend lässt sich sagen, dass die genannten Forderungen die Fähigkeiten heutiger, serientauglicher Wahrnehmungssysteme bei Weitem überschreiten. Hier besteht deshalb, wie auch im Hinblick auf die Eigendiagnose-Fähigkeit von Wahrnehmungsalgorithmen (vgl. Kapitel 5.1), noch erheblicher Forschungs- und Entwicklungsbedarf.

8 Aktives Fail-Safe-Konzept für ein autonomes Stauassistenzsystem

Nachdem in den Kapiteln 5 bis 7 Detektionsmechanismen vorgestellt wurden, mit denen zur Laufzeit Systemgrenzenüberschreitungen in vollautomatischen bzw. autonomen Fahrerassistenzsystemen (FAS) festgestellt werden können, widmet sich dieses Kapitel nun den entsprechenden Fehlerbehandlungsmaßnahmen. Da zu Beginn der Arbeit das Ziel formuliert wurde, bei den genannten FAS im Fehlerfall immer eine Systemdeaktivierung und die Einnahme eines Notaus-Zustands anzustreben (vgl. Kapitel 1.3), werden im Folgenden ausschließlich Fail-Safe-Mechanismen (FS) behandelt. Alle anderen in Bild 3.3 aufgeführten Fehlerbehandlungsmaßnahmen, die bei aktiviertem FAS möglich sind, gehen mit einem Fortlaufen des Betriebs des Systems einher und sind daher ungeeignet. Wie bereits in Abschnitt 2.2.2 erwähnt wurde, erfolgt die Beschreibung der FS-Mechanismen in der Form sogenannter Aktionspläne. Diese definieren eine genaue zeitliche Abfolge verschiedener Aktionen, die das System „Fahrer-Fahrzeug-umliegender Verkehr“ wieder in einen sicheren Zustand überführen.

Da bei vollautomatischen FAS (VA FAS) angenommen werden darf, dass der Fahrer als operative Rückfallebene zur Verfügung steht, sind die Deaktivierungsprozesse dieser Systeme identisch mit denen semiautomatischer FAS (SA FAS). Da Letztere bereits Stand der Technik sind (vgl. 3.4.1), ist es nicht notwendig ein spezielles FS-Konzept für VA FAS zu erarbeiten. Grundsätzlich lässt sich feststellen, dass auch hier eine Fahrerübernahmeaufforderung (FÜA) der wesentliche Bestandteil des Aktionsplans ist. Übernimmt der Fahrer die automatische Fahrzeugführung nach einer FÜA nicht innerhalb einer vordefinierten Zeitspanne, wird das FAS einfach deaktiviert. Neben der Übernahme der Fahrzeugführung durch den Fahrer existiert somit keine weitere Rückfallebene.

Im Gegensatz dazu müssen autonome FAS (A FAS), im Falle eines ausbleibenden Fahrereingriffs nach einer FÜA überdies in der Lage sein, das Fahrzeug selbstständig in einen Notaus-Zustand zu manövrieren. Wie in Kapitel 3.4.2 beschrieben wurde, ist dieser zweite, sichere Rückfallebenen-Zustand bei Automobilen der Stillstand an einem sicheren Ort. Die Aktionspläne A FAS müssen deshalb, neben der Ausgabe einer FÜA, auch einen, die Normalfunktion überlagernden Eingriff in die Bremse und, abhängig vom Fehlerfall, eventuell auch einen Eingriff in die Lenkung vorsehen (vgl. Kapitel 4.2). Man bezeichnet ein derartiges Verhalten als aktives FS (vgl. Kapitel 3.1).

Wie in Kapitel 3.4.3 beschrieben wurde, sind aus dem Stand der Technik bereits einige hochautomatisierte, bewegte Systeme bekannt, die über ein aktives FS-Verhalten verfügen. Im Folgenden soll die Eignung dieser Ansätze für eine Übertragung auf A FAS kurz erörtert werden. Die Konzepte aus dem Bereich der mobilen Roboter und der unbemannten U-Boote sind nicht auf A FAS übertragbar, da sich A FAS im Straßenverkehr, also in einer wesentlich komplexeren Umgebung, bewegen und daher auch während des Deaktivierungsvorgangs Objekte im Umfeld des Fahrzeugs berücksichtigt werden müssen. Die pauschale Ansteuerung eines Aktors im Fehlerfall zur Auslösung einer ab diesem Zeitpunkt unkontrollierten

Bremsung bzw. eines unkontrollierten Auftauchens ist daher nicht zielführend. Besser übertragbar erscheinen dagegen die Ansätze aus dem Bereich der Nothalteassistenzsysteme, die im Falle einer Verhinderung des Fahrers durch einen Eingriff in die Längs- und Querführung automatisch den Stillstand an einem sicheren Ort ansteuern. So muss auch bei einem A FAS, wie im Zusammenhang mit Nothalteassistenzsystemen erläutert, eine optische und akustische FÜA ausgegeben und der umliegende Verkehr mittels der Warnblinkanlage vor dem Abbremsen bzw. dem Stillstand des Fahrzeugs gewarnt werden. Der Abbremsvorgang sollte dabei ebenfalls, prinzipiell ähnlich wie in Bild 3.10 angedeutet, situationsadaptiv und unter Berücksichtigung von Umfeldinformationen erfolgen. Zudem muss auch bei einem A FAS nach Erreichen des Stillstands die Parkbremse eingelegt werden, um den sicheren Zustand dauerhaft abzusichern. Die Ansteuerung der Bremse, um den Fahrer, wie von [Aizawa et al. 2004] vorgeschlagen, haptisch zur Übernahme aufzufordern, erscheint dagegen bei Komfortsystemen generell, also auch bei A FAS, nicht sinnvoll, da eine Gewöhnung des Fahrers an ein Bremsruckeln bzw. an einen Bremsruck vermieden werden sollte. Das Ansprechen dieses Sinneskanals sollte Sicherheitsfunktionen, also automatisch intervenierenden FAS, vorbehalten bleiben, die ausschließlich in Notsituationen eingreifen, die durch einen Fahrfehler des Fahrers hervorgerufenen wurden und in denen, anders als bei eigensicheren A FAS, ein Fahrereingriff zwingend notwendig ist, um die Gefahr abzuwenden. Im Gegensatz zu den Aktionen von Nothalteassistenten müssen sich die FS-Mechanismen eines A FAS auch dann anwenden lassen, wenn ein systeminterner Fehler aufgetreten ist. Das pauschale Auslösen einer Notbremse, wie es in diesem Fall für ein automatisch fahrendes Fahrzeug von [Gudat et al. 1999] für diesen Fall vorgeschlagen wird, ist dabei, wie bereits weiter oben in diesem Abschnitt beschrieben, allein nicht zielführend. Die einzigen, etwas differenzierteren Überlegungen hinsichtlich einer Reaktion auf interne Systemfehler stammen aus dem Forschungsprogramm „Partners for Advanced Transit and Highways“ (vgl. [Lygeros et al. 1995]). Hier wird vorgeschlagen, abhängig von der Kritikalität des internen Fehlers, entweder eine Vollbremsung („Crash Stop“) oder eine Bremsung mit definierter Verzögerung („Gentle Stop“) auszuführen. Allerdings ist auch hier kein korrigierender Querführungseingriff, um einen sicheren Ort zu erreichen, angedacht. Das einzige System, das in der Lage ist, auch während einer Notbremsung im Fehlerfall die Querführung sinnvoll fortzuführen ist der Zug, da hier der Fahrtweg durch die Schienen vorbestimmt ist. Dies lässt sich aber natürlich nicht auf ein Straßenfahrzeug übertragen. Zusammenfassend lässt sich feststellen, dass für A FAS keine umfassenden FS-Konzepte bestehen, mit denen auf sämtliche potentielle Systemgrenzenüberschreitungen adäquat reagiert werden und durch die zu jeder Zeit ein sicherer Zustand garantiert werden kann (vgl. Prinzip der „Garantie eines sicheren Zustands“ in Kapitel 2.3).

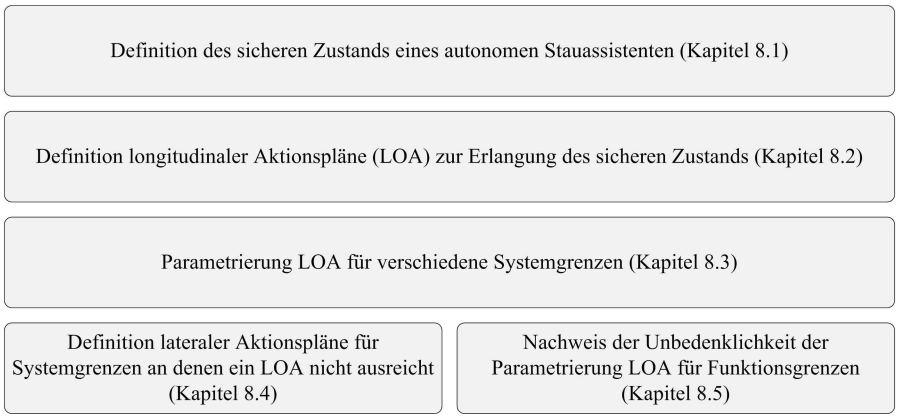

Bild 8.1: Struktureller Aufbau des Kapitels 8

Nachdem die genaue Spezifikation der sicherheitsgerichteten Ausfallreaktionen eines A FAS nur unter Berücksichtigung von dessen definierter Funktionalität bzw. Einsatzbereich möglich ist, soll im Folgenden im Abgleich mit den eben angesprochenen Erfahrungen aus dem Stand der Technik die Konzipierung eines aktiven FS-Konzepts für ein autonomes Stauassistenzsystem beschrieben werden[28]. Dazu wird zu Beginn des Kapitels (vgl. Bild 8.1) zunächst definiert, was der sichere Notaus-Zustand bzw. der sichere Ort für den Stillstand bei einem Stauassistenten (STA) ist (Kapitel 8.1).

Danach werden sogenannte longitudinale Aktionspläne zum überlagerten Eingriff in die Längsführung beschrieben, durch die der Stillstand an einem sicheren Ort erreicht werden kann (Kapitel 8.2). Ziel während der Entwicklung war es hierbei, möglichst wenige, einfache Aktionspläne zu konzipieren, die flexibel parametrierbar sind und somit eine Reaktion auf jede mögliche Systemgrenzenüberschreitung, vor allem auch auf systeminterne Fehler, ermöglichen (vgl. übergeordnete Prinzipien der „Einfachheit und Prädizierbarkeit“ sowie der „Garantie eines sicheren Zustands“ in Kapitel 2.3).

Kapitel 8.3 führt entsprechend aus, wie die longitudinalen Aktionspläne im Falle verschiedener Systemgrenzenüberschreitungen zu parametrieren sind und welche fundamentalen Forderungen daraus an die Normalfunktion resultieren. Hierbei wird besonders auf Fehler in den verschiedenen Komponenten der Normalfunktion, die jeweils eine Einschränkung der Leistungsfähigkeit des A FAS zur Folge haben, sowie auf situative Unplausibilitäten eingegangen.

Zum besseren Verständnis soll an dieser Stelle anhand von Bild 8.2 nochmals kurz der Ablauf zur Ansteuerung und Abarbeitung eines Aktionsplans im Rahmen der in Kapitel 4.2 beschriebenen funktionalen Architektur des Sicherheitskonzepts beschrieben werden. Als konkretes Beispiel wird ein Ausfall des Fahrspurdetektors, wie er etwa durch eine temporäre Verschmutzung der Kamera hervorgerufen werden kann, betrachtet. Im Bild ist zu Erkennen, dass der angesprochene Systemfehler, gemäß des in Kapitel 5.1 ausführlich beschriebenen Mechanismus, von dem funktionalen Softwaremodul „Fahrstreifendetektor“ über den lokalen Modul-Überwacher an den globalen Überwacher (GLÜ) gemeldet wird, der daraufhin den

[28] Das Konzept wurde bereits vorveröffentlicht (vgl. [Hörwick & Siedersberger 2009] und [Hörwick & Siedersberger 2010a]).

Aktionsplan „Bremsung auf Ziel“ mit einer entsprechenden Parametrierung (vgl. Kapitel 8.2 und 8.3) beim Aktionsplan-Umsetzer (APU) anfordert bzw. ansteuert. Der APU berechnet dann unter Verwendung von Eigenbewegungs- und Umfeldmodelldaten eine Verzögerungsvorgabe, mit der sodann die Längsführungsvorgaben der Normalfunktion in kombinierter Weise überlagert werden. Zudem wird durch den APU zu gegebener Zeit eine Fahrerübernahmeaufforderung (FÜA) ausgegeben und die Warnblinkanlage aktiviert. Durch die kombinierte Überlagerung der Längsführung wird auch im Fehlerfall, im Rahmen der durch den Fehler vorgegebenen Möglichkeiten, eine Adaption des Fahrzeugverhaltens an die Verkehrssituation im unmittelbaren Umfeld des Fahrzeugs[29] erreicht. Es sei an dieser Stelle angemerkt, dass davon ausgegangen wird, dass der Fahrer die automatisierte Fahrzeugführung, sowohl im Normalbetrieb des autonomen STA, als auch während der Abarbeitung von Aktionsplänen, jederzeit mittels eines Eingriffs in Gas, Bremse oder Lenkung übersteuern kann und die automatisierte Fahrzeugführung, sowie die FÜA und die Warnblinkanlage daraufhin sofort vollständig deaktiviert werden.

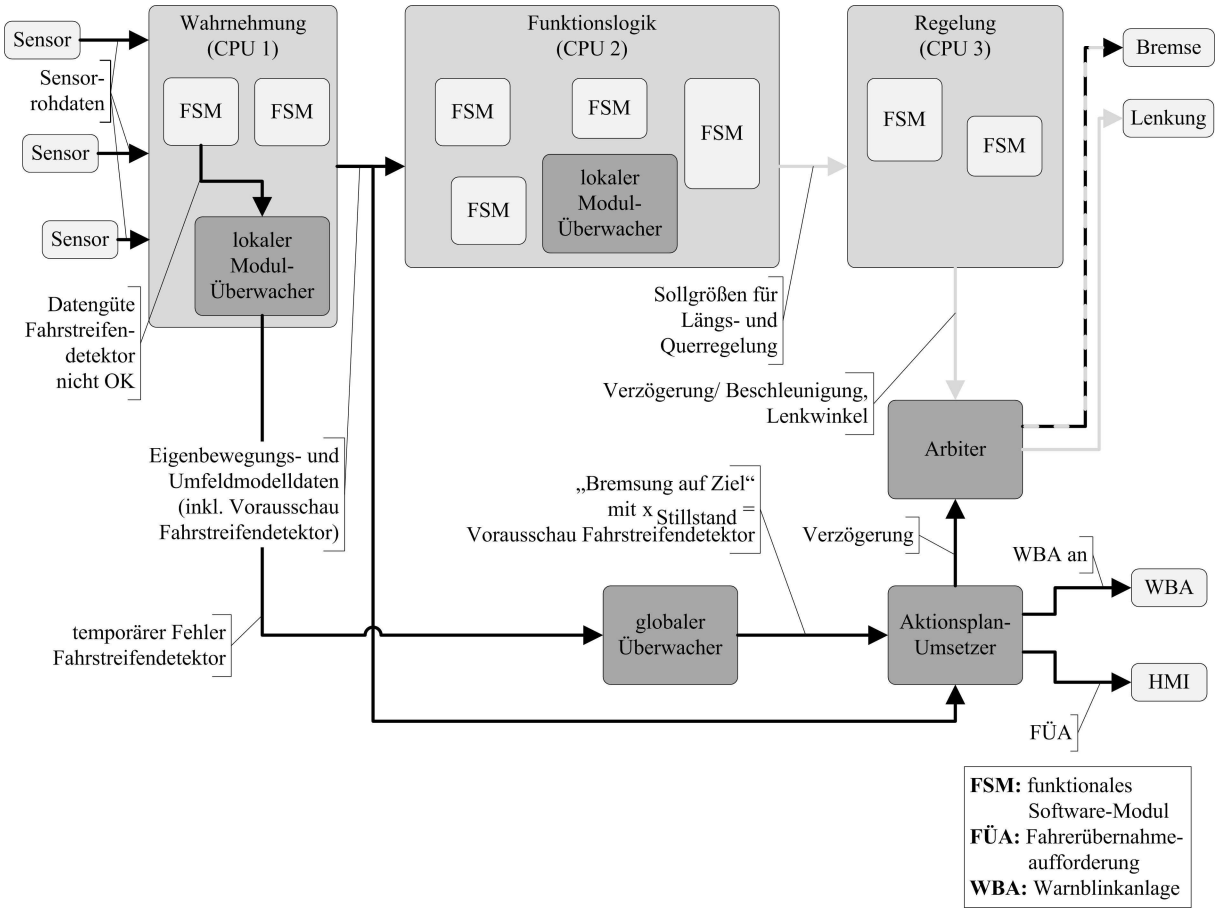

Bild 8.2: Aktionsplan-Ansteuerung bei systeminternen Fehlern (Beispiel aus Versuchsträger: Ausfall des Fahrstreifendetektors)

Wie bereits in Bild 8.1 angedeutet wurde und in Kapitel 8.3 genauer dargelegt wird, existieren einige Systemgrenzen bei denen zusätzlich zu einem Eingriff in die Längsführung auch ein

[29] In diesem konkreten Beispiel könnte dies beispielsweise ein starkes Abbremsen des Vorder-Fahrzeugs sein, das mittels des Radarsensors detektiert wird.

Eingriff in die Querführung notwendig ist. Dieser Eingriff geschieht durch einen sogenannten lateralen Aktionsplan, der die Normalfunktion im Falle einer Aktivierung vollständig übersteuert (vgl. Bild 4.3). Seine Funktionsweise wird in Kapitel 8.4 detailliert beschrieben.

Nachdem longitudinale Aktionspläne auch im fehlerfreien Betrieb des STA unmittelbar vor der Überschreitung von Funktionsgrenzen ausgelöst werden sollen, stellen sie in diesem speziellen Fall eine funktionale Erweiterung der Normalfunktion dar, die unter allen Umständen gefahrlos sein muss. Aus diesem Grund soll in Kapitel 8.5 abschließend sowohl für den Fall einer Stauauflösung als auch für den Fall eines Autobahnendes die Unbedenklichkeit der Verwendung des jeweils ausgewählten und entsprechend parametrierten Aktionsplans durch eine systematische Bewertung nachgewiesen werden. Der Formalismus dieser Bewertung ist dabei an den der Gefährdungsanalyse und Risikoeinstufung (vgl. Kapitel 1.3) angelehnt.

8.1 Definition des sicheren Zustands

In Kapitel 3.4.2 wurde ausgeführt, dass der sichere FS-Zustand eines Automobils laut [Isermann 2010] der Stillstand an einem sicheren Ort ist. Um nun speziell den sicheren Notaus-Zustand eines autonomen STA zu definieren, muss geklärt werden, was in diesem Kontext der anzustrebende sichere Ort für den Stillstand ist. Nachdem in Kapitel 1.2 bereits definiert wurde, dass ein Spurwechsel aufgrund der hohen Komplexität dieses Manövers nicht Teil des Funktionsspektrums des STA ist, wäre es bei einer Systemgrenzenüberschreitung insbesondere im Falle eines systeminternen Fehlers, der die Leistungsfähigkeit des Systems einschränkt, unsinnig, gerade dieses hochkomplexe Manöver auszuführen. Aus diesem Grund ist der Standstreifen bzw. der rechten Straßenrand, wie es für Nothalteassistenten im Rahmen des Projekts SAVE oder von BMW vorgeschlagen wurde (vgl. Kapitel 3.4.3.1), als sicherer Ort für einen autonomen STA ungeeignet. Als möglicher Ort verbleibt somit nur die Fahrspur, in dem sich der STA aktuell befindet. Da sich in einem Autobahnstau hinter dem STA-Fahrzeug zu jeder Zeit ein anderes Fahrzeug befindet[30], dessen Fahrer das STA-Fahrzeug im Blickfeld hat, kann davon ausgegangen werden, dass dieser Fahrer bei vorschriftsgemäßer Fahrweise und dem ohnehin vorherrschenden niedrigen Geschwindigkeitsniveau auch auf ein starkes Abbremsen des STA-Fahrzeugs in den Stillstand noch rechtzeitig reagieren können sollte, zumal ein zwischenzeitliches Anhalten des Vorderfahrzeugs im Stau auch kein ungewöhnliches Verhalten ist. Für Stauassistenzsysteme wird daher der Stillstand innerhalb der eigenen Fahrspur als anzustrebender sicherer Notaus-Zustand definiert. Aus den eben genannten Gründen erscheint eine Warnung des Hintermanns per Car-2-Car-Kommunikation, wie es im Rahmen des Forschungsprogramms „Partners for Advanced Transit and Highways“ (vgl. Kapitel 3.4.3.1) vorgeschlagen wurde, nicht zwingend notwendig. Ähnlich wie bei einem Atomkraftwerk (vgl. Kapitel 3.5), ist es auch bei einem A FAS notwendig, den sicheren Zustand durch das Fortführen einer Aktion, in diesem Fall der Aufrechterhaltung des Warnblinkens, dauerhaft abzusichern.

[30] Bezüglich des Stauerkennungsmechanismus ergibt sich daher die Forderung, dass nur dann auf einen Stau geschlossen werden darf, wenn sich hinter dem STA-Fahrzeug ein anderes Fahrzeug befindet.

8.2 Longitudinale Aktionspläne

Im vorangegangenen Kapitel wurde erläutert, dass der sichere Notaus-Zustand eines autonomen STA der Stillstand innerhalb der eigenen Fahrspur ist. Die nun vorgestellten longitudinalen Aktionspläne haben das Ziel, nach Überschreitung einer Systemgrenze den Teilaspekt „Stillstand“ des so definierten sicheren Zustands herbeizuführen. Ihr Aufbau ist dabei prinzipiell immer derselbe, lediglich die zeitlichen Abstände zwischen den einzelnen Aktionen sind unterschiedlich. So wird der Fahrer zunächst immer durch eine FÜA aufgefordert, die Fahrzeugführung zu übernehmen. Kommt er dieser Forderung nicht innerhalb der erforderlichen Zeit nach, so wird eine Bremsung eingeleitet. Gleichzeitig wird der umliegende Verkehr, insbesondere der Fahrer des Fahrzeugs hinter dem STA, durch die Betätigung der Warnblinkanlage gewarnt[31]. Außerdem wird ab diesem Zeitpunkt die immer noch aktive FÜA verstärkt. Es wird daher im Folgenden zwischen einer schwachen und einer starken FÜA unterschieden[32]. Übernimmt der Fahrer die Fahrzeugführung während des Bremsvorgangs immer noch nicht, so wird nach Erreichen des Stillstands die Parkbremse eingelegt, um den Stillstand dauerhaft abzusichern. Die FÜA und die Warnblinkanlage bleiben dabei weiterhin aktiv.

Je nachdem, welche Ursache der Auslösung eines Aktionsplans zugrunde liegt, wird entweder die Forderung impliziert, dass der sichere Zustand innerhalb einer definierten Zeitspanne oder aber innerhalb eines definierten, noch verfügbaren Fahrtweges erreicht werden muss. Entsprechend werden, im Sinne größtmöglicher Einfachheit, lediglich zwei longitudinale Aktionspläne konzipiert, die durch einige wenige freie Variablen parametriert werden können und mit denen aber in allen denkbaren Fehlerfällen eine adäquate FS-Reaktion möglich erscheint. Die beiden Aktionspläne werden, entsprechend dem Ziel das sie verfolgen, als „Bremsung“ bzw. „Bremsung auf Ziel“ bezeichnet. Grundsätzlich ist es im Sinne einer möglichst ausgeprägten Modularität und Adaptierbarkeit des FS-Konzepts auf verschiedenste Fehlerfälle (vgl. entsprechendes übergeordnetes Prinzip in Kapitel 2.3) vorgesehen, dass beide Aktionspläne bzw. gleiche Aktionspläne in unterschiedlicher Parametrierung parallel ablaufen können, wobei aber jede der oben genannten Aktionen nur genau einmal ausgelöst werden kann. Werden in diesem Zusammenhang unterschiedlich starke Verzögerungen angefordert, so wird, wie bereits in Kapitel 4.2 erläutert, die stärkste Verzögerung an den Bremsaktuator durchgestellt (vgl. Bild 4.3). Um dabei das durch die Normalfunktion vorgegebene Fahrzeugverhalten nicht unnötig stark zu manipulieren, sollte darauf geachtet werden, dass durch einen Aktionsplan keine Verzögerung angefordert wird, die größer als unbedingt nötig ist.

[31] Zur Warnung des umliegenden Verkehrs ist theoretisch auch die Betätigung der Hupe denkbar.

[32] Die genaue Definition eines Fahrerwarnkonzepts ist nicht Aufgabe eines Sicherheitskonzepts, sondern erfolgt in der Regel im Rahmen der ergonomischen Auslegung eines jeden FAS. Das hier aufgeführte, zweistufige Konzept ist daher lediglich als Vorschlag zu betrachten. Dieser sieht, als schwache FÜA einen einmaligen, dezenten Gong, sowie eine nicht-animierte, visuelle Warnung vor. Als starke FÜA erfolgen dagegen ein wiederholtes Gongen und die Ausgabe einer blinkenden, visuellen Warnung.

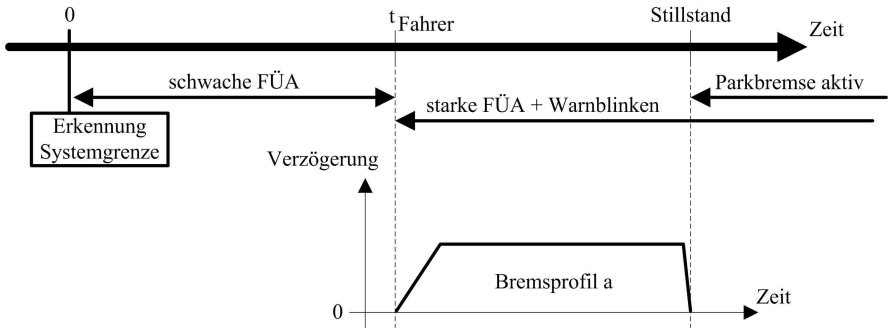

Bild 8.3: Longitudinaler Aktionsplan „Bremsung“

In Bild 8.3 ist der Ablauf des Aktionsplans „Bremsung“, durch den sich das Erreichen des Stillstands innerhalb einer definierten Zeitspanne realisieren lässt, schematisch dargestellt. Wie man sieht, löst er nach Erkennung einer Systemgrenzenüberschreitung sofort eine schwache FÜA aus. Danach wird dem Fahrer ein Zeitraum der Länge t_{Fahrer} gewährt, um die Kontrolle über das Fahrzeug wieder zu übernehmen. Reagiert er jedoch innerhalb dieses Zeitraums nicht, erfolgt eine Verschärfung der FÜA und zudem die Aktivierung der Warnblinkanlage. Gleichzeitig beginnt eine Bremsung gemäß einem vordefinierten Bremsprofil a. Nach Erreichen des Stillstandes wird die Parkbremse aktiviert, wobei die starke FÜA und das Warnblinken weiterhin aktiv bleiben. Da das Bremsprofil a in abgespeicherter Form vorliegt, benötigt der Aktionsplan, nachdem er angetriggert wurde, keinerlei Eigenbewegungs- oder Umfeldmodelldaten. Zur vollständigen Beschreibung einer speziellen Instanz dieses Ablaufschemas ist es notwendig die freien Parameter t_{Fahrer} und ein beliebiges Bremsprofil a zu definieren. Entsprechend wird an dieser Stelle die Bezeichnung „Bremsung (t_{Fahrer}, a)“ eingeführt.

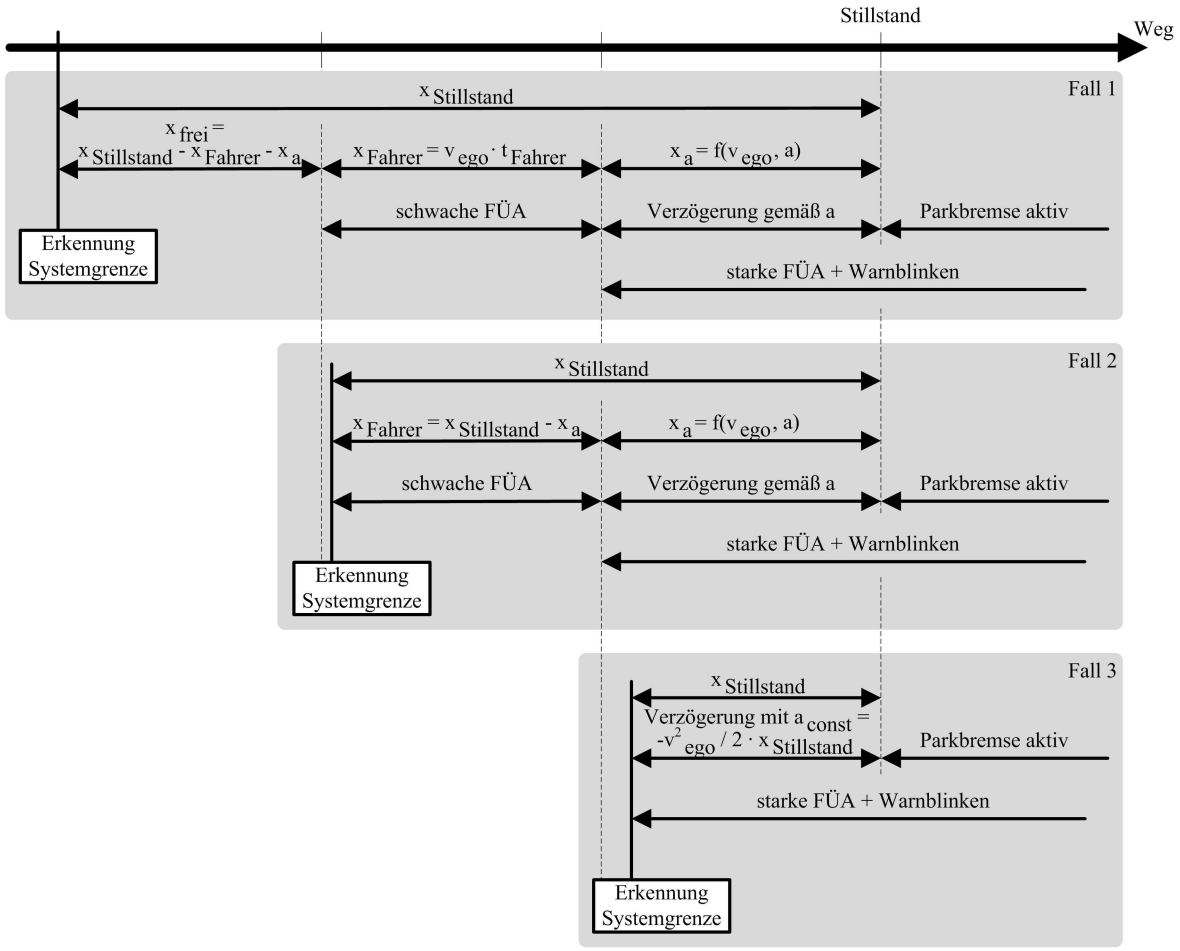

Bild 8.4: Longitudinaler Aktionsplan „Bremsung auf Ziel“

Der Aktionsplan „Bremsung auf Ziel“ ist anzuwenden, falls die Einnahme des Stillstands des Fahrzeugs, ausgehend von seiner aktuellen Position, innerhalb einer definierten Weglänge $x_{Stillstand}$ erfolgen muss. Da die Auslösung der verschiedenen Aktionen bei diesem Ablaufschema im Gegensatz zu einer „Bremsung (t_{Fahrer}, a)“ nicht zeitlich, sondern auf Basis einer Berechnung verschiedener Wegabschnitte bzw. virtueller Wegpunkte geschieht und der angestrebte Zielhaltepunkt zum Zeitpunkt der Auslösung des Aktionsplans im Allgemeinen unterschiedlich weit von der aktuellen Fahrzeugposition entfernt sein kann, muss, wie auch in Bild 8.4 zu sehen ist, zwischen drei Fällen unterschieden werden. In jedem dieser Fälle wird dabei durch die zyklische Integration der momentanen Geschwindigkeit v_{ego}, der seit der Auslösung des Aktionsplans vom STA-Fahrzeug bereits zurückgelegte Weg berechnet. Immer wenn ein virtueller Wegpunkt überschritten wurde (gestrichelte Linie im Bild), wird eine neue Aktion ausgeführt. Als Ausgangslage zur detaillierten Beschreibung der Funktionsweise des Ablaufschemas sei im Folgenden der Aktionsplan „Bremsung (t_{Fahrer}, a)“ betrachtet. Im ersten, sozusagen günstigsten Fall erfolgt die Entscheidung zum Auslösen des Aktionsplans so früh, dass noch gewartet werden kann, bis der Fahrer zur Übernahme der Fahrzeugführung aufgefordert werden muss. Dabei lässt sich, auf Basis von v_{ego} und unter Annahme eines prinzipiell identischen Ablaufschemas wie beim Aktionsplan „Bremsung“, der Weg x_a berechnen, den das Fahrzeug beim Abfahren des vorgegebenen Bremsprofils a bis zum Stillstand zurücklegt. Dazu ist eine zweifache Integration des Verzögerungsverlaufs von a über die Zeit notwendig. Ebenso kann durch die Multiplikation von v_{ego} mit der

vordefinierten, tolerablen Fahrerreaktionszeit t_{Fahrer} der während dieser Zeit zurückgelegte Weg x_{Fahrer} bestimmt werden. Unter Berücksichtigung von x_a und x_{Fahrer} kann nun auf Basis von $x_{Stillstand}$, wie in Bild 8.4 zu sehen ist, auf den Weg x_{frei} geschlossen werden, der bis zur Auslösung einer schwachen FÜA noch zurückgelegt werden kann. Somit sind alle virtuellen Wegpunkte für den Fall 1 definiert. Ungünstigerweise kann es nun passieren (Fall 2), dass eine drohende Systemgrenzenüberschreiten derart spät festgestellt wird, dass $x_{Stillstand}$ kleiner ist als die Summe der für den Bremsvorgang erforderlichen Weglänge x_a und der dem Fahrer zur Reaktion zugestandenen Weglänge x_{Fahrer} aus Fall 1. In dieser Situation ist vorgesehen, sofort eine schwache FÜA auszugeben. Sämtliche Aktionen ab Beginn des Bremseingriffs und damit auch die Berechnung von x_a werden aber wie in Fall 1 beibehalten. Entsprechend wird x_{Fahrer} durch eine Subtraktion von $x_{Stillstand}$ mit x_a bestimmt. Noch extremer ist ein derart später Auslösungszeitpunkt des Aktionsplans (Fall c), so dass nicht einmal durch sofortiges Ansteuern des Bremsprofils a ein rechtzeitiges Anhalten möglich ist. In einem derartigen Fall wird sofort eine starke FÜA ausgegeben, die Warnblinkanlage aktiviert und eine Bremsung mit einer konstanten Verzögerung a_{const} gestartet. Die Berechnung der Verzögerung a_{const} erfolgt in diesem Fall in Abhängigkeit von $x_{Stillstand}$ und v_{ego}, durch Umformung der Formel (7.1) auf Seite 91, wobei hierin g a_{const}, v v_{ego} und x_{brems} $x_{Stillstand}$ entspricht. Wie man Bild 8.4 entnehmen kann, sind für das Funktionieren des Aktionsplans lediglich Eigenbewegungsdaten, aber keine Umfeldmodelldaten notwendig. Freie Parameter sind wie auch beim Aktionsplan „Bremsung“ die Zeit t_{Fahrer}, das Bremsprofil a und überdies noch die Weglänge $x_{Stillstand}$. Entsprechend wird zur vollständigen Beschreibung dieses Ablaufschemas die Bezeichnung „Bremsung auf Ziel (t_{Fahrer}, a, $x_{Stillstand}$)“ eingeführt.

Tritt der Stillstand infolge einer Bremsung durch die Normalfunktion früher ein, als dies durch eines der beiden vorgestellten Ablaufschemata geplant war, so wird sofort die Parkbremse eingelegt und ein Weiterfahren des STA verhindert. Ist in diesem Fall insbesondere eine Instanz des Aktionsplans „Bremsung auf Ziel“ aktiv, so wird mit dem Einlegen der Parkbremse außerdem automatisch ein Aktionsplan „Bremsung“ angetriggert, bei dem die Variablen t_{Fahrer} und a in identischer Weise wie beim erstgenannte Aktionsplan parametriert sind. Dadurch wird, sofern dies noch nicht geschehen ist, nach Erreichen des Stillstands eine schwache FÜA ausgegeben und zu gegebener Zeit auch eine Verschärfung der FÜA sowie eine Aktivierung der Warnblinkanlage ausgelöst. Sinnvoll ist dieses Verhalten beispielsweise an der Funktionsgrenze „Spurende“ (vgl. Kapitel 5.3), da diese oftmals erst erkannt wird, wenn das vor dem STA befindliche Fahrzeug die Spur wechselt und daher ein sofortiges Bremsen in den Stillstand notwendig ist. In diesem Fall erfolgt zur Sicherstellung, dass das Spurende nicht überfahren wird, die Ansteuerung einer „Bremsung auf Ziel“, wobei t_{Fahrer} sehr klein und die Verzögerungswerte des Bremsprofils a sehr hoch gewählt werden. Aufgrund dieser Parametrierung wird die Weglänge x_{frei} sehr groß. Nachdem die Normalfunktion noch völlig intakt ist, wird sie im Normalfall selbstständig vor Erlangung des Spurendes sicher in den Stillstand abbremsen, wobei aber, aufgrund der Aktionsplanparametrierung, keine Aktion des Aktionsplans ausgeführt werden wird. Dies ist sinnvoll, da absehbar ist, dass der Fahrer in diesem Fall selber nicht schnell genug eingreifen können wird. Die Forderung, die Fahraufgabe wieder zu übernehmen, erfolgt durch den oben beschriebenen Mechanismus erst, wenn der Fahrer nach Erlangung des sicheren Zustands auch gefahrlos dazu in der Lage ist.

Sollte im Rahmen von Probandenstudien festgestellt werden, dass eine FÜA den Fahrer in bestimmten Fehlerfällen in Panik versetzt und ihn dadurch zu einem zu schnellen, inadäquaten Eingriff in die Fahrzeugführung verleitet, so ist es aufgrund der selben Intention wie im Falle des „Spurendes“ denkbar, die FÜA auch optional erst nach Einnahme des sicheren Notaus-Zustands auszugeben. Dies gilt insbesondere, wenn ein Aktionsplan „Bremsung“ mit einer sehr geringen Zeit t_{Fahrer} sowie einem sehr radikalen Bremsprofil parametriert wurde und dem Fahrer deshalb kaum eine Chance gegeben wird, vor oder während dem Bremseingriff adäquat zu reagieren.

8.3 Parametrierung von Aktionsplänen und resultierende Forderungen an die Normalfunktion

Longitudinale Aktionspläne reichen im Falle externer Einflüsse oder bei Funktionsgrenzenüberschreitungen aus, um den sicheren Zustand zu erreichen. Ein Übersteuern der Querführung ist dabei nicht notwendig. Dies liegt daran, dass die Normalfunktion in den genannten Fällen noch uneingeschränkt funktionsfähig ist und daher auch nach Auslösung eines Aktionsplans weiterhin sowohl die Querführung als auch die Längsführung übernimmt, bis schließlich ein überlagerter Bremseingriff erfolgt (vgl. Bild 4.3). Bei externen Einflüssen ist üblicherweise der Aktionsplan „Bremsung“ anzuwenden, wobei sich für t_{Fahrer} verhältnismäßig große und für a verhältnismäßig kleine Werte empfehlen, um einen entsprechend sanften Übergang in den sicheren Zustand zu generieren. Hinsichtlich der Aktionsplanparametrierung bei Funktionsgrenzenüberschreitungen sei auf Kapitel 8.5 verwiesen.

Treten systeminterne Fehler in funktionalen Softwaremodulen (FSM) der Wahrnehmung oder in einem Sensor auf, so hat dies zur Folge, dass einzelne Datenstrukturen des Umfeldmodells nicht mehr sinnvoll befüllt werden können und eine Quer- und Längsführung deshalb nicht mehr möglich ist[33]. Für ein ausreichend schnelles Erreichen des sicheren Zustands bietet es sich in diesen Fällen an, den longitudinalen Aktionsplan „Bremsung auf Ziel“ auszulösen (vgl. Bild 8.2). Entscheidend ist hierbei die Variable $x_{Stillstand}$ so zu parametrieren, dass auf keinen Fall eine Kollision mit anderen Objekten erfolgt. Entsprechend müssen auf Basis der letzten validen Werte der nun korrupten Datenstruktur des Umfeldmodells Worst Case-Annahmen getroffen werden, aus denen sich $x_{Stillstand}$ ableiten lässt. Die Aufrechterhaltung der Querführung während des Übergangs in den Stillstand soll im Falle eines Wahrnehmungsfehlers weiter durch die Normalfunktion erfolgen. Daraus leitet sich die Forderung ab, dass die Funktionslogik der Normalfunktion im Falle teilweise korrupter Umfeldmodelldaten in der Lage sein muss, die Querführung auf Basis der Kenntnis der Verkehrssituation unmittelbar vor dem Wahrnehmungsfehler noch bis zur Erlangung des Stillstands sicher aufrechtzuerhalten. Die Funktionslogik benötigt dazu ein Gedächtnis, welches das Wissen über die Entwicklung der Verkehrssituation in den vergangenen

[33] Fehler in der Inertial-Sensorik bzw. in FSM zur Generierung von Eigenbewegungsdaten werden über entsprechende Redundanzen abgefangen (vgl. Kapitel 4.3).

Sekunden abspeichert. Die genannte Forderung ist sinnvoll, da die FSM der Funktionslogik in diesem Fall noch voll funktionsfähig sind und davon auszugehen ist, dass die Aufgabe der Querführungsplanung im Falle einer eingeschränkten Wahrnehmungsleistung auf Basis der dort hinterlegten Algorithmen besser durchgeführt werden kann, als durch einen redundanten Algorithmus des Sicherheitskonzepts. Tabelle 8.1 zeigt, wie im Falle verschiedener Wahrnehmungsfehler der Wert $x_{Stillstand}$ des Aktionsplans „Bremsung auf Ziel“ auf Basis entsprechender Worst Case-Annahmen zu parametrieren ist[34]. Nachdem sich, wie Eingangs bereits erwähnt, sämtliche Wahrnehmungsfehler letzten Endes immer im Defekt einzelner Datenstrukturen des Umfeldmodells (vgl. Kapitel 4.1) widerspiegeln, werden auch nur diese Fehlerfälle betrachtet. Weiterhin wird davon ausgegangen, dass die Informationen über statische Objekte, Freiräume, unbekannte Gebiete in Form einer einzelnen Datenstruktur ausgegeben werden.

korrupte Umfelddaten	Aktionsplan	Worst Case-Annahme
Fahrstreifeninformationen	"Bremsung auf Ziel" $x_{Stillstand}$ = Vorausschau des Fahrstreifendetektors	Die Fahrstreifenmarkierungen fallen im Bereich nach der Vorausschau komplett weg. Der Betrieb des STA ist dennoch auf jeden Fall bis zum Vorausschauende sicher.
Informationen über dynamische Objekte	"Bremsung auf Ziel" $x_{Stillstand}$ = Abstand zum Vorder-Fahrzeug (VFzg) + Bremsweg des VFzgs bei einer Vollverzögerung	Das VFzg macht unmittelbar nach dem Datenausfall eine Vollbremsung. Der Betrieb des STA ist dennoch auf jeden Fall bis zum Ort des Stillstands des VFzgs sicher.
Informationen über statische Objekte, Freiräume und unbekannte Gebiete	"Bremsung auf Ziel" $x_{Stillstand}$ = Abstand zum VFzg	Im Bereich, der infolge einer Verdeckung durch das VFzg unbekannt ist, befindet sich ein Hindernis. Der Betrieb des STA ist dennoch auf jeden Fall bis zum VFzg-Heck sicher.
prädiktive Streckeninformationen	"Bremsung auf Ziel" $x_{Stillstand}$ = Abstand zur nächsten Autobahnausfahrt (bzw. bis zum nächsten kritischen Routenpunkt)	Der Fahrstreifen des STA geht an der nächsten Autobahnausfahrt in einen Verzögerungsstreifen über. Der Betrieb des STA ist dennoch auf jeden Fall bis zu dieser Autobahnausfahrt sicher.

Tabelle 8.1: Aktionsplanauswahl und -Parametrierung bei internen Wahrnehmungsfehlern

Treten systeminterne Fehler in Bereichen nach der Wahrnehmung auf, also in FSM der Funktionslogik bzw. der Regelung[35], oder werden durch die automatische Plausibilitätsprüfung entsprechende situative Unplausibilitäten festgestellt (vgl. Kapitel 7), so muss ebenfalls durch einen longitudinalen Aktionsplan der sichere Zustand angesteuert werden. Kann die Querführung durch die Normalfunktion nicht aufrecht erhalten werden, ist es zudem erforderlich, korrigierend in die Lenkung einzugreifen (vgl. Bild 4.3) und explizit einen sicheren Ort anzusteuern. Nachdem die Umfeldmodelldaten in den genannten Fehlerfällen noch zur Verfügung stehen, ist ein derartiger Querführungseingriff, der das Fahrzeug in seiner Fahrspur hält, prinzipiell möglich (vgl. lateraler Aktionsplan „Notlenken“ in Kapitel 8.4). Er kann aber lediglich als Ergänzung zur Ausführung eines longitudinalen

[34] Werte für die Parametrierung von t_{Fahrer} und a müssen empirisch ermittelt werden und sind deshalb an dieser Stelle nicht mit aufgeführt.

[35] Fehler in der Aktorik, also Defekte der elektronisch ansteuerbaren Bremse oder Lenkung, werden über entsprechende Redundanzen abgefangen (vgl. Kapitel 4.3).

Aktionsplans erfolgen, da ja gemäß der Definition des sicheren Zustands auf jeden Fall der Stillstand des Fahrzeugs erreicht werden muss[36].

Die folgende Tabelle zeigt, welche Aktionspläne ausgelöst werden, wenn mittels des in Kapitel 5.1 beschriebenen Überwachungskonzepts Fehler in den Ausgangsdaten von Funktionslogik und Regelung (vgl. Bild 4.1) detektiert werden und wie $x_{Stillstand}$ im Falle einer „Bremsung auf Ziel“ zu parametrieren ist[34]. Alle anderen internen Fehler in Funktionslogik und Regelung spiegeln sich letztendlich in diesen Fehlern wieder. Nachdem die Längsregelung des STA an das Vorderfahrzeug gekoppelt ist und ihre Hauptaufgabe darin besteht, einen entsprechenden Sicherheitsabstand einzuhalten, hat ein Ausfall der Datenstruktur des Umfeldmodells, die dynamische Objekte beschreibt, immer auch zur Konsequenz, dass die Soll-Größen für die Längsregelung bzw. die Bremsaktuatorstellgrößen nicht mehr berechnet werden können. Aus diesem Grund ist die Aktionsplanauswahl und -Parametrierung in diesen Fällen dieselbe wie im Falle nicht verfügbarer Informationen über dynamische Objekte (vgl. Tabelle 8.1). Können die Eingangsgrößen für die Querregelung oder den Lenkaktuator nicht mehr bestimmt werden, so ist es primär wichtig ein „Notlenken“ zu initiieren, um die Querführung aufrecht zu erhalten. Gleichzeitig muss aber auch ein Aktionsplan „Bremsung“ aktiviert werden, um den Fahrer zur Übernahme aufzufordern, wobei ihm dazu ausreichend Zeit zugestanden werden kann. Für den Fall, dass der Fahrer nicht eingreift, ist ein sehr moderates Bremsprofil sinnvoll.

korrupte Ausgabedaten	Aktionsplan
Sollgrößen für Längsregelung	"Bremsung auf Ziel" $x_{Stillstand}$ = Abstand zu Vorder-Fahrzeug (VFzg) + Bremsweg des VFzgs bei einer Vollverzögerung
Sollgrößen für Querregelung	"Bremsung" + "Notlenken"
Bremsaktuator-Stellgrößen	"Bremsung auf Ziel" $x_{Stillstand}$ = Abstand zu Vorder-Fahrzeug (VFzg) + Bremsweg des VFzgs bei einer Vollverzögerung
Lenkaktuator-Stellgrößen	"Bremsung" + "Notlenken"

Tabelle 8.2: Aktionsplanauswahl und -Parametrierung bei internen Fehlern in der Funktionslogik und Regelung

Situative Unplausibilitäten treten entweder dann auf, wenn systeminterne Fehler von der Normalfunktion im Rahmen der Systemeigendiagnose nicht als solche erkannt werden oder aber die Verkehrssituation dramatisch eskaliert ist. In diesen Fällen ist ein weiterer Betrieb

[36] Es sei an dieser Stelle angemerkt, dass zur schnellstmöglichen Erlangung des sicheren Zustands hinsichtlich der Längsführung eine sofortige Vollbremsung durch einen entsprechend parametrierten Aktionsplan „Bremsung“ notwendig ist, für dessen Abarbeitung es keinerlei Eingangsdaten bedarf (vgl. Kapitel 8.2). Im Gegensatz dazu sind zur Aufrechterhaltung der Querführung immer, also auch während der angesprochenen Vollbremsung, Informationen über die Beschaffenheit des unmittelbaren Fahrzeugumfelds erforderlich.

des STA höchst sicherheitskritisch, weshalb der Normalfunktion sofort jeglicher Einfluss auf die Fahrzeugführung entrissen und der sichere Notaus-Zustand angesteuert werden muss. Daher soll im Falle situativer Unplausibilitäten, unabhängig davon welcher Detektionsmechanismus einen Fehler gemeldet hat, immer ein „Notlenken“ und eine „Bremsung (0s, 9,81m/s^2)“, also eine sofortige Vollbremsung, ausgeführt werden.

8.4 Lateraler Aktionsplan

Der nun vorgestellte, laterale Aktionsplan „Notlenken“ hat das Ziel, das STA-Fahrzeug im Falle der in Kapitel 8.3 aufgeführten Fehlerfälle unter Berücksichtigung der Objekte in seinem Umfeld in der Fahrspur zu halten und es damit an einem „sicheren Ort“ zu positionieren. Wie bereits aus dem vorangegangenen Kapitel deutlich wurde, darf eine Aktivierung dieses Aktionsplans nur in Kombination mit einem longitudinalen Aktionsplan erfolgen. Eine spezielle Parametrierbarkeit wie bei longitudinalen Aktionsplänen ist nicht vorgesehen.

Grundsätzlich beeinflussen sich die Längs- und Querdynamik eines Fahrzeugs über die aktuelle Geschwindigkeit und den Kurvenwiderstand gegenseitig (vgl. [Roppenecker 1994]). Diese Querbeziehung kann aber für das System STA aufgrund der niedrigen Geschwindigkeiten im Stau und der sehr großen Kurvenradien auf Autobahnen vernachlässigt werden. Die Auslegung des lateralen Aktionsplans kann daher vollständig unabhängig von der Längsführung bzw. den longitudinalen Aktionsplänen erfolgen. Überdies wird davon ausgegangen, dass die Stabilitätssysteme ABS und ESP (elektronisches Stabilitätsprogramm) während des Betriebs des STA aktiv bleiben und dafür sorgen, dass keine unkontrollierbaren, fahrdynamischen Zustände eintreten.

Aus der Robotik sind verschiedene sogenannte Steuerungsarchitekturen bekannt, durch die eine „Umsetzung von abstrakt formulierten Aufgaben in ausführbare Handlungen“ bei automatisierten Systemen erfolgen kann. Hierbei wird zwischen unterschiedlichen Kategorien unterschieden. Die im Kontext des Notlenkens wichtigste Unterscheidung betrifft deliberative und reaktive Steuerungsarchitekturen (vgl. Bild 8.5). Deliberative Ansätze basieren darauf, dass Sensorinformationen aufgenommen werden und eine sich kontinuierlich verändernde Modellvorstellung der Umwelt, das sogenannte Weltmodell, beeinflussen, welches systemintern, wie eine Art menschliches Gedächtnis, abgespeichert ist. Die auszuführende Handlung wird hierbei unter Berücksichtigung der aktuell empfangenen Sensorinformationen und des Weltmodells aufwändig vorausgeplant und danach entsprechend in die Tat umgesetzt. Im Gegensatz dazu verwenden reaktive Architekturen kein Weltmodell, sondern entscheiden in jedem Zeitschritt auf Basis einfacher Verhaltensregeln vollkommen neu, welche Reaktion unter Berücksichtigung der eingehenden Sensorinformationen als nächstes erfolgen soll. (vgl. [Lehmann 2008])

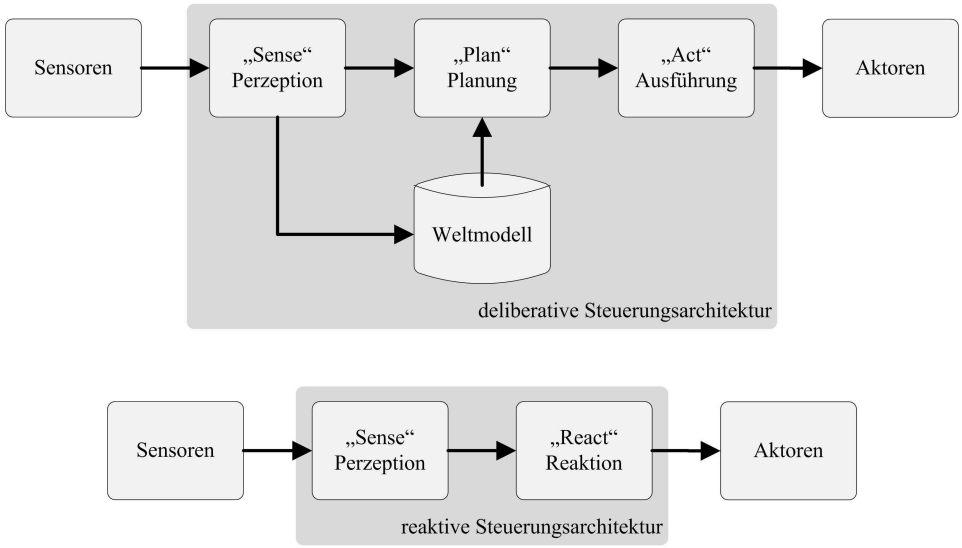

Bild 8.5: Schematische Darstellung einer delibertativen und einer reaktiven Steuerungsarchtektur in Anlehnung an [Lehmann 2008]

Da bei der Entwicklung des Sicherheitskonzepts großer Wert auf die Erfüllung des übergeordneten Prinzips der „Einfachheit und Prädizierbarkeit“ gelegt werden soll (vgl. Kapitel 2.3), kommt ein deliberativer Ansatz für den Notlenk-Algorithmus nicht in Betracht, da der Aufbau eines Weltmodells und die anschließende Planung komplex und fehleranfällig ist[37]. Ziel ist es stattdessen, einen reaktiven Ansatz zu verfolgen und damit ein reflexartiges, Kollisionen vermeidendes Querführungsverhalten zu realisieren, das in kritischen Fahrsituationen größtmögliche Sicherheit garantiert (vgl. übergeordnetes Prinzip der „Garantie eines sicheren Zustands“). Ein eventuell resultierendes unruhiges Lenkverhalten kann dabei in Kauf genommen werden, da der laterale Aktionsplan ja nur kurzzeitig während eines Übergangs in den sicheren Zustand aktiv ist.

Der aus der Robotik stammende DAMN-Ansatz (Distributed Architecture for Mobile Navigation) bietet ein derartiges einfaches und leicht verständliches Konzept zur reaktiven Querführung eines Automobils. Da der Ansatz zudem bereits in zwei realen Fahrzeugen von Entwicklerteams der technischen Universität Braunschweig sowie der Universität der Bundeswehr München erfolgreich implementiert wurde und erwiesener Maßen auch in komplexen kritischen Situationen ein sehr verlässliches Fahrverhalten ermöglicht (vgl. [Berger & Rumpe 2008], [Basarke et al. 2007] und [Von Hundelshausen et al. 2008]), wurde das Konzept bei der Entwicklung des lateralen Aktionsplans „Notlenken“ angewendet.

Das Verfahren basiert darauf, in jedem Zeitschritt beliebige vordefinierte Bahnkurven bzw. Pfade, jeweils einzeln durch ein zentrales Modul nach beliebigen Kriterien zu bewerten (vgl. Bild 8.6). Die Bewertung geschieht dabei vor allem unter Beachtung der Beschaffenheit der

[37] Es wird an dieser Stelle darauf hingewiesen, dass der longitudinale Aktionsplan „Bremsung“ einen reaktiven Ansatz und der longitudinale Aktionsplan „Bremsung auf Ziel“ streng genommen einen deliberativen Ansatz verfolgt, bei dem das Weltmodell in der Speicherung des bereits zurückgelegten Weges bzw. $x_{Stillstand}$ besteht. Da dieses Weltmodell aber extrem einfach gehalten ist, ist ein deliberativer Ansatz in diesem speziellen Fall auch im Rahmen eines Sicherheitskonzepts zulässig.

Umgebung um das Fahrzeug: „DAMN functions at the level of geometrical reasoning, which is essential to the successful performance of an autonomous mobile (…) system.“ Die Ergebnisse der verschiedenen Bewertungen werden danach durch eine gewichtete Summe der Einzelbewertungen kombiniert und der in Gesamtheit beste Pfad auswählt. Daraus wird danach ein entsprechender Aktuatorstellbefehl abgeleitet und an die elektronisch ansteuerbare Lenkung gestellt, wodurch sich das Fahrzeug, soweit es innerhalb eines Zeitschritts möglich ist, in Richtung der Krümmung am Anfang der Bahnkurve orientiert. Im nächsten Zeitschritt wird das beschriebene Verfahren komplett von neuem wiederholt. Man beachte hierbei, dass die jeweils zuletzt ausgewählte, potentiell beste Bahnkurve zu Beginn jedes Zyklus wieder verworfen und daher niemals komplett abgefahren wird. (vgl. [Rosenblatt 1997])

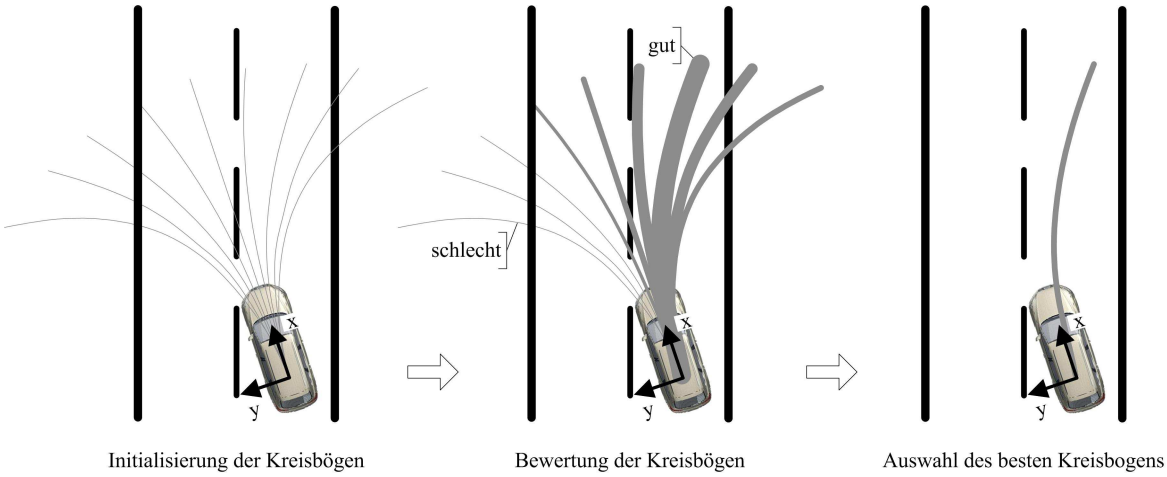

Bild 8.6: DAMN-Querführungs-Algorithmus

Wie im obigen Bild zu erkennen ist, besteht der vordefinierte Satz an Bahnkurven beim „Notlenken“ ausschließlich aus Kreisbögen, die jeweils im Fahrzeug-Koordinatensystem tangential zur x-Achse beginnen. Dies hat den Vorteil, dass sich über den Radius des ausgewählten Kreisbogens gemäß dem Einspurmodell als Ausgangsgröße des APU, der das „Notlenken“ durchführt, direkt ein entsprechender konstanter Radlenkwinkel berechnen lässt (vgl. [Mitschke & Wallentowitz 2004]). Auf diese Weise ist, wie im Zusammenhang mit dem übergeordneten Prinzip der „Echtzeitfähigkeit“ gefordert, eine direkte Ansteuerung der Lenkaktuatorregelung möglich.

Als Eingangsinformationen dienen dem lateralen Aktionsplan Eigenbewegungs- und sämtliche Umfeldmodelldaten, mit Ausnahme der prädiktiven Streckendaten. Die Umfeldmodelldaten werden vor Eingang in den DAMN-Algorithmus in drei Schritten umfangreich vorverarbeitet. Zunächst wird dabei jeder unbekannte Bereich, wie es auch im Rahmen der automatischen Plausibilitätsprüfung geschieht, aus denselben dort genannten Gründen in einen belegten Bereich umgewandelt (vgl. Kapitel 7.2). Der Bereich außerhalb der Fahrspur wird jedoch nicht als belegt interpretiert, da es dem Notlenk-Algorithmus erlaubt sein soll, zur Vermeidung einer Kollision, kurzeitig die eigene Fahrspur zu verlassen. Um das STA-Fahrzeugs unter Vernachlässigung seiner Ausdehnung im DAMN-Algorithmus als punktförmiges Objekt behandeln zu können, wird die Ausdehnung aller dynamischen und aller (umgewandelten) statischen Objekte im zweiten Schritt um die halbe Fahrzeugbreite in beide y-Richtungen des Fahrzeug-Koordinatensystems (vgl. Bild 8.6) vergrößert. Diese

Vereinfachung ist zulässig, da angenommen werden kann, dass die Bewegung des STA hauptsächlich in x-Richtung erfolgt. Es ist auf diese Weise möglich, das Gebiet beim Abfahren eines Kreisbogens, wie in Bild 8.6 dargestellt, als Linie zu betrachten, wodurch sich die Bewertung der Pfade erheblich erleichtert. Wie bereits in Kapitel 8.3 angedeutet wurde, liegen die Umfeldmodellinformationen über die Ausdehnung und Position von statischen Objekten und Freiräumen in einer gemeinsamen Datenstruktur vor. Diese Datenstruktur beschreibt die Kontur der Grenzflächen zwischen den beiden Bereichen ähnlich wie in einer Landkarte, die auch Belegungskarte genannt wird (vgl. [Reichel et al. 2010]). Um bei der Querführung auch andere Fahrzeuge berücksichtigen zu können, werden im dritten Vorverarbeitungsschritt alle dynamischen Objekte, die üblicherweise in Form einer Objektliste vorliegen, durch ein im Folgenden beschriebenes Verfahren in diese Belegungskarte projiziert. Dadurch ist es später möglich, dass die oben angesprochene geometrische Bewertung (engl. geometrical reasoning) der verschiedenen Kreisbögen bezüglich nicht überfahrbarer Hindernisse im DAMN-Algorithmus nur noch auf Basis einer einzigen Datenstruktur und ohne eine Unterscheidung von statischen und dynamischen Objekten erfolgen kann.

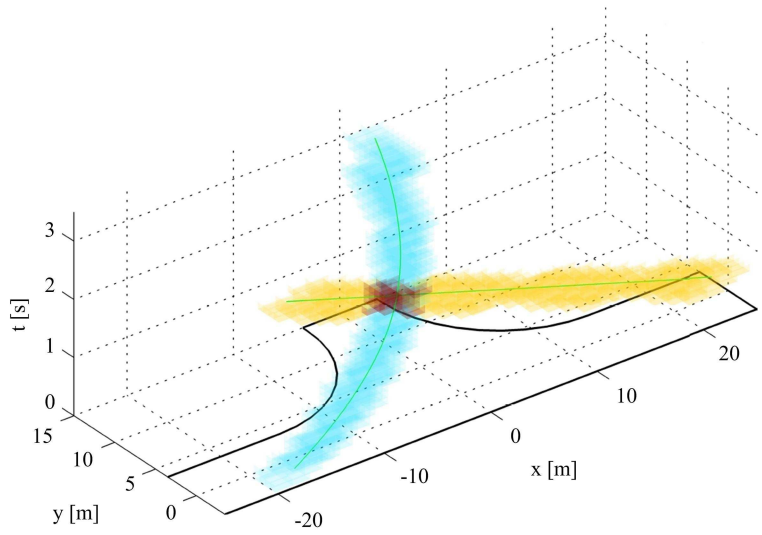

Bild 8.7: Belegung derselben Raumelemente bei einer Kollision (dunkel) durch Abbieger (von links kommend) und Gegenverkehr (von rechts kommend) nach [Meitinger 2008]

Das angesprochene Verfahren basiert auf Überlegungen von [Meitinger 2008], der im Rahmen des BMW Forschungsprojekts „Kreuzungsassistent“ den Hergang von Kollisionen in einer Kreuzung in einem dreidimensionalen Aufenthaltsraum beschreibt, der durch die zwei möglichen Bewegungsrichtungen der Fahrzeuge und die Zeit aufgespannt wird (vgl. Bild 8.7). Die beiden dargestellten Kurven beschreiben die Aufenthaltsgebiete zweier Fahrzeuge in diesem Raum. Schneiden sich die Gebiete, stellt dies eine Kollision dar. Die Aufenthaltsgebiete von Fahrzeugen können unter Annahme ihres zukünftigen Bewegungsverhaltens prädiziert werden, wobei diese Annahmen gemäß dem übergeordneten Prinzip der Einfachheit im Falle des Notlenkens so simpel wie nur möglich gehalten werden sollten. Entsprechend werden im Rahmen dieser Arbeit für alle Fahrzeuge im Umfeld des STA einfache constant-acceleration-Modelle (engl. für konstante Beschleunigung) verwendet, bei denen davon ausgegangen wird, dass die Fahrzeuge ihren momentanen Beschleunigungswert konstant aufrecht erhalten und sich weiter in ihre momentane

Bewegungsrichtung fortbewegen (vgl. [Li & Jilkov 2003]). Das zukünftige Verhalten des STA-Fahrzeug kann dagegen in longitudinaler Richtung auf Basis des Bremsprofils des ausgewählten longitudinalen Aktionsplans und in lateraler Richtung auf Basis des im letzten Zeitschritt durch den DAMN-Algorithmus berechneten Radlenkwinkels deutlich genauer prädiziert werden.

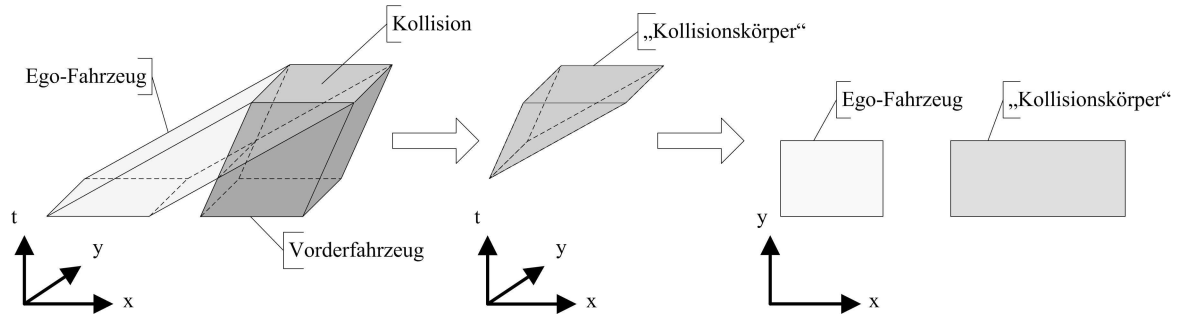

Bild 8.8: Verfahren zur Projektion dynamischer Objekte in eine Belegungskarte

Auf Basis der beschriebenen Modellvorstellung werden im dritten Vorverarbeitungsschritt für das STA-Fahrzeug und jedes im unmittelbaren Umfeld befindliche Fahrzeug die zukünftig belegten Raumelemente im Aufenthaltsraum berechnet. Ergeben sich potentielle Kollisionen in Form sogenannter „Kollisionskörper“, so werden diese in die zweidimensionale xy-Raumebene der Fahrzeuge projiziert. Diese Projektionsflächen werden dann im Rahmen der Datenvorverarbeitung in die oben angesprochene Belegungskarte als statisch belegte Bereiche eingetragen. In Bild 8.8 ist dieser Vorgang für eine potentielle Kollision zwischen Vorderfahrzeug und Ego-Fahrzeug (EFzg) dargestellt, wobei sich beide Fahrzeuge unbeschleunigt mit konstanter Geschwindigkeit in x-Richtung bewegen. Indem den Projektionsflächen der Kollisionskörper mittels des Aktionsplans „Notlenken“ ausgewichen wird, können Kollisionen mit dynamischen Hindernissen verhindert werden.

Nachdem die Umfeldmodelldaten vorverarbeitet wurden, kann nun die Bewertung der verschiedenen Kreisbögen durch den DAMN-Algorithmus erfolgen. Um eine gesamtheitliche Bewertung zu ermöglichen, ist die Definition relevanter Bewertungskriterien und eines sinnvollen Bewertungsschemas zur Verknüpfung dieser Kriterien notwendig. Sie werden im Folgenden beschrieben.

Grundsätzlich wird hinsichtlich jedes einzelnen Kreisbogens für jedes Bewertungskriterium i ein Güte-Werte w_i bestimmt, der einen Wertebereich von Null bis Eins hat, wobei Null die schlechteste und Eins die bestmögliche Bewertung ist. Das erste von vier Bewertungskriterien, der sogenannte „longitudinale Abstand“, beschreibt die Weglänge x_{long} entlang eines Kreisbogens beginnend im Fahrzeug-Koordinatensystem bis zum Auftreffen auf ein Hindernis. Unter dem Aspekt der Sicherheit ist dieses Bewertungskriterium das wichtigste, da es jene Bahnkurve auswählt, die am weitesten in den Freiraum steuert und somit Kollisionen mit Hindernissen vermeidet. Der korrespondierende Güte-Wert w_{long} berechnet sich durch den Quotienten von x_{long} und der absoluten Länge des Kreisbogens. Letztere ist vordefiniert und für alle Kreisbögen identisch.

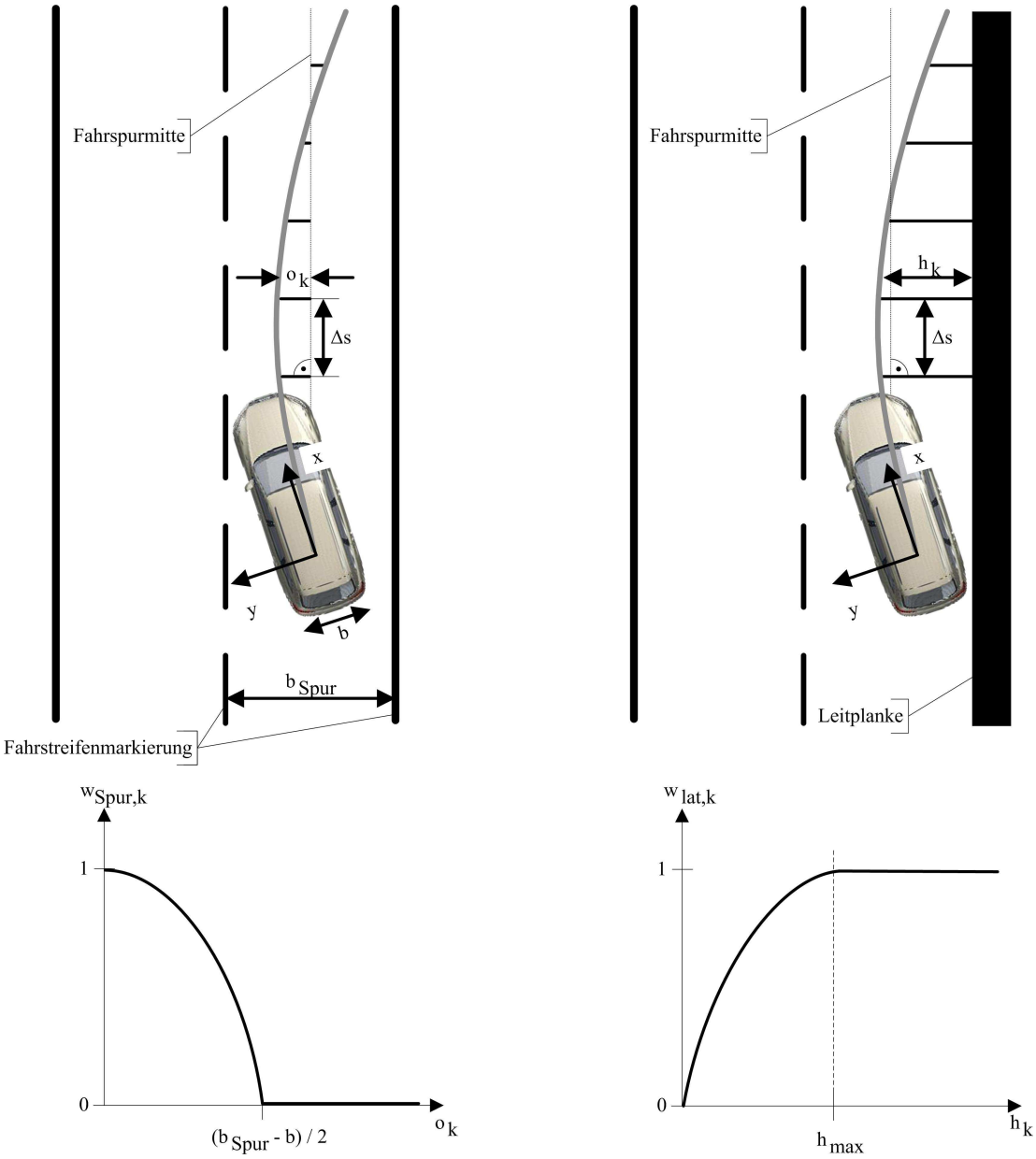

Bild 8.9: Bewertungskriterien „Fahrspur“ (links) und „lateraler Abstand“ (rechts)

Nachdem es beim Übergang in den sicheren Zustand das Ziel ist, den STA innerhalb der eigenen Fahrspur zu halten, ist das Bewertungskriterium „Spurabstand“, das den Abstand eines jeden Kreisbogens zur Spurmitte beschreibt, das zweitwichtigste. Ein kurzzeitiges Verlassen der eigenen Fahrspur ist damit nur zulässig, wenn es der Vermeidung einer Kollision dient. Bild 8.9 ist an die Grafik auf der rechten Seite in Bild 8.6 angelehnt und beschreibt die Bestimmung des Güte-Werts w_{Spur} für den dort abgebildeten Kreisbogen. Wie man sieht, wird zunächst geometrisch in regelmäßigen Abständen Δs die Ablage o_k des Kreisbogens zur Spurmitte bestimmt. Für jedes o_k eines Pfades wird dann, gemäß der abgebildeten Funktion, ein Gütewert $w_{Spur,k}$ berechnet. w_{Spur} ergibt sich schließlich aus dem arithmetischen Mittel dieser einzelnen Gütewerte. Wie man sieht, nimmt $w_{Spur,k}$ ab einem o_k-Wert, bei der das EFzg die Spurmarkierung übertritt, den Wert Null an. Da eine Änderung der Ablage in relativ weiter Entfernung der Spurmitte verhältnismäßig stärker bewertet werden soll als nahe der Spurmitte, wurde der dargestellte quadratische Verlauf zur Berechnung von

$w_{Spur,k}$ gewählt. Das drittwichtigste Kriterium „lateraler Abstand“ bewertet den Abstand eines jeden Kreisbogens zu Hindernissen in lateraler Richtung. Es soll hiermit erreicht werden, dass Hindernissen nicht unnötig knapp ausgewichen wird. Wie in Bild 8.9 dargestellt, wird zur Berechnung des entsprechenden Güte-Werts w_{lat} zunächst, ähnlich wie auch beim Kriterium „Spurabstand“, in regelmäßigen Abständen Δs orthogonal zur Fahrspur- bzw. Fahrstreifenrichtung der Abstand h_k zum nächsten Hindernis bestimmt und daraus mittels der abgebildeten Funktion jeweils ein Gütewert $w_{lat,k}$ berechnet. Aus allen Werten von $w_{lat,k}$ wird dann wieder der arithmetische Mittelwert gebildet, aus dem sich dann w_{lat} ergibt. Mittels des quadratischen Verlaufs des ersten Teils der Funktion soll erreicht werden, dass lateral sehr nahe Hindernisse eine besonders schlechte Bewertung erzeugen. Da es ab einem gewissen lateralen Abstand $h_{k,max}$ nicht mehr wichtig ist, ob der STA noch weiter entfernt an einem Hindernis vorbei fährt, da bereits ein genügend großer, lateraler Sicherheitsabstand eingehalten wird, nimmt die dargestellte Funktion ab diesem Punkt den Wert Eins an. Das letzte Kriterium „Krümmung“ bewertet die Krümmung der Kreisbögen. Eine geringe Krümmung ist aus Sicht der Systemsicherheit besser, weil auf ihr eine geringe Querbeschleunigung aufgebaut wird. Bei einer geringeren Querbeschleunigung sind, gemäß dem Kammschen Kreis (vgl. [Mitschke & Wallentowitz 2004]), innerhalb der Haftungsgrenzen größere Verzögerungen und damit theoretisch kürzere absolute Bremswege möglich. Nachdem das STA-Fahrzeug durch das zweitstärkste Kriterium w_{Spur} bereits in der Fahrspur gehalten wird und die Kurvenradien auf Autobahnen sehr große sind, werden ohnehin keine Kreisbögen ausgewählt, die, auch im Falle einer Vollverzögerung, nennenswert unterschiedliche Bremswege bedingen. Um ein möglichst ruhiges, komfortables Fahrverhalten zu realisieren, wird dennoch ein Gütewert $w_{Krümmung}$ als Komfortkriterium im DAMN-Algorithmus berücksichtigt, der sich gemäß folgender Formel berechnet. Hierin ist c_0 die Krümmung des betrachteten Kreisbogens und $c_{0,max}$ die Krümmung des Wendekreises des Fahrzeugs.

$$w_{Krümmung} = 1 - \frac{c_0}{c_{0,\max}} \tag{8.1}$$

Die Definition eines sinnvollen Bewertungsschemas zur Verknüpfung der Gütewerte w_i ist notwendig, da die verschiedenen aufgeführten Kriterien gegenläufig sein können. Ein entsprechendes Beispiel ist ein vollständig frei befahrbarer Kreisbogen mit großer Krümmung. In diesem Fall resultiert eine gute Bewertung für w_{long} und eine schlechte für $w_{Krümmung}$. Da der „longitudinaler Abstand“ das ausschlaggebende Kriterium zur Vermeidung von Kollisionen darstellt, darf dieser Aspekt unter keinen Umständen durch ein anderes Kriterium überstimmt werden. Entsprechend wurde deshalb ein hierarchisches Bewertungsschema definiert, das zunächst jene Pfade vorausgewählt, deren w_{long}-Wert innerhalb eines Toleranzintervalls definierter Länge unterhalb des besten w_{long}-Werts aller Kreisbögen liegt. Alle anderen Kreisbögen werden verworfen. Im zweiten Schritt wird dann eine gewichtete Summe der Einzelbewertungen der verbleibenden Kreisbögen gebildet:

$$w_{ges} = \alpha_1 \cdot w_{Spur} + \alpha_2 \cdot w_{lat} + \alpha_3 \cdot w_{Krümmung} \tag{8.2}$$

Die Gewichtungsfaktoren α_i haben ebenfalls einen Wertebereich von Null bis Eins und werden unter Beachtung einer Relevanzreihenfolge parametriert. Letztere ist, wie bereits im

vorangegangenen Abschnitt angedeutet wurde, folgendermaßen festgelegt: „longitudinaler Abstand“, „Spurabstand“, „lateraler Abstand“ und „Krümmung“. Nachdem der kombinierte Gütewert w_{ges} für alle verbleibenden Kreisbögen gemäß Formel (8.2) berechnet und die Krümmung des besten Kreisbogens bestimmt wurde, wird daraus der entsprechende Lenkradwinkel berechnet und an die Lenkaktuatorregelung gestellt.

8.5 Aktionsplanbewertung an Funktionsgrenzen

Nachdem longitudinale Aktionspläne an den Funktionsgrenzen des STA auch im fehlerfreien Betrieb häufig in Kraft treten, stellen sie in diesen Fällen, wie bereits erwähnt, eine funktionale Erweiterung der Normalfunktion dar. Da ein Abbremsen des STA im Falle einer Stauauflösung bzw. eines Autobahnendes für umliegende Verkehrsteilnehmer, anders als bei der Funktionsgrenze Spurende, aus dem Kontext der Verkehrssituation nicht vorhersehbar ist, soll in diesem Kapitel systematisch nachgewiesen werden, dass dieses Verhalten nicht sicherheitskritisch ist. Dazu wird zunächst jeweils die Parametrierung der Aktionspläne in den genannten Fällen beschrieben und danach das Risiko der Anwendung in einer Worst Case-Situationen analysiert.

Im Falle eines sich auflösenden Staus wird eine „Bremsung (7s, -1m/s^2)“ und im Falle eines Autobahnendes eine „Bremsung auf Ziel (7s, -2m/s^2, 150m)“ ausgeführt. Der Wert 7s für t_{Fahrer} wurde empirisch festgelegt, genauso wie das Bremsprofil einer konstanten Verzögerung von -2m/s^2 im Falle des Autobahnendes. Für eine Stauauflösung wurde eine geringere Verzögerung definiert, da ein Abbremsen des STA in dieser Situation aufgrund des höheren Geschwindigkeitsniveaus für die anderen Verkehrsteilnehmer noch unvorhersehbarer ist. $x_{Stillstand}$ wurde für den Fall des Autobahnendes mit dem Wert 150m festgelegt, da somit bei der beschriebenen Parametrierung von t_{Fahrer} und a, gemäß Bild 8.4, immer ein Fall 1 provoziert wird.

Im Hinblick auf eine Stauauflösung sei die im Folgenden beschriebene Worst Case-Situation betrachtet. Das STA-Fahrzeug ist unbeschleunigt und hat eine Geschwindigkeit nahe der Geschwindigkeitsobergrenze (ca. 60km/h). Betrachtet wird nun eine potentielle Kollision mit dem dahinter befindlichen Fahrzeug. Es wird der Einfachheit halber angenommen, dass dieses ebenfalls unbeschleunigt ist, aber bereits eine Geschwindigkeit von ca. 80km/h hat, da der ursprüngliche Hintermann des STA-Fahrzeugs bereits zum Überholen die Spur gewechselt hat, und das besagte nachfolgende Fahrzeug nun auf den STA auffährt. Die Zeitlücke zwischen den beiden Fahrzeugen sei, gemessen an den bei ACC-Systemen üblichen Werten, gering und betrage ca. 0,7s, was in etwa 16m entspricht. In dieser Konstellation beginnt das STA-Fahrzeug gemäß der oben aufgeführten Aktionsplanparametrierung mit -1m/s^2 zu verzögern. Der Fahrer des hinteren Fahrzeugs beginnt nach einer gewissen Reaktionszeit mit -7m/s^2 zu verzögern. Dieser Verzögerungswert entspricht in etwa dem, was ein Normalfahrer im Rahmen einer Vollbremsung stellen kann. Um nun zu analysieren, wie kritisch diese Worst Case-Situation ist, soll nun der Bewertungsformalismus einer Gefährdungsanalyse und Risikoeinstufung zur Bestimmung von Automotive Safety Integrity Leveln (ASIL, vgl. Kapitel 1.3) auf den genannten Fall angewendet werden. Es sei darauf hingewiesen, dass dieses Vorgehen keine Gefährdungsanalyse im klassischen Sinne darstellt, da hier

normalerweise nur Fehlfunktionen betrachtet werden, die auf systeminterne Fehler zurückgehen, nicht aber das definierte Verhalten der Normalfunktion. Das Schadensausmaß wird für den beschriebenen Worst Case-Fall mit S1 bewertet[38]. Dies liegt daran, dass sich auch im Falle dessen, dass der Hintermann keine Bremsung einleitet und mit konstant 80km/h frontal auf den verzögernden STA auffährt, nur eine Kollisionsdifferenzgeschwindigkeit von ca. 27km/h ergibt, wodurch lediglich leichte Verletzungen zu erwarten sind. Die Aufenthaltshäufigkeit in dieser Situation wird mit E2 bewertet, da mit der beschriebenen Konstellation im Autobahnstau nur wenige Male pro Jahr zu rechnen ist. Auf Basis einer einfachen Rechnung kann gezeigt werden, dass eine Kollision gerade noch vermeidbar ist, wenn der Fahrer des hinteren Fahrzeugs ca. 1,2s nach Beginn des Bremsvorgangs des STA mit den oben genannten -7m/s^2 zu verzögern beginnt. Da dies eine relativ große Zeitspanne darstellt, wird die Kontrollierbarkeit mit C1, also als einfach beherrschbar eingeschätzt. Gemäß Tabelle 1.1 ergibt sich somit ein ASIL von QM, das im Sinne der Norm [ISO DIS 26262: 2009] unkritisch ist und keiner weiteren Maßnahmen bedarf.

Im Bezug auf ein nahendes Autobahnende wird als Worst Case-Fall wiederum eine potentielle Frontal-Kollision zwischen dem STA und einem rückwärtigen Fahrzeug betrachtet, wobei sich diesmal beide Fahrzeuge mit einer Geschwindigkeit von ca. 60km/h bewegen. Der Abstand sei wiederum mit 16m angenommen. In dieser Konstellation startet das STA-Fahrzeug, wie im Aktionsplan vorgesehen, eine Verzögerung mit -2m/s^2. Der Hintermann verzögert wiederum nach einer gewissen Reaktionszeit mit -7m/s^2. Nimmt man, wie auch im Falle der Stauauflösung, zur Bewertung der Schadensschwere an, dass der Hintermann ungebremst auf den STA auffährt, ergibt sich eine Differenzgeschwindigkeit für die Frontalkollision beider Fahrzeuge von etwa 29km/h. Nachdem dieser Wert im selben Bereich wie beim vorherigen Beispiel liegt, resultiert auch hier ein Schadensausmaß von S1. Auch die Aufenthaltshäufigkeit in dieser Situation ist vergleichbar mit dem obigen Beispiel und wird deshalb ebenfalls mit E2 bewertet. Die maximale, dem Fahrer zur Verfügung stehende Reaktionszeit um eine Kollision gerade noch vermeiden zu können, lässt sich in identischer Weise wie beim Worst Case-Fall der Stauauflösung berechnen und beträgt in diesem Fall ca. 1,4s. Somit resultiert auch hier ein Kontrollierbarkeitswert von C1 und damit in Summe eine ebenfalls unbedenkliche ASIL-Einstufung von QM.

Fasst man die Ergebnisse aus Kapitel 8.3 und 8.5 zusammen, so wird ersichtlich, dass wirklich auf jegliche Systemgrenzenüberschreitung adäquat reagiert und somit, wie Eingangs gefordert, zu jeder Zeit ein sicherer Zustand bzw. ein sicherer Betrieb des autonomen STA garantiert werden kann.

[38] Die Bewertung der Kriterien S, E und C erfolgte in Zusammenarbeit mit einem Experten für Systemsicherheit der Audi AG.

9 Prototypische Umsetzung für ein autonomes Stauassistenzsystem

Die in Kapitel 5, 7 und 8 vorgestellten Überwachungskonzepte und Fail-Safe-Mechanismen (FS), die im Rahmen eines funktionalen Sicherheitskonzepts architekturell in ein autonomes Fahrerassistenzsystem (A FAS) zu integrieren sind (vgl. Kapitel 4), wurden prototypisch für das System Stauassistent (STA) in einem realen Fahrzeug umgesetzt und validiert. Im Folgenden wird dieser Versuchsträger zunächst kurz beschrieben (Kapitel 9.1) und danach auf die hierin implementierte Funktionalität eingegangen (Kapitel 9.2). Besonderes Augenmerk wird dabei auf das FS-Verhalten des Fahrzeugs bei der Überschreitung verschiedener Systemgrenzen in gestellten Fahrsituationen am Testgelände sowie in realen Verkehrssituationen gelegt. Es sei angemerkt, dass das in Kapitel 6 präsentierte Fahrerüberwachungskonzept für vollautomatische FAS (VA FAS) lediglich theoretisch erarbeitet wurde und als Abrundung der Arbeit, im Hinblick auf eine möglichst ganzheitliche Betrachtung der aus einer vollständigen Fahrzeugführungsautomatisierung resultierenden Sicherheitsproblematik, zu sehen ist.

9.1 Versuchsträger

Als Versuchträger dient der in Bild 9.1 dargestellte Audi Q7 3,0 TDI, der zusätzlich zum serienmäßigen elektronischen Stabilitätsprogramm (ESP) mit einem gesonderten Inertialsensorik-Cluster zur Bestimmung von Eigenbewegungsgrößen ausgestattet ist.

Bild 9.1: Versuchsträger am Testgelände (links) und im aktiven Stauassistent-Betrieb auf einer realen Autobahn (rechts)

Zur Umfelderfassung sind außerdem folgende Sensoren im Fahrzeug verbaut (vgl. Bild 9.2):

- Eine monokulare Kamera mit einer Auflösung von 512*1024 Bildpunkten und einem Öffnungswinkel von etwa 45°
- Ein Doppel-Long-Range-Radar-System, das bei einer Frequenz von 77GHz betrieben wird und einen Öffnungswinkel von ca. 30° sowie eine Reichweite von etwa 250m aufweist

- Ein Laserscanner, dessen Kanäle einen Öffnungswinkel von ca. 4° in vertikaler und 1-4° in horizontaler Richtung aufweisen und der einen Erfassungsbereich von etwa 160°, sowie eine Reichweite von ca. 80m hat
- Ein Navigationssystem mit GPS (Global Positioning System)-Receiver, das prädiktive Streckendaten generiert

Zudem dienen sämtliche serienmäßig über verschiedene Fahrzeugbusse verfügbare Daten als weitere, den Fahrzeugstatus beschreibende Informationsquelle.

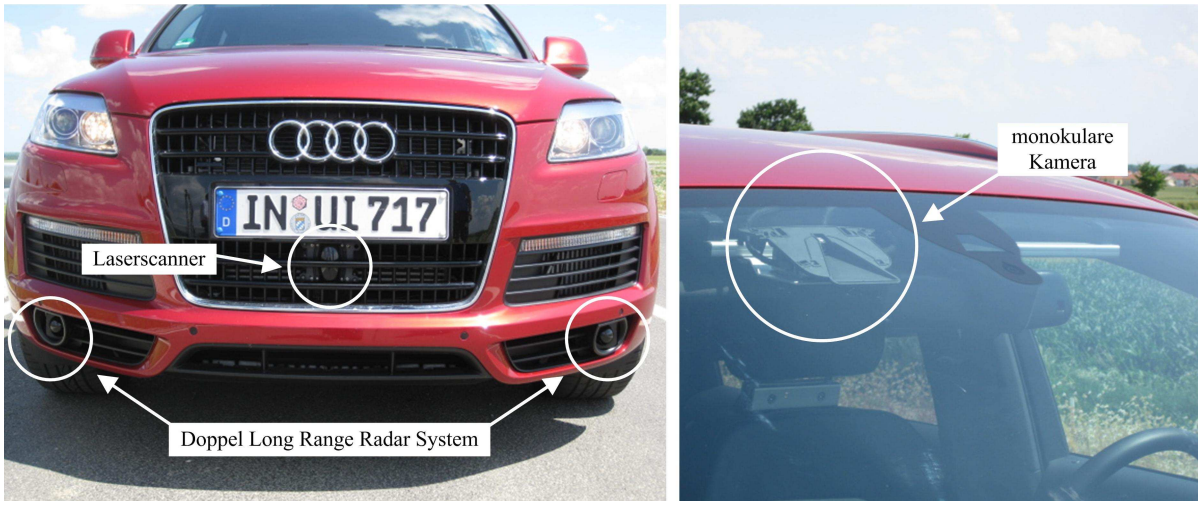

Bild 9.2: Umfeldsensorik des Stauassistent-Versuchsträgers

Der Eingriff in Bremse und Gas erfolgt über eine bereits serienmäßig vorhandene, zentrale Steuerungskomponente, an die über einen Fahrzeugbus Beschleunigungs- und Verzögerungsanforderungen gestellt werden können. Die Steuerungskomponente koordiniert daraufhin die Weiterleitung dieser Anforderungen an das Motor- und das ESP-Bremsen-Steuergerät. Um in die Lenkung einzugreifen, ist ein zusätzlicher, elektronisch ansteuerbarer Aktor in den Versuchsträger eingebaut, mit dem die Lenkstange rotiert werden kann.

Die funktionalen Softwaremodule (FSM) der Wahrnehmung, Funktionslogik und Regelung sind, wie bereits in Bild 4.1 vorgeschlagen, jeweils auf einer eigenen Recheneinheit implementiert. Es handelt sich hierbei um zwei handelsübliche Dual Core-PCs mit einer Taktfrequenz von 2,6 bzw. 2,2GHz und 2048 MB Arbeitsspeicher (Wahrnehmung und Funktionslogik), sowie einen Echtzeitrechner vom Typ „Autobox“ der Firma dSpace (Regelung). Die Recheneinheiten kommunizieren per Ethernet und CAN miteinander. Bild 9.3 zeigt die beschriebenen Rechner an ihrem Verbauort im Kofferraum des Versuchsträgers. Die Kiste vorne links im Bild ist kein PC, sondern eine Platte mit Anschlüssen für die verschiedenen Fahrzeugbusse.

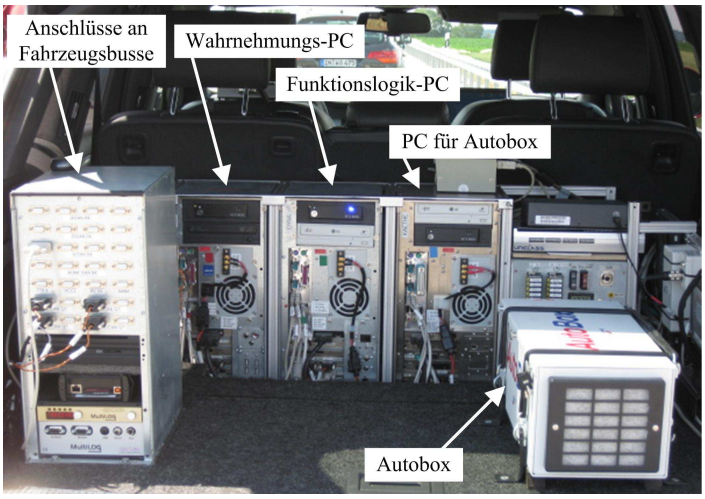

Bild 9.3: Rechner und Anschlüsse an Fahrzeugbusse im Kofferraum des Stauassistent-Versuchsträgers

Als Software-Entwicklungsumgebung wird MS Visual Studio .NET 2005 und das Automotive Data and Time triggered Framework (ADTF) der Firma Elektrobit (vgl. [Elektrobit Automotive GmbH 2010]) in der Version 2.3.1 eingesetzt. ADTF ist ein Programmentwicklungssystem für die PC-basierte FAS-Entwicklung, das den Entwickler bei der raschen Implementierung neuartiger FAS-Funktionen unterstützt, indem es eine Vielzahl an vordefinierten Standardkomponenten bereithält, mit denen es möglich ist, PC-seitig über verschiedene im Automotive-Bereich gängige Schnittstellen zu kommunizieren, sowie beliebige Daten aufzunehmen, wiederzugeben und zu visualisieren. Zudem bietet es eine umfassende Softwarebibliothek, mit der unter C++ schnell eigener Code generiert und in die Entwicklungsumgebung eingebunden werden kann.

9.2 Implementierung

Bevor ein Überblick über die prototypische Umsetzung des Sicherheitskonzepts gegeben wird, soll zunächst, im Rahmen einer Blackbox-Betrachtung, auf die Datenstrukturen an den Schnittstellen zwischen Wahrnehmung, Funktionslogik und Regelung eingegangen und zudem das implementierte Bedienkonzept zur Aktivierung und Deaktivierung des autonomen STA vorgestellt werden. Aufbauend auf dieser Abstraktion der Normalfunktion wird dann die Realisierung des Sicherheitskonzepts beschrieben.

Seitens der Wahrnehmung werden Eigenbewegungs- und alle in Kapitel 4.1 beschriebenen Umfeldmodelldaten in Form mehrerer kompakter Datenstrukturen zur Verfügung gestellt. Eine Klassifikation der dynamischen Objekte in Fahrzeuge und Menschen erfolgt allerdings nicht. Zudem sind die Umfeldinformationen selbstverständlich nur in dem durch den Erfassungsbereich der Sensoren (vgl. Kapitel 9.1) vorgegebenen Bereich verfügbar. Die FSM der Funktionslogik generieren aufbauend auf den Daten der Wahrnehmung Sollwerte für die nachfolgende Längs- und Querregelung, die sie in zwei definierten Datenstrukturen zur Verfügung stellen. Zur Längsregelung werden als Sollwert der gewünschte Abstand zu einem virtuellen Zielfahrzeug und als Ist-Werte der entsprechende momentane Abstand, sowie die aktuelle Relativ-Geschwindigkeit und Beschleunigung des Zielfahrzeugs übergeben. Hinsichtlich der Querregelung werden eine Krümmung und eine Krümmungsänderung

definiert, welche den Verlauf einer virtuellen Klothoide beschreiben, die abgefahren werden soll, und welche Querregler-seitig in die Vorsteuerung eingehen. Da die Klothoide nicht ortsbehaftet ist, werden zusätzlich noch der Winkel und die Ablage des Fahrzeugs bezüglich dieser Kurve übergeben. Die Quer-Regelung hat zur Aufgabe, diese beiden Ist-Größen auf Null auszuregeln. Die Regelung selbst liefert zur Ansteuerung des Arbiters einen Beschleunigungs- bzw. Verzögerungswert, sowie einen Radlenkwinkel (vgl. Bild 4.3).

Bild 9.4: Bedienkonzept zur Systemaktivierung

Bild 9.4 zeigt das prototypisch umgesetzte Bedienkonzept zur Aktivierung des autonomen STA in einer realen Verkehrssituation. Wie man sieht, kann das System aus der manuellen Fahrt kommend bei Erkennung eines Autobahnstaus, durch die Betätigung einer Bedientaste am Lenkrad aktiviert werden. Die Normalfunktion hält das Fahrzeug daraufhin automatisch innerhalb der momentanen Fahrspur und folgt dem Vorderfahrzeug in sicherem Abstand. Der aktuelle Systemzustand „STA aktivierbar“ bzw. „STA aktiv“ wird über eine Anzeige im Kombidisplay visualisiert. Dem Fahrer ist es bei aktiviertem System jederzeit möglich, die Fahrzeugführung durch einen Eingriff in Lenkung, Gas oder Bremse wieder komplett zu übernehmen.

Nachdem nun die grundsätzliche Funktionsweise der prototypisch realisierten Normalfunktion des STA dargelegt wurde, wird im Folgenden die konkrete Umsetzung des Sicherheitskonzepts beschrieben. Im Versuchsträger sind alle wesentlichen funktionalen Komponenten zur Systemgrenzenüberwachung des autonomen STA implementiert (vgl. dunkelgrau dargestellte Komponenten in Bild 4.2)[39]. Auf die Umsetzung der in Kapitel 4.3 beschriebenen, notwendigen redundanten Überwachungseinheiten sowie aller weiterer Redundanzen wird verzichtet, da hierdurch kein zusätzlicher Erkenntnisgewinn erwartet wurde. Ingesamt sind auf dem Wahrnehmungs- und dem Funktionslogik-PC zwei lokale Modul-Überwacher (LMÜ) instanziiert, durch die das in Kapitel 5.1 erläuterte Überwachungskonzept zur Erkennung von Fehlern in Einzelkomponenten erfolgreich in einem verteilten System getestet werden konnte. Als Anwendungsbeispiel dient, wie bereits in Kapitel 8 angedeutet wurde (vgl. Bild 8.2), ein Erblinden der Kamera, das durch die Positionierung eines Blattes Papier vor der Kameralinse hervorgerufen werden kann. Der

[39] Die Implementierung der im Folgenden aufgezählten Komponenten erfolgte mit Hilfe der Unterstützung von Semestranden und Diplomanden: Funktionsgrenzen-Überwacher (vgl. [Gunsell et al. 2008]), Plausibilitäts-Überwacher (vgl. [Prosser et al. 2009]), Überwacher externer Einflussgrößen und globaler Überwacher (vgl. [Kohlhuber et al. 2009]) sowie Aktionsplan-Umsetzer (vgl. [Kohlhuber et al. 2009] und [Prosser et al. 2009]).

Zustand „Kamera blind“ wird im Rahmen der Eigendiagnose des Fahrstreifendetektors auf dem Wahrnehmungs-PC erkannt und als „temporärer Fehler“ an den dort befindlichen LMÜ gemeldet, der diese Informationen an den auf dem Funktionslogik-PC implementierten globalen Überwacher (GLÜ) weiterleitet. Der GLÜ propagiert den Fehler daraufhin über die Rechnergrenze zwischen Wahrnehmung und Funktionslogik bis zur Eingangsschnittstelle des Verhaltensentscheidungsmoduls, an welcher der Aktionsplan „Bremsung auf Ziel“ hinterlegt ist (vgl. Tabelle 8.1). Der Aktionsplan wird dann beim Aktionsplan-Umsetzer (APU) angefordert. Genau wie der APU sind auch ein Überwacher externer Einflussgrößen, ein Funktionsgrenzen-Überwacher und ein Plausibilitätsüberwacher auf dem Funktionslogik-PC instanziiert. Ersterer liest verschiedene Botschaften des CAN-Bus aus und überprüft dadurch unter anderem, ob die Fahrertüre des Fahrzeugs geöffnet wurde. Mittels des Funktionsgrenzen-Überwachers können eine Stauauflösung, ein Autobahnende und ein Spurende, also vollständig alle für einen STA relevanten Systemgrenzenüberschreitungen überwacht werden. Dies gilt, mit Ausnahme der Existenz von „Menschen in der Fahrspur“[40] auch für die Überwachung sämtlicher situativer Unplausibilitäten im Plausibilitätsüberwacher (vgl. Bild 7.5), nachdem der im Rahmen der Forschungsinitiative AKTIV generierte Quellcode der Ausweichanalyse (AWA) durch die entsprechenden Entwickler freundlicherweise zur Verfügung gestellt wurde. Alle genannten Überwachungsmodule melden erkannte Systemgrenzenüberschreitungen, wie in Bild 4.2 dargestellt, an den GLÜ, der daraufhin auf Basis zuvor erhaltener Anmeldedaten den APU ansteuert. Die Parametrierung der Aktionspläne erfolgt, je nachdem welche Systemgrenze überschritten wurde, gemäß der in Kapitel 8.3 und 8.5 bereits beschrieben Art und Weise. Der APU greift schließlich über den auf dem Regelungs-Echtzeitrechner befindlichen Arbiter durch Vorgabe eines Verzögerungswerts und optional auch eines Radlenkwinkels in die Fahrzeugführung ein.

Es wurde bereits im vorangegangenen Kapitel in Bild 8.2 dargelegt, welche Aktionen der Ausfall des Fahrstreifendetektors innerhalb der Komponenten des Sicherheitskonzepts anstößt. Wie im vorigen Abschnitt beschrieben, wurde der Fehlerbehandlungsmechanismus für diesen Fall in Form der abgebildeten funktionalen Softwaremodule prototypisch implementiert und hat sich dabei als zielführend erwiesen. Der Vollständigkeit halber ist im folgenden Bild 9.5 am Beispiel der situativen Unplausibilität „Ego-Fahrzeug verlässt eigene Fahrspur“ in identischer Form dargestellt, wie im Versuchsträger die Ansteuerung eines überlagerten Lenkeingriffs erfolgt.

[40] Eine explizite Erkennung von Menschen ist, wie bereits zu Beginn von Kapitel 9.2 erwähnt, im Rahmen der FSM der Wahrnehmung nicht implementiert.

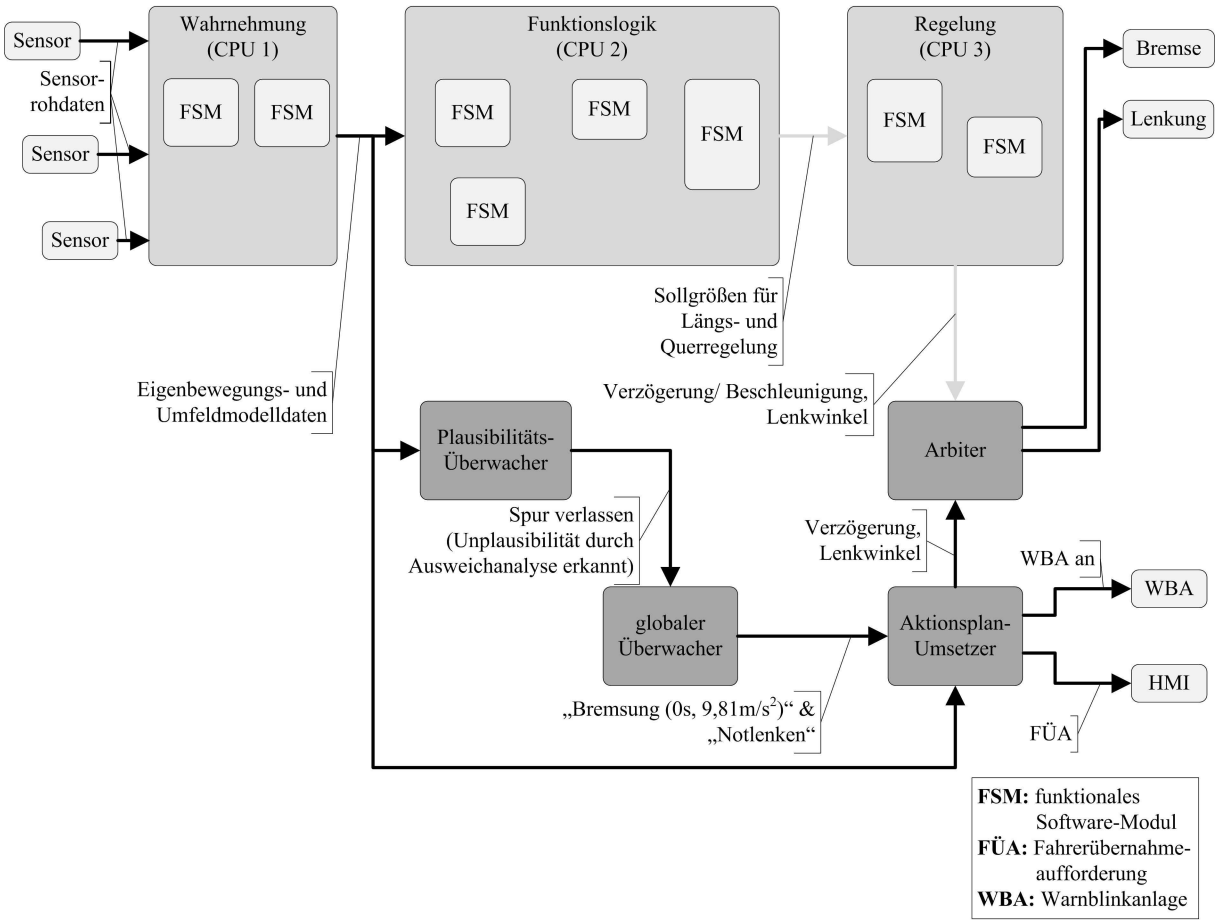

Bild 9.5: Aktionsplan-Ansteuerung bei einer situativen Unplausibilität (Beispiel aus Versuchsträger: Verlassen der Fahrspur)

Da die drei Aktionspläne „Bremsung“, „Bremsung auf Ziel“ und „Notlenken“ den funktional erlebbaren Teil des Sicherheitskonzepts ausmachen, soll nun ihr Wirken in drei beispielhaften, realen Versuchsszenarien beschrieben und somit deren vollständige prototypische Umsetzung nachgewiesen werden.

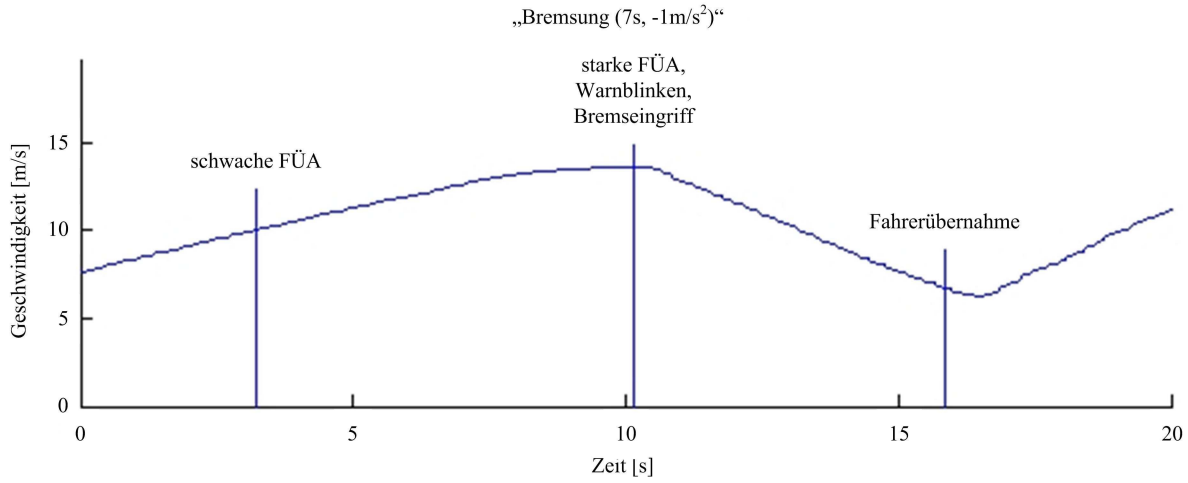

Bild 9.6: Zeit-Geschwindigkeits-Diagramm bei einer Stauauflösung im Realverkehr

Bild 9.6 zeigt ein Zeit-Geschwindigkeits-Diagramm des zunächst autonom fahrenden STA-Versuchsträgers bei einer Stauauflösung im Realverkehr. Wie man sieht, wird in diesem Fall,

wie in Kapitel 8.5 beschrieben, der Aktionsplan „Bremsung (7s, -1m/s^2)“ ausgeführt, welcher zunächst eine schwache Fahrerübernahmeaufforderung (FÜA) in Form eines einmaligen Gongs, sowie eines visuellen Warnhinweises im Kombidisplay vorsieht (vgl. Fußnote 32 auf Seite 101). Da die Fahrerübernahme zunächst ausbleibt, erfolgt nach 7s zeitgleich ein Bremseingriff, die Aktivierung der Warnblinkanlage, sowie eine Verstärkung der FÜA. Letztere äußerst sich in einem Blinken des Warnhinweises im Kombidisplay und einem wiederholten Gongen. Der Fahrer übernimmt nach etwa weiteren 5s die Fahrzeugführung, indem er zunächst an das Lenkrad greift und danach das Gaspedal betätigt. Bild 9.7 zeigt den in Bild 9.6 dargestellten Verlauf aus Sicht des Fahrers, beginnend mit dem Zustand kurz nach dem Start des Bremseingriffs. Im mittleren Bild ist links unten zu sehen, wie sich die Hand des Fahrers Richtung Lenkrad bewegt. Auf dem rechten Bild hat der Fahrer die Fahrzeugführung vollständig übernommen und ist in die manuelle Fahrt übergegangen. Nachdem sich der Versuchsträger nicht mehr im Stau befindet, ist die Anzeige im Kombi-Display nun auf „STA nicht aktivierbar“ geschaltet.

Bild 9.7: Fahrerübernahme bei einer Stauauflösung

Neben einer Stauauflösung kann das Verhalten des Versuchsträgers auch bei Erreichen eines Autobahnendes im Realverkehr getestet werden. Wie in Kapitel 8.5 beschrieben, wird in diesem Fall eine „Bremsung auf Ziel (7s, -2m/s^2, 150m)“ ausgeführt. Bild 9.8 zeigt das aufgezeichnete Weg-Geschwindigkeits-Diagramm einer entsprechenden Testfahrt. Wie man sieht, ist der Aktionsplan bereits lange Zeit aktiv, bevor die schwache FÜA erfolgt. Die Fahrerübernahme geschieht in diesem Beispiel, anders als im obigen Fall der Stauauflösung, erst nachdem das STA-Fahrzeug bereits den Stillstand erreicht hat. Die Reihenfolge der ausgeführten Aktionen ist aber identisch.

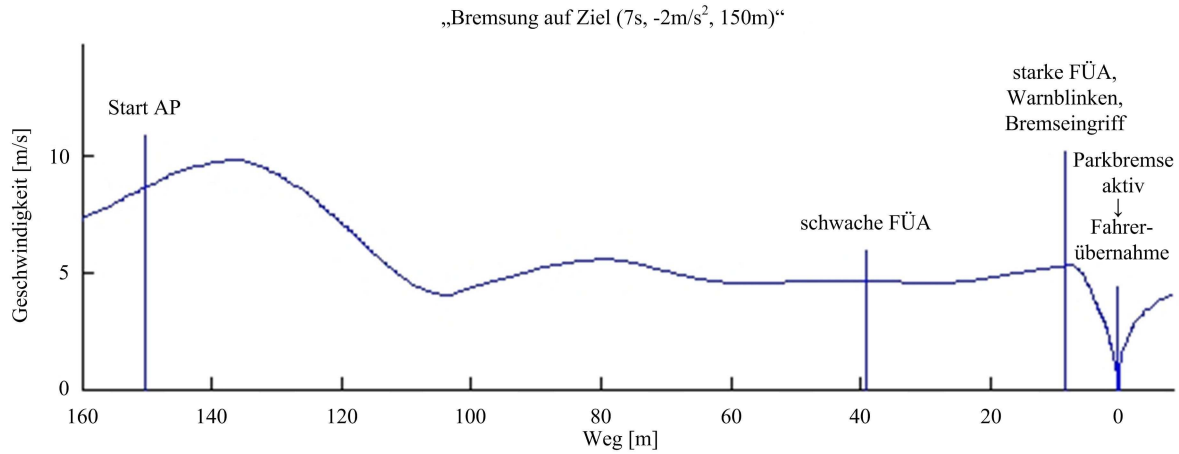

Bild 9.8: Weg-Geschwindigkeits-Diagramm bei einem Autobahnende im Realverkehr

Abschließend seien noch aufgezeichnete Daten aus einer Versuchsfahrt dargestellt, bei der das STA-Fahrzeug die eigene Fahrspur infolge einer künstlich provozierten situativen Unplausibilität verlässt (vgl. Bild 9.9) und daher, anders als in den beiden zuvor aufgeführten Fällen, auch die Querführung durch den APU erfolgt. Da, wie in Kapitel 8.3 beschrieben, das Auftreten situativer Unplausibilitäten sehr sicherheitskritisch ist und immer eine radikale Reaktion, in Form einer sofortigen Vollbremsung („Bremsung (0s, 9,81m/s^2)“), sowie eines „Notlenkens“ zur Folge hat, entstammen die abgebildeten Diagramme einer Testfahrt auf einer unbefahrenen Teststrecke. Wie man aus dem Zeit-Geschwindigkeits-Diagramm erkennt, erfolgt direkt mit dem Beginn der Ausführung des Aktionsplans „Bremsung“ eine starke FÜA[41], die Aktivierung der Warnblinkanlage und ein Eingriff in die Längsführung. Der zeitliche Versatz zwischen angefordertem Bremseingriff und der real einsetzenden Geschwindigkeitsverringerung ist der Tot- und Schwellzeit der Bremse geschuldet, welche in Summe eine Größenordnung von etwa 0,7s haben. Ausgelöst wird das Verlassen der Fahrspur durch eine extra hierfür entwickelte Bedienschnittstelle, die den Querregler dazu manipuliert, konstant einen Radlenkwinkel von 0° zu stellen. Auf gerader Straße führt dies dazu, dass das Fahrzeug langsam von der Fahrspur driftet. Betrachtet man das Zeit-Radlenkwinkel-Diagramm, erkennt man, dass der Lenkwinkel zunächst bei konstant 0° liegt und ab dem Zeitpunkt der zeitgleichen Auslösung des longitudinalen und des lateralen Aktionsplans rasch in den negativen Bereich absinkt, was einem Gieren des Fahrzeugs nach rechts entspricht. Dieses Verhalten ist sinnvoll, nachdem das Fahrzeug in diesem Fall die linke Fahrstreifenmarkierung übertreten hat (vgl. Bild 9.10). Nachdem sich das Fahrzeug wieder in Richtung Spurmitte bewegt hat, wird auch der Lenkwinkel wieder zurückgenommen und bleibt nach Erreichen des Stillstands konstant, bis der Fahrer die Fahrzeugführung durch Betätigung des Lenkrads wieder übernimmt. Kurze Zeit später erfolgt dann auch die Betätigung des Gaspedals und eine daraus resultierende Geschwindigkeitserhöhung.

[41] In dem aufgeführten Beispiel erfolgte trotz einer einsetzenden Vollbremsung zusätzlich eine starke FÜA. Ob dieses Verhalten an dieser Stelle sinnvoll ist, muss allerdings, wie bereits in Kapitel 8.2 erwähnt, in Probandenstudien geklärt werden.

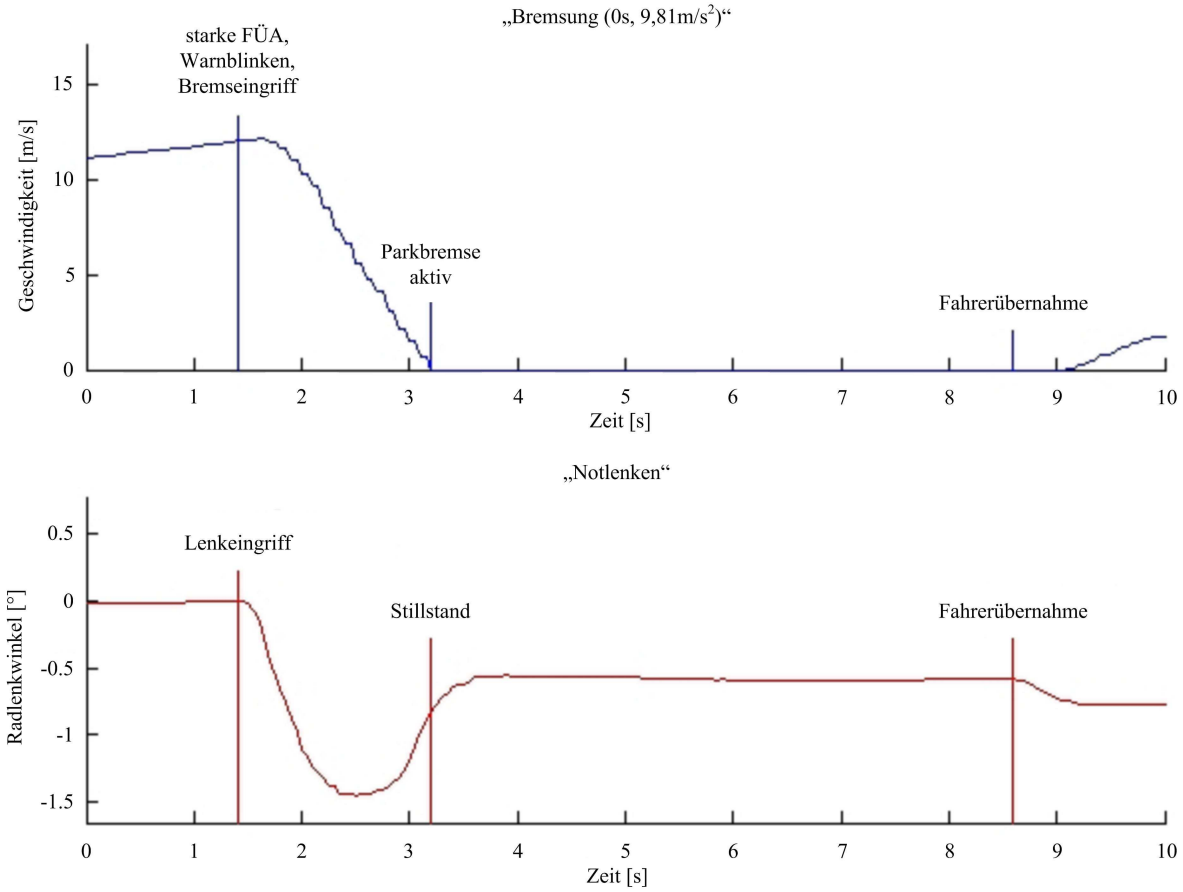

Bild 9.9: Zeit-Geschwindigkeits-Diagramm (oben) und Zeit-Radlenkwinkel-Diagramm (unten) beim Verlassen der Fahrspur auf einer Teststrecke

Bild 9.10 zeigt das Verhalten des Versuchsträgers bei der in Bild 9.9 beschriebenen Testfahrt aus Sicht des Fahrers. Die linke Seite zeigt den Zustand unmittelbar vor Lenk- und Bremseingriff. Man erkennt, dass das Lenkrad nicht ausgelenkt ist und das Fahrzeug kurz davor ist, die linke Fahrstreifenmarkierung zu überfahren. Auf dem rechten Bild ist der Lenkeingriff bereits erfolgt, was an der Lenkradstellung deutlich zu sehen ist. Außerdem kann man erkennen, dass sich der Oberkörper des Fahrers infolge der momentan starken Verzögerung nach vorne bewegt hat.

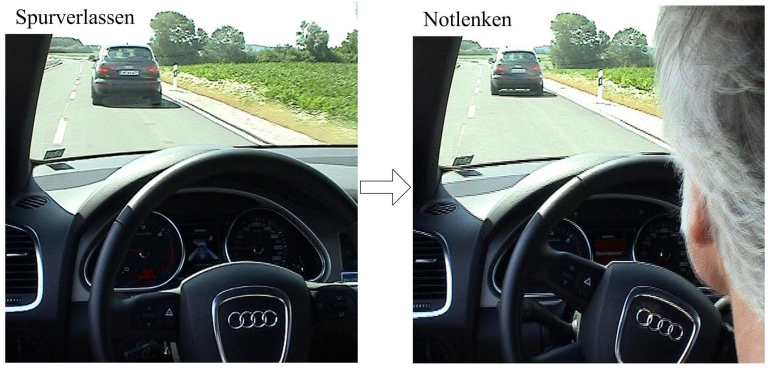

Bild 9.10: Notlenken beim Verlassen der Fahrspur

10 Zusammenfassung und Ausblick

Da die vollständige Automatisierung der Fahrzeugführung durch ein Fahrerassistenzsystem (FAS) zu Nebenbeschäftigungen und Unaufmerksamkeit verleitet, ist der durchschnittliche Fahrer nicht in der Lage, die Fahraufgabe im Falle einer Systemgrenzenüberschreitung des FAS wieder rechtzeitig zu übernehmen. Ohne entsprechende Maßnahmen bewegt sich das Fahrzeug in derartigen Situationen deshalb unkontrolliert fort und kann im schlimmsten Fall Kollisionen verursachen. Die vorliegende Arbeit stellt in Anlehnung an die Norm [ISO DIS 26262: 2009], ein funktionales Sicherheitskonzept zur Lösung dieses Problems vor. Das Sicherheitskonzept zeigt auf, wie die Systemgrenzen zukünftiger FAS zur vollautomatischen Fahrzeugführung überwacht werden können und das Fahrzeug durch Fail-Safe-Mechanismen (FS) in einen sicheren Zustand überführt werden kann. Es wird damit ein wichtiger Beitrag geleistet, die Einführung von Fahrfunktionen zur vollständig automatisierten Fahrzeugführung in zukünftigen Serienfahrzeugen voranzutreiben. Die Beschreibung funktionsspezifischer Aspekte des Sicherheitskonzepts erfolgt am Beispiel des Systems Stauassistent (STA), das ein vollautomatisches Fahren im Autobahnstau ermöglicht. Im Rahmen einer umfangreichen exemplarischen Implementierung der wichtigsten Komponenten des Sicherheitskonzepts, konnten dessen Tauglichkeit in einem realen Versuchträger erfolgreich nachgewiesen werden.

Die angesprochenen Mechanismen zur Systemgrenzenüberwachung umfassen unter anderem ein Watchdog-Konzept zur Erfassung systeminterner Fehler sowie Konzepte zur Überwachung externer Einflüsse und funktionsspezifischer funktionaler Grenzen. Den im Hinblick auf die Systembeobachtung und Systemkontrolle zentralen Aspekt der Arbeit stellt jedoch die überschlagsmäßige Überprüfung des funktionalen Gesamtverhaltens des Fahrzeugs durch eine den zuvor genannten Überwachungsmechanismen unterlagerte Kontrollinstanz dar. Ihre Aufgabe ist es, sogenannte situative Unplausibilitäten festzustellen. Hierbei handelt es sich um kritische Fahrsituationen, die objektiv betrachtet gar nicht hätten zustande kommen dürfen, die aber dennoch, entweder durch nicht erkannte systeminterne Fehler oder durch eine dramatische Eskalation der Verkehrssituation, eingetreten sind. Da diese letzte Kontrollinstanz entweder der Mensch oder aber das FAS selbst darstellen kann, es dem Fahrer in Konsequenz also entweder verboten oder aber gestattet sein kann, sich stärker als bei manueller Fahrt abzulenken, ist eine Unterteilung der FAS zur vollautomatischen Fahrzeugführung in sogenannte vollautomatische und autonome FAS notwendig. Für vollautomatische FAS (VA FAS) wird entsprechend ein kombiniertes Fahrerüberwachungs- und Interaktionskonzept vorgeschlagen mit dem es möglich ist, den Fahrer aktiv im Loop zu halten und ihn somit als letzte Kontrollinstanz bestehen zu lassen. Für autonome FAS wird dagegen exemplarisch am Beispiel des Systems STA aufgezeigt, wie das funktionale Gesamtverhalten des Fahrzeugs maschinell plausibilisiert werden kann.

Das FS-Verhalten zukünftiger VA FAS besteht, nachdem der Fahrer aktiv im Loop gehalten wird, notwendigerweise nur aus der Ausgabe einer Fahrerübernahmeaufforderung (FÜA) und unterscheidet sich damit nicht von heutigen semiautomatischen Seriensystemen wie ACC S&G. Entsprechend konzentriert sich die Arbeit hinsichtlich FS-Mechanismen auf autonome

FAS (A FAS) und stellt am Beispiel des Systems STA ein aktives FS-Konzept vor, mit dem es auch ohne Zutun des Fahrers in jedem Fehlerfall möglich ist, durch einen Eingriff in die Fahrzeuglängs- und Querführung wieder einen sicheren Zustand herzustellen.

Der aus Sicht der Systemsicherheit entscheidende Entwicklungsschritt für einen baldigen Serieneinsatz VA FAS ist die Konzeption eines Mechanismus, mit dem der Fahrer nachweislich im Loop gehalten werden kann. Das vorgeschlagene kombinierte Fahrerüberwachungs- und Interaktionskonzept stellt diesbezüglich einen vielversprechenden Ansatz dar. Um die Tauglichkeit des lediglich theoretisch erarbeiteten Konzepts zu bewerten, sind in der Zukunft eine entsprechende prototypische Umsetzung sowie die Durchführung einer Probandenstudie zur Bestimmung sinnvoller Werte für die freien systeminternen Parameter notwendig. Dies ist Aufgabe eines aktuell bei der Audi AG angelaufenen Promotionsprojekts.

Im Vergleich zu VA FAS erscheinen A FAS noch wesentlich weiter von einer Serienreife entfernt. Dies liegt im Wesentlichen daran, dass das vorgestellte Sicherheitskonzept umfangreiche Forderungen an die Normalfunktion autonomer FAS stellt, die vor allem im Bereich der sensorischen Wahrnehmung noch einigen Forschungs- und Entwicklungsaufwand notwendig machen. So ist es erforderlich, Mechanismen zur Eigendiagnose von sensorischen Signalverarbeitungs- und Fusionsalgorithmen sowie zur Erkennung invalider Sensorrohdaten zu entwickeln, da systeminterne Wahrnehmungsfehler im Rahmen der oben erwähnten automatischen Plausibilitätsprüfung von einem A FAS nicht selbstständig erkannt werden können. Gleichsam müssen sich die Auswirkungen derartiger Fehler in verlässlichen Gütemaßen bezüglich der die Umwelt beschreibenden Umfelddaten widerspiegeln. Letzteres ist notwendig, da eine weitere Forderung des Sicherheitskonzept darin besteht, dass die Funktionslogik des A FAS beim Empfang teilweise korrupter Umfelddaten in einen Notmodus umschalten muss. Durch diesen Notmodus muss es der Normalfunktion möglich sein, die Querführung, auf Basis der Kenntnis über die Verkehrssituation unmittelbar vor dem Wahrnehmungsfehler, noch für ein kurzes Wegstück definierter Länge sicher aufrechtzuerhalten. Diese Weglänge leitet sich aus der Vorausschau der invaliden Umfelddaten ab. Im Hinblick auf Fahrstreifendetektoren impliziert dies wiederum die Forderung, dass in den generierten Fahrstreifendaten eine verlässliche Angabe darüber gemacht wird, bis in welcher Entfernung der Fahrstreifenverlauf erkannt wurde. Weitere hohe Anforderungen, die speziell die Wahrnehmung dynamischer Objekte betreffen, resultieren aus dem Konzept zur automatischen Plausibilitätsprüfung. Da dieses vorsieht, dass A FAS aus Sicherheitsgründen beim Erscheinen von Fußgängern zu deaktivieren, ist es zum einen notwendig, innerhalb der dynamischen Objekte explizit Menschen zu klassifizieren. Zum anderen muss zur Überwachung definierter Mindestsicherheitsabstände auch eine Objekterkennung und -verfolgung im Seitenbereich des Fahrzeugs möglich sein. Letzteres bedeutet nicht nur einen großen Forschungs-, sondern auch einen hohen Kostenaufwand, da im Vergleich zu dem in dieser Arbeit verwendeten Versuchsträger entsprechende zusätzliche Sensoren notwendig sind. Der finanzielle Aufwand vergrößert sich zusätzlich noch durch die erforderliche redundante Auslegung der Inertial- und Umfeldsensorik, sowie der Bremse und Lenkung.

Nachdem in den vorangegangenen Absätzen dargelegt wurde, welche Anstrengungen im Hinblick auf eine Kommerzialisierung vollautomatischer und autonomer Fahrfunktionen aus Sicht der Systemsicherheit noch unternommen werden müssen, soll nun abschließend noch geklärt werden, inwiefern sich die FS-Mechanismen für einen autonomen STA auf FAS übertragen lassen, die eine autonome Fahrzeugführung bei höheren Geschwindigkeiten realisieren. Nach [Isermann 2010] ist der sichere Notaus-Zustand eines Automobils als „Stillstand an einem sicheren Ort“ definiert. Da bei grundsätzlich allen A FAS, systeminterne Fehler auftreten können, die einen sofortigen Übergang in diesen Zustand erforderlich machen, erscheint als Ort für den Stillstand nur die eigene Fahrspur sinnvoll. Die Erlangung jedes anderen Orts, beispielsweise des Standstreifens, ist mit komplexen Fahrmanövern verbunden, die insbesondere im Falle einer eingeschränkten Systemleistungsfähigkeit nicht realisierbar erscheinen. Entsprechend können die für einen STA vorgeschlagenen longitudinalen und lateralen Aktionspläne, die eine Auslösung von FÜA, Warnblinkanlage (WBA) sowie Brems- bzw. Lenkeingriff vorsehen und in ihrer Intensität und zeitlichen Abfolge an den jeweiligen Fehlerfall anzupassen sind, prinzipiell direkt übernommen werden. Da eine Bremsung in den Stillstand aus höheren Geschwindigkeiten aber die Gefahr hervorruft, dass es infolge einer zu späten Reaktion des rückwärtigen Verkehrs zu Kollisionen kommt, sind neben der Aktivierung der WBA gegebenenfalls zusätzliche Anstrengungen notwendig, um den Ort des Stillstands entsprechend abzusichern. Konkret müssen nachkommende Fahrzeuge im Falle schwerer Systemfehler, die ein starkes Abbremsen notwendig machen, rechtzeitig gewarnt oder, falls dies nicht möglich ist, ebenfalls automatisch abgebremst werden. Hierfür muss das autonome Fahrzeug zum einen mit Funktechnologie zur Kommunikation mit anderen Fahrzeugen ausgestattet werden. Zum anderen ist eine spezielle Infrastruktur notwendig, die dafür sorgt, dass alle anderen Fahrzeuge im Umfeld des autonomen Fahrzeugs ebenfalls über eine derartige Car-2-Car-Verbindung verfügen, mittels der sie gegebenenfalls gewarnt bzw. abgebremst werden können (vgl. [CAR 2 CAR Communication Consortium 2007]).

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[Aizawa et al. 2004] AIZAWA, H., SAKANE, S., IMOTO, Y., KISHIMOTO; M.: *Automatische Bremssteuervorrichtung zum Generieren von Bremskraft in Abhängigkeit vom Aufmerksamkeitsniveau des Fahrers*. Offenlegungsschrift des deutschen Patent- und Markenamts, DE 103 27 597 A1, 2003.

[Altmüller 2007] ALTMÜLLER, T: *Driver Monitoring and Drowsiness Detection by Steering Signal Analysis*. Dissertation an der Universität der Bundeswehr München, Neubiberg, 2007.

[Anders 2008] ANDERS, E.: *Ein Beitrag zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems*. Dissertation an der TU Dresden, Dresden, 2008.

[Bähnisch 2007] BÄHNISCH, S.: *Kampf der Müdigkeit*. AutoBild.de, 13.12.2007, http://www.autobild.de/artikel/mercedes-quot-attention-assist-quot-_509888.html, Stand 2.8.2010.

[Bainbridge 1983] BAINBRIDGE, L.: *Ironies of Automation*. Automatica, 19 (6), 1983.

[Basarke et al. 2007] BASARKE, C., BERGER, C., CORNELSEN, K., DOERING, M., EFFERTZ, J., HOMEIER, K., LIPSKI, C., NOTHDURFT, T., WILLE, J.: *Team CarOLO*. Technical paper as part of the qualification process for the 2007 DARPA Urban Challenge, 2007.

[Bekiaris 1999] BEKIARIS, E.: *System for effective Assessment of the driver state and Vehicle control in Emergency situations (SAVE)*. Telematics Applications Programme (Transport) Final Report TR 1047, 1999.

[Bekiaris & Peters 1999] BEKIARIS, E., PETERS, B.: *Automatic vehicle control in emergency situations*. ATA Motor Car Engineering Journal, 52 (3), 1999.

[Berger & Rumpe 2008] BERGER, C., RUMPE, B.: *Autonomes Fahren - Erkenntnisse aus der DARPA Urban Challenge*. Information Technology, 4/2008, Oldenbourg Wissenschaftsverlag, München, 2008.

[Blischke & Murthy 2000] BLISCHKE, W., MURTHY, D.: *Reliability – Modeling, Prediction, and Optimization*. John Wiley & Sons, New York, USA, 2000.

[BMW AG 2010] BMW AG: *Active Cruise Control with Stop & Go function*. BMW Technology Guide, http://www.bmw.com/com/en/insights/technology/technology_guide/articles/active_cruise_control_stop_go.html, Stand 2.8.2010.

[Bode & Hellwagner 2006] BODE, A., HELLWAGNER, H.: *Leistungsbewertung und Fehlertoleranz*. Informatik Handbuch, Carl Hanser Verlag, 4. Auflage, München, 2006.

[Boecker & Hoetzer 2005] BOECKER, J., HOETZER, D.: *Abstands- und Geschwindigkeitsregler mit Stauerkennung*. Offenlegungsschrift des deutschen Patent- und Markenamts, DE 10 2005 050 277 A1, 2005.

[Breu & Maurer 2007] BREU, A., MAURER, M.: *Prozess zur Komplexitätsbeherrschung bei der Entwicklung eines Stillstandsmanagements für ein hochvernetztes Fahrerassistenzsystem*. Tagung Stillstandsmanagement, Haus der Technik, Essen, 2007.

[Brinkschulte & Ungerer 2007] BRINKSCHULTE, U., UNGERER, T.: *Mikrocontroller und Mikroprozessoren*. Springer, 2. Auflage, Berlin, 2007.

[Brookhuis et al. 1998] BROOKHUIS, K., DE WAARD, D., PETERS, B., BEKIARIS, E.: *SAVE - System for detection of driver impairment and emergency handling*. Journal of International Association of Traffic and Safety Sciences (IATSS RESEARCH), 22 (2), 1998.

[Buld & Krüger 2004] BULD, S., KRÜGER, H.: *Die Auswirkung von Teilautomation auf das Fahrverhalten*. DLRG-Bericht „Entscheidungsunterstützung für die Fahrzeug- und Prozessführung“, Bonn, 2004.

[Brunner & Zeltner 1980] BRUNNER, R., ZELTNER, W.: *Lexikon zur pädagogischen Psychologie und Schulpädagogik*. Ernst Reinhard Verlag, München, 1980.

[CAR 2 CAR Communication Consortium 2007] CAR 2 CAR COMMUNICATION CONSORTIUM: *Overview of the C2C-CC System*. C2C-CC Manifesto, Version 1.1, 2007.

[Daimler AG 2008] DAIMLER AG: *Bitte nicht einschlafen*. Daimler HighTechReport: Faszination Technologie, 2/2008, 2008.

[Deppe 2010] DEPPE, P.: *Mercedes-Benz gewinnt mit dem Müdigkeitswarner ATTENTION ASSIST britischen Sicherheitspreis*. Mercedes-Benz passion Blog, 28.1.2010, http://blog.mercedes-benz-passion.com/2010/01/mercedes-benz-gewinnt-mit-dem- dem-mudigkeitswarner-attention-assist-britischen-sicherheitspreis/, Stand 2.8.2010.

[DIN EN 50129: 2003] DEUTSCHES INSTITUT FÜR NORMUNG (DIN): *Bahnanwendungen. Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme. Sicherheitsrelevante elektronische Systeme für Signaltechnik*. DIN EN 50129, 2003.

[DIN VDE 0119-207-5: 2004] DEUTSCHES INSTITUT FÜR NORMUNG (DIN), VERBAND DER ELEKTROTECHNIK ELEKTRONIK INFORMATIONSTECHNIK (VDE): *Zustand der Eisenbahnfahrzeuge – Leittechnik – Teil 207-5: Sicherheitsfahrschaltung (Sifa)*. DIN VDE 0119-207-5, 2004.

[Dong et al. 2009] DONG, Y., HU, Z., UCHIMURA, K., MURAYAMA, N.: *Driver Inattention Monitoring System for Intelligent Vehicles : A Review*. IEEE Intelligent Vehicles Symposium, Xi’an, China, 2009.

[Doth 1989] DOTH, T.: *Failsafe brake for a multi-wheel vehicle with motor controlled steering*. United States Patent US 004 887 013 A, 1989.

[ECE R 79 2006] ECONOMIC COMMISSION FOR EUROPE: *R 79: Einheitliche Bedingungen für die Genehmigung der Fahrzeuge hinsichtlich der Lenkanlage*. Revision 2, 2006.

[Elektrobit Automotive GmbH 2010] ELEKTROBIT AUTOMOTIVE GMBH: *EB Assist ADTF - Fahrerassistenz*. http://www.elektrobit.com/was_wir_ihnen_bieten/automotive_software/produkte/eb_assist_adtf_-_fahrerassistenz, Stand 2.8.2010.

[Endsley 1988] ENDSLEY, M.: *Situation awareness global assessment technique (SAGAT)*. Proceedings of the IEEE National Aerospace and Electronics Conference (NAECON), New York, USA, 1988.

[Endsley & Kiris 1995] ENDSLEY, M., KIRIS, E.: *The out-of-the-loop performance problem and level of control in automation*. Human Factors, 37 (2), 1995.

[Esch & Kern 2007] ESCH, S., KERN, D.: *Stillstandsmanagement – Herausforderungen bei BMW*. Tagung Stillstandsmanagement, Haus der Technik, Essen, 2007.

[Fenner et al. 2003] FENNER, W., NAUMANN, P., TRINCKAUF, J.: *Bahnsicherungstechnik*. Publicis Corporate Publishing, 2. Auflage, Erlangen, 2010.

[Ferguson 2003] FERGUSON, J.: *Semi-submersible AUVs*. Technology and Applications of Autonomous Underwater Vehicles, Taylor & Francis, London, 2003.

[Flemisch 2003] FLEMISCH, F.: *The H-Metaphor as a Guideline for Vehicle Automation and Interaction*. Technical Report NASA/TM2003-212672, 2003.

[Flemisch & Dittrich 2008] FLEMISCH, F., DITTRICH, J.: *Reiter der Lüfte – Fahren und Fliegen mit gleichem Bedienkonzept*. DLR Nachrichten 119, 2008.

[Gayko 2009] GAYKO, J.: *Lane Keeping Support*. Handbuch Fahrerassistenzsysteme, Vieweg + Teubner, Wiesbaden, 2009.

[Geyer & Prostrednik 2006] GEYER, H., PROSTREDNIK, D.: *Sicherheit von Schienenfahrzeugen aus technischer Perspektive*. Elektrotechnik & Informationstechnik, 123 (9), 2006.

[Glasstone & Sesonske 1994] GLASSTONE, S., SESONSKE, A.: *Nuclear Reaktor Engineering*. Chapman & Hall, New York, USA, 1994.

[Gudat et al. 1999] GUDAT, A., HUN SHIN, D., WHITTAKER, W., KLEIMENHAGEN, K., CLOW, R., SINGH, S., CHRISTENSEN, D., KEMNER, C., BRADBURY, W., KOEHRSEN, C., KYRTSOS, C., LAY, N., PETERSON, J., SCHMIDT, L., STAFFORD, D., WEINBECK, L., DEVIER, L.: *Apparatus And Method For Autonomous Vehicle Navigation Using Absolute Data*. United States Patent US 005 956 250 A, 1999.

[Gunsell et al. 2008] GUNSELL, H., HÖRWICK, M., HEIßING, B., STENSSON TRIGELL, A.: *Analysis and Perception of Situational Function Boundaries for Advanced Driver Assistance Systems*. Masterarbeit am Lehrstuhl für Fahrzeugtechnik der TU München, Garching, 2008.

[Hakuli et al. 2009] HAKULI, S., BRUDER, R., FLEMISCH, F., LÖPER, C., RAUSCH, H., SCHREIBER, M., WINNER, H.: *Kooperative Automation*. Handbuch Fahrerassistenzsysteme, Vieweg + Teubner, Wiesbaden, 2009.

[Halang & Konakovsky 1999] HALANG, W., KONAKOVSKY, R.: *Sicherheitsgerichtete Echtzeitsysteme*. Oldenbourg Industrieverlag, München, 1999.

[Hofmann 2004] HOFMANN, U.: *Zur visuellen Umfeldwahrnehmung autonomer Fahrzeuge*. Dissertation an der Universität der Bundeswehr München, Neubiberg, 2004.

[Honda AG 2010] HONDA AG: *LKAS (Lane Keeping Assist System)*. http://www.honda.de/content/service/car/48526.php, Stand 2.8.2010.

[Hörwick et al. 2009] HÖRWICK, M., SIEDERSBERGER, K.-H., SCHICKRAM, S.: *Verfahren zur Steuerung des Betriebs eines vollautomatischen, zur unabhängigen Fahrzeugführung ausgebildeten Fahrerassistenzsystems eines Kraftfahrzeugs und Kraftfahrzeug*. Patenteinreichung am deutschen Patent- und Markenamt, DE 10 2009 050 404, 2009.

[Hörwick et al. 2010a] HÖRWICK, M., PROSSER, T., SIEDERSBERGER, K.-H.: *Verfahren zur Steuerung des Betriebs eines vollautomatischen, zur unabhängigen Fahrzeugführung ausgebildeten Fahrerassistenzsystems eines Kraftfahrzeugs und Kraftfahrzeug*. Patenteinreichung am deutschen Patent- und Markenamt, DE 10 2010 021 591, 2010.

[Hörwick et al. 2010b] HÖRWICK, M., WIMMER, M., SIEDERSBERGER, K.-H., OSTGATHE, N.: *Verfahren zur Steuerung des Betriebs eines vollautomatischen, zur unabhängigen Fahrzeugführung ausgebildeten Fahrerassistenzsystems eines Kraftfahrzeugs und Kraftfahrzeug*. Patenteinreichung am deutschen Patent- und Markenamt, DE 10 2010 022 433, 2010.

[Hörwick & Herbort 2009] HÖRWICK, M., HERBORT, S.: *Verfahren zum Betrieb eines Stauassistenzsystems*. Patenteinreichung am deutschen Patent- und Markenamt, DE 10 2009 052 773, 2009.

[Hörwick & Siedersberger 2009] HÖRWICK, M., SIEDERSBERGER, K.-H.: *Verfahren zur Steuerung des Betriebs eines vollautomatischen, zur unabhängigen Fahrzeugführung ausgebildeten Fahrerassistenzsystems eines Kraftfahrzeugs und Kraftfahrzeug*. Patenteinreichung am deutschen Patent- und Markenamt, DE 10 2009 050 399, 2009.

[Hörwick & Siedersberger 2010a] HÖRWICK, M., SIEDERSBERGER, K.-H.: *Aktionspläne zur Erlangung eines sicheren Zustandes bei einem autonomen Stauassistenten*. Aktive Sicherheit durch Fahrerassistenz, München, 2010.

[Hörwick & Siedersberger 2010b] HÖRWICK, M., SIEDERSBERGER, K.-H.: *Strategy and Architecture of a Safety Concept for Fully Automatic and Autonomous Driving Assistance Systems*. IEEE Intelligent Vehicles Symposium, San Diego, USA, 2010.

[Hörwick & Wimmer 2010] HÖRWICK, M., WIMMER, M.: *Kombiniertes Fahrerüberwachungs- und Interaktionskonzept für vollautomatische Fahrerassistenzsysteme*. Fachtagung Fahrermodellierung, Berlin, 2010.

[Howland 2010] HOWLAND, H.: *Mercedes führt drei neue Fahrer-Assistenzsysteme ein*. portel.de, 20.7.2010, http://www.portel.de/nachricht/artikel/45083-mercedes-fuehrt-drei-neue-fahrer-assistenzsysteme-ein/12/, Stand 2.8.2010.

[Hutter 2007] HUTTER, D.: *S-Bahn verliert Waggons - Zug teilt sich bei voller Fahrt*. sueddeutsche.de, 17.7.2007, http://www.sueddeutsche.de/muenchen/s-bahn-verliert-waggons-zug-teilt-sich-bei-voller-fahrt-1.754926, Stand 2.8.2010.

[ISO 15622: 2010] INTERNATIONAL ORGANISATION FOR STANDARDIZATION (ISO): *Transport information and control systems - Adaptive Cruise Control systems - Performance requirements and test procedures*. ISO 15622, 2010.

[ISO DIS 26262: 2009] INTERNATIONAL ORGANISATION FOR STANDARDIZATION (ISO): *Road Vehicles – Functional Safety*. ISO DIS 26262, 2009.

[Isermann 2010] ISERMANN, R.: *Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance*. Springer, 2. Auflage, London, 2010.

[Jan et al. 2005] JAN, T., KARNAHL, T., SEIFERT, K., HILGENSTOCK, J., ZOBEL, R.: *Don't sleep and drive – VW's Müdigkeits- und Aufmerksamkeitserkennung für Fahrer*. VDI-Berichte Nr. 1919, 2005.

[Kämpchen et al. 2010] KÄMPCHEN, N., HOMM, F., WALDEMANN, P.: *Umfelderfassung für den Nothalteassistenten – ein System zum automatischen Anhalten bei plötzlich reduzierter Fahrfähigkeit des Fahrers*. 11. Braunschweiger Symposium AAET 2010, Braunschweig, 2010.

[Kohlhuber et al. 2009] KOHLHUBER, F., HÖRWICK, M., HEIßING, B.: *Sicherheitskonzept für autonome Fahrerassistenzsysteme*. Semesterarbeit am Lehrstuhl für Fahrzeugtechnik der TU München, Garching, 2009.

[Kopischke 2000] KOPISCHKE, S.: *Entwicklung einer Notbremsfunktion mit Rapid Prototyping Methoden*. Dissertation an der TU Braunschweig, Braunschweig, 2000.

[Kramer 2009] KRAMER, O.: *Informatik im Fokus - Computational Intelligence - Eine Einführung*. Springer, Berlin, 2009.

[Krüger 2008] KRÜGER, M.: *Grundlagen der Kraftfahrzeugelektronik: Schaltungstechnik*. Carl Hanser Verlag, München, 2008.

[Lamb & McHugh 2008] LAMB, A., MCHUGH, B.: *Driver-alert systems made simple*. The Province, BCAA Traffic Safety Foundation, 2008.

[Lehmann 2008] LEHMANN, A.: *Neues Konzept zur Planung, Ausführung und Überwachung von Roboteraufgaben mit dynamischen Petri-Netzen*. Dissertation an der Universität Karlsruhe, Karlsruhe, 2008.

[Lexus 2010] LEXUS: *Driver Monitoring System*. http://www.lexus.eu/range/ls/key-features/safety/safety-driver-monitoring-system.aspx, Stand 2.8.2010.

[Li & Jilkov 2003] LI, R., JILKOV V.: *Survey of Maneuvering Target Tracking*. IEEE Transactions on Aerospace and Electronic Systems, 39(4), 2003.

[Luh 2006] LUH, A.: *Untersuchung des Einflusses des horizontalen Sichtbereichs eines ACC-Sensors auf die Systemperformance*. Dissertation an der TU Darmstadt, Darmstadt, 2006.

[Lygeros et al. 1995] LYGEROS, J., GODBOLE, D., BROUKE, M.: *Design of an Extended Architecture for Degraded Modes of Operation of AHS*. American Control Conference, Seattle, USA, 1995.

[Maurer 2000] MAURER, M.: *Flexible Automatisierung von Straßenfahrzeugen mit Rechnersehen*. Dissertation an der Universität der Bundeswehr München, Neubiberg, 2000.

[Meitinger 2008] MEITINGER, K.-H.: *Top-Down-Entwicklung von Aktiven Sicherheitssystemen für Kreuzungen*. Dissertation an der TU München, Garching, 2008.

[Michel 1992] MICHEL, E.: *Fehlererkennung mit Überwachungsrechnern in Multiprozessorsystemen*. Dissertation an der Friedrich Alexander Universität Erlangen, Erlangen, 1992.

[Miller et al. 2005] MILLER, C., FUNK, H., WU, P., GOLDMANN, R., MEISNER, J., CHAPMAN, M.: *The Playbook™ Approach to Adaptive Automation*. Proceedings of Human Factors and Ergonomics Society Annual Meeting, Aerospace Systems, Orlando, USA, 2005.

[Mitschke & Wallentowitz 2004] MITSCHKE, M., WALLENTOWITZ, H.: *Dynamik der Kraftfahrzeuge*. Springer, 4. Auflage, Berlin, 2004.

[Mottok et al. 2008] MOTTOK, J., TREFFLICH, B., SCHICHTL, R.: *Fahreradaptives ACC – Adaption von ACC Warnungen an die Fahreraufmerksamkeit*. 24. VDI/VW-Gemeinschaftstagung 2008 - Integrierte Sicherheit und Fahrerassistenzsysteme, VDI-Berichte Nr. 2048, 2008.

[Murphy-Chutorian et al. 2007] MURPHY-CHUTORIAN, E., DOSHI, A.., TRIVEDI, M.: *Head Pose Estimation for Driver Assistance Systems: A Robust Algorithm and Experimental Evaluation*. IEEE Intelligent Transportation Systems Conference, Seattle, USA, 2007.

[Naab & Reichart 1998] NAAB, K., REICHART, G.: *Grundlagen der Fahrerassistenz und Anforderungen aus Nutzersicht*. Seminar Fahrerassistenzsysteme, Haus der Technik, Essen, 1998.

[Oasis 1996] OASIS: *Don't Look Back in Anger*. (What's the Story) Morning Glory?, Creation Records, London, England, 1996.

[Ostgathe et al. 2010] OSTGATHE, N., HÖRWICK, M., HEIßING, B.: *Kombiniertes Fahrerüberwachungs- und Interaktionskonzept für vollautomatische Fahrerassistenzsysteme*. Semesterarbeit am Lehrstuhl für Fahrzeugtechnik der TU München, Garching, 2010.

[Papp & Zoutendijk 2003] PAPP, Z., ZOUTENDIJK, A.: *A Runtime Framework for System Safety*. IEEE Intelligent Vehicles Symposium, Delft, Niederlande, 2003.

[Pellkofer 2003] PELLKOFER, M.: *Verhaltensentscheidung für autonome Fahrzeuge mit Blickrichtungssteuerung*. Dissertation an der Universität der Bundeswehr München, Neubiberg, 2003.

[Petermann & Niemann 2010] PETERMANN, I., NIEMANN, J.: *Driver in the Loop: Manöverbasiertes Fahren als Automationsansatz in der Fahrzeugführung*. 52. Tagung experimentell arbeitender Psychologen und Psychologinnen (TEAP), Saarbrücken, 2010.

[Pfeiffer et al. 2007] PFEIFFER, A., HAß, C., STEINLE, J., LEHNER, S.: *Stillstandsmanagement für Fahrerassistenzfunktionen bei der BMW Group am Beispiel von ACC Stop&Go*. Tagung Stillstandsmanagement, Haus der Technik, Essen, 2007.

[Prosser et al. 2009] PROSSER, T., HÖRWICK, M., HEIßING, B.: *Plausibilitätsüberwachung des funktionalen Verhaltens eines autonomen Fahrzeugs und Konzeptionierung eines Querführungsmechanismus zur Erhaltung eines sicheren Zustandes*. Diplomarbeit am Lehrstuhl für Fahrzeugtechnik der TU München, Garching, 2009.

[RAS-Q 1996] FORSCHUNGSGESELLSCHAFT FÜR STRASSEN- UND VERKEHRSWESEN: *Richtlinien für die Anlage von Strassen – Teil: Querschnitt (RAS-Q) – RQ31*. 1996.

[Rauch 2009] RAUCH, N.: *Ein verhaltensbasiertes Messmodell zur Erfassung von Situationsbewusstsein im Fahrkontext*. Dissertation an der Universität Würzburg, Würzburg, 2009.

[Reichel et al. 2010] REICHEL, M., BOUZOURAA, M., SIEGEL, A., SIEDERSBERGER, K.-H., MAURER, M.: *Erweiterte Umfelderkennung und Nutzung einer Ausweichanalyse als Grundlage einer aktiven Gefahrenbremsung*. AAET Symposium, Braunschweig, 2010.

[Ritter 2007] RITTER, H.: *Volvo Driver Alert: Zeit für eine Pause*. Autokiste.de, 15.11.2007, http://www.autokiste.de/psg/0711/6679.htm, Stand 2.8.2010.

[Roppenecker 1994] ROPPENECKER, G.: *Fahrzeugdynamik: Grundlagen der Modellierung und Regelung*. Automatisierungstechnik, 42 (10), 1994.

[Rosenblatt 1997] ROSENBLATT, J.: *DAMN: A Distributed Architecture for Mobile Navigation*. Dissertation an der Carnegie Mellon University, Pittsburgh, USA, 1997.

[Schaller 2009] SCHALLER, T.: *Stauassistenz - Längs- und Querführung im Bereich niedriger Geschwindigkeit*. Dissertation an der TU München, Garching, 2009.

[Schäuffele & Zurawka 2006] SCHÄUFFELE, J., ZURAWKA, T.: *Automotive Software Engineering*. Friedr. Vieweg & Sohn Verlag, 3. Auflage, Wiesbaden, 2006.

[Schickram et al. 2009] SCHICKRAM, S., HÖRWICK, M., HEIßING, B.: *Integrales Fahrerüberwachungskonzept für vollautomatische Fahrerassistenzsysteme*. Semesterarbeit am Lehrstuhl für Fahrzeugtechnik der TU München, Garching, 2009.

[Schmitt 2000] SCHMITT, G.: *Mikrocomputertechnik mit dem Controller C167: Programmierung in Assembler und C. Schaltungen und Anwendungen*. Oldenbourg Wissenschaftsverlag, München, 2000.

[Schnieder 2007] SCHNIEDER, E.: *Verkehrsleittechnik – Automatisierung des Straßen- und Schienenverkehrs*. Springer, Berlin, 2007.

[Schöning et al. 2006] SCHÖNING, V., KATZWINKEL, R., WUTTKE, U., SCHWITTERS, F., ROHLFS, M., SCHULER, T: *Der Parklenkassistent „Park Assist" von Volkswagen*. 22. Internationalen VDI/VW-Gemeinschaftstagung Integrierte Sicherheit und Fahrerassistenzsysteme, Wolfsburg, 2006.

[Schröder 2009] SCHRÖDER, C.: *BMW entwickelt Nothalteassistenten – Auto steuert bei Fahrerausfall autonom Nothalt an*. ATZ online, 4.6.2009, http://www.atzonline.de/Aktuell/Nachrichten/1/9837/, Stand 2.8.2010.

[Schröder 2010] SCHRÖDER, C.: *Mercedes-Benz F800 Style Teil 2: Komfort und Sicherheit von morgen*. ATZ online, 24.2.2010, http://www.atzonline.de/Aktuell/Nachrichten/1/11353/Mercedes-Benz-F800-Style-Teil-2-Komfort-und-Sicherheit-von-morgen.html, Stand 2.8.2010.

[Seeing Machines 2008] SEEING MACHINES INC: *DSS Manual*. Acton, USA, 2008.

[Seeing Machines 2010] SEEING MACHINES INC: *DSS Advanced Fatigue Management*. http://www.seeingmachines.com/pdfs/brochures/DSS-Fleet.pdf, Stand 2.8.2010.

[Siedersberger 2003] SIEDERSBERGER, K.-H.: *Komponenten zur automatischen Fahrzeugführung in sehenden (semi-)autonomen Fahrzeugen*. Dissertation an der Universität der Bundeswehr München, Neubiberg, 2003.

[Smart Eye AB 2010] SMART EYE AB: *AntiSleep 2.0 – Monitoring Fatigue and Attention Cues in Automotive Applications*. Technical Whitepaper, http://smarteye.se/files/AntiSleep2_whitepaper.pdf, Stand 2.8.2010.

[Smith et al. 2003] SMITH, P., SHAH, M., DA VITORIA LOBO, N.: *Determining Driver Visual Attention With One Camera*. IEEE Transactions on Intelligent Transportation Systems; 4 (4), Orlando, USA, 2003.

[SZ 2009] SÜDDEUTSCHE ZEITUNG: *240 Kilometer zu weit geflogen*. sueddeutsche.de, 23.10.2009, http://www.sueddeutsche.de/reise/721/492083/text/, Stand 2.8.2010.

[Trefflich 2009] TREFFLICH, B.: *Videogestützte Überwachung der Fahreraufmerksamkeit und Adaption von Fahrerassistenzsystemen*. Dissertation an der TU Ilmenau, Ilmenau, 2009.

[Urbas et al. 2008] URBAS, L., LEUCHTER, S., SCHAFT, T., HEINATH, M.: *Modellgestützte Bewertung der Ablenkungswirkung von neuen interaktiven Diensten im Fahrzeug*. Sicherheit 2008, Saarbrücken, 2008.

[Van Zanten & Kost 2009] VAN ZANTEN, A., KOST, F.: *Bremsenbasierte Assistenzfunktionen*. Handbuch Fahrerassistenzsysteme, Vieweg + Teubner, Wiesbaden, 2009.

[Vehicle Vibes 2009] VEHICLE VIBES: *Avoid Distracted Driving and Arrive Accident Free*. vehiclevibes.com, 21.7.2009, http://www.vehiclevibes.com/2009/07/avoid-distracted-driving/, Stand 2.8.2010.

[Volkswagen AG 2010] VOLKSWAGEN AG: *Spurhalteassistent „Lane Assist“*. Volkswagen Technik-Lexikon, http://www.volkswagen.de/vwcms/master_public/virtualmaster/de3/metacontent/Technik_Lexikon/lane_assist.index.html, Stand 2.8.2010.

[Von Hundelshausen et al. 2008] VON HUNDELSHAUSEN, F., HIMMELSBACH, M., HECKER, F., MÜLLER, A., WÜNSCHE, H.-J.: *Driving with tentacles: Integral structures for sensing and motion*. Journal of Field Robotics, 25 (9), 2008.

[Weilkes et al. 2002] WEILKES, M., BAUM, D., HUMMEL, M., SAUERBREY, J.: *Stauassistent: Systemkonzept und Funktionalität*. VDI-Berichte Nr. 1728, 2002.

[Weiss 1988] WEISS, E.: *Untersuchung- und Rekonstruktion von Ausweich- und Fahrspurwechselvorgängen*. VDI-Berichte Nr. 96, 1988.

[Welford & Birren 1965] WELFORD, A., BIRREN, J.: *Behavior, aging and the nervous system*. Charles C Thomas, Springfield, USA, 1965.

[Wernstedt et al. 2004] WERNSTEDT, J., OTTO, P., EICHHORN, M., KARIMANZIRA, D., LIEBEZEIT, T., PFÜTZENREUTER, T., ZERBE, V.: *Aktiv autonomes Unterwasserfahrzeug für große Tauchtiefen*. Abschlussbericht des Teilprojekts 6 „Prädiktives Führungssystem“ des BMBF-Verbundvorhabens DeepC, Ilmenau, 2004.

[Winner et al. 2006] WINNER, H., HAKULI, S., BRUDER, R., KONIGORSKI, U., SCHIELE, B.: *Conduct-by-Wire – ein neues Paradigma für die Weiterentwicklung der Fahrerassistenz*. 4. Workshop Fahrerassistenzsysteme, Löwenstein, 2006.

[Winner et al. 2009] WINNER, H., DANNER, B., STEINLE, J.: *Adaptive Cruise Control*. Handbuch Fahrerassistenzsysteme, Vieweg + Teubner, Wiesbaden, 2009.

[Wohland 2007] WOHLAND, T.: *Stillstandsmanagement für Fahrerassistenzsysteme in Mercedes-Benz PKW's*. Tagung Stillstandsmanagement, Haus der Technik, Essen, 2007.

[Wolf et al. 2006] WOLF, H., ZÖLLNER, R., BUBB, H.: *Ergonomischer Lösungsansatz für die gleichzeitige Ergonomischer Lösungsansatz für die gleichzeitige*. Aktive Sicherheit durch Fahrerassistenz, München, 2006.

[Wüst 2009] WÜST, K.: *Grundlagen, Architekturen, Schaltungstechnik und Betrieb von Mikroprozessoren und Mikrocontrollern*. Vieweg + Teubner, 3. Auflage, Wiesbaden, 2009.

[Xi et al. 2007] XI, C., JUEJING, F., HILLER, M., LAUER, V.: *Application of Software Watchdog as a Dependability Software Service for Automotive Safety Relevant Systems*. IEEE/IFIP International Conference on Dependable Systems and Networks, Edinburgh, Großbritannien, 2007.